Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Návrh a zabezpečení sítě školní počítačové učebny

Jiří Melen

© 2011 ČZU v Praze

! ! !

Místo této strany vložíte zadání bakalářské práce.
(Do jedné vazby originál a do druhé kopii)

! ! !

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Návrh a zabezpečení sítě školní počítačové učebny"jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne _____27.3.2011_____

Poděkování

Rád bych touto cestou poděkoval Ing. Martinu Havránkovi za pozornost věnovanou mé práci a za odborné rady, které mi pomohly k jejímu zdárnému vypracování.

Návrh a zabezpečení sítě školní počítačové učebny

Concept and security of school computer classroom's network

Souhrn

Tato práce se zabývá problematikou počítačových sítí, jejich realizací, správou a zabezpečením. Je rozdělena do několika dílčích celků:

Teoretická část se věnuje obecnému pohledu na sítě, na jejich výhody a přínosy, na jejich základní rozdělení, na protokoly probíhající v nich, a na jednotlivé struktury zapojení sítí, tzv. topologie. Také je tato část věnována referenčnímu síťovému modelu OSI. Rovněž se tato část bude věnovat hardwaru používaném v počítačových sítích, zejména v sítích typu LAN. Budou rozebrány jednotlivé aktivní i pasivní prvky a popsány jejich vlastnosti, funkce, popřípadě výhody.

V praktické části bude na základě faktů z teoretické části vybrán vhodný model sítě pro zvolenou školní učebnu a budou vybrány vhodné komponenty, jako jsou switch, pracovní stanice, kabeláž nebo server. Následně budou zvoleny operační systémy jednotlivých stanic. Zvýšená pozornost poté bude věnována konfiguraci síťových protokolů pro připojení stanic do sítě a jejich komunikace se serverem. Bude taktéž proveden výběr vhodného operačního systému pro server se stručnou charakteristikou jeho komponent.

Poslední část práce se bude věnovat samotnému zabezpečení sítě, a to jak mechanickému, tak softwarovému. Budou zde take zmíněny nejčastější útoky na počítačové sítě, a metody, jak těmto útokům čelit.

Summary

This bachelor thesis is engaged in matter of computer network, their implementation, management and security. It's divided into three fractional ensembles:

Theoretic part is dedicated to common look at networks, at their advantages and benefits, at their base apportionment, at protocolls that run in them, and at particular structures of their connection, so-called „topologies". Theoretic part is aswell dedicated to

referential network OSI model. There's also mention about hardware used in computer network, namely in LAN type networks. There's gonna be analyzed individual active and passive components and there's gonna be described their attributes, functions, eventualy advantages.

In practice part, there's gonna be chosen a right network model for selected classroom, based on the facts from theoretic part. Also there's gonna be picked the right components, such as switch, work stations, cabling or server. Consequently, there's gonna be chosen an operation systems for computer stations. Increased attention will be dedicated to configuration of network protocols in order to connect stations into the network, and their communication with server. There's aswell gonna be made a pick of right operation system for server, with brief characteristics of his components.

Last part of this thesis is gonna be devoted to network security, both mechanical and software. There's gonna be mentioned the most often attacks at computer networks, and will be adverted methods to prevent those attacks.

Klíčová slova: Síť, topologie, protokol, LAN, kroucená dvojlinka, Ethernet, server, Firewall.

Keywords: Network, topology, protocol, LAN, twisted pairs, Ethernet, server, Firewall.

Obsah

1 Úvod

Pro svoji bakalářskou práci si autor vybral téma "Návrh a zabezpečení sítě školní počítačové učebny". Důvodem byl zájem o téma síťování a vůbec o celý koncept propojování počítačových stanic. Záměrem práce je uplatnit dosavadní zkušenosti, obohacené o informace z odborné literatury, a aplikovat je na konkrétní model.

V poslední dekádě zaznamenaly počítačové sítě velký rozkvět. Lze se s nimi setkat prakticky ve všech firmách a institucích, ale také ve většině domácností. Jejim uživatelům ulehčují počítačové sítě spoustu nadbytečné práce a úkonů. S rozkvětem sítí ale také vzrostl vliv jejich narušitelů. Chybně navržená či zabezpečená síť může představovat hrozbu například v podobě úniku a následného zneužití důležitých informací, nebo zneužívání a poškozování jejího vybavení.

Pro navrhnutí funkční a spolehlivé sítě je nutná obeznámenost se šetřenou problematikou, zahrnující znalost jednotlivých síťových architektur, topologií, protokolů, nebo funkcí používaného hardwaru.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem práce je na základě získaných teoretických vědomostí analyzovat principy a metody propojování samostatných počítačových stanic sítěmi, a na základě vyvozených poznatků navrhnout funkční počítačovou síť. Dále chce práce seznámit s možnými typy zabezpečení sítě, s ohledem na nejběžnější typy útoků na ni.

Práce je zaměřena na propojení 21 stanic v rámci jedné místnosti.Vzhledem k rozloze a homogennosti pracovních stanic lze síť považovat za malou.

2.2 Metodika

Údaje pro psaní této práce byly čerpány převážně z tištěné literatury. V oblastech, kde bylo potřeba charakterizovat novější trendy, než byly popsány v literatuře bylo použito online zdrojů. Pro řešení problému bylo použito deduktivní metody: postupovalo se od obecných aspektů síťové problematiky až po konkrétní návrh zvolené sítě.

Ve výsledcích autor provádí analýzu řešení podle objektivních kritérií, a také podle zkušeností, které získal během svého působení v tomto oboru.

3 Teoretický rozbor

Před samotnou realizací sítě je nutné získat alespoň obecný přehled o principech jejího fungování. Je také vhodné objasnit si základní pojmy, zejména ty, které se budou vyskytovat v praktické části.

3.1 Počítačová síť

Pod tímto pojmem si lze představit množinu vzájemně propojených a komunikujících stanic. Hlavní účel této komunikace je poté především sdílení, či výměna informací, nebo jejich zdrojů. Těmito mohou být data v podobě souborů, nebo programů, ale také vstupní a výstupní zařízení jako např. skenery nebo tiskárny.

3.2 Model OSI

Model OSI resp. Referenční model ISO/OSI byl vypracován a přijat organizací ISO v roce 1984. Hlavním úkolem organizace bylo řešení komunikace v počítačových sítích pomocí vrstveného modelu. Model se skládá ze sedmi vrstev. Jednotlivé vrstvy na sebe působí v tom smyslu, že každá z nich využívá služeb sousední nižší vrstvy, a naopak její služby jsou poskytovány vrstvě vyšší. Specifické charakteristiky a funkce jednotlivých vrstev jsou vyjmenovány níže. [5]

3.2.1 Fyzická vrstva

V pořadí první a také nejnižší vrstva modelu OSI vyjadřuje elektrické, mechanické a funkční vlastnosti. Lze pomoci ní rozeznat jakým signálem je reprezentována logická jednička, jak přijímající stanice pozná začátek bitu, nebo jaký je tvar konektoru. [5]

3.2.2 Linková vrstva

Poskytuje spojení mezi dvěma sousedními systémy například PC – switch, zajišťuje nastavení parametrů přenosu linky a eventuelně hlasí neopravitelné chyby. [5]

3.2.3 Síťová vrstva

Tato vrstva zajišťuje síťové adresování. Spojuje i bezprostředně nesousedící systémy, smazává rozdíly mezi vlastnostmi technologií v přenosových sítích. Pracují na ni routery, které vysílají data do jiných sítí v podobě paketů. To vše má na starosti Internet Protocol (IP) [5]

3.2.4 Transportní vrstva

Hlavním úkolem v pořadí čtvrté vrstvy je poskytování efektivních přenosových služeb své bezprostředně vyšší (relační) vrstvě. Tato služba zodpovídá za transfer dat mezi koncovými uzly. Její jednotkou informace je segment. [5]

3.2.5 Relační vrstva

Relace představuje spojení dvou koncových účastníků na úrovni bezprostředně vyšší, než je transportní vrstva. Relační vrstva zajišťuje synchronizaci dialogu mezi spolupracujícími relačními vrstvami obou systémů a řídí jejich výměnu dat. Relační spojení může vytvořit, ukončit, obnovit, či oznámit vyjímečné stavy. [5]

3.2.6 Prezentační vrstva

Počítače zpravidla používají odlišné způsoby reprezentace dat. Podmínkou korektní výměny vzájemných informací je přítomnost prezentační vrstvy, která se stará o zajištění nezbytných konverzí těchto dat. [5]

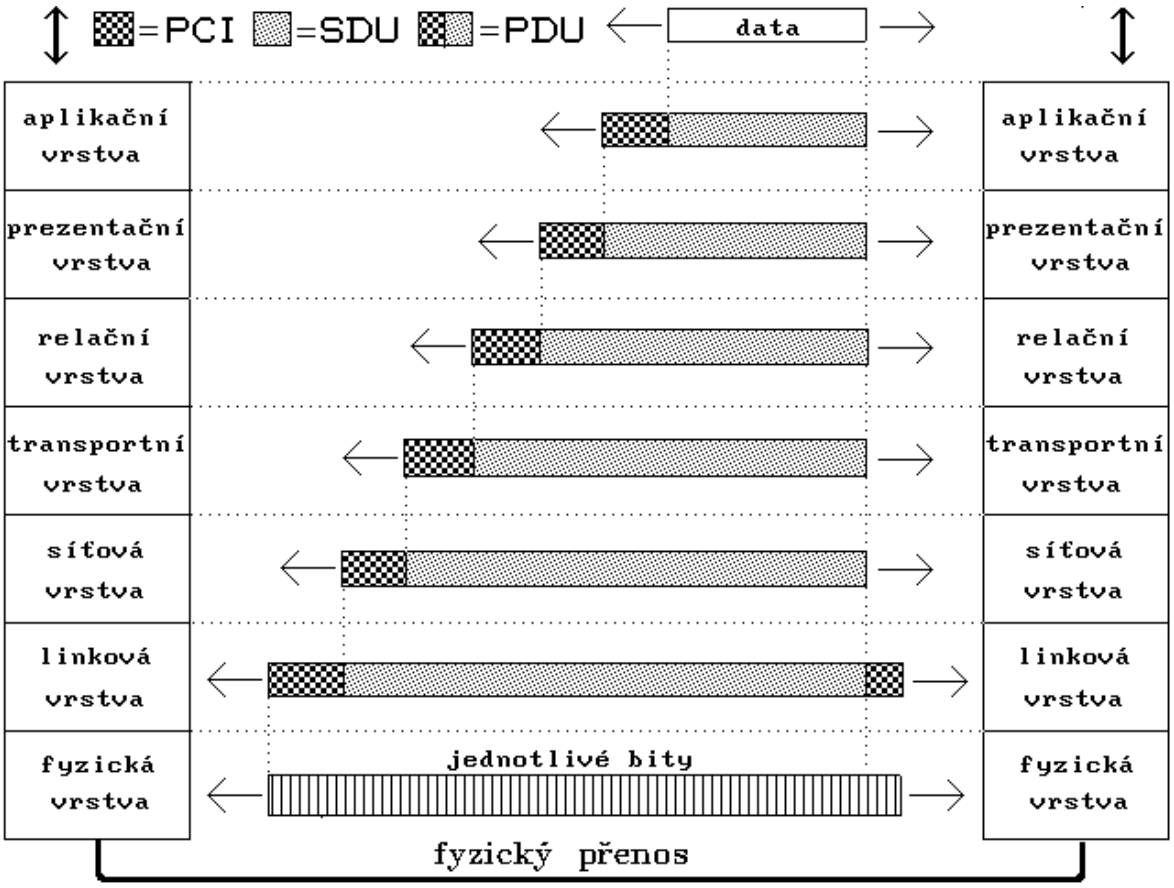
3.2.7 Aplikační vrstva

Na této vrstvě se nacházejí jednotlivé aplikace , které spolu chtějí po síti komunikovat, přičemž k tomu využívají jen protokoly TCP nebo UDP. Tyto protokoly jsou jim zprostředkovávány jádrem operačního systému a jeho síťové vrstvy. Mezi výše jmenované služby a protokoly patří například:

- DHCP (Dynamic Host Configuration Protocol) – protokol pro automatické přidělování IP adres pro koncové stanice v síti. Tento protokol využívá porty UDP 68 pro klienta a UDP 67 pro server.
- DNS (Domain Name System) – zajišťuje převádění domén na adresy IP, stejně tak jako zpětný překlad IP adres na doménové jméno, využívá porty TCP/53 i UDP/53.
- FTP (File Transfer Protocol) – Protokol pro přenos souborů mezi stanicemi, využívá porty TCP/20 a TCP/21.
- POP3 (Post Office Protocol version 3) – Protokol pro získání e-mailů ze vzdálených poštovních serverů, používá port TCP 110.
- IRC (Internet Relay Chat) – Jednoduchý chat po internetu.

- SSH (Secure Shell) – tzv. „bezpečný shell“, neboli protokol, pomocí kterého lze bezpečně komunikovat v rámci dvou počítačů za transparentního šifrování přenášených dat. [5]

Následující obrázek znárorňuje přenos dat mezi jednotlivými vrstvami. PCI (Protocol control information) – složka obsahující informace řídící povahy, SDU (service data unit) – složka obsahující „užitečná data“, PDU (Protocol data unit) – spojení PCI a SDU



Obr.1 : Průchod přenášených dat vrstvami ISO/OSI modelu

3.3 Rozdělení sítí podle rozsáhlosti

Z tohoto hlediska mají sítě velmi široký význam. Mohou jimi být dva spojené počítače, několik PC spojených například v jedné místnosti či jednom poschodí, metropolitní sítě spojující stanice v jednom městě, či celosvětová síť, spojující uživatele několika kontinentů. Podle těchto kritérií se síťe dělí na:

3.3.1 Sítě LAN

Pod zkratkou LAN se skrývá název „Local Area Network“, což předpovídá, že se bude jednat o sítě lokální. Jedná se o nejméně rozsáhlé sítě z této kategorie. Používají se k propojení stanic v jednotlivých budovách , nebo v budovách bezprostředně spolu sousedících. Počet počítačů zapojených do těchto sítí zpravidla nepřesahuje několik desítek. Vrámci jedné budovy je dnes nejčastěji jako propojovací médium používána kroucená dvojlinka, více budov se poté propojuje již bezdrátově, pomocí optických kabelů, či bezdrátových pojítek (radiová, mikrovlnná). [1]

3.3.2 Sítě MAN

Střední vrstvu co do rozsahu tvoří síťe typu MAN (Metropolitian Area Network). Většinou jsou tvořeny několika menšími sítěmi LAN, které jsou propojeny navzájem v rámci určitého území. Jedná se o sítě velkých podniků, či sítě na území měst. [1]

3.3.3 Sítě WAN

WAN, neboli „Wide Area Network“, jsou sítě velmi vysokých rozsahů. Jedná se o propojení mnoha sítí LAN i WAN. Do této skupiny patří zejména „síť sítí“, což je samozřejmě Internet. [1]

3.4 Rozdělění síťí podle jejich architektury

Klíčové kritérium v tomto typu rozdělení hraje vnitřní architektura síťí. Podle tohoto kritéria se síťě dělí na dvě skupiny, a to sice:

3.4.1 Klient-to-Server

Architektura Klient-to-Server se vyznačuje tím, že v ni jedna z připojených stanic hraje roli serveru, čili počítače poskytujícím služby ostatním pracovním stanicím. Službami lze rozumět zejména management sítě a řízení jejich funkcí. Pracovní stanice se k serveru hlásí právě jako klienti, a využívají jeho služeb. Sítě klient-to-server se používají převážně při provozování středních a větších sítí. [5]

3.4.2 Peer-to-Peer

V sítích peer-to-peer není přítomen server, a tudíž jsou si všechny pracovní stanice, co do práv a administrace sítě rovni. Takovéto sítě nacházejí uplatnění tam, kde se zpravidla nepřipojuje více, než 10 PC. [5]

3.5 Síťové topologie

„Síťová topologie je způsob fyzického zapojení síťových zařízení. Strukturovaná kabeláž poskytuje „dálnici“, po které se data stěhují z jednoho místa na druhé. Topologie popisuje, jak budou jednotlivá zařízení navzájem komunikovat a jak bude síť fungovat jako celek. Znalost síťových technologií – tedy toho, jak jsou zapojené dráty – je v textu o síťové kabeláži velice užitečná.“.(Kállay, F., Peniak, P*,2003, s.53)*

Topologií existuje několik druhů , právě podle toho, jakým způsobem jednotlivé stanice propojují.

3.5.1 Topologie sběrnice

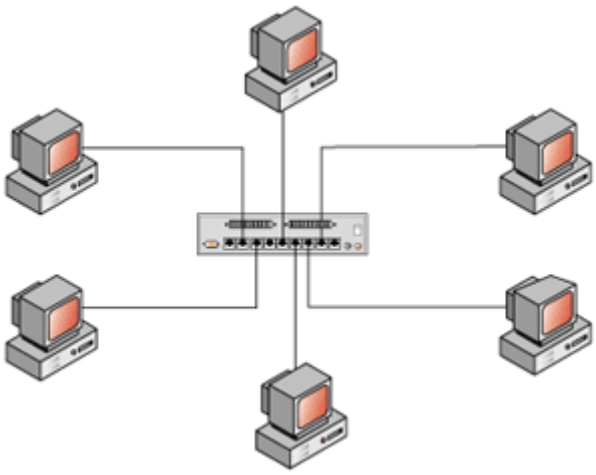
Topologie sběrnice neboli bus topology používá ke spojení průběžné vedení, od stanice ke stanici. Stanice jsou k vedení připojeny pomocí odbočovacích prvků. Tato topologie je používána zejména u sítí s koaxiálním kabelem, a dnes je používána jen velmi zřídka.

Za výhody lze pokládat především nízkou spotřebu kabelu čili nižší cenu kabeláže. Tato výhoda je však vykoupena faktem, že dojde-li na některém místě vedení k poruše, je tím afektována cela síť. Dalším negativem je poměrně obtížná lokalizace takovýchto poruch. [1]

3.5.2 Topologie hvězda

Hvězdicová topologie (star topology) je charakteristická tím, že každá stanice v ni je připojena vlastním kabelem. Jednotlivé kabely jsou soustředěny do rozbočovače (dříve hub, dnes hlavně switch). Rozbočovač poté tvoří pomyslný střed sítě. K přenosu dat se nejčastěji používá kroucená dvojlinka. Star topology je dnes nejpoužívanější topologií.

Ve výhodách je především záhodné zmínit fakt, že oproti předchozí topologii při poruchách jednoho kabelu nedochází k výpadku celé sítě, nýbrž jen samotné síťové stanice. Do nevýhod lze začlenit vyšší nákladovost, jelikož dochází k větší spotřebě kabeláže. [1]



Obr. 2: Topologie hvězda

3.5.3 Topologie kruh

Topologie token ring se vyznačuje spojováním stanic do souvislého kruhu a dovoluje tak použít metodu postupného předávání zpráv. Nevýhodou přetrvává výpadek celé sítě při přerušení jednoho vodiče, podobně jako u sítí typu sběrnice. Částečně bývá tento problém eliminován zdvojováním kabelů. [1]

3.6 Síťové protokoly

Síťový protokol definuje pravidla komunikace, kterými je řízena výměna dat v síti. Aby komunikace v síti probíhala korektně, je nezbytné, aby všechny její stanice používaly stejný protokol, respektive stejnou sadu protokolů. Protokoly spolu navzájem musejí spolupracovat. Síť učebny bude typu LAN, a proto bude věnována pozornost jen protokolům souvisejícím s tímto typem sítě. [1]

3.6.1 NetBEUI

Dnes již nepoužívaný protokol NetBEUI byl vyvinut firmou IBM v době, kdy na sítě nebyly kladeny takové požadavky, jako dnes. Do dnešní doby přetrval jen kvůli zpětné kompatibilitě systémů. NetBUI nepodporuje směrování a tudíž za jeho pomoci nelze vytvořit síťové segmenty [2]

3.6.2 IPX/SPX

Tato sada protokolů byla vyvinuta firmou Novell pro její síťový OS NetWare, zejména pro verze 3.x a 4.x. Novější verze vedle těchto protokolů prvotně používají protokol TCP/IP.

Činnosti obou protokolů jsou následující:

Činnost IPX

IPX pracuje na úrovni síťové vrstvy ISO/OSI. Jeho úkolem je přenášení paketů vyšších protokolů a přenos dat mezi stanicemi. Jedná se o nespojově orientovaný protokol, což znamená, že nekontroluje správnost přenosu. [2]

Činnost SPX

SPX je nadřazeným protokolem IPX a narozdíl od něj je spojově orientovaný. Tento protokol pracuje na úrovni transportní vrstvy a kontroluje správnost přenesených paketů. V případě zjištění chyby vyžaduje opakování procesu. [2]

3.6.3 TCP/IP

Spolehlivě nejrozšířenější skupinu protokolů v dnešní době tvoří skupina TCP/IP. Používají se v sítích Novellu i Microsoftu, kde zcela vytlačili své předchůdce. Protokol lze rozdělit na tři vrstvy: aplikační vrstvu, transportní vrstvu a síťovou vrstvu. [2]

3.6.4 Vrstvy protokolu TCP/IP

Jak již bylo zmíněno , protokol TCP/IP je rozdělěn na dílčí vrstvy, reprezentované samostatnými protokoly.

Aplikační vrstva

Tvoří ji množina protokolů spolupracujících s jednotlivými aplikačními programy. Aplikační protokoly této vrstvy byly vyjmenovány v odstavci 3.2.7 Aplikační vrstva.

Transportní vrstva

Tato vrstva tvoří jádro TCP/IP, tvoří jej 2 protokoly, TCP a UDP.

Protokol TCP (Transmission Control Protocol)

Jeho princip je takový, že přebere od aplikační vrstvy data, která rozdělí na segmenty, očísluje a seřadí podle toho, jak mají být postupně odeslány. Zahájí relaci s transportní vrstvou protějšího PC a začne vysílat a potvrzovat jednotlivé datové segmenty. [2]

Protokol UDP (User Datagram Protocol)

UDP analogicky jako TCP převezme od aplikace data, ze kterých následně sestaví segmenty a ty posléze předá k odeslání síťové vrstvě. Od TCP se liší tím , že nepotřebuje vytvářet před přenosem relaci s potějškem a zpětně neověřuje, zda byly datagramy skutečně protějškem přijaty. [2]

Protokol IP (Internet Protocol)

Protokol IP pracuje na síťové vrstvě TCP/IP. Přijímá datové segmenty od protokolů transportní vrstvy s požadavkem na jejich odeslání. Segmenty obohatí o vlastní hlavičku, čímž vznikne IP datagram. IP hlavička je významná především tím, že obsahuje IP adresu příjemce a odesílatele. Z těchto poznatků lze vyvodit, že hlavní účel protokolu je adresování a směrování datagramů mezi počítači. [2]

3.7 Adresace v sítích TCP/IP

Adresování v sítích s protokoly TCP/IP se významně liší od sítí IPX/SPX, kde adresace a konfigurace sítě probíhá automaticky. TCP/IP tuto možnost sice částečně poskytuje v podobě DHCP (Dynamic Host Configuration Protocol), ale tato služba není vždy k dispozici. Často tedy bývá nutný zásah uživatele.

Pravidla adresace jsou taková, že každá stanice musí mít originální číslo. Také je požadováno, aby toto číslo vypovídalo o umístění stanice v síti či síťovém segmentu. Každá stanice má svoji IP adresu vyjádřenou čtveřicí tečkou od sebe oddělených čísel. Čísla se pro uživatelskou přehlednost zapisují v desítkové soustavě, a mohou nabývat hodnot 0-255. IP adresa může tedy například vypadat takto : 192.168.1.11. [2]

3.7.1 Třídy IP adres

Pro počítače zapojené do síťě nelze uvést pouze číslo konkrétní stanice, ale také číslo sítě, které počítač náleží. IP adresa je poté rozdělěna na tu část, která vyjadřuje číslo sítě a na tu, která popisuje číslo počítače. Podle toho , jaká část charakterizuje síť a jaká PC, jsou IP adresy rozděleny do tříd. [3]

	Rozsah adres prvního čísla	Počet čísel vyhrazených pro adresu sítě	Počet čísel vyhrazených pro adresu uzlu	Použití
Třída A	0-127	1 (adresuje 126 sítí)	3 (adresuje cca 17 mil. uzlů = PC)	Pro rozsáhlé sítě
Třída B	128-191	2 (adresuje 16 tis. Sítí)	2 (adresuje cca 65 tis. uzlů)	Středně velké sítě
Třída C	192-223	3 (adresuje 2 mil. sítí)	1 (adresuje cca 254 uzlů)	Menší sítě

Tabulka 1: Třídy IP adres

Než se IP adresy začaly používat v lokálních sítích, byly standartně využívány v Internetu. Z důvodu omezení konfliktů těchto adres byly v každé třídě IP adres vymezeny pro lokální sítě rozsahy, a to následovně:

- Třída A: 10.0.0.0 až 10.255.255.255
- Třída B: 172.16.0.0 až 172.31.255.255
- Třída C: 192.168.0.0 až 192.168.255.255

3.7.2 DHCP a DNS

Tyto dva pojmy úzce souvisejí s adresací TCP/IP. V dřívějších dobách byly v souvislosti s konfigurací malých sítí LAN používány jen zřídka. V dnešní době se s nimi i v této oblasti lze setkat již běžně.

DHCP (Dynamic Host Configuration Protocol) je služba, která automaticky přiděluje IP adresy. Tato služba je dnes součástí většiny síťových operačních systémů (DHCP server). Funguje tak, že jakmile je pracovní stanice připojena do sítě, server jí přidělí IP adresu.

DNS (Domain Name System) je služba vytvořena pro Internet. Převádí IP adresy na lépe zapamatovatelná jména. Je to proto, že v síti internet je velké množství počítačů, z nichž každý musí mít unikátní IP adresu, a při existenci pouhých IP adres by nebylo možné si zapamatovat, pod kterým číslem jsou skryty hledané údaje. DNS pracuje tak, že rozděluje jednotlivé PC do zón, nazývaných domény (např. počítače v ČR mají doménu .cz). [3]

3.7.3 Informace o protokolu TCP/IP

„Pro zjišťění základních informací o nastavení TCP/IP je ve Windows k dispozici příkaz IPCONFIG, Ten pracuje v příkazovém režimu, do něhož se dostaneme poklepáním na tlačítko Start/Spustit, v okně Spustit zadáme příkaz cmd. (Okno Spustit vyvoláme také rychlou volbou – současným stiskem kláves Windows a R). Po zadání cmd již máme okno příkazové řádky k dispozici. Po napsání příkazu ipconfig vidíme základní údaje o TCP/IP. Chceme-li získat informace detailní, přidáme ještě parametr all, příkaz bude mít tvar ipconfig/all.“(Horák, Keršláger, 2006, s.62)

3.8 Standardy síťového hardwaru

Jednotlivé prvky síťového hardwaru je možné různě kombinovat (používat různé topologie, přístupové metody, jiné kabely doplněné o různé aktivní prvky). Tato variabilita však přináší zásadní problém – různě sestavené sítě se spolu nemusí domluvit.

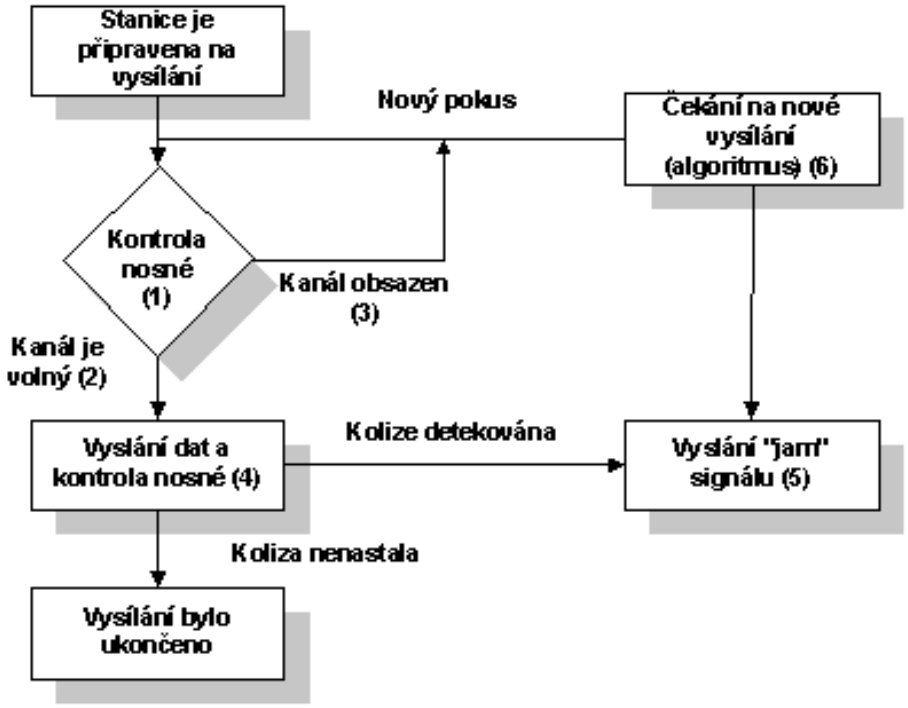
Pro tyto případy byly přijaty určité standardy, které definují základní požadavky na technické provedení sítí. Přijaty byly organizací IEEE (Institute of Electricial and Electronics Engineers).

3.8.1 Ethernet (10 Mb/s)

Ethernet je nejrozšířenější standard sítí LAN. Vyvíjel se od roku 1976 a byl navržen firmou Xerox. Jaho základní znak je kolizní přístupová metoda CSMA/CD. Ve stavbě ethernetové sitě je nutné dodržovat pravidla topologií, především délku segmentů. Značení ethernetu má následující pravidla : první číslice vyjadřuje rychlost, s níž standard pracuje, slovo BASE popisuje signalizační metodu, ve většině případů jde o metodu BASE, a písmeno na konci kabelu popisuje jeho typ – F = optický kabel, T = nestíněná kroucená dvojlinka. [2]

3.8.1.1 CSMA/CD

Ethernet pro spravování šíření sígnálů v sítích používá metodu CSMA/CD (Carrier Multiple Access with Collision Detection). Tato metoda u stanice chystající se k vysílání nejprve zkontroluje, zda se již kabeláží nešíří nějaké signály. Je-li kabel volný, začne vysílat. Pokud ve stejném okamžiku začne vysílat stejná stanice, dochází ke konfliktu. V tomto případě se vysílající počítače odmlčí a za náhodně stanovenou dobu začnou vysílat znovu. Výhodou je nízká cena komponent (CSAM-CD zajišťuje síťová karta), nevýhodou pak je fakt, že se stoupajícím počtem stanic dojde k zahlcení sítě (zvyšuje se pravděpodobnost kolizí). [2]



Obr. 3: Základní algoritmus metody CSMA/CD

3.8..2 Fast Ethernet (100 Mb/s)

Dnes nejrozšířenější formu standardu Ethernet tvoří právě tato skupina. Je to norma odpovídající doporučení 802.3. Rozdílná od normy Ethernetu 10Mb/s je vedle rychlosti také nemožnost použití koaxiálního kabelu.

Rychlý ethernet nese označení 100BASE-T a je definován ve třech variantách:

3.8.2.1 100BASE-TX

Ethernet této třídy pracuje na kabelech s nestíněnou dvojlinkou kategorie 5 s využitím dvou párů (o jeho zapojení bude zmínka v kapitole 4.2.2.1 Volba přenosového média). Použít lze i stíněnou dvojlinku. Maximální délka jednoho segmentu pro tuto třídu je 100m. [2]

3.8.2.2 100BASE-FX

Třída 100BASE-FX je určena pro optickou kabeláž s délkou segmentu až 412 metrů. Tato délka se vztahuje k vícevidovým vláknům s poloviční duplexem. Pro jednovidová vlákna s duplexním režimem je možno použít délku až 10000m. [2]

3.8.2.3 100Base-T4

Jedná se o starší normu používající kroucenou dvojlinku kategorie 3 a 4 s maximální délkou 100m. Pro přenos dat jsou použity všechny 4 páry. Dnes se v praxi již nepoužívá. [2]

3.8.2.4 Pravidla pro instalaci sítě standardu Fast Ethernet

Pro instalaci sítě založené na standardu Ethernet 100Mb/s platí velmi přísná topologická pravidla. Fast ethernet rozeznává dvě kategorie koncentrátorů (hubů, rozbočovačů):

Class 1 : (translational repeater), realizuje převod signálu do digitální formy. Výsledkem je zpoždění signálu. Proto může být v doméně pouze jeden rozbočovač, ale lze zde kombinovat obě fyzická schémata, 100base-TX i 100Base-T4.

Class 2 : (transparent repeater), realizuje pouze zesílení signálu. Proto je nutné použití pouze jedné normy (100Base-TX nebo 100Base-T4). Oproti Class 1 zde mohou být použity 2 rozbočovače typu Class 2, s maximální vzájemnou vzdáleností 5m. [2]

	Max délka pro UTP	**Max délka pro Optiku**	**UTP + Optika (TX + FX)**
stanice- stanice, stanice – switch, switch – switch (poloviční nebo plný duplex)	100 m	421m	Nelze použít
Hub Class I (poloviční duplex)	200m	272m	260,8m (100m kabelu UTP + jeden optický spoj)
Hub Cvlass II (poloviční duplex)	200m	320m	308,8m (100m kabelu UTP + jeden optický spoj)
2X Class II hub (poloviční duplex)	205m	228	216,2 (105 kabelu UTP + jeden optický spoj)

Tabulka 2: délky kabelů pro jednotlivé standardy Ethernetu

3.8.3 Gigabitový Ethernet (1000 Mb/s)

Tvoří nejnovější variantu Ethernetu. Gigabitový ethernet je standardizovaný pro optické kabely a kroucenou dvoulinku. [2]

3.8.3.1 1000Base-X (802.3x)

Tento ethernet je navržen pro optické kabely. Dělí se na 2 typy , podle toho, jaký používá světelný zdroj. Světelným zdrojem jsou kódovány přenášené informace.

- 1000Base-SX: používá krátkovlnný světelný zdroj 850 nm. Zdroj světla může být dioda nebo laser. Používá se u kratších vedení a u páteřních propojení
- 1000BaseLX: pro přenos světla o vlnách 1310 nm. Zdrojem je laser a používá se pro větší vzdálenosti. [2]

3.8.3.2 1000Base-T (802.3ab)

Používá se pro kovové kabely, zejména pro kroucenou dvojlinku kategorie 5 nebo 5e. Významným rozdílem oproti ethernetu 10 BASE-T a 100 BASE-TX je to, že tyto kabely používají při gigabitovém přenosu všechny 4 páry vodičů. [2]

3.9 Síťový hardware

Síťový hardware jsou technické prostředky, kterými je realizováno fyzické propojení jednotlivých stanic.

3.9.1 Aktivní prvky

Aktivní prvky tvoří klíčové technické vybavení, bez kterého síť nemůže fungovat. Tyto prvky aktivně ovlivňují dění v síti. Mají na starosti například výběr trasy, kontrolu správnosti paketů, nebo rozhodování, do které sítě má paket projít, a do které ne.

3.9 1.1 Opakovač (repeater)

Opakovač, zesilovač, nebo také repeater se používá pro udržení síly signálu. Je ho zapotřebí zejména tam, kde je kabeláž tak dlouhá, že se předpokládá, že na jejím konci nebude signál dostatečně silný. Repeater se tedy používá k prodloužení dosahu kabeláže. Konstrukčne má podobu krabičky se dvěma stejnými konektory, a používá se nejčastěji u koaxiálních sítí. Pro zesílení signálu z jednoho typu kabelu na jiný se poté používá tzv. transceiver. [5]

3.9 1.2 Rozbočovač (hub)

Býval svého času nezbytným prvkem pro hvězdicovou topologii a jeho základní funkce byla rozbočování signálu. Dnes je však nahrazen výkonnějším switchem, a proto neboť v naší síti nebude použit. [5]

3.9 1.3 Přepínač (switch)

Jak bylo zmíněno výše, switch je aktivním prvkem, který se stal nástupcem zastaralých a pro dnešní dobu bezpečnostně nepříliš vyhovujících hubů. Funkce hubu spočívala v rozesílaní paketů všem stanicím v síti, kde následně po jejich přečtení paket přijala pouze ta stanice, pro kterou byl určen.

Switch vytváří v tomto směru velice významnou inovaci v tom, že si při průchodu paketu přečte cílovou adresu a směruje paket pouze tomu PC, pro které je paket určen. Jinými slovy, u přicházejícího rámce přečte zdrojovou MAC adresu, a zároveň vytvoří v paměti tabulku MAC adres a portů, odkud pochází. Pomocí tabulky MAC adres (Content Adressable Memory) je tedy možné zjistit, na jaký port má switch určený rámec odeslat.

Eliminuje se tedy zahlcování sítě. Switch vytvoří spojení pouze mezi komunikujícími stanicemi, toto spojení je oddělené od ostatních stanic v síti, a tak nedochází ke zpomalovaní vlivem cizích paketů a komunikace probíhá maximální rychlostí. [5]

„Switch má význam především u větších sítí, snižuje totiž pravděpodobnost zahlcení sítě a významně zvyšuje její propustnost. U malých sítí není switch nutností, ale jeho cena není o moc vyšší, než je tomu u HUBu, takže se s ním setkáme i tady.“ (Horák,2003, s.21)

Obr. 4: 24-portový switch

3.9.1.5 Síťová karta

Síťová karta je prvek umožňující a zprostředkující komunikaci mezi PC a sítí. Jedná se o rozhraní mezi těmito prvky, přičemž musí vyhovovat oběma subjektům. Síťová karta musí také vyhovovat určitému standardu (v naší síti jím je Ethernet).

V dnešní době bývá zpravidla integrována na základní desce. [3]

Pravidla pro správnou spolupráci s PC jsou následující:

- Karta musí jít zasunout do patice v počítači = musí vyhovovat správnému typu sběrnice (tam, kde není integrovaná).
- Karta musí spolupracovat s operačním systémem, je tedy nutno nainstalovat správný ovladač.

Pro spolupráci se sítí je zapotřebí:

- Podpora vhodné normy IEEE. Ve vyšetřované síti jí bude Ethernet (implementace metody CSMA/CD, originální adresa karty, práce s pakety).
- Přenosová rychlost vyhovující koncentrátoru (Switchi).

3.9.2 Pasivní prvky

Pasivní prvky jsou takové, které se podílejí na přenosu dat sítě, avšak svým působením tato data nijak neovlivňují.

3.9.2.1 Kabely UTP

Jedná se o kabeláž používanou pro lokální sítě, zejména pro hvězdicovou topologii. Jsou složeny z osmi vodičů tvořící čtyři páry, umístěné do vnější plastické izolace. Vodiče každého páru jsou krouceny okolo sebe. Má to svá odůvodnění – při šíření signálů několika souběžnými vodiči dochází ke vzájemnému rušení. Toto rušení se může ve výsledku projevit zkreslením dat. Kroucení kabelů kolem sebe eliminuje právě tyto škodlivé vlivy. Uvnitř kabelu jsou mimo jiné vůči sobě krouceny i samotné páry – z tohoto typického znaku pochází označení pro tento typ kabeláže – kroucená dvojlinka.

Kroucená dvojlinka je vyráběna ve dvou verzích – STP = Shielded twisted pairs (stíněná kroucená dvojlinka), nebo UTP = Unshielded twisted pairs (nestíněná kroucená dvojlinka). Stíněná dvojlinka se používá velmi málo, ani v sítí učebny nebude použita, a proto bude následný popis věnován pouze kabelu UTP.

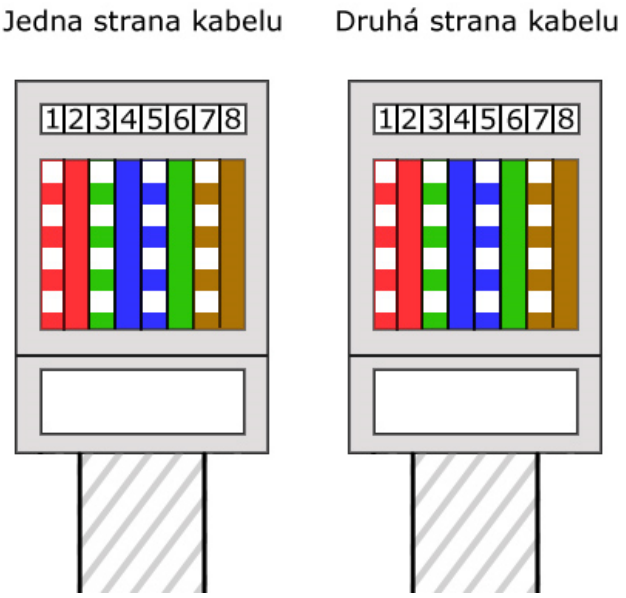
Pro způsob vedení kabelů UTP, jak bylo již zmíněno, se používá hvězdicová topologie. K propojování jednotlivých aktivních a pasivních prvků se používá buď UTP kabel v provedení „lanko“ (zejména jako patch kabel pro propojení např. stanic se zásuvkami nebo patch panel se switchem), nebo v provedení „drát“ (používá se na místech, kde se předpokládá, že se s kabelem již nebude hýbat, například mezi zásuvkami a patch panelem). [3]

3.9.2.2 Zapojení RJ 45

Z předchozí kapitoly je patrné, že kabely UTP jsou tvořeny osmi vodiči po čtyřech párech. Tyto vodiče mají stejný barevný základ, ale barva jednoho z nich je doplněna bílým proužkem. Nalisování koncovky se provádí tzv. krimpovacími kleštěmi. Krimplovací kleště slouží pro nacvaknutí konektoru RJ 45 na kabel UTP. [3]

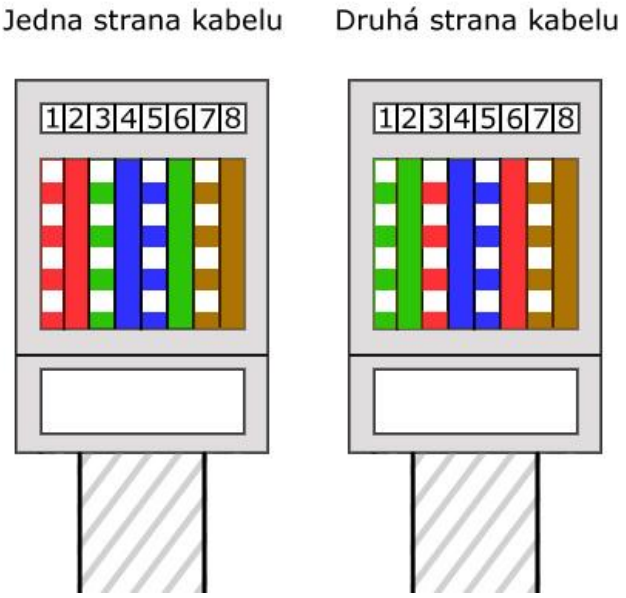
Konce kabelů lze takto zapojit dvěma způsoby:

- Jedna k jedné, kdy je každý vodič připojen ke stejným kontaktům konektoru. Jedná se o nejčastější zapojení pro kabel PC- switch



Obr. 5: zapojení RJ 45 jedna k jedné

- Kříženě – vodiče dvou párů jsou vzájemně překříženy. Toto zapojení se používá pro spojení dvou PC nebo např. dvou switchů.



Obr. 6: křížené zapojení RJ 45

3.9.2.3 Zásuvka RJ 45

Aby nebyly kabely vedeny volně po celé učebně, bude použita sada zásuvek RJ 45. Tyto zásuvky se vyrábějí buď v provedení s jedním, nebo se dvěma porty. Ze schématu zapojení vyplývá, že dvojice počítačů v každé řadě bude mít společnou právě jednu dvouportovou zásuvku RJ 45.

3.9.2.4 Patch panel

Jedná se o prvek propojující kabely od počítačů se switchem. Patch panel je osazen několika porty RJ 45 (12 nebo 24), a standartmě je umístěn v racku. Přední stranu panelu tvoří výstupní porty a kabely od PC se zapojují na zadní stranu pomocí zářezového narážecího stroje. Zadní strana patch panelu je tvořena řádkou kontaktů, které jsou označeny stejnými barvami jako jsou barvy vodičů u UTP kabelu. Vodič je potřeba zatlačit do daného kontaktu a zaříznout. Po montáži kabelů do panelu a upevnění panelu do racku je dobré kabely svázat páskami, aby se nezamotaly dohromady, a také kvůli lepšímu proudění vzduchu pro chlazení switchů.

3.10 Hardwarové požadavky na server

Síť je budována především kvůli výměně, sdílení a ochraně dat. Server je místem, kde jsou tyto data uložena. Tvoří nejdůležitější, ale také zároveň nejzranitelnější článek celé sítě. Server může tvořit prakticky jakýkoliv počítač v síti, který disponuje síťovým operačním systémem. Má-li však být naše síť efektivní, má-li zvládat současně obsluhovat několik pracovních stanic, a zaručit bezpečnost uložených dat, je potřba na hardware serveru klást daleko vyšší požadavky , než na hardware pracovních stanic. [2]

3.10.1 Mikroprocesor

Na mikroprocesor je požadován logicky co nejvyšší výkon. Levné servery mohou použít obyčejné „desktopové“ procesory, jako jsou například Intel C2D nebo AMD Athlon 64. Pro vyšetřovanou síť bude použit jeden z procesorů vyvinutých speciálně pro servery.

3.10.2 Operační paměť

Měla by být dostatečně veliká. Jednak pro poskytnutí prostoru pro aplikace vyžadované uživateli, jednak samozřejmě pro soubory síťového operačního systému. K tomu všemu musí umět zajistit cacheování pevných disků. Spodní hranice takovéto paměti je 1 GB. Operační paměť serveru by měla podporovat technologie registered a ECC. [2]

3.10.2.1 Kešování (cache)

Server musí velmi často číst data z pevného disku. Tato operace je ve srovnání čtení dat z operační paměti velmi pomalá. Kešování uchovává dříve načtená data v operační paměti. To zajišťuje, že přijde-li nějaký požadavek na čtení dat, hledají se tyto nejprve v operační paměti serveru a v případě neúspěchu jsou přečtena z pomalejšího pevného disku. Většina uživatelů používá stejný program uložený na serveru. Tento fakt

zvyšuje pravděpodobnost uložení a následného nalezení dat v operační paměti. Kešování významně zrychluje práci serveru. [2]

3.10.2.2 ECC

Paměti disponující funkcí ECC (Error Checking and Correcting) jsou schopny zjistit a opravit chyby v paměti. Jedná se v podstatě o samoopravný kód, který opravuje jednobitové a dvoubitové chyby. Pro správnost fungování modulu ECC je zapotřebí zpětná kompatibilita se základní deskou serveru. [2]

3.10.2.3 Registered

Tyto moduly používají speciální vstupně-výstupní buffery. Zmiňované buffery slouží ke zvyšování stability a spolehlivosti přenosu dat. Podmínkou je podpora registrovaných modulů chipsetem základní desky serveru. [2]

3.10.3 Pevné disky

Další nedílnou součást serveru tvoří pevné disky. Jedná se o média, na něž se ukládají data z celé sítě, a proto jsou na ně kladeny patřičné nároky. Mezi tyto nároky je možné uvést dostatečnou kapacitu (počínaje u 100 GB, zpravidla ale jsou používány podstatně větší disky), zvýšené požadavky na bezpečnost uložených dat (sdružování disků do diskových polí RAID), a použití specifického rozhraní pro serverové disky (SCSI – Small Computer System Interface). [2]

3.10.3.1 Disková pole

Diskové pole se nazývá skupina disků, které se navenek „tváří“ jako jeden disk. Přijde-li od serveru požadavek na čtení či zápis dat, pole samo organizuje, na který disk budou data uložena, či ze kterého budou přečtena. Tento postup má za úkol zvyšovat bezpečnost uložených dat. Umístění těchto polí může být jak interní (uvnitř serveru), tak externí (mimo server) [2]

3.10.3.2 RAID

Disková pole ke své organizaci používají metody RAID (Redundant Array of Inexpensive Disks). Problematika RAID je poměrně složitá věc, a proto v rámci této práce nebude rozebírána. Pro účely naší sítě postačí pouze popsat základní vlastnosti diskových polí. Rozhraní RAID je možno tvořit dvěma způsoby, a to:

- Pomocí softwaru, kdy je RAID vytvořeno síťovým operačním systémem
- Pomocí hardwaru, kdy je RAID vytvořeno řadičem pevných disků

Hlavním principem vyšší bezpečnosti diskových polí je nadbytečnost (redundance) dat. Jedná se v podstatě o to, že jsou stejná data zapisovány na více disků. Nadbytečná data

pak například při havárii některého z disků doplní chybějící údaje. Nevýhodu metod RAID lze vysledovat zejména ve snížení použitelného diskového prostoru. [2]

3.10.4. Ostatní hardwarové prvky

Kromě zmíněných základních součástí musí server standartně obsahovat ještě jíné, méně, či více významné komponenty.

DVD-ROM - jako základní čtecí médium , pro instalaci síťového OS atp.

Pásková jednotka – toto zařízení se používá pro zálohování dat odděleně od serveru. Tímto způsobem jsou data chráněna proti krádeži, požáru serveru nebo celé budovy. Z páskové jednotky je možné data obnovovat, respektive vracet se k jejich předchozí verzi. Síťové operační systémy na tyto pásky zapisují zejména v časech , kdy server není v plném provozu (např. v noci). Eliminuje se tím nízká rychlost pásky. Na páskové jednotky jsou kladeny požadavky zejména z pohledu kapacity – musí být úměrná velikosti dat, která na nich chceme zálohovat.

Základní deska – musí být kompatibilní s veškerým hardwarem, musí dovolovat multiprocessoring a mít dostatečnou kapacitu pro operační paměť.

Síťová karta – dnes standardně o rychlosti 1 GB/s.

Záložní zdroje – tzv. Záložní zdroje UPS (Uninterruptable Power Supply) – zdroje chránící server před výpadkem elektrické sítě. Tématu záložních zdrojů se bude více věnována kapitola 4.4 Fyzické zabezpečení sítě. [2]

3.10.5 Umístění serveru

Hardware (ani software) nekladnou žádné specifické požadavky na umístění serveru. Server je možno umístit na kterékoliv místo v naší síti. Prakticky je ale vhodné umístit server na místo, kde by svým hlukem nerušil okolí, a kde by byl dobře zabezpečen proti krádeži, či proti neodborné obsluze.

3.11 Softwarové požadavky na server

Tvorí skupinu služeb, které budeme od serveru vyžadovat. Tyto služby bude zajišťovat operační systém. [2]

3.11.1 Souborový server

Prvotní funkci každého serveru je tzv. Souborový server (file server). Funkce file serveru má na starosti:

- víceuživatelský přístup k souborům – možnost více uživatelů pracovat se stejným souborem
- vedení evidence uživatelů, kteří se mohou k serveru přihlásit, a má přehled o uživatelských právech pro disky, adresáře, či samotné soubory [2]

3.11.2 Tiskový server

Server zprostředkující přístup více uživatelům k jedné tiskárně se nazývá tiskový server (print server). Určuje meze možností operací jednotlivých uživatelů s danou tiskárnou (tiskárnami). Definuje, kdo může jen tisknout, kdo může např. konfigurovat nebo mazat tiskové úlohy atd. [2]

3.11.3 Aplikační server

Na aplikačních serverech běží programy (aplikace), které jsou společné všem uživatelům sítě. Aplikace mohou mít různý charakter, závisle na tom, o jaký typ sítě se jedná (ekonomické systémy, skladové evidence atd.).

Mnoho aplikačních programů je dodáváno výrobci softwaru společně se síťovými operačními systémy. Takovéto aplikace zpravidla doplňují základní serverové funkce. Mezi nejčastěji dodávané patří:

- DHCP server
- DNS server (DHCP a DNS servery jsou vysvětleny v kapitole 3.6 Adresace sítí v TCP/IP)
- Program pro připojení k internetu, rozdělen na dvě položky. První je tzv. Proxy server (slouží pro uložení prohlížených internetových dat. Když si uživatelé sítě prohlížejí stejná data, jsou tyto data čteny z proxy, nikoliv z Internetu.). Druhou složku tvoří Firewall – nástroj pro zamezení přístupu do naší sítě z Internetu – viz kapitola 4.5 Logické zabezpečení sítě.
- Program pro elektronickou poštu
- Programy pro správu velkých databází

  Výrobci operačních systémů nabízejí také aplikace ve formě tzv. „softwarových balíků“. Základem je operační systém obohacen o jednotlivé aplikace. [2]

4. Vlastní zpracování

4.1 Struktura sítě učebny

Učebna bude obsahovat celkem 21 stanic, z čehož bude 20 stanic vyhrazeno pro studenty a 1 stanice vyhrazena pro vyučujícího. Stanice budou propojeny v rámci jedné místnosti. Svazek UTP kabelů od stanic, resp. od jejich zásuvek bude poté veden otvorem ve zdi do vedlejší serverové místnosti (viz příloha č.7). Server, patch panel, switch i záložní napájecí zdroj UPS budou umístěny v serverové místnosti v zamykatelné kovové skříni, tzv. racku.

Z předchozí kapitoly byl získán teoretický základ pro práci se sítěmi. Lze tedy určit, jaký charakter by síť učebny měla mít:

- síť učebny by měla být lokání (LAN)
- měla by mít hvězdicovou topologii
- měla by pracovat na architektuře Client-to-Server
- měla by pracovat na principu adresace TCP/IP.

Jak jednotlivé stanice propojit fyzicky a jak celou síť zprovoznit bude rozebráno v následujících kapitolách.

4.2 Výběr hardwaru

V teoretické části byly popsány jednotlivé prvky síťového technického vybavení. Tato část se bude věnovat jejich konkrétní aplikaci. Na základě požadavků budou vybrány vhodné aktivní i pasivní prvky.

4.2.1 Výběr aktivních prvků

Výběr aktivních prvků musí zohledňovat mnoho kritérií, která vycházejí již z důvodů, proč vůbec síť budovat, jaké budou její přínosy, jaké objemy dat se budou v síti přenášet, nebo jak spolu budou jednotlivá zařízení komunikovat.

4.2.1.1 Požadavky na switch sítě

Přenosová rychlost - Standartně se switche vyrábějí s 10Mb/s, 100 Mb/s a 1000 Mb/s. Pro naši síť bude bohatě vyhovovat střední varianta, čili Ethernetový switch s rychlostí 100 Mb/s.

Počet portů – Počet portů se pohybuje v rozmezí 5-24 na jeden switch. Ve třídě bude pro začátek 21 stanic. Tuto kapacitu by měl bohatě pokrýt jeden 24 portový switch. Zbývající sloty se nechají volné pro případ rozšíření počtu stanic, či připojení dalšího switche.

Typ portů – Použije se port RJ-45. Jelikož bude použito hvězdicové topologie, budou použity kabely kroucené dvojlinky, které tento port vyžadují.

Podpora funkce VLAN – Funkce pro sdružování portů do virtuálních sítí, umožňující na jednom switchi provozovat více nezávislých sítí.

Podpora funkce TRUNKING – Umožňuje více portů sdružit do jednoho kanálu a znásobit tak jejich rychlost.

Centralizovaná správa switche – Neboli Web Management, znamená, že switch lze nastavovat z jakékoliv stanice v síti. Podmínkou je znalost přístupového jména a hesla. Tato funkce dovoluje např. : regulovat šířku pásma jednotlivých portů, nebo tyto porty povolovat, či zakazovat.

Stohovatelnost switche – Neboli možnost mezi sebou propojit více switchů. Při možnosti budoucího rozšíření počtu stanic je tato vlastnost velice užitečná. Propojené switche jsou velmi lehce zpravovatelné. Máme-li napřáiklad 3 switche, je možné z jednoho PC připojeného k prvnímu switchi spravovat switch č.3 bez toho, aniž by bylo nutné vstávat a přepojovat kabely mezi switchi.

Na základě výše uvedených požadavků byl vybrán 24-portový switch TP-Link TL-SL2428WEB jakožto kombinace příznivé ceny a kvalitních vlastností. Switch disponuje kompaktním designem formátu 19”, čili je snadno umístitelný do racku. Kromě standartních 24 portů s rychlostí až 100 Mbps je vybaven dvojicí portů s rychlostí až 1 Gbps pro propojení s dalšími prvky sítě jako jsou další switche, servery, diskové stanice a další. V neposlední řadě disponuje podporou nejrůznějších síťových protokolů, detekcí kroucených kabelů a informačními LED diodami pro jednotlivé porty.

4.2.1.2 Volba pracovních stanic

Volba pracovních stanic by měla respektovat požadavky moderního hardwaru i softwaru. Zejména z důvodu implementace operačního systému Windows 7 (64-bit) by stanice měli býti dostatečně výkonné zejména v oblasti procesoru a operační paměti. Microsoft uvádí následující minimální požadavky pro chod těchto systémů:

- 1GHz procesor
- 1GB operační paměti
- 16GB volného místa na disku
- Grafická karta s podporou DirectX 9

V učebně budou použity stanice s následující konfigurací:

- Dvoujádrový procesor Intel Atom N330 s frekvencí 1,6 GHz
- 2 GB Operační paměť DDR2 s frekvencí 533 MHz
- 160 GB pevný disk
- Integrovaná grafická karta s podporou DirectX 9
- Základní deska podporující Fast Ethernet 10/ 100 Mbit/s LAN

4.2.1.3 Konfigurace serveru

Server by měl být schopen vyvinout dostatečný výkon pro obsluhu veškerého síťového zařízení a bez problémů zvládat správu všech stanic v síti, či běh aplikací společných pro její uživatele. Pro tyto potřeby bude nasazen server s procesorem Intel Xeon X3430, jehož čtyři jádra jsou taktována frekvencí 2,4 GHz. Dále byla zvolena DDR3 operační paměť o velikosti 2GB. Podpora kešování, technologií Registered a ECC jsou samozřejmostí. Pro komunikaci v síti je server vybaven Gigabitovým síťovým adaptérem pro zajištění nepřetržitého spojení v režimu odolnosti proti selhání s využitím akcelerace TCP/IP. Provedení serveru s výškou 1U (1 palec) a hloubkou méně než 60 cm umožní integraci do 19“ rack rozvaděče. Nasazenému software na server se věnuje kapitola 4.3.2 Operační systém serveru.

4.2.2 Výběr pasivních prvků

Teoretická část nastínila funkci, princip a použití pasivních prvků. Zde bude proveden jejich výběr, popřípadě způsob zprovoznění.

4.2.2.1 Volba přenosového média

Vzhledem k topologii a charakteru sítě byl výběr zúžen pouze na kroucenou dvojlinku. Budou použity kabely UTP standartního typu pro přenosovou rychlost 10/100Mbit, čili kategorie 5e. Společně s nimi budou použity dvouportové RJ 45 zásuvky v provedení „na omítku“. Pro propojení stanic se zásuvkami RJ 45 bude použito patch kabelu. Pro trasu od zásuvek do serverovny, respektive do patch panelu se použije horizontální UTP rozvod z měděného drátu. Od patch panelu do switche a následně do serveru poté opět povede UTP patch kabel.

Nacvaknutí konektorů na kabel

Kabel UTP se oholí asi 1,5cm na jeho konci a rozpletou se jednotlivé vodiče. Kabel se zastrčí do konektoru, vodiče se natlačí až k úplnému konci konektoru. Je však nutné

dávat pozor, aby se vodiče uvnitř konektoru nepřekřížily. Takto provedený konektor lze spolehlivě nacvaknout krimpovacími kleštěmi.

4.2.2.2 Vedení kabeláže

K vedení kabelů od stanic, respektive zásuvek k serveru, se použijí lišty připevněné na stěnách. Tato alternativa dostala přednost před vedením kabelů ve zdech pomocí tzv. „husích krků“. Rozvod kabelů ve zdech by vyžadoval zásah to infrastruktury místnosti a vedle zvýšení nákladů na realizaci sítě by se také zvýšila pracnost celého projektu. Proto i za cenu menší estetičnosti byla zvolena první možnost. Výjimku tvoří vedení kabelu z místnosti učebny do místnosti serverovny. Zde je nutné k překlenutí stěny mezi oběma místnostmi vést kabely vyvrtaným otvorem. Během trasy kabelů a na jejich koncích je nutné ponechávat dostatečné rezervy, tzv. distanční smyčky. Při koncentraci více kabelů v jednom místě (serverová místnost) by se kabely měly svazovat do svazku po max 48 kusech. Svazování se provede pomocí vyvazovacích pásků. Při svazování je nutné dbát na to, aby kabely nebyly přílíš utaženy, a aby bylo zamezeno jejich ohybům, prořízntutí izolace, nebo promáčknutí obalu kabelu.

Souběžnost napájecích a datových kabelů

Při vedení kabeláže je nutno respektovat jisté podmínky. Při vodorovném vedení datových kabelů je potřeba dodržovat jejich vzdálenost od kabelů napájecích, která je v případě nestíněné kroucené dvojlinky 50mm (v případě stíněné kroucené dvojlinky je tato vzdálenost nulová). Dojde-li v některém místě k překřížení kabelů, musí se kabely křížít pod úhlem 90°.

4.3 Software použitý v síti

Tato kapitola se bude zabývat instalací softwarových produktů pro hardware v naší síti. Bude popisovat jak software pro pracovní stanice, tak software pro server. Zvláštní pozornost bude věnována konfiguraci síťového rozhraní a některým důležitým komponentům použitého síťového operačního systému.

4.3.1 Operační systémy pracovních stanic

Zde bude uvedena charakteristika použitých operačních systémů pro PC v učebně. Stanice budou obsahovat jak operační systém Windows, tak konkurenční Linux. Učiněno je tak proto, aby si studenti v rámci výuky prohloubili znalosti v obou systémech.

4.3.1.1 Windows 7 Professional CZ 64-bit (OEM)

Windows 7 je operační systém vyprodukovaný firmou Microsoft. Je určený pro použití na osobních počítačích, či laptopech. Byl vydán na podzim roku 2009. V síti bude použita licence OEM. Jedná se o nejlevnější variantu systému, která se po instalaci se stává součástí počítače, přičemž nemůže být převedena na jiné PC. Verze Professional obsahuje například oproti verzi Home pro naši síť nutnou funkci připojení k doméně. Po úspěšné instalaci je nutno provést několik dílčích kroků, vedoucím k úspěšnému připojení do sítě:

Instalace ovladače síťové karty

Oproti svým předchůdcům je Windows 7 výrazně modernizován a cílem je jeho plná kompatibilita s existujícími ovladači zařízení, aplikací a hardwaru. Detekce a instalace síťové karty by v tomto případě měla proběhnout zcela automaticky.

Konfigurace TCP/IP protokolu

Potřebné parametry připojení (Ovládací panely-Síť a Internet-Síťová připojení-Vlastnosti-Protokol IP verze 4-Vlastnosti) lze buďto nechat vygenerovat automaticky pomocí DHCP a DNS serverů, nebo je přidělit ručně. Ruční nastavení je zobrazeno v příloze č.3.

4.3.1.2 Linux Debian 5.0

Debian GNU/Linux je volně šiřitelný operační systém, který je možno volně používat, ale také různě modifikovat. Oproti komerčním distribucím, jako jsou Red Hat nebo SuSe, nepoužívá balíčkový systém RPM, ale disponuje vlastním balíčkovým systémem deb-balíčků. Použit bude systém s jádrem 2.6.26.

Síťová rozhraní

Jsou v linuxu uvedeny pod zkratkami, za nimiž následuje číslo, které značí pořadí detekce v systému, např.: eth0.

Instalace síťové karty

Přítomnosti síťové karty v Linuxu lze zjistit příkazem *cat /proc/net/dev*. Pokud nebyla karta rozpoznána, může to být tím, že jednotlivá jádra jsou kompilována co nejmenší a ovladače jsou k dispozici ve formě modulů. Takovéto moduly se zavádí pouze v případě potřeby, nejsou tedy automaticky aplikovány. Moduly pro síťové karty se nachází v adresáři */lib/modules*. Následně již není problém zjistit informace o zařízeních na PCI sběrnicích pomocí příkazu *$lspci*. Poté není nic snadnějšího, než zjistit typ síťové karty a doinstalovat potřebný modul.

Konfigurace sítě

Nastavení sítě pomocí DHCP zajišťují jednotlivé konfigurační nástroje dodávané s danou distribucí linuxu. Síťová rozhraní lze ručně nastavit příkazem *ifconfig*. Takovýto příkaz bez dalších parametrů vypíše stávající konfiguraci sítě. Vlastní nastavení lze provést například takto :

ifconfig lo 127.0.0.1 netmask 255.0.0.0 broadcast 127.255.255.255

ifconfig eth0 10.0.0.7 netmask 255.255.255.0 broadcast 10.0.0.255

route add default gw 10.0.0.1

Dále je potřeba nastavit DNS, aby při práci byla možnost používat jména počítačů namísto jejich IP adres. Základním souborem pro převod jmen na IP adresy je soubor */etc/hosts*. Dekativaci síťového rozhraní se provádí příkazem *ifconfig eth0 down*.

„Základním souborem pro převod jmen na IP-adresy je soubor /etc/hosts, ve kterém můžeme vyjmenovat IP-adresy a k nim přiřadit libovolná jména. Linux je obvykle nastaven tak, že tento soubor má při převodu jmen na IP-adresu přednost. Lze tedy předdefinovat převod jmen na konkrétní IP-adresy, ovšem musíme dávat pozor, aby správce nezměnil IP-adresu zde uvedeného počítače. V takovém případě by se náš počítač pokoušel připojit na již neexistující IP-adresu.“(Horák, Keršláger, 2006, s.200)

Soubor */etc/hosts* by mohl vypadat například takto:

127.0.0.1 localhost

10.0.0.7 skola.mojedomena.cz skola

První sloupec obsahuje IP adresy, dále následuje plné jméno počítače včetně domény, a dále jsou uvedena mezerou oddělená zkrácená jména počítače.

4.3.2 Operační systém serveru

Téma síťových operačních systémů je velmi rozsáhlé a jeho detailní rozbor by vydal na další bakalářskou práci. Proto bude pozornost v této kapitole upřena pouze na vybraný typ a distribuci síťového OS, a na jeho základní, nebo nějakým způsobem důležité funkce.

Pro server byla zvolena opět verze Debianu 5.0. Tato distribuce je k dispozici ve třech verzích: stable, testing a unstable. Stable nabízí verze balíčků, které se aktualizují jen jednou za dlouhou dobu – cca 1 rok. Verze unstable nabízí mnohem interaktivněji updatované verze, prakticky každý den. Jejich nevýhoda ale spočívá v tom, že balíky z verze ustable zpravidla nebývají dostatečně otestovány, a proto by se mohlo stát, že by

například některý z nich nefungoval. Volba se tedy zužuje pro verzi testing: tato verze již byla spolehlivě otestována uživateli verze unstable, a tak lze nové verze balíčků, byť s určitým zpožděním, bezpečně používat. [4]

Celá instalace Debianu je podrobně popsaná v instalačním manuálu, proto ji v rámci této práce nebude věnována pozornost. Probrány budou pouze důležité komponenty serveru, které nejsou nedílnou součástí základní verze.

4.3.2.1 Apache HTTP Server

Jedná se o jeden z nejrozšířenějších webových serverů s otevřeným kódem pro GNU/Linux, ale také pro jiné platformy, jako například Max OS, nebo Microsoft Windows. Vyvíjen je od roku 1993 a v dnešní době se používá na více než 70% všech serverů.

Instalace Apache je v Debianu velmi triviální. Jediné, co je potřeba udělat je instalace balíčku apache2: *aptitude install apache2*. Po instalaci a spuštění serveru lze jeho funkčnost zkontrolovat zadáním ip adresy serveru do prohlížeče. Standartně by se měl objevit nápis „It works!“, znamenající, že instalace proběhla v pořádku.

Konfigurace Apache má velmi komplexní a bohaté možnosti. V Debianu se tato konfigurace nachází v /etc/apache2 a hlavním konfiguračním souborem je apache2.conf.[7]

4.3.2.2 PHP

PHP je programovací jazyk, pracující na straně serveru. Lze pomocí něj ukládat a měnit data webových stránek. Co se týká samotné instalace PHP, ani zde není příliš velký problém, jen je potřeba nějakým způsobem propojit PHP a Apache. O to se postará balíček libapache2-mod-php5: *aptitude install libapache2-mod-php5 php5*. Po restartu Apache je k dispozici webový server schopný běhu PHP aplikací. [7]

4.3.2.3 MySQL

MySQL je databázový systém vlastněný společností Sun Microsystems. Jedná se o multiplatformní databázi, komunikující pomocí jazyka SQL. V současnosti má velmi vysoký podíl na používaných databázích. Je to velmi výkonný software a jeho šiřitelnost je zcela volná.

Pro instalaci MySQL je nutná přítomnost PHP modulu, který by byl schopný s MySQL pracovat. Zde ji představuje komponenta php5-mysql. Instalace MySQL serveru, klienta a modulu pro PHP se provede příkazem: *aptitude install php5-mysql mysql server*. [9]

4.3.2.4 Konfigurace POP 3

Pokud bude na serveru zřízen poštovní uzel, který bude přijímat poštu pro doménu sítě, je potřeba zajistit i možnost přenosu dopisů, které budou uloženy v lokálních poštovních schránkách, do programů, které používají uživatelé v lokální síti. Nejčastěji používaný protokol POP3 je nejjednodušší variantou. [8]

Podmínkou zprovoznění jsou balíčky *xinetd* a *imap*. Pro správnou funkci stačí založit uživatele, nastavit jeho heslo, povolit službu POP3 a restartovat démona *xinetd*:

adduser lojza
passwd lojza
chkconfig ipop3 on
etc/init.d/xinetd restart

4.3.2.5 Samba

Jelikož se na pracovních stanicích nachází dva rozdílné typy operačních systémů (MS Windows a Linux), je potřeba vyřešit jejich kominukaci s operačním systémem serveru. V připadě linuxu je tato problematika vyřešena – operační systém serveru i stanice je na stejné bázi. Vdruhém případě je však potřeba zavést určitou emulaci, která by umožňovala sdílet soubory mezi linuxovým serverem a stanicí se systémem MS Windows.

Unixové systémy sdílejí soubory pomocí NFS (Network FileSystem). Počítače se systémem MS Windows mezi sebou však zpravidla používají tzv. Sdílení v sítích Microsoft, a s ním související SMB protokol. Samba je název projektu, který umožňuje sdílení souborů umístěných na Linuxovém serveru způsobem, jako by na něm běžel MS Windows.

Nastavení Samby se nachází v souboru */etc/samba/smb.conf*. Sambu lze nastavit pomocí prohlížeče www prostřednictvím nástroje Swat. Program Swat je možno zprovoznit následujícím způsobem:

- Povolení služby swat a xinetd – V nastavení démona xinetd je nutno povolit službu swat, poté při příchodu na port 901 démon xinetd předá řízení programu swat.
- Přikázání démonovi xinetd znovu načíst konfigurační soubor - */etc/init.d/xinetd reload*.
- Spuštění prohlížeče – vložení jména počítače s programem Swat doplněného za dvojtečkou číslem portu 901, např http://skola:901.
- Autorizace do programu Swat – jako Administrátor, čili uživatel root.

Základní nastavení Samby

Kominukace Samby s klientskými stanicemi probíhá pomocí protokolu TCP/IP. Pro spolupráci s Windows 7 je zapotřebí alespoň verze Samby 3.4.3. Uživatelé budou mít na Linuxu založené stejné účty, které budou sloužit pro přihlašování ke stanicím s MS Windows. Práva pro sdílené soubory budou pak přímo vycházet z práv, která má k daným souborům uživatel v Linuxu. V takovémto režimu je možné provozovat Sambu i jako PDC (Primary Domain Controller), kde se uživatelé přihlašují do domény a jejich jména a hesla jsou ověřována proti serveru, na kterém je Samba spuštěna. Pro přihlašování do domény je možné používat skripty nebo profily. Na server lze také ukládat uživatelská nastavení. [10]

Konfigurace Klienta

Klienta ze stanice MS Windows lze připojit k Sambě aktivací Klienta sítě Microsoft na daném PC. Je také nutné přidat protokol TCP/IP, jelikož právě pomocí něj Samba se stanicí komunikuje. U protokolu TCP/IP se nastaví IP adresa, brána a připadně adresa DNS serveru.

4.3.2.6 Připojení k Internetu

Připojení lokální sítě k internetu bude vyřešeno pomocí přidání Wifi karty do serveru. Server tedy bude skýtat dvě karty: Ethernetovou pro propojení se switchem a lokálními stanicemi, a Wifi kartu pro připojení k internetu. O přítomnosti obou karet se lze přesvědčit pomocí příkazu *dmesg*. [8]

Následně je potřeba nastavit ip adresu síťové karty:

ifconfig eth0 192.168.0.1

ifconfig eth0 up

Dále je potřeba získat ovladač pro Wifi kartu, například *HostAP*, který je dostupný na adrese *http://hostap.epitest.fi.* Po úspěšné instalaci se Wifi karta nastaví následujícím způsobem:

ifconfig wlan0 <*ip_adresa_pridelena*_providerem>

ifconfig wlan0 up

Maškaráda

Maškaráda je terminus technicus pro službu, která zprostředkovává přístup do Internetu počítačům, které ve vnitřní síti používají privátní IP adresy (tj. neveřejné, obvykle 10.x.x.x, 192.168.x.x atp). Při průchodu prvního datagramu z privátní sítě směrem do Internetu přepíše odesílající port a IP adresu (z privátního rozsahu) na veřejnou IP

adresu, kterou router disponuje. Zároveň do maškarádovací tabulky zavede záznam, podle kterého bude proveden zpětný překlad (při příchodu datagramu s odpovědí). [8]
Syntaxe nastavení maškarády v Linuxu je následující:

iptables -P FORWARD DROP

povolení průchodu paketů ze síťové karty na Wifi kartu:

iptables -A FORWARD -i eth0 -o wlan0 -j ACCEPT

povolení provozu z wlan na eth0:

iptables -A FORWARD -i wlan0 -o eth0 -m state --state ESTABLISHED,RELATED –j ACCEPT

zapnutí maškarády pro počítače ve vnitřní síti:
iptables -A POSTROUTING -t nat -o wlan0 -j MASQUERADE

4.4 Fyzické zabezpečení sítě

Tato a následující kapitola se budou věnovat druhé oblasti práce, a to sice zabezpečení sítě.

4.4.1 Záložní zdroje UPS

Náhlé přerušení přívodu elektrické energie k serveru může způsobit značné problémy. Dojde-li k výpadku elektřiny, pro síťový operační systém i všechny běžící aplikace to znamená okamžité ukončení bez možnosti uložení dat. Následkem tohoto může být nutnost nové instalace systému nebo programu. Aby se předešlo podobným výpadkům, uchovávají se v rámci sítě takzvané záložní zdroje UPS (Uninterruptible Power Supply).

Takovéto zdroje se skládají z hermetizovaného zdroje (nesmí z něj vycházet jedovaté výpary) a usměrňovače (kvůli jejich nabíjení). Podle zapojení rozlišujeme 3 typy zdrojů UPS: [2]

UPS off-line

Tvoří nejnižší a nejlevnější typ těchto zdrojů.Obsahují jednoduchý napájecí obvod s usměrňovačem pro nabíjení akumulátorů a jednoduchý střídač napětí s většinou nekvalitním lichoběžníkovým výstupem. Zdroj funguje tak, že poklesne-li napájecí hodnota v rozvodné síti, začne se server napájet z akumulátoru. Napájení z těchto zdrojů zpravidla nemá sinusový průběh, ale počítačům to příliš moc nevadí.

UPS on-line

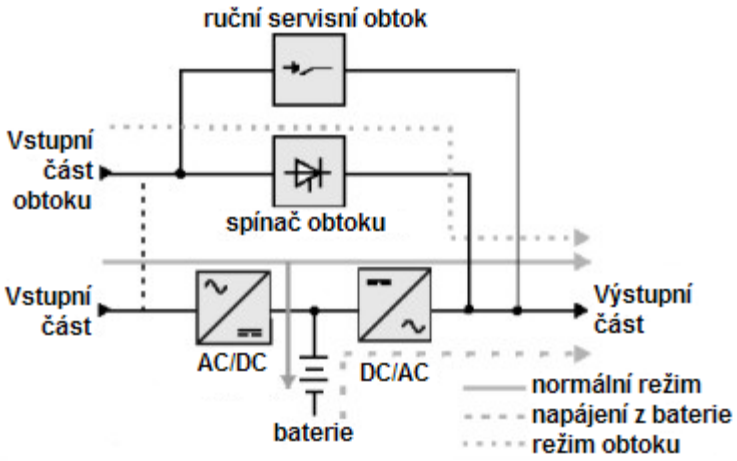
Jsou nejvyšší třídou zdrojů UPS. Jejich princip je takový, že výstup z UPS je vždy tvořen střídačem napájeným z akumulátorů a akumulátor je stále dobíjen z elektrorozvodné sítě. Počítače nejsou nikdy připojeny k napákecí síti, jsou tedy odděleny od všech poruch a nepravidelností v ní.

UPS line interactive

Tvoří mezičlánek mezi výše jmenovanými variantami. Zpravidla je spotřebič napájen přímo z elektrorozvodné sítě, ale napájecí napětí je v UPS upravováno tak, že jsou odfiltrovány šumy. Někdy si také elektronické obvody poradí bez účasti akumulátorů s mírným podpětím či přepětím.

Při výběru pro naši síť byl vybrán typ UPS line interactive, jako vhodná kombinace mezi spolehlivostí a cenou. Při výběru zdrojů UPS také hrají významnou roli technické parametry:

- Výkon – Udává se ve VA (voltampérech). Tento výkon musí být o něco vyšší, než výkon napájecího zdroje serveru. Jelikož se výkon zdroje serveru udává ve W (wattech), a vztah mezi VA a W je 0,7, měl by být výkon záložního zdroje 0,7 krát větší, než zdánlivý výkon napájecího zdroje serveru.
- Čas napájení UPS – Jedná se o dobu, během níž je UPS schopná napájet server energií ze své baterie. Slouží k překlenutí krátkodobých výpadků, a proto je její horní hranice kolem 20 minut. Při vyšším výkonu UPS (vzhledem k výkonu zdroje serveru) se doba napájení z baterií prodlužuje. Kdyby byl např. použili zálohovací zdroj 1000VA pro server se zdrojem 450W, vzroste doba napájení z baterií na cca 60 minut.
- Softwarové vybavení – Zdroje UPS také obsahují program, který se nahrává do operačního systému serveru. Havní funkcí tohoto softwaru je legální ukončení operačního systému serveru po určité době (např. v době, kdy hrozí nebezpečí, že se vybíjí akumulátor v UPS). Pro komunikaci se serverem se používá sériový port nebo USB.
- Stav baterií – U většiny UPS je tento stav možné vyčíst z jejich čelního panelu z kontrolních diod. Také lze tyto informace zjistit softwarově. Životnost baterií bývá 3 až 4 roky. [2]



Obr. 7: Schéma napájení pomocí zdrojů UPS

4.4.2 Zabezpečení serveru a klíčových hardwarových prvků v síti.

V případě serveru, swiche a záložního zdroje bude mít zabezpečení podobu zamykatelné skříně (racku). U stanic by měly být v BIOSu zakázány USB porty, aby nebylo možné pomocí tohoto rozhraní externě implementovat různé škodlivé aplikace. PC by měly také disponovat přepěťovými zásuvkami, které by je chránily pro případ zkratů nebo nadproudů z elektrické sítě.

4.5 Logické zabezpečení sítě

Vedle fyzického zabezpečení hraje to logické možná ještě významnější roli, neboť útoky na síť způsobené fyzicky mohou být zpravidla ihned vypozorovány. Logické útoky oproti tomu mohou zůstat neodhaleny po velmi dlouhou dobu, a útočníkovi se tak otevírá velmi výrazný prostor pro zneužívání naší sítě. Následující kapitoly budou věnovány nejčastějším typům útoků takovéhoto rázu, a budou pro ně navrženy vhodná řešení.

4.5.1 Odposlech na síti

K této formě narušení sítě není zapotřebí žádného složitého zařízení. Útočníkovi postačí obyčejný počítač s tím „správným“ softwarem, připojený k síti. S takovýmto vybavením je pak již možno při troše zručnosti sledovat veškeré toky na celé síti.

Jediný způsob, jak tomuto útoku předejít je šifrování důležitých kanálů. Uživatelé používají pro přístup k jednomu PC stále ten samý účet, přestože přistupují různými způsoby. Stačí tedy, aby útočník odposlechl například heslo pro FTP, a má zároveň i

přístup k SSH, přestože toto je šifrované. Je tedy vhodné šifrovat všechny protokoly, jimiž procházejí citlivé informace (hesla,pošta). [4]

4.5.2 Man-in-the-middle

Šifrování však k bezpečnosti sítě nemusí vždy úplně postačovat. Může se stát, že prohlížeč předloží ohlášení, že nedokázal certifikát ověřit. Uživatel obvykle na tuto skutečnost reaguje tak, že ji „odkliká“, aby ji měl co nejrychleji z krku a mohl pokračovat dál. Zde vzniká hrozpa útoku: certifikát může být vydaný útočníkem typu man-in-the-middle, což je metoda útoku, kdy narušitel používá počítač, který se chová stejně jako ten, ke kterému se uživatel chce připojit. Po odsouhlasení certifikátu a vyplnění údajů je falešný počítač přijme, a odešle je správnému stroji. Poté je již schopen sledovat a odposlouchávat obousměrnou komunikaci.

Proti tomuto útoku existuje jediná zarčená ochrana: dostatečná osvěta uživatelů sítě. Uživatel by certifikát po jeho příchodu měl prozkoumat a podle otisku zjistit, zda je vše v pořádku. [4]

4.5.3 DoS (Denial of Service)

Tento typ útoku se liší od ostatních dvou. Nekompromituje napadený systém ani se nesnaží získat práva administrátora. Jeho podstata spočívá v tom, že se útočník snaží vyřadit některý systém opakovaným vysíláním velkého množství požadavků. Zahlcený stroj poté není schopen obsluhovat běžné dotazy uživatelů, či může dojít k jeho zkolabování. Mnohem „ničivějším“ druhem jsou útoky typu DDoS, na jejichž provedení se podílí větší množství strojů, obvykle řízené z jednoho místa.

„*Zahlcení nesmyslnými dotazy může být sice na první pohled jen „nevinnou“ hrou, ale lze to také dobře využít k podpoře dalších útočníkových aktivit. Pokud například v síti běží vyhrazený počítač, který sbírá logy, kontroluje odposlechy a podobně, je DoS velmi pohodlnou cestou, jak tuto nepříjemnost odstranit z cesty.“(Krčmář,2008, s.45)*

Aktivitu DoS je možné ohlídat například pomocí firewallu prostřednictvím iptables. O firewalech přijde zmínka v kapitole 4.5.5. Paketový filtr a firewall [4]

4.5.4 Detekce podvržených ARP údajů

Další možností, jak se zlotřilý systém může vydávat za důvěryhodný počítač je prostřednictvím podvržených ARP údajů. Tato metoda narušení je možna pouze u lokálních sítí, a tou vyšetřovaná síť bezpochyby je. Měla by ji tedy v rámci této práce býti věnována pozornost. Nejprve je nutné vysvětlit, co to vlastně ARP je, a jak pracuje.

ARP, neboli Address Resolution Protocol slouží v počítačových sítích s IP protokolem pro získání ethernetové MAC adresy sousedního stroje z jeho IP adresy. Používá se tedy v případě, kde je potřeba odeslat IP datagram na adresu ležící ve stejné síti, jako odesílatel. Odesílající vyšle ARP dotaz, který obsahuje hledanou IP adresu a údaje o sobě. Dotaz je broadcastem poslán na MAC adresu identifikující všechny účastníky dané sítě. Vlastník hledané IP adresy poté odešle ARP dotazateli odpověď obsahující IP adresu a MAC adresu. ARP protokol defacto slouží k překladu IP adresy na Mac adresu síťové karty.

Značnou nevýhodu ARP protokolu tvoří fakt, že je tento protokol bezstavový. Znamená to tedy, že nesleduje, na jaké dotazy dostal odpověď a následkem toho přijme odpověď, na kterou se třeba vůbec neptal. Stačí tedy rozeslat podvržené ARP odpovědi s informací, že IP adrese původního systému odpovídá Mac adresa systému útočníka. [6]

K prevenci před podvrženými ARP údaji se používá například program Arpwatch, který pracuje tak, že přepne síťové rozhraní do promiskuitního režimu, odposlouchává provoz a postupem času zaznamenává dvojice IP/MAC adres. Narazí-li na anomální chování, jímž může být například změna již známé dvojice IP/MAC, zaznamená tuto událost do syslogu.

Ve chvíli, kdy se začne Arpwatch učit dvojice IP--/-MAC adres, můžeme z logu vyčíst např. následující záznamy:

Jun 5 12:42:27 jura arpwatch: new station 192.168.0.65 0:7:e9:40: 8a:57

Změna známé dvojice IP/MAC se projeví takto:

Jun 5 12:45:12 jura arpwatch: changed ethernet address 192.168.0.65 0:11:11:bc:27:4a (0:7:e9:40: 8a:57)

Jun 5 12:45:17 jura arpwatch: flip flop 192.168.0.65 0:7:e9:40: 8a:57 (0:11:11:bc:27:4a)

Jun 5 12:45:17 jura arpwatch: flip flop 192.168.0.65 0:11:11:bc:27:4a (0:7:e9:40: 8a:57)

První záznam odpovídá první přijaté zfalšované odpovědi, následující záznamy vznikají v důsledku kolizí mezi legitimními a falešnými odpověďmi.

4.5.5 Paketový filtr a firewall

Slovo Firewall je zejména v posledním desetiletí čím dál více skloňováno v souvislosti se síťovým připojením. V doslovném překladu znamená firewall „protipožární zeď“, a toto označení podstatu firewallu dokonale vystihuje. Jedná se o službu systému, která chrání naši síť před útoky a nezvanými hosty.

V Linuxu se skrývá firewall za částí jádra zvanou iptables. Tato služba je velmi komplexní. Mezi její funkce patří práce s pakety, například jejich třídění, propouštění, přesměrovávání nebo zahazování. Pomocí iptables lze tedy nejen realizovat firewall, ale také libovolnou činnost na úrovni paketů. Paketový filtr použitý v našem síťovém OS nese název Netfilter a jeho základní komponentou je chain. Chain obsahuje seznam pravidel uplatňujících se na jednotlivé pakety podle toho, jak do systému vstupují, vystupují, nebo jím procházejí. Standartně obsahuje systém 3 hlavní chainy : INPUT, OUTPUT a FORWARD. Chain INPUT se vztahuje na pakety, které jsou přijímány systémem, OUTPUT se vztahuje na pakety vzniklé v lokálním systému a FORWARD se aplikuje na pakety, které systém předává z jednoho rozhraní na druhé. [6]

„*Pakety procházející počítačem vstoupí jen do řetězce FORWARD. Neplatí tedy IMPUT-FORWARD-OUTPUT, jak si často začátečníci myslí. Při definici pravidel je toto potřeba mít na paměti, neboť se v této věci velmi často chybuje.“ (Krčmář,2008, s.51)*

Před definicí konkrétních pravidel je potřeba nasstavit výchozí chování jednotlivých chainů. Toto se nastavuje volbou –P, neboli „policy“.

iptables –P INPUT DROP

iptables –P FORWARD DROP

Tímto je zajištěno, že firewallem projdou jen ty pakety, které budou následujícími pravidly povoleny. Chain OUTPUT zůstane nenastaveno, jelikož odchozí provoz z firewallu filtrován nebude. Syntaxe příkazu iptables je zobrazena v příloze č.4.

4.5.6 Ochrana před SPAMem a viry v emailech

Nevyžádaná pošta (tzv. SPAM) je aktuálním současným problémem. Nejčastěji se šíří z chybně nakonfigurovaných poštovních uzlů (MTA), které jsou ochotny od kohokoliv přijmout poštu a rozeslat ji na tisíce adres (tzv. open-relay). Spammer v takovém případě

předá špatně nakonfigurovanému MTA jeden mail a uvede v obálce stovky až tisíce příjemců.

Částečnou ochranou před šířením SPAMů může být využití on-line databáze, která obsahuje seznam IP adres takových počítačů (blacklisty). Tyto služby provozují různé velké firmy podnikající na Internetu - např. freemaily. Jejich účinnost není 100%, nicméně je funkční. Většina těchto služeb je ochotna více či méně automatizovaným způsobem přijímat spamy, které se dostávají do sítě a z nich pak získávat seznamy podezdřelých počítačů. Postižený poštovní uzel je nejprve otestován a když se prokáže, že je open-relay, umístěn do blacklistu. [8]

V případě sendmailu stačí do makrosouboru přidat následující řádky, které zajistí kontrolu ze tří asi nejpoužívanějších databází:

```
FEATURE(`enhdnsbl',`list.dsbl.org',  `"Spam blocked using DSBL
  - see <http://DSBL.org/listing.php?ip="$&{client_addr}">")dnl
FEATURE(`enhdnsbl',`relays.ordb.org',`"Spam blocked using ORDB
 - see <http://ORDB.org/lookup/?host="$&{client_addr}">")dnl
FEATURE(`enhdnsbl',`bl.spamcop.net', `"Spam blocked using SpamCop
  - see <http://SpamCop.net/bl.shtml?"$&{client_addr}">")dnl
define(`confBIND_OPTS', `WorkAroundBrokenAAAA')dnl
```

Druhým významným opatřením může být blokování mailů, které obsahují tzv. nebezpečné přílohy. V případě sendmailu nejjednodušší řešení využívá rozhraní MILTER které umožňuje psát externí programy, jež přes definované API mohou analyzovat, odmítat či modifikovat emaliy, které skrz sendmail procházejí.

5 Výsledky a diskuse

V této práci byl vytvořen návrh modelu počítačové sítě školní učebny a jejího následného zabezpečení. Vycházelo se přitom z teoretické části, kde byly popsány základní aspekty síťové problematiky. Postup při řešení návrhu byl pojat deduktivně – z obecného určení pojmů a oblastí jejich využití až po jejich konkrétní uplatnění v praktické části.

V návrhové části byl nejprve proveden výběr vhodného technického vybavení učebny, počínaje aktivními prvky, kabeláží, a konče hardwarem pro server.Upřednostněny byly prvky respektující požadavky moderních sítí. V oblasti aktivních prvků byly kladeny nároky zejména na použitý switch, od něhož se požadoval zejména dostatečný počet portů, možnost umístění do racku, nebo jeho podpora web managementu.

Z pasivních prvků byla nejvíce upřena pozornost na výběr přenosového média. Vzhledem k topologii sítě a Ethernetovému standardu byla volba jednoznačná – použil se kabel typu UTP (nestíněná kroucená dvojlinka). Pro propojení mezi PC a zásuvkami RJ 45 se použil kabel v provedení „lanko“, jelikož lze předpokládat, že se s kabelem bude v budoucnu nadále manipulovat. Pro vedení od zásuvek do serverovny bylo použito UTP kabelů ze standartního měděného drátu. Oproti lanku má lepší fyzické vlastnosti, zejména větší tvrdost, což poslouží ke snadnějšímu vedení kabelu, především v místě průchodu zdí z učebny do serverovny. Hardware stanic a serveru byl volen úměrně potřebám jejich programového vybavení, především operačním systémům.

Stanice disponují dvěma operačními systémy: Windows 7 a Linux Debian 5.0. Je tomu učiněno proto, aby studeni měli možnost seznámit se s prací v obou systémech. Jako operační systém serveru byla použita distribuce Linuxu. Tento fakt má určité výhody: jednak je Linux volně šiřitelný a proto je například oproti systému Windows poskytován zdarma, jednak disponuje mnohem propracovanějšími nástroji pro správu sítě, zejména v rámci bezpečnosti, a bezpečnost je to hlavní, o co v naší síti jde.

Závěrečná část práce byla věnována síťovému zabezpečení. Zaprvé je potřeba podotknout, že při analýze všech možných rizik a způsobů narušení sítě vyplyne fakt, že nikdy není možné dosáhnout stoprocentní bezpečnosti.Teoreticky se lze takovéto bezpečnosti přiblížit, ale za cenu astronomických nákladů. Bezpečnost je vždy kompromisem mezi náklady a úrovní zabezpečení, a zvolení takovéto úrovně je na každém správci. V rámci této práce byly popsány pouze nejběžnější typy útoků na počítačovou síť, a následně bylo nastíněno, jak si v případě jejich výskytu poradit.

6 Závěr

Od doby, kdy se poprvé podařilo zprovoznit komunikaci mezi dvěma PC se spousta věcí změnila. Množství elementů, pomocí kterých lze v dnešní době sestavit funkční počítačovou síť je nespočet. Jejich různými kombinacemi je možno sestavit libovolně složité komplexy, od malých domácích sítí až po sítě pokrývající plochu několika firemních poboček, či celých měst. Jedna věc by ale měla zůstat pro všechny takovéto komplexy společná: při jejich realizaci by se měl člověk řídit striktními pravidly.

Problematika počítačových sítí je velmi rozsáhlá. Tato bakalářská práce obsahuje pouze několik fragmentů z této problematiky. Z důvodu omezenosti rozsahu této práce byla pozornost upírána zejména k takovým částem, které bezprostředně souvisí s tématem práce. Byly demonstrovány způsoby propojení stanic, metody komunikace mezi nimi, ale také s vnějším okolím. S ohledem na typ sítě byla zvolena adekvátní úroveň zabezpečení.

7 Seznam použitých zdrojů

[1] Kállay, F., Peniak, P. Počítačové sítě a jejich aplikace: LAN, MAN, WAN. Praha: Grada, 2003. ISBN 80-247-0545-1

[2] Horák, J., Keršláger, M. Počítačové sítě pro začínající správce. Brno: Computer Press, 2006 ISBN 80-251-2073-6

[3] Horák, J. Malá počítačová síť doma a ve firmě. Praha: Grada, 2003. ISBN 80-247-0582-6

[4] Krčmář, P., Linux: postavte si počítačovou síť. Praha: Grada, 2008. ISBN 80-247-1290-1

[5] Kostroun, A., Stavíme si malou síť. Praha: Computer Press, 2001. ISBN 80-7226-510-5

[6] Lockhart, A. Bezpečnost sítí na maximum. Praha: Computer press, 2005. ISBN 80- 251-0805-8

[7] Linuxexpres [online]. 2009 [cit. 2009-09-01] <http://www.linuxexpres.cz/praxe/sprava-linuxoveho-serveru>

[8] otakar.4fan.cz [online]. 2010 [cit. 2010-11-24] <http://otakar.4fan.cz/otakar.php?clid=pcpraxe>

[9] root.cz [online]. 2010 [cit. 2010-5-11] <http://www.root.cz/clanky>

[10] abclinuxu.cz [online]. 2010 [cit. 2009-6-11] < http://www.abclinuxu.cz/clanky/site>

8 Přílohy

Seznam příloh

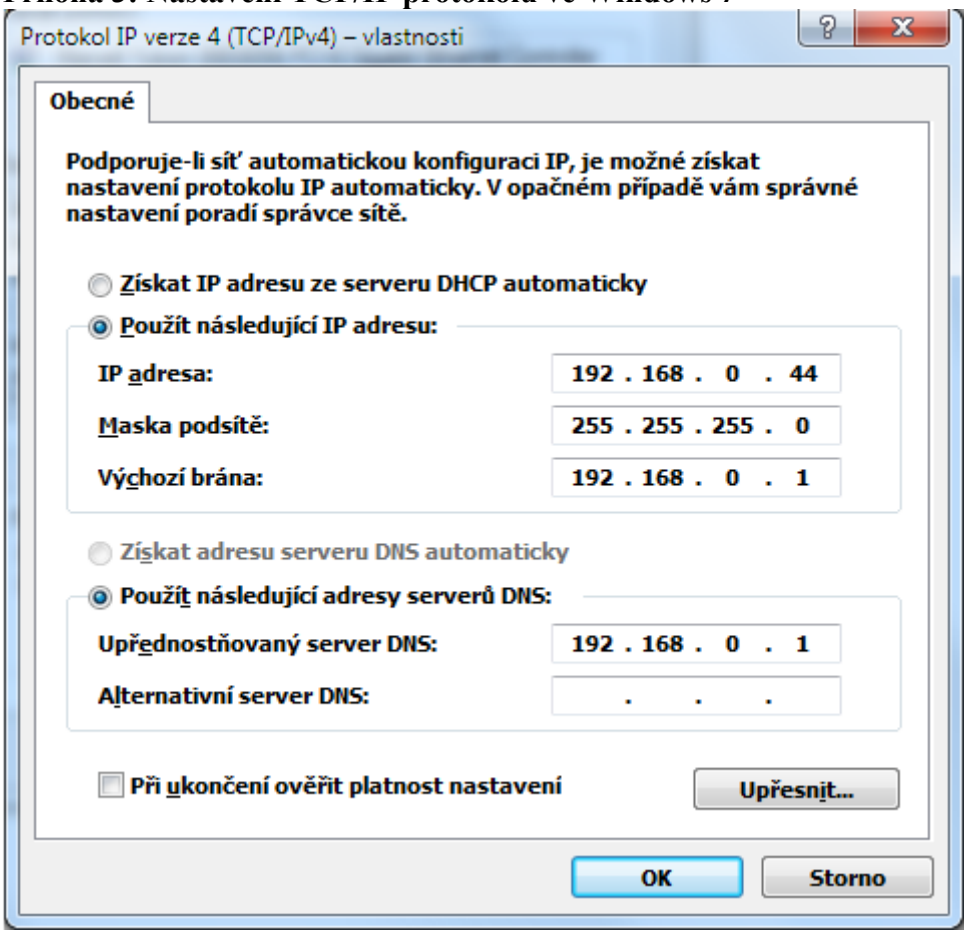
Příloha 1: Srovnání síťových topologií:

Topologie	Výhoda	Nevýhoda	Rozsah použití
Sběrnice	Nízké pořizovací náklady	Poruchovost, obtížné vyhledávání místa závady, porucha kabeláže vyřazuje cleou síť	Dožívá ve starších kabelážích
Hvězda	Spolehlivá, rychlá	Nutnost koncentrátoru (switche)	Dnes nejpoužívanější
Kruh	Pravidelné předávání zpráv v kruhu	Stejné jako u sběrnicové topologie, řeší se zdvojením vedení	Používají ji méně rozšířené sítě IBM Token Ring a FDDI

Příloha 2: Přehled balíků jednotlivých výrobců síťových OS

Produkt	Microsoft Small Business Server 2008	Novell Small Business Suite 6.6	Linux
Operační systém	Microsoft Windows Server 2008	Novell Netware 6.5	Linux
Připojení k Internetu	Microsoft ISA 2006	BorderManager	Proxy cache Squid
Elektronická pošta	Exchange 2007 Server	GroupWise	Sendmail, IMAP a LDAP servery
Správa databází	Microsoft SQL Server		PostgreeSQL, MySQL

Příloha 3: Nastavení TCP/IP protokolu ve Windows 7



Příloha 4: Syntaxe příkazu iptables

Pro práci s iptables jsou zapotřebí pochopitelně práva uživatele root. Základní syntaxe vypadá následovně:

iptables [tabulka] [akce] [řetězerc] [pravidla] [cíl]

Lze tedy začít nastavovat pravidla, která budou propouštět provoz dovnitř. První je pravidlo pro povolení provozu na TCP port 80 – což je port webového serveru:

iptables -A FORWARD –m state –state NEW –p tcp –d 192.168.1.20 --dport 80 –j ACCEPT

Dále je nutno povolit port TCP 25, což je standartní port protokolu SMTP:

iptables -A FORWARD –m state –state NEW –p tcp –d 192.168.1.20 --dport 25 –j ACCEPT

následně bude požadováno na poštovní server povolit přístup i pro protokoly POP3, IMAP a IMAP+SSL:

POP3:

iptables -A FORWARD –m state –state NEW –p tcp –d 192.168.1.20 --dport 110 –j ACCEPT

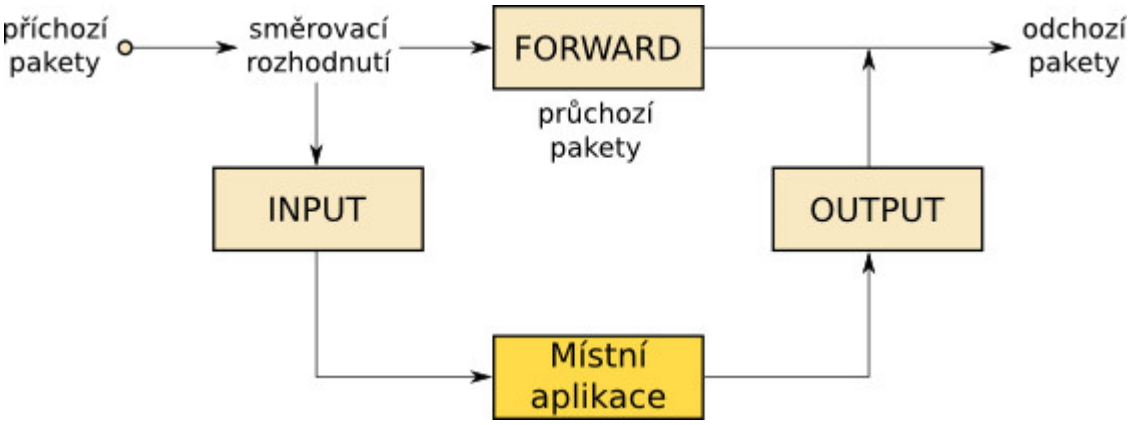
IMAP:

iptables -A FORWARD –m state –state NEW –p tcp –d 192.168.1.20 --dport 143 –j ACCEPT

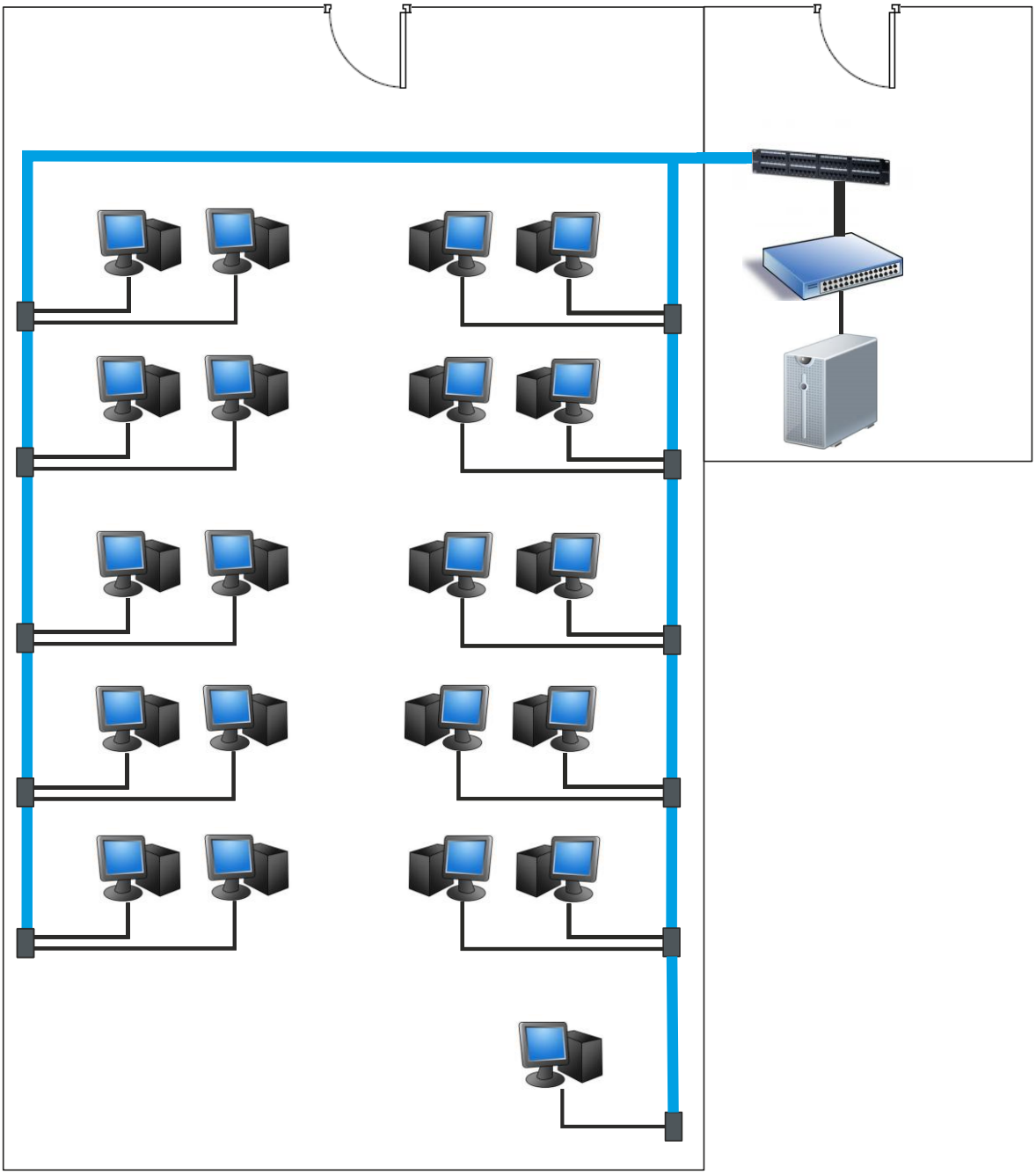
IMAP+SSL:

iptables -A FORWARD –m state –state NEW –p tcp –d 192.168.1.20 --dport 993 –j ACCEPT

Příloha 5: Algoritmus v linuxovém paketovém filtru



Příloha 6: Schéma učebny a serverovny



Příloha 7: Kalkulace nákladů

Název	Počet Ks/m	Cena za kus/metr (Kč)	Cena celkem (Kč)	Cena s DPH (Kč)
Kabel UTP - lanko	43	7	301	358
Kabel UTP - drát	97	6	582	693
Koncovka RJ 45	88	3	264	314
Zásuvka RJ 45	11	82	902	1 073
19“RACK	1	2 129	2 129	2 534
Pracovní stanice	21	8230	172 830	205 668
Patch panel	1	1	509	611
Switch	1	1 801	1 801	2 143
Server	1	20 746	20 746	24 687
Zdroj UPS	1	7 499	7 499	8 999
Lišty	100	19	1 900	2 261
Finální náklady			207 653	249 341

Pozn.: Cena operačního systému Windows 7 Professional CZ 64-bit je započtena v cenách za pracovní stanice (jedná se o licenci OEM dodávanou pouze společně s PC).