Návrh učebny počítačových sítí

Design of computer network training room

bakalářská práce

Jiří Krhánek, DiS.

Vedoucí bakalářské práce: Ing. Ladislav Beránek, CSc.

Jihočeská univerzita v Českých Budějovicích
Pedagogická fakulta
Katedra informatiky
2008

Prohlášení

Prohlašuji, že svoji bakalářskou práci jsem vypracoval samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě pedagogickou fakultou elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách.

V Českých Budějovicích dne

.....

Podpis autora

.....

Anotace

Tato práce se zabývá návrhem počítačové učebny pro výuku počítačových sítí. Nejprve se věnuji postupu vytvoření počítačové sítě. Rozhoduji jaký hardware a síťové prvky jsou potřeba pro realizaci plně funkční počítačové sítě. Poté popisuji síťové nastavení v operačních systémech. Nakonec jsem se zaměřil na řešení konkrétních případů, které by studenti mohli v takovéto počítačové učebně řešit.

Abstract

This project describe design of computer classroom for learning computer networking. At first I explain how create computer network. I decide about hardware and network items to use for realization fully functional computer network. Below I describe network setting in Operating Systems. At the end I fixate to solution particular cases which could be resolved by students in this computer classroom.

Poděkování

Rád bych poděkoval vedoucímu bakalářské práce Ing. Ladislavu Beránkovi, CSc. za pomoc při zpracování tématu této práce.

Obsah

1 Úvod

Pro tuto bakalářskou práci jsem si vybral téma „Návrh počítačové učebny pro výuku počítačových sítí“. Práci jsem si zvolil záměrně, neboť mne téma počítačových sítí zajímá a také již mám nějaké zkušenosti s tímto oborem.

Práci jsem rozdělil do čtyř hlavních kapitol. V první kapitole se zaměříme na rozbor sítí obecně, na jejich výhody. Další teoretickou část věnuji rozdělení počítačových sítí podle různých hledisek. Na základě těchto informací se dostaneme k praktickému výběru požadavků na síť a z toho nám i vyplyne, jak síť realizovat. Jakou zvolit topologii, normu a třeba i jaký síťový protokol budeme v síti používat.

Druhá část se týká hardwaru použitého v běžné počítačové síti založené na normě Ethernet. Vždy se seznámíme se síťovým prvkem, popíšeme si jeho funkci a také se pokusíme vybrat vhodnou variantu pro naší síť. Ve větší míře se věnuji hlavně aktivním síťovým prvkům jako je síťová karta a switch.

V další kapitole se věnuji popisu práce s operačními systémy. Zaměříme se hlavně na práci související se síťovou konfigurací systému a síťové karty. Také si ukážeme, jak nastavit síťový protokol TCP/IP a to jak v systému Windows, tak i v systému Linux.

Poslední kapitola se věnuje ukázkovým příkladům pro výuku, které se dají řešit v dané síti. Stěžejní jsou první tři příklady, které na sebe navazují a student se naučí základní principy správy sítě. Nalezneme zde i příklady, které nevyžadují přímo realizaci v počítačové síti. Například když si musíme spočítat adresový prostor pro počítače a sítě.

Na závěr práce se pokusím zhodnotit přínos práce a obtížnost tématu. Zdůvodnit metodiku práce a zvolený koncept.

2 Návrh počítačové sítě

Než se pustíme do návrhu sítě, tak se musíme alespoň částečně seznámit s teorií týkající se počítačových sítí, abychom měli představu o tom, co obnáší veškeré pojmy, které poté budeme v praktické části používat v textu. Na úplný začátek si ovšem povíme, proč vůbec používat počítačovou síť a jaké nám to přináší výhody.

2.1 Počítačová síť obecně

Co je to počítačová síť? Síť je pojem pro dvě či více zařízení, která jsou mezi sebou propojená a to za účelem sdílení informací nebo jejich zdrojů. Takovéto propojení může být realizováno několika způsoby. Může být uskutečněno pomocí kabelů nebo pomocí bezdrátových technologií.

Spojovací kabely mohou být různých typů: koaxiální, kroucené dvojlinky a optické kabely. Propojení bezdrátových zařízení využívá rádiové signály, technologie laseru, infračerveného paprsku či satelitního přenosu.

Ještě dodejme, že sdílené informace a zdroje mohou být například datové soubory, aplikační programy, modemy, tiskárny a další hardwarové zařízení.

2.2 Proč propojovat počítače?

Výhodou počítače je, že může fungovat jako samostatná výpočetní jednotka. Nabízí se tedy otázka, proč spojovat počítače do jedné sítě. Odpovědí je hned několik i podle publikace *Počítačové sítě* [5].

2.2.1 Sdílení výstupních zařízení

Mnohé firemní sítě vznikly právě z důvodu sdílení výstupních zařízení, a to hlavně společných tiskáren. Šetřil se tím čas i peníze a uživatelé si začali uvědomovat, že takto propojené počítače mohou sdílet i další zařízení jako plottery, různá grafická zařízení využívající elektronická pera a nebo například sdílení faxu. Fax ovšem můžeme sdílet i jako vstupní zařízení.

2.2.2 Sdílení vstupních zařízení

V síti můžeme sdílet vstupní zařízení jako skenery, digitální kamery a další. Tyto zařízení sdílíme hlavně proto, že jsou využívána sporadicky a pokud jsou na vyšší kvalitativní úrovni, bývají dosti drahá. A tak je rozumné takového zařízení sdílet v síti.

2.2.3 Sdílení ukládacích zařízení

Další důležitý prvek v sítích jsou právě ukládací zařízení. Sdílení síťových pevných disků, disketových mechanik, CD a DVD mechanik, paměťových zařízení je velkou výhodou pro práci v síti, jelikož na ně můžeme data ukládat jako by to bylo zařízení v našem počítači. Takovéto sdílení můžeme využít i u dalších zařízení typu ZIP, JAZ, magneticko-optické disky a v podstatě jakýkoliv další ukládací zařízení.

2.2.4 Sdílení modemů a internetového připojení

Důležitou funkcí a schopností sítí je sdílení modemu, ISDN linky, kabelových modemů a xDSL adaptéry. Přes takováto síťová zařízení můžeme celou síť připojit k Internetu, a to pomocí jediné telefonní linky nebo jednoho účtu u poskytovatele připojení.

2.2.5 Sdílení dat a aplikací

Jak hardwarové zařízení, tak i datové soubory a aplikační programy mohou být poskytnuty širšímu počtů uživatelů. Takovéto sdílení je velice efektivní využití úložné kapacity disků a také výrazně usnadňuje spolupráci více uživatelů na společných projektech. Projekt je uložen na centrálním místě a všichni uživatelé k němu mají rovnocený přístup.

Aplikační programy bývají nainstalovány na serveru. Uživatelé se pak mohou připojit na tento server a jeho sdílený prostor a spustit z něj aplikaci na svých počítačích bez nutnosti použití úložné kapacity jejich pevných disků.

2.3 Výhody sítí

V předešlém bloku jsme si nastínili některé důvody, proč se sítě používají, a tak po shrnutí nám vyplynou i výhody počítačových sítí.

Jako první výhodu bych uvedl **sdílení dat** a tedy, že sdílené soubory jsou společné pro všechny uživatele sítě. Také můžeme snadno přenášet data. Překopírovat data z jednoho počítače do druhého není žádný problém, nepotřebujeme žádné přenosné médium, jako disketu nebo FLASH disk a nejsme tak omezeni ani jejich kapacitou. Další výhodou je, že můžeme **sdílet hardwarové prostředky,** jak jsem již uváděl, tiskárny, skenery, disky a tak dále.

Také **komunikace v síti** je jednoduchá záležitost. Mezi jednotlivými počítači mohou putovat zprávy či dopisy. Dnes se již hojně využívá propojování celých sítí k Internetu a tak mají všichni uživatelé k dispozici služby Internetu jako e-mail, webové stránky a tak dále.

Jako poslední výhodu zde uvedu **ochranu dat**, o které jsem se ještě nezmiňoval. Spočívá v možnosti soustředit všechna důležitá data na jedno místo v síti, většinou server. Zde uložená data je pak možné zpřístupnit jen některým uživatelům a jiným je skrýt. Snadnější je také pravidelné zálohování dat nahromaděných na pevných discích serveru.

2.4 Síťový model

Abychom lépe pochopili fungování počítačové sítě, popíšeme si zde dva základní síťové modely. Síťové modely slouží jako základy pro standardizaci. Modely také popisují, jak by měla probíhat datová komunikace. Z toho vyplývá, že pokud se výrobce síťových komponent drží těchto standardů v každé vrstvě modelu, měly by tyto komponenty pracovat s komponenty vyrobenými ostatními výrobci. Informace jsem čerpal z publikace *Počítačové sítě pro začínající správce* [1].

2.4.1 Model OSI

Mezinárodní organizace pro standardizaci a normalizaci počítačových sítí nazývaná ISO (International Organization for Standardization) vypracovala referenční model ISO/OSI (Open Systems Interconnection).

Tento model se skládá ze 7 vrstev. Každá vrstva jasně definuje funkce potřebné pro komunikaci a pro svou činnost využívá služeb své sousední nižší vrstvy,
přičemž své služby pak poskytuje sousední vyšší vrstvě.

1) Fyzická vrstva *(ang. physical layer)*

Tato vrstva aktivuje, udržuje a deaktivuje fyzické spoje, tedy navazuje a ukončuje spojení. V této vrstvě také dochází k modulaci (demodulaci) digitálních dat na signál používáný přenosovým médiem. Také zajišťuje, aby všechny zdroje byly efektivně rozloženy mezi všechny uživatele.

Zařízení pracující na 1. vrstvě jsou **síťové karty**, **huby** a **opakovače**.

2) Linková (spojová) vrstva *(ang. data link layer)*

Poskytuje spojení mezi dvěma sousedními systémy. Je zodpovědná za přijímání a přenos datových rámců. Také formátuje fyzické rámce a opatřuje je fyzickou adresou. Mezi hlavní funkce patří přenos dat mezi jednotlivými síťovými prvky a detekuje či případně opravuje chyby, které vznikly na fyzické vrstvě.

Řadíme sem zařízení jako **mosty** *(ang. bridge)* a **přepínače** *(ang. switch)*.

3) Síťová (směrovací) vrstva *(ang. network layer)*

V této vrstvě dochází k směrování v síti a síťové adresování. Spojuje systémy, které spolu přímo nesousedí. Umožňuje překlenout rozdílné vlastnosti technologií v přenosových sítích. Poskytuje směrovací funkce, které hlavně používají směrovače v sítích.

Na této vrstvě pracují **směrovače** *(ang. router)* a posílají data do jiných sítí. Routery již pracují s hierarchickou strukturou adres. Data se posílají v podobě *paketů* a proto zde také najdeme nejznámější protokol **Internetevý protokol IP** (Internet Protocol).

4) Transportní vrstva *(ang. transport layer)*

Transportní vrstva je zodpovědná za přenos dat mezi koncovými uzly. Hlavními protokoly této vrstvy jsou TCP (Transport Control Protocol) a UDP (User Data Pentagram). Jednotkou informace pro tuto vrstvu nazýváme **segment**.

TCP dodává spojovanost a spolehlivost k protokolu IP ze 3. vrstvy a to tak, že vytváří virtuální okruh mezi koncovými aplikacemi. **UDP** zachovává nespolehlivost a nespojovanost z protokolu IP. Nemá tedy fázi navazování a ukončení spojení a už první segment UDP obsahuje aplikační data.

5) Relační vrstva *(ang. session layer)*

Vrstva zajišťuje spojení, jinak řečeno smyslem vrstvy je organizovat a synchronizovat dialog mezi spolupracujícími relačními vrstvami obou systémů a řídit výměnu dat mezi nimi.

6) Prezentační vrstva *(ang. presentation layer)*

Vrstva transformuje data do tvaru, které již používají samotné aplikace. Formát dat se může lišit na různých systémech. Důležité je, že vrstva se zabývá jen strukturou dat, ale již ne jejich významem, což je práce poslední aplikační vrstvy.

7) Aplikační vrstva *(ang. application layer)*

Poskytuje aplikacím přístup ke komunikačnímu systému a umožňuje tak jejich spolupráci. Do této vrstvy patří následující služby a protokoly:

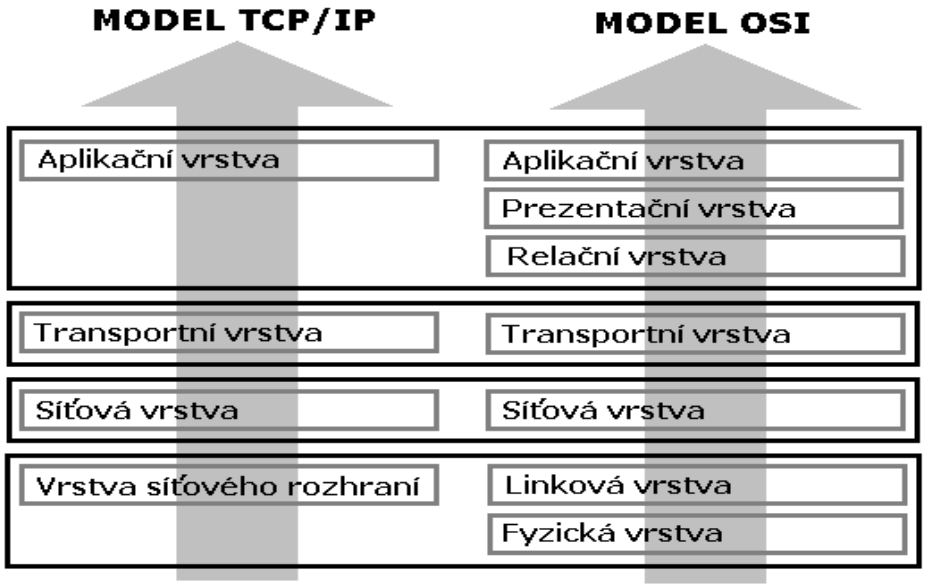
- FTP (File Transfer Protocol) - protokol slouží k přenosu dat.
- DNS (Domain Name System) - stará se o převod doménových jmen na IP adresy.
- DHCP (Dynamic Host Configuration Protocol) - slouží k automatickému přidělování IP adres koncovým stanicím v síti.
- POP3 (Post Office Protocol version 3) - protokol se používá ke stahovaní e-mailových zpráv z poštovních serverů.
- SMTP (Simple Mail Transfer Protocol) - internetový protokol určený pro přenos e-mailových zpráv mezi stanicemi.
- SSH (Secure Shell) - je to protokol umožňující bezpečnou komunikaci mezi dvěma počítači za transparentního šifrování přenášených dat.
- Telnet (Telecommunicatons Network) - také klient/server protokol, který dovoluje uživateli klientského terminálu se připojit ke vzdálené stanici.
- TFTP (Trivial File Transfer Protocol) - protokol pro přenos souborů, ale obsahuje pouze základní funkce FTP.

2.4.2 Model TCP/IP

Také se můžeme setkat s označením **DoD** (Department of Defense), jelikož tyto dva protokoly byly vyvíjeny současně v rámci koncepce projektu **ARPAnet** (Advanced Research Projects Agency Network).

Model TCP/IP má pouze 4 vrstvy na rozdíl od modelu OSI, který jich má 7. Ovšem tyto 4 vrstvy modelu TCP/IP se dají namapovat na 7 vrstev modelu OSI, což ukazuje i následující obrázek 1.

Všimněme si také, že číslování jednotlivých vrstev jde odspoda nahoru.



Obrázek 2 - Mapování vrstev TCP/IP modelu na model OSI

1) Vrstva síťového rozhraní *(ang. network interface)*

Pracují zde protokoly fyzické vrstvy, které umožňují přístup k fyzickému přenosovému médiu, ale také standardní protokoly Ethernetu a Token Ringu.

2) Síťová vrstva *(ang. network layer)*

Zabývá se směrováním na základě logických adres. Také překládá logické adresy

na MAC (Media Access Control) adresy, o což se stará protokol **ARP** (Address Resloution Protocol) nebo jeho opačný kolega **RARP** (Reverse Address Resolution Protocol). Tento překlad je nezbytný, jelikož nižší vrstvy jsou schopny interpretovat pouze MAC adresy.

Vrstva také zajišťuje síťovou adresaci a předávání datagramů. Proto zde najdeme další důležité protokoly, jako **IP** (Internet Protocol), **ICMP** (Internet Control Message Protocol), atd.

3) Transportní vrstva *(ang. transport layer)*

Je implementována až v koncových zařízeních, tedy počítačích, a přizpůsobuje chování sítě potřebám aplikace. Na této vrstvě pracují protokoly TCP a UDP.

4) Aplikační vrstva *(ang. application layer)*

Aplikační vrstva slouží programům či procesům k přenosu dat po síti. Aplikační programy využívají dvou základních služeb z transportní vrstvy, a to TCP, UDP a případně obojí pomocí DNS. K rozšíření aplikačních protokolů se používají **porty**. Porty jsou jakási domluvená číselná označení aplikací. Tedy každé síťové spojení aplikace je jednoznačně určeno číslem portu, transportním protokolem a adresou počítače.

2.5 Síťové standardy a specifikace

Při návrhu a realizaci počítačové sítí bychom měli dodržovat předepsané normy a standardy. Většinou se tím musí již řídit výrobci hardwarů a softwarů. Tyto standardy vydává velké množství organizací a zajišťují nám hlavně kompatibilitu prvků v síti. Čerpáno z *Návrh a realizace sítí Cisco* [7].

My se pouze krátce zastavíme u organizací definující standardy. Jsou to hlavně tyto:

- ISO (International Organization for Standardization)
- IEC (International Electrotechnical Commission)
- ITU (International Telegraph Union)
- IETF (Internet Engineering Task Force)
- IEEE (Institute of Electrical and Electronics Engineers)

ISO je velice známou organizací definující standardy, ale jak můžeme vidět ze seznamu výše, není to jediná organizace, která se standardizací zabývá.

Ještě se krátce pozastavíme u standardu **IEEE**, který prosazuje výměnu informací a vyvíjí standardy a specifikace pro síťové technologie na nižších úrovních. Pro síťové odborníky je důležitá zejména specifikace tvořící projekt IEEE 802. Na tento projekt navazují další standardy. Například standard IEEE 802.11 se věnuje bezdrátových technologiím a popisuje jakým způsobem implementovat bezdrátové sítě LAN.

2.6 Rozdělení sítí

Sítě lze dělit do několika různých kategorií v závislosti na charakteristikách souvisejících s jejich administrací nebo řešením problémů. Dělit sítě můžeme podle fyzických vlastností nebo podle charakteristiky programového vybavení. Dělit sítě můžeme například podle následujících kritérií:

- fyzický tvar
- struktura a metoda administrace
- síťový operační systém
- síťové protokoly
- topologie
- architektura

2.6.1 Dělení sítí podle fyzického tvaru

V podstatě se jedná o rozsah sítě prostorově než o to jak se síť celkové velká. Uvádějí se tedy 3 kategorie. Nejmenší je lokální síť **LAN** (Local Area Network), nejrozsáhlejší je síť **WAN** (Wide Area Network). Jakási síť mezi těmito dvěma je metropolitní síť **MAN** (Metropolitan Area Network). Tyto sítě jsou také víceméně odlišeny na základě finančních nákladů na realizaci a udržování sítě. Avšak nejdůležitějším faktorem, který takovéto členění ovlivňuje je geografická rozloha, kterou síť pokrývá.

2.6.2 Dělení sítí podle struktury a metody administrace

Toto dělení nám říká, jak a kým jsou sdílené zdroje spravovány. Síť tedy může být dělena do dvou struktur.

První struktura je je pracovní skupina **peer-to-peer**, ve které pracuje každý počítač jak v roli klienta, tak v roli serveru. Každý uživatel provádí administraci zdrojů týkajících se jeho vlastního počítače.

Druhá struktura se nazývá síť **klient/server**. Zde probíhá veškerá administrace na centrálním serveru, na kterém běží speciální síťový operační systém NOS (Network Operating System), který autorizuje uživatelská jména a hesla, čímž umožňuje přístup ke sdíleným zdrojům.

Výhody a nevýhody popisovaných struktur ukazuje tabulka 1.

Výhody	
Sítě peer-to-peer	**Sítě klient/server**
Méně finančně náročná na implementaci.	Nabízí větší bezpečnost.
Nevyžaduje NOS na serveru.	Při větší velikosti sítě mnohem snazší administrace, jelikož je centralizována.
Nevyžaduje zvláštního administrátora sítě.	Všechna data mohou být zazálohována z jednoho místa.
Nevýhody	
Sítě peer-to-peer	**Sítě klient/server**
Nehodí se příliš pro větší sítě, administrace by poté byla takřka nemožná.	Vyžaduje speciální a drahý NOS.
Každý uživatel musí být dostatečně zkušený, aby zvládl administrační úkony.	Vyžaduje nákladný a výkonnější hardware, který bude fungovat jako server.
Menší bezpečnost.	Vyžaduje profesionálního administrátora.
Všechny počítače, které sdílí zdroje negativním způsobem ovlivňují výkonnost sítě.	Pokud je pouze jeden server, je právě jediným slabým bodem sítě. Uživatelská data nemusí tedy být v případě výpadku serveru dostupná.

Tabulka 1 - Výhody a nevýhody sítí peer-to-peer a klient/server [5]

Z tabulky je patrné, že výběr struktury a příslušné administrace závisí na mnoha faktorech, jako jsou množství počítačů a uživatelů v síti, bezpečnostní požadavky, hardware a dostupný rozpočet.

2.6.3 Dělení sítí dle síťového operačního systému NOS

Sítě jsou také někdy kategorizovány podle síťových operačních systémů **NOS**

(Network Operating System), které jsou instalovány na serverech a používány pro kontrolu nad celou sítí.

Nejčastější systémy jsou **Windows**, **NetWare** a **UNIX**. Mnoho sítí však kombinuje dva nebo více operačních systémů. Tyto sítě se často nazývají *hybridní sítě*.

2.6.4 Dělení sítí podle protokolu

Sítě také můžeme členit podle protokolu, který používají pro komunikaci jednotlivé stanice. Síťové protokoly jsou určitá pravidla, dle kterých mají být počítače v síti propojeny a jejich vzájemná komunikace udržována.

Nejznámější protokoly pro sítě LAN jsou **NetBEUI**, **IPX/SPX** a **TCP/IP**. Případné další protokoly mohou být například AppleTalk a sada protokolů OSI.

2.6.5 Dělení síti podle topologie

Jedná se o dělení podle jejich fyzické nebo logické topologie. Fyzická topologie je pouhý tvar sítě, tedy způsob jak sou dané kabely strukturované. Kdežto logickou topologií je míněna cesta, kterou putuje daný signál od jednoho počítače k druhému přes další síťové prvky.

Fyzická a logická topologie mohou být naprosto shodné. Například v síti uspořádané lineárně (počítače v síti jsou uspořádány za sebou), putují data po rovné lince od jednoho počítače k druhému. Ale síť může disponovat také logickou a fyzickou topologií, které vůbec shodné nejsou. Jednotlivé segmenty mohou připojovat všechny počítače do centrálního hubu ve tvaru hvězdy, avšak uvnitř hubu může být logika vytvořena tak, že signál putuje od jednoho portu k druhému a tvoří tak uzavřený kruh.

Nejznámější topologie sítí LAN:

- lineární
- kruhová
- hvězdicová
- síťová
- hybridní

2.6.6 Dělení sítí podle architektury

Poslední dělení je podle architektury. Architektura sítě zahrnuje určitou sadu specifikací definujících fyzické a logické topologie, použitý typ kabelu, vzdálenostní omezení, metody přístupu, velikost paketů, hlaviček a mnoho dalších faktorů. S těmito specifikacemi se můžeme setkat pod názvem *data link layer protocols*.

Asi nejpopulárnějšími současnými architekturami sítí LAN jsou **Ethernet** a **Token Ring**. Mezi dalšími je dobré ještě zmínit AppleTalk a ARCnet.

2.7 Požadavky na naší síť

V předchozí kapitole jsme si rozdělili sítě podle různých kritérií. Stručně jsme si popsali každou možnost dělení. V této kapitole bych se chtěl podrobněji věnovat předchozímu rozdělení sítí a to tím způsobem, že z každého jednotlivého dělení vždy vyberu jen ten případ, který je podstatný pro náš návrh sítě.

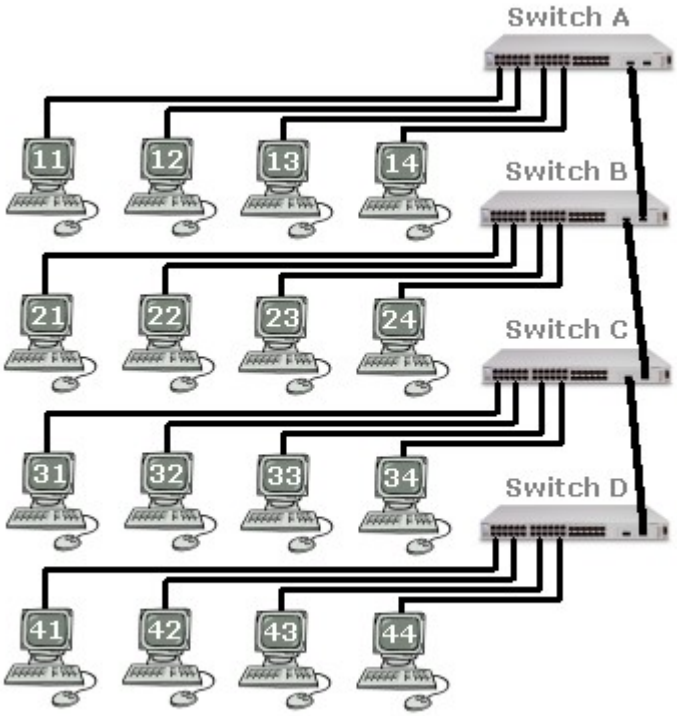
Ještě než se pustíme do charakteristiky naší sítě, ujasněme si jak bude naše síť vypadat a jaké komponenty bude obsahovat.

2.7.1 Návrh naší sítě

V mém návrhu sítě počítám se **16 osobními počítači**, které budou rozděleny na čtveřice. Každá čtveřice odpovídá jedné řadě stolů v učebně a tomu také odpovídá označení počítačů. Každý počítač má číselné označení, které se skládá ze dvou cifer, kde první cifra nám říká, v kolikáté řadě je počítač umístěn. Druhá cifra udává pořadí daného počítače od levého kraje v dané řadě. Z toho vyplývá, že každý počítač má jedinečné číslo v síti a do budoucna není problém síť rozšířit od další počítače a pokračovat tak i v přehledném značení.

Každá takováto čtveřice počítačů je připojena pomocí **UTP kabelů** ke switchi. V síti máme **4 switche** a ke každému je připojená jedna řada nebo-li čtveřice počítačů. Switche jsou označeny písmeny A až D, kde A odpovídá první řadě počítačů. Switch jsou stohovatelné a tak jsou ještě propojeny mezi sebou opět kroucenou dvojlinkou.

Celé schéma a topologie sítě, ale také značení komponent v síti, je přehledně vidět na následujícím obrázku 1.



Obrázek 1 - Schéma zapojení počítačů a switchů ve hvězdicové topologii

Původní návrh obsahoval ještě jeden switch, který by byl připojen do celoškolní sítě a tedy i k Internetu. V obrázku není zakreslen. Uvažoval jsem, že by každý počítač měl dvě síťové karty a právě jedna z nich by byla připojená nastálo ke tomuto switchi. Každý počítač by tak měl přístup k Internetu i během cvičných pokusů na druhé síťové kartě. Student by si tak mohl hledat i informace k zadaným úlohám, které budou také na Internetu prezentovány.

Řekli jsme si, že pokud dělíme sítě podle fyzického tvaru, máme na výběr sítě typu LAN, MAN a WAN. Proto si teď také popíšeme jenom síť typu LAN a od sítí MAN a WAN se distancujeme, protože nejsou pro náš návrh počítačové učebny důležité. Podobným způsobem budeme postupovat i u dalších dělících kritérií.

2.7.2 Lokální síť LAN

Mým úkolem je navrhnout síť, která se bude rozkládat v jedné počítačové učebně a tak je patrné, že z nabízených variant se bude jednat o síť typu **LAN** (Local Area Network).

Síť LAN je tedy limitována určitým prostorem a tak to musí být počítače umístěné blízko sebe. Ale i tak se velikost sítí LAN může výrazně lišit. Může se jednat o dva počítače vedle sebe a nebo také desítky až stovky počítačů rozmístěných v několika patrech celé budovy. Samozřejmě, že počet počítačů je také ovlivněn použitým typem přenosového média a síťovou architekturou, což si přiblížíme později.

Větší sítě LAN mohou být pro snažší administraci rozděleny do pracovních skupin tzv. *workgroups*, kde se sdílejí stejné zdroje jakou soubory, tiskárny a aplikace.

Pro naše výukové účely bude stačit síť LAN, která nebude rozdělena do pracovních skupin. Jak jsem již naznačil celá naše síť bude realizována v jedné místnosti a předpokládaný počet bude 16 pracovních stanic.

2.7.3 Charakteristika sítě peer-to-peer

Když jsme dělili sítě podle metody administrace, tak jsme měli na výběr ze dvou variant a to klient/server nebo peer-to-peer síť. Jelikož v naší malé síti nebude realizován server, tak volíme právě síť peer-to-peer.

Server do sítě nekomponujeme zatím hlavně z finančních důvodů, ale je dobré počítat s jeho budoucím nasazením. Přidání serveru by v budoucnu neměl být problém a takovéto rozšíření naší počítačové sítě nebude mít zásadní vliv na přestavbu sítě.

Uvážíme-li, že struktura peer-to-peer se hodí zejména pro menší sítě, ve kterých není striktně vyžadována bezpečnost, tak to vyhovuje přesně naším požadavkům. Také implementace takovéto sítě není vůbec finančně náročná a se soudobými operačními systémy typu Windows a různými verzemi Linuxu se zabudovanými síťovými komponenty také velice jednoduchá.

Administrace uživatelů a zdrojů je v takovéto síti decentralizována. Každý počítač je v síti v roli jak klienta tak i serveru, což znamená, že každý počítač může sdílet své zdroje s ostatními a může také přistupovat ke zdrojům počítačů ostatních. Každý uživatel je sám zodpovědný za administraci konkrétních počítačových zdrojů, například tvorba uživatelských účtů, sdílených položek a přiřazování příslušných práv pro přístup. Každý uživatel je také sám zodpovědný za zálohu dat na tom kterém počítači.

2.7.4 Sítě Windows a UNIX

Naše síť bude tzv. hybridní, jelikož na všech klientech budeme mít nainstalovány dva operační systémy a to MS Windows XP a distribuci Linuxu Debian. Operační systémy podrobněji probereme v kapitole 4 Softwarové vybavení počítačů.

2.7.5 Protokol TCP/IP a adresace v síti

Protokol TCP/IP

Z nabízených protokolů si vybereme protokol **TCP/IP** (Transmission Control Protocol / Internet Protocol) a to i navzdory skutečnosti, že se jedná o řešení nejpomalejší a nejnáročnější na konfiguraci. Ale i tak je sada protokolů TCP/IP zdaleka nejrozšířenější. Existuje hned několik dobrých důvodů, proč tomu tak je:

- TCP/IP využívá flexibilní adresní schéma, které je dobře směrovatelné, a to i v rámci rozsáhlých sítí.
- Téměř všechny operační systémy a platformy mohou s TCP/IP pracovat.
- Dostupná je celá řada nástrojů a pomůcek, některé jsou implementovány přímo v protokolu a některé jsou dodávány jako samostatné programy ulehčující práci s TCP/IP.
- TCP/IP je protokolem globálního Internetu. Aby se mohl systém připojit do sítě Internet, musí na něm běžet protokol TCP/IP.

Adresace v sítích TCP/IP

Abychom mohli identifikovat konkrétní zařízení v síti, musíme znát jeho **IP adresu** (Internet Protocol). Veškerá posílaná data v síti a Internetu obsahují v hlavičce právě tuto adresu a to jak příjemce tak odesílatele. V hlavičce je mnoho dalších informací, kterými se teď zabývat nebudeme.

Dnes existují dvě verze IP adresy. **Adresy IPv4** a **adresy IPv6**. Rozdíl je mezi nimi hlavně v počtu bitů. IPv4 má 32 bitů, kdežto IPv6 jich má 128 a tedy i mnohem vyšší adresový prostor. My však budeme v naší síti používat starší verzi a tak se adresami IPv6 více zabývat nebudeme.

Adresa IPv4 se skládá ze **32bitového čísla**. Je zapisována po jednotlivých bajtech a ty oddělujeme tečkami. Hodnoty jednotlivých bajtů zapisujeme pro přehlednost v desítkové soustavě. Například IP adresa portálu www.google.com je 209.85.135.103.

Můžeme si tedy dopočítat, že možných adres je 2^{32} = 4 294 967 296. Část z tohoto adresového prostoru je ovšem určena pro protokoly a nemohou být nikomu přiděleny.

Adresu si rozdělme na tři základní části. Adresa sítě, adresa podsítě a adresa počítače. Původně se IP adresa dělila jenom na adresu sítě a adresu počítače, ale toto dělení se ukázalo jako příliš hrubé. Lokální část adresy se tedy rozdělila na podsíť a počítač. Můžeme tedy říci, že mezi počítači se stejnou adresou sítě a podsítě můžeme data dopravovat přímo, jelikož oba počítače jsou ve stejném Ethernetu. Nachází-li se adresa v jiné síti, je již nutné datagram směrovat a přes směrovač dopravit dále do jiné sítě.

Adresu sítě nám poskytuje poskytovatel připojení. Lokální část adresy určuje správce té dané sítě. Také rozhoduje, zda budou v síti podsítě a jak velký budou mít adresový prostor.

Hranici mezi adresou podsítě a počítače určuje **maska podsítě**. Maska má stejný zápis jako IP adresa. Důležité je, že v binárním tvaru obsahuje jedničky od začátku adresy a ty značí, že se jedná o síť a podsíť. Zbytek adresy jsou nuly a ty platí pro počítač. IP adresa s maskou je nezbytnou součástí konfigurace síťového rozhraní, čemuž se budeme věnovat později.

Nyní se dostáváme k adresování v síti. IP adresy jsou rozděleny do **tříd** a to podle toho, jak velká část adresy reprezentuje síť a jak velký zbytek počítač. Odpovídající třídu poznáme podle prvního bajt, počítač jí pozná podle pár prvních bitů. Můžeme se o tom přesvědčit z následující tabulky 2.

Třída	První bity	První bajt	Bity pro síť	Bity pro PC	Počet sítí	Počítačů v síti	Maska
A	0	0-127	7	24	126	16777214	255.0.0.0
B	10	128-191	14	16	16384	65534	255.255.0.0.
C	110	192-223	21	8	2097152	254	255.255.255.0
D	1110	224-239	*multicast*				
E	1111	240-255	*rezerva*				

Tabulka 2 - Rozdělení IP adres do tříd

Nejnižší adresa v síti, tedy adresa počítače obsahuje samé nuly, je **adresa sítě**. Naopak nejvyšší adresa v síti, tedy adresa počítače obsahuje samé jedničky, je určena pro **broadcast**. Broadcast je všesměrové vysílání. Adresy 127.x.x.x, nejčastěji 127.0.0.1, reprezentují **loopback**. Loopback je smyčka a umožňuje posílat pakety sám sobě. Tyto adresy můžeme zařadit do tzv. **vyhrazených adres**.

Do vyhrazených adres ještě začleníme neveřejné, interní adresy, které mají třídy A, B a C. Tyto adresy používáme pro adresování ve vnitřních sítích.

- Třída A - 10.0.0.0 až 10.255.255.255 (16 777 214 adres)
- Třída B - 172.16.0.0 až 172.16.255.255 (1 048 544 adres)
- Třída C - 192.168.x.0 až 192.168.x.255 (65 024 adres)

S těmito adresami budeme nejčastěji pracovat při řešení příkladů uvedených v poslední kapitole.

2.7.6 Hvězdicová topologie

Volíme hvězdicovou síť, též nazývanou *star* nebo *star bus*. Je to nejoblíbenější uspořádání počítačů v sítích LAN. Oblíbená je hlavně proto, že má také velmi jednoduchou implementaci a to tak, že každý počítač připojíme do hubu, v našem případě switche. Switch si popíšeme v kapitole 3 Hardwarové vybavení učebny.

Jako přenosové médium v síti založené na hvězdicové topologii volíme obvykle nestíněnou kroucenou dvojlinku UTP (Unshielded Twisted Pair) a tomu odpovídá i zvolená architektura Ethernet 10BaseT nebo 100BaseT.

Výhody hvězdicové sítě:

Takováto síť je mnohem více tolerantní k chybám, což znamená, že pokud je jeden počítač odpojen nebo je porušen kabel, týká se to pouze tohoto počítače a zbytek sítě může bez problému komunikovat dále.

Další výhodou je, že tato topologie nabízí velice jednoduchou rekonfiguraci. Přidáváme-li nebo naopak odebíráme-li počítač ze sítě, stačí pouze jednoduše zapojit či vypojit kabel. I řešení problémů ve fyzické vrstvě je s touto topologií také velice snadné, zejména pokud použijeme inteligentní hub či switch obsahující diagnostické nástroje.

Nevýhody hvězdicové sítě:

První nevýhodou je, že toto řešení sítě je mnohem více náročné na množství kabelů, než jaké je tomu u topologie lineární nebo kruhové, protože každý počítač musí mít od sebe natažený kabel na celou vzdálenost až k centrálnímu hubu. Za druhé musíme do sítě zakomponovat právě buď hub a nebo switch, což je další zdroj finančních nákladů.

2.7.7 Ethernet

Ethernet byl vyvinut v 60. letech a je definován specifikací IEEE 802.3 a dodnes je nejpopulárnější architekturou. Bližší specifikace je ještě IEE 802.3u, která platí pro normu 100BaseT.

Jelikož jsme si pro síť zvolili hvězdicovou topologii, tak tím pádem musíme použít i architekturu Ethernetu. Sítě Ethernetu používají metody přístupu k médiu CSMA/CD (Carrier Sense Multiple Access/Collision Detection). Standardní Ethernet je limitován rychlostí 10 Mbps. Dnes se ale již běžně využívá tzv. Fast Ethernet nebo-li rychlý Ethernet, který běží již na rychlostech 100 Mbps a také 1 Gbps.

A tak v závislosti na použitém kabelu můžeme Ethernet rozdělit na různé subkategorie jako například 10Base5, 10Base2, 10BaseT, 100BaseT, 1000BaseT, 100BaseVG-Any LAN, 10BaseFL,100BaseFL a další.

Pro lepší pochopení jen dodávám, že číslo před slovem „Base“ udává přenosovou rychlost a písmeno či číslo za slovem „Base“ udává typ kabelu, který je použit pro spojení síťových prvků. Například 10Base5 je Ethernet s maximální přenosovou rychlostí 10 Mbps a jako přenosové médium je použit tlustý koaxiální kabel s dosahem signálu 500 metrů.

Jelikož naše počítače jsou vybaveny síťovými kartami o rychlostech 100 Mbps a použitá kabeláž bude metalická, přesně nestíněná kroucená dvojlinka, tak se zaměříme na specifikaci Ethernetu 100BaseT.

Ethernet 100BaseT:

Již klasifikace 100BaseT v názvu nám napovídá, že Ethernet poběží rychlostí 100 Mbps. Písmeno T je zkratkou pro *twisted*, tedy použijeme kroucený dvojlinku. Nestíněná kroucená dvojlinka se značí UTP (Unshielded Twisted Pair) a stíněná kroucená dvojlinka se označuje jako STP (Shielded Twisted Pair).

Kabel UTP se vyrábí a dodává v několika stupních identifikovaných jako číslované kategorie. V tabulce 3 máme kategorie UTP kabelů a jejich využití.

UTP kategorie	Max. přenosová rychlost	Charakteristiky a použití
Cat 1	Pouze hlas	Starší telefoní instalace
Cat 2	4 Mbps	Nedoporučováno pro datové přenosy
Cat 3	16 Mbps	Špatná datová rozpoznávací schopnost, používáno pro telefonní rozvody
Cat 4	20 Mbps	Vhodné pro ethernetové sítě 10 Mbps
Cat 5	100 Mbps - 1 Gbps	Nejpopulárnější v sítích LAN, používáno pro rychlý Ethernet (100 Mbps)
Cat 5e	155 Mbps	Používáno pro rychlý Ethernet a 155 Mbps ATM (Asynchronous Transfer Mode)
Cat 6 & 7	1 Gbps a výše	Používáno pro nové gigabitové ethernetové technologie

Tabulka 3 - Dostupné kategorie UTP kabelů [1]

Je tedy jasné, že UTP kabel podporuje mnohem vyšší rychlosti než koaxiální kabel, který dosahuje rychlosti maximálně 10 Mbps. UTP kabel je také velice flexibilní a dobře se instaluje. Na konec kabelu se dává RJ konektor, což je typ modulárních zásuvek užívaný pro klasické telefony. Přestože telefony využívají menší RJ-11 konektor, většina ethernetových kabelů je připojena trochu větším konektorem RJ-45.

Z tabulky 3 je také patrné, že pro síť 100BaseT použijeme jako propojovací kabely kategorie Cat 5 nebo Cat 5e.

Ještě bych podotkl, že mnoho síťových karet a prvků je navrženo tak, aby podporovaly i nižší přenosové rychlosti, například 10 Mbps, což je poté při přechodu na vyšší verzi Ethernetu velice přínosné. Navíc je možné s využitím správného vybavení provozovat síť v jedné části na 10 Mbps a ostatních částech na 10 Mbps.

2.8 Připojení k Internetu

Je jasné, že nebudeme pro naší malou síť žádat poskytovatele (*ang. providera*)

o přidělení adresy sítě, přes kterou bychom měli přímý přístup i Internetu. Využijeme již existující univerzitní síť, kde si necháme přidělit určitý rozsah vnitřních neveřejných IP adres, jako je tomu u ostatních počítačových učeben.

Právě kvůli připojení k Internetu počítáme v návrhu sítě s použitím **dvou síťových karet** v jednom počítači. První síťová karta bude sloužit po pokusné účely v laboratoři, kdežto druhá bude sloužit k propojení na vyhrazený switch, který již bude propojen na školní router. To už se ale dostáváme ven z naší počítačové sítě a tomu se již věnovat nebudeme.

Od počítače ke switchům tedy vždy povede pár síťových kabelů až k patch panelům v racku a zde teprve dojde k dělení účelu kabelů. Také síťovou kartu, přes kterou budeme připojeni k Internetu, nastavíme podle hodnot od správce celé sítě a v budoucnu již toto nastavení nebudeme měnit.

3 Hardwarové vybavení učebny

V této kapitole se zaměříme hlavně na hardwarové vybavení počítačové učebny. Do hardwaru zařadíme jak samotné počítače, tak síťové komponenty aktivní i pasivní. Mezi pasivní prvky řadíme kabely, konektory, patch panely, zásuvky, atd. Aktivní síťové prvky jsou takové, které již nějakým způsobem pracují se signálem, jako například síťová karta, huby, switche, bridge, routery, firewally atd. Popíšeme si hlavně prvky, které v naší síti použijeme a také se budeme zabývat jejich nastavením či případně instalací ovladačů.

Ale abychom zvolili správný síťový hardware, musíme se nejdříve blíže seznámit se standardy síťového hardwaru. A proto byli přijaty normy, které definují základní požadavky na technické provedení sítí. Tuto normalizaci provádí **organizace IEEE** (Institute of Electrical and Electronics Engineers). O této organizaci jsem se zmínil již ve druhé kapitole. Teď se na ní podíváme blíže.

3.1 Standard IEEE pro sítě LAN

Jednotlivé normy standardu IEEE nesou její označení. My se zaměříme na normu **IEEE 802.3**, která se věnuje standardům sítě Ethernet. Použitý zdroj *Počítačové sítě LAN / MAN / WAN* [3].

Norma IEEE nám udává technické parametry všech síťových hardwarových komponent. Nás však z praktického hlediska budou nejvíce zajímat následující vlastnosti definované tímto standardem:

- Přístupová metoda
- Topologie sítě
- Typ kabelu, jeho délka, konektory
- Rychlost přenosu dat

Norma se také zabývá důkladným popisem všech detailů sítě, jako složením datového paketu, tvarem elektrických signálů atd. Ale my se budeme věnovat pouze výše popsaným vlastnostem.

Ještě než se pustíme do rozboru Ethernetu, je nutné si uvědomit že Ethernet má několik variant a ty sou děleny podle přenosové rychlosti v síti. My si podrobněji

popíšeme pouze jeden z nich a to ten, který bude normou pro naši síť. Je to **Fast Ethernet**. Ale pro úplnost si nejdříve uvedeme seznam těch, se kterými se můžeme v praxi potkat:

- Ethernet - pro přenosovou rychlost 10 Mb/s
- Fast Ethernet - pro přenosovou rychlost 100 Mb/s
- Gigabit Ethernet - pro přenosovou rychlost 1000 Mb/s
- 10Gb Ethernet (standard 802.3ae) - pro přenosovou rychlost 10 Gb/s

3.1.1 Fast Ethernet

Fast Ethernet je označení pro Ethernet, který dosahuje přenosové rychlosti 100 Mb/s. Fast Ethernet je stále nejrozšířenější normou a odpovídá doporučení IEEE 802.3. Z toho také vyplývá, že metoda pro přenos dat je založena na přístupu CSMA/CD (Carrier Sense Multiple Access with Collision Detection).

CSMA je metoda využívající vícenásobný přístup. Přípona **CD** nám říká, že stanice při svém vysílání současně kontroluje přenosové médium, jestli nezachytí jiné vysílání na médiu, se kterým by kolidovala. Jestliže stanice zjistí kolizi, přestává vysílat a začne čekat náhodnou dobu a poté opakuje své vysílání znova.

Fast Ethernet má dále ještě tři varianty 100BASE-TX, 100BASE-FX a 100BASE-T4.

1) 100BASE-TX

Tato varianta využívá jako přenosové médium stíněnou či nestíněnou kroucenou dvojlinku kategorie 5 a využívá dva páry ze čtyř možných. To značí písmeno „T“ v názvu. Maximální délka kabelu je stanovena na 100 m. Tuto variantu využijeme v naší počítačový síti.

2) 100BASE-FX

Zde se volí optické kabely jako přenosové médium, což značí F v názvu. Délka segmentu může být až 412 metrů pro multividové kabely s polovičním duplexem nebo až 10 000 metrů pro jednovidové kabely s duplexním režimem.

3) 100BASE-T4

Je to starší norma, která se v praxi téměř nepoužívá. Jako přenosové médium je

také stanovena kroucená dvojlinka, ale zde je to kategorie 3 a 4 a využívají se všechny čtyři páry v kabelu. Maximální délka je stejná jako u normy TX 100 metrů.

3.2 Síťové kabely

Jako přenosové médium si můžeme zvolit metalické kabely, optické kabely a nebo vzduch čili bezdrátové přenosové prostředí. V naší síti budeme počítače a síťové prvky propojovat metalickými kabely. Hlavní důvody jsou snadná realizace a nízká cena. Ovšem metalických kabelů máme několik druhů, které bychom mohli teoreticky použít. Když vynecháme koaxiální kabely, které se používali v době minulé, zbude nám pouze jedna varianta a to **kroucená dvojlinka**.

V síti bychom mohli a měli použít i **optické kabely** a to na propojení switchů. Ovšem switche, které budeme instalovat v naší síti toto neumožňují. Popis switche si ještě uvedeme v jedné z následujících kapitol.

Jelikož budeme používat kroucenou dvojlinku, budu se podrobněji věnovat právě tomuto přenosovému médiu.

3.2.1 Kroucená dvojlinka

Proč dvojlinka a proč kroucená? Dvojlinka je vžitý název pro tento kabel, protože v kabelu je dvojce vodičů a to ne jenom jedna, ale čtyři dvojce či páry vodičů. Kroucená je proto, že tyto páry jsou krouceny kolem sebe, ale jsou krouceny i jednotlivé páry. Dva vodiče jsou krouceny kolem sebe z důvodu zlepšení elektrických vlastností kabelu. Omezují se tak přeslechy mezi páry a potlačuje se elektromagnetické záření do okolí a i jeho příjem z okolí.

Obrázek 3 - UTP kabel

Mezi základní dělení patří, jestli je dvojlinka stíněná či nestíněná. Stíněná dvojlinka se značí **STP** (Shelded Twisted Pair) a nestíněná dvojlinka se značí **UTP** (Unshelded Twisted Pair). U stíněné dvojlinky může nalézt stínění v podobě tenkého kovového obalu, který je ještě případně opleteno tenkými drátky. Podobné stínění můžeme pozorovat na koaxiálních kabelech. Toto stínění slouží ještě k většímu potlačení rušivých jevů jako právě elektromagnetické záření. Stíněný kabel bývá obvykle o trochu dražší a také měně ohebný. Právě z důvodu ohebnosti ho nebudeme používat v naší síti, protože předpokládáme, že s kabely bude často manipulováno a nepružnost by byla jen na obtíž.

S tímto souvisí i další kritérium a to jestli jsou vodiče vyrobeny jako jednolitý drát či jako lanko složeno z několika jemných drátků. Zde budeme volit sice dražší, ale zato více flexibilní lanko. U lanka také nedochází tak často k ukroucení a zlomení kabelu.

Přes tuto volbu se dostáváme dále a to k podstatné části kabelu, což jsou **konektory**. Ty se právě nepatrně liší podle použitého typu vodiče. Tedy pro drát je jiný konektor než pro lanko. Konektory se liší v kovových kontaktech. Do lanka jsou kontakty zařezávány, kdežto drátek je ovinut kontaktem.

Obrázek 4 - konektor RJ-45

Ovšem oba tyto konektory mají úplně stejné označení a to **konektor RJ-45**. Je podobný konektoru na telefonním kabelu, který má označení RJ11, ale je o něco větší. To vyplývá z počtů vodičů přivedených do konektorů, kde u síťového kabelu je vodičů osm a u telefonního kabelu jsou pouze čtyři. Již jsme si řekli, že ne všechny páry v kabelu musí být využity.

Také již víme z předchozích kapitol, že použijeme kabel kategorie 5, který vyhovuje naší normě Fast Ethernetu. Nyní se podíváme na to, jak ke kabelu připojit konektor.

3.2.2 Krimpování kabelu

Krimpování kabelu je pojem pro „nacvaknutí“ konektoru na kabel. Nakrimpování kabelu není nijak složitá a po chvíli praxe jde vše snadno. Budeme ovšem potřebovat **krimpovací kleště**, kterými konektor v závěru na kabel připevníme. Ovšem než dojde k samotnému nakrimpování konektoru, musíme si kabel připravit. Pokud vyrábíme patch kabel, tak si ucvakneme požadovanou délku kabelu. K tomu nám poslouží značení v metrech přímo na obalu kabelu. Pokud ovšem taháme kabel zdí nebo lištou, je lepší kabel nechat namotaný na cívce a ucvaknout ho až po protažení. Nemůžeme se tak splést v délce kabelu.

Pokud chceme chránit konektor před ulomením záklopky, navlečeme v první řadě krytku konektoru na kabel. Kabel pak oholíme asi 1,5 cm od konce a rozpleteme jednotlivé vodiče. Vodičů je 8, jsou to tedy 4 páry. Každý pár má svoji barvu. Jeden z vodičů v páru je barevný a jeden barevný s přerušovanou bílou barvou. Jak vodiče seřadit vedle sebe nám udávají dva standardy **T568A** a **T568B**. Pro normu 100BASE-TX platí hodnoty z Tabulky 4.

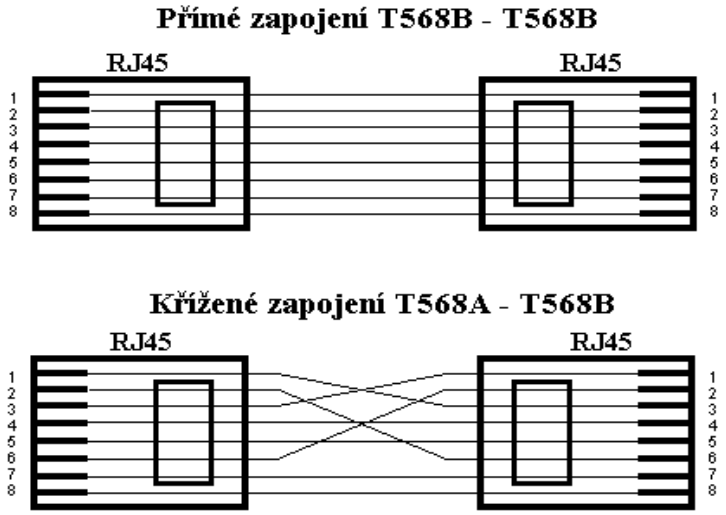
T568A			**T568B**		
1	zelená - bílá	RD +	1	oranžová - bílá	TD +
2	zelená	RD -	2	oranžová	TD -
3	oranžová - bílá	TD +	3	zelená - bílá	RD +
4	modrá	nic	4	modrá	nic
5	modrá - bílá	nic	5	modrá - bílá	nic
6	oranžová	TD -	6	zelená	RD -
7	hnědá - bílá	nic	7	hnědá - bílá	nic
8	hnědá	nic	8	hnědá	nic

Tabulka 4 - Standardy pro zapojení vodičů do konektoru

Jak je patrné z Tabulky 4, k přenosu dat nám slouží pouze čtyři vodiče. Jsou to vodiče **RD** (Receive Data) pro příjem dat a **TD** (Transmit Data) pro odeslání dat. Plus či mínus značí napětí na vodiči.

Chceme-li propojit počítač s aktivním síťovým prvkem jako je hub, switch nebo router, použijeme **přímý kabel**. Oba konektory na kabelu zapojíme podle stejné normy, tedy buď T568A - T568A nebo T568B - T568B. V praxi se používá spíše druhá varianta, ale není to podmínkou.

Pro přímé propojení dvou počítačů ovšem použijeme **křížený kabel**. Pak použijeme zapojení konektorů T568A - T568B. Pro úplnost ještě dodejme, že existuje třetí varianta a to **převrácený kabel**. Tedy vodič 1 bude na druhé straně 8, vodič 2 bude 7, atd.



Obrázek 5 - Zapojení konektorů

Dejme tomu, že si chceme nacvaknout konektor podle normy T568B. Vezmeme konektor před sebe a nastavíme ho tak, aby jsme viděli dovnitř konektoru a kontakty směřovali vzhůru. Do konektoru zastrčíme kabel, tak že vodiče budou natlačeny až k úplném konci konektoru a dotlačíme i bužírku do konektoru co nejhlouběji. Musíme si ale dávat pozor, aby se nám vodiče v konektoru nepřekřížili a dodrželi jsme tak zapojení podle normy T568B. Tedy první kabel zleva bude bílo-oranžový. Dobře nasazený konektor můžeme nacvaknout krimpovacími kleštěmi.

Obrázek 6 - Pomůcky pro krimpování kabelu

Totéž provedeme na druhém konci kabelu a máme hotový přímý kabel.Teď už ho zbývá pouze změřit, jestli jsme někde neučinili chybu. K tomuto účelu se používá speciální **tester kabelů**.

3.3 Patch panel a zásuvky

Pro lepší vedení kabelů po učebně je dobré použít patch panely a zásuvky.

3.3.1 Patch panel

Patch panel je název pro propojovací prvek mezi kabely od počítačů a switchem. Většinou se umísťuje do **racku**, kde jsou i switche a někdy i server. Proto se patch panely vyrábí i v takových velikostech, aby byli snadno umístěné do racku. Nejčastější rozměr je 19 palců. Na patch panelu je několik desítek portů pro konektory RJ-45. Počet se většinou volí podle počtů portů na switchi, většinou 12 nebo 24 portů.

Porty na přední straně panelu jsou jako výstupní. Kabely od počítačů se fixují ze zadní strany. Opět montáž kabelu je dosti jednoduchá a po chvilce praxe nám nebude dělat žádný problém. Otočíme si panel zadní stranou k sobě a můžeme vidět, že pro každý port je určená speciální kostka nebo řádka kontaktů, která je označená barvami stejnými jako jsou barvy vodičů v kabelu. Pomocí **zářezového narážecího nástroje** každý vodič natlačíme do dané pozice a vodič zařízneme. Pokud máme naraženy všechny kabely, můžeme patch panel připevnit do racku. Poté je ještě dobré kabely svázat vázacími páskami, aby se nám kabely nemotaly různě po racku a také aby docházelo k lepšímu proudění vzduchu potřebnému k chlazení switchů.

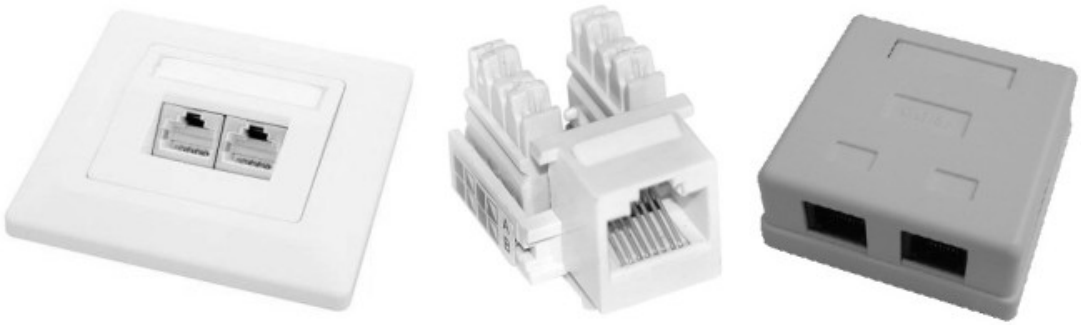
Obrázek 7 - Patch panel, narážecí zařízení, patch panel - zadní strana

Obrázek 7 nám ukazuje jak má vypadat správné vyvázání kabelů a také naražení kabelu z druhé strany pomocí zářezového narážecího zařízení.

3.3.2 Zásuvka RJ-45

Zásuvka je v principu podobná patch panelu. Ale u zásuvky se můžeme setkat s jedním nebo dvěma porty. Pro naše účely bude lepší použít jednu dvou-portovou zásuvku pro jeden počítač, jelikož počítáme s tím, že počítač bude propojen do dvou síti.

Jedna síť je pro pokusné příklady v naší laboratoři a druhá by měla být využita pro stálé připojení k internetu. Jak jsem již naznačil, narážení kabelu je stejné jako u patch panelu, tak se jím dále nebudeme zabývat. Snad jen ještě dodejme, že jak na zásuvku, tak na patch panel můžeme umístit popisky, abychom věděli, který port patří k té které zásuvce.

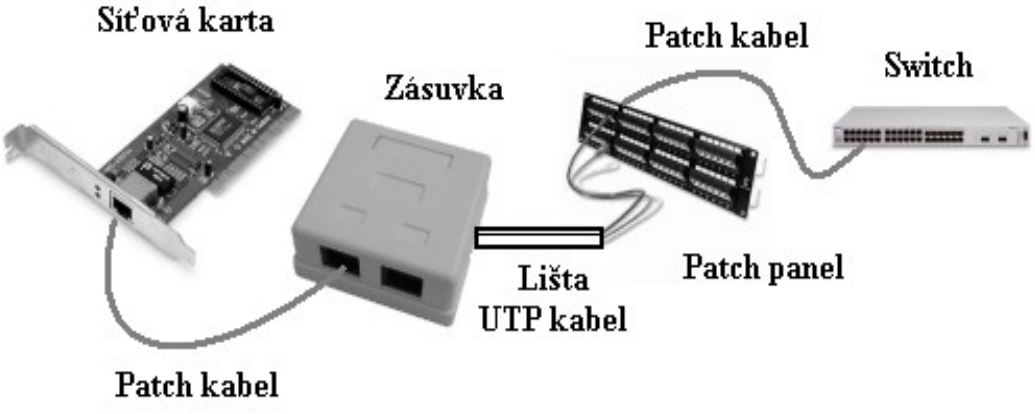


Obrázek 8 - Zásuvky RJ-45

3.3.3 Praktické vedení kabelu

Nejjednodušší je vést kabel ze síťové karty v počítači přímo do switche. Ale tato technika má spousty nevýhod. Kabel má pevnou délku a tak přemístění switche či počítače může vést k problémům. Jelikož počítáme s častější manipulací s kabely, brzo by byly polámané, atd.

My ale zvolíme profesionálnější přístup k vedení kabelu. Použijeme jeden UTP kabel, dva patch kabely, jednu dvou-zásuvku, lišty a patch panel.



Obrázek 9 - Vedení kabelu

Na obrázku 9 můžeme vidět propojení od počítače (síťové karty) až ke switchi. Ze síťové kary do zásuvky vede patch kabel. Zásuvka je umístěna například na stole vedle počítače a kabel z ní je veden dále lištami až k racku s patch panel. V poslední fázi je switch propojen opět patch kabelem s patch panelem. Všechny kabely jsou přímé.

3.4 Síťová karta

Síťová karta je v počítačovém světě také označována jako NIC (Network Interface Cards) a je nezbytnou součástí pro připojení počítače k síti. Karta se stará o komunikaci mezi počítačem a sítí podle pravidel daných síťovým standardem. Hlavně musí vyhovět normám na příslušný síťový protokol, přístupovou metodu a kabeláž.

Dnes je většinou síťová karta integrována na základní desce počítače.

Síťové karty můžeme dělit například ze dvou hledisek.

1) Parametry z hlediska PC

- Typ sběrnice základní desky
- Wake-On
- Ovladače karty

2) Parametry ze strany sítě

- Standard síťového hardwaru
- Typ kabeláže
- Případný duplexní provoz
- Případné vzdálené bootování

3.4.1 Sběrnice základních desek

Většina počítačů má síťovou kartu integrovanou na základní desce. Ale může se stát jako v našem případě, že potřebujeme mít zapojené dvě síťové karty nebo na desce není síťová karta instalována, tak v tom případě musíme instalovat kartu novou.

A právě pro instalaci nové karty použijeme systémovou sběrnici. Sběrnice je zakončena konektorem a těch máme několik druhů. V dnešní době se můžeme setkat hlavně se sloty **PCI** (Peripheral Component Interconnect) a **PCI Express** (PCIe). Starými 8 a 16 bitovými ISA sloty se již nebudeme zabývat.

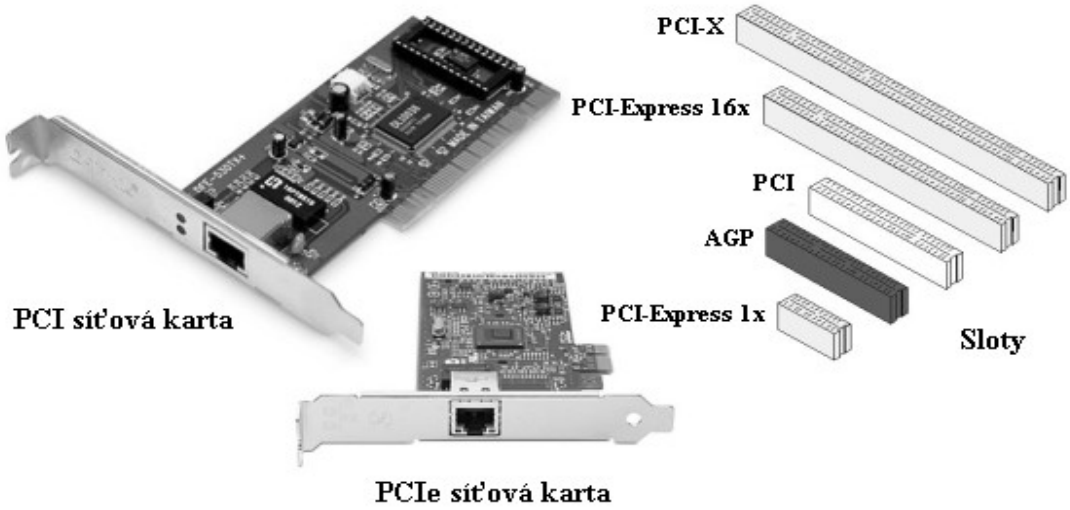
PCI je bílý konektor s řadou kontaktů uprostřed a má v sobě jeden zámek. Je 32bitová a pracuje na frekvenci 33 MHz. Sběrnice je paralelní.

PCIe je novější sběrnice a je tedy rychlejší. Důležité je vědět, že tato sběrnice je již sériová a existuje ve více variantách. Varianty se od sebe liší počtem vodičů použitých pro přenos dat. Čím více vodičů, tím větší délka konektoru.

Pro síťové karty se používá nejpomalejší sběrnice označována **PCI Express x1**, která má propustnost 250 MB/s a má 2 vodiče pro jeden směr.

S rozmachem univerzální sériové sběrnice **USB** (Universal Serial Bus) můžeme využít i tento druh připojení. Je to výhodné zapojení například pro notebooky. U notebooku ještě můžeme využít rozšiřující slot **PCMCIA** (Personal Computer Memory Card International Association).

Podle volného slotu v počítači také volíme typ síťové karty. Sloty a síťové karty můžeme vidět na následujícím obrázku 10.



Obrázek 10 - Síťové karty a sloty k propojení

3.4.2 Wake-On

Díky vlastnosti Wake-On můžeme spustit počítač zapojený do sítě z jiného počítače povelem přeneseným v síti. Také je nutná podpora Wake-On základní deskou. Základní deska musí být v provedení **ATX** (Advanced Technology Extended). ATX je systém, který definuje rozložení prvků na desce a také zavádí nový způsob napájení. I když je počítač vypnutý, je stále napájen ATX zdrojem. Ve skutečnosti základní deska tedy vypnutá není, jen se tak jeví a čeká tak i na případný signál bud z tlačítka pro start systému a nebo ze sítě, kterým se probudí.

Aby funkce Wake-On byla funkční, musíme ještě propojit zdířku označenou Wake-On na kartě se stejnou zdířkou na základní desce.

3.4.3 Standard síťového hardwaru

Normu IEEE jsme si popsali výše a této normě musí odpovídat i síťová karta. V dokumentaci k síťové kartě se vyskytuje údaj o tom, pro který síťový standard je karta určena, například Ethernet, Token Ring, nebo přesnou definicí například 100Base-TX.

Standard rovněž určuje způsob adresace karet. U Ethernetu má každá síťová karta originální číslo, kterému říkáme **MAC adresa** (Media Access Control). MAC

adresu používají různé protokoly druhé linkové vrstvy OSI modelu. Je přiřazena síťové kartě hned po její výrobě, ale dnes je již možné tuto adresu dodatečně měnit. Adresa se skládá ze 48 bitů a měla by se zapisovat jako tři skupiny čtyř hexadecimálních čísel (např. 1234.5678.90ab). Ovšem mnohem častěji se setkáme s dvojciferným hexadecimálním zápisem čísel oddělených pomlčkami nebo dvojtečkami (např. 12-34-56-78-90-ab nebo 12:34:56:78:90:ab).

3.4.4 Typ kabelu

Typ kabelu je také závislý na síťovém standardu, ale jednotlivé standardy mohou používat odlišné druhy kabeláže s různými konektory. Síťová karta může být určena pro jeden i více typů kabelů.

Nejčastější konektor na síťové kartě je konektor RJ-45 pro 10BASE-T, 100BASE-T nebo 1000BASE-T. Dříve byl používán konektor BNC pro 10Base-2, přes který se zapojuje tenký koaxiální kabel. Na síťové kartě také můžeme nalézt koncovky ST nebo SC pro optické kabely. V takovém případě je karta vybavena vždy dvojicí konektorů, jeden pro vstup a druhý pro výstup.

Vedle konektorů na kartě jsou ještě umístěny kontrolky, které nás informují o aktivitě síťové karty a o rychlosti přenosu dat, 10 Mb/s nebo 100 Mb/s.

3.4.5 Duplexní provoz

Většina Ethernetových karet může pracovat ve dvou režimech.

- **Duplexní režim** (ang. Full duplex) - tento režim dovoluje přenos mezi vysílací a přijímací stanicí v obou směrech.
- **Simplexní režim** (ang. Half duplex) - tento režim dovoluje přenos dat mezi vysílací a přijímací stanicí v daném čase pouze v jednom směru.

K duplexnímu provozu potřebujeme jak duplexní síťovou kartu tak i duplexní switch. Oba dva musejí být do duplexního režimu přepnuty.

3.4.6 Vzdálené bootování

Bootování je pojem pro nastartování systému. Nejprve se provedou **POST** (Power On Self Test) testy a pak se z pevného disku načte operační systém. Součástí operačního systému je i síťový klient, tedy software pro připojení počítače k síti.

Ovšem ne každý počítač musí mít pevný disk. Pro takový případ se nachází na síťové kartě patice pro elektronický obvod **BootROM** (Boot Read Only Memory). V obvodu je uložen program, jehož prostřednictvím se uživatel připojí k serveru. Ze serveru přenese do operační paměti bezdiskové stanice operační systém a síťového klienta. Stanice pak může pracovat s dalšími programy na serveru.

Díky operačním systémům Windows se dnes již bezdiskové stanice nepoužívají. Přesuny objemných programů po síti by bylo velice zdlouhavé.

3.4.7 Instalace ovladače

Pro správnou činnost je nutné nahrání ovladačů nové síťové karty do operačního systému. Všechny síťové karty v provedení PCI a PCIe splňují normu **PnP** (Plug and Play). Metoda PnP „zastrč a hraj“ znamená maximální usnadnění rozšíření počítače o novou rozšiřující desku, v našem případě síťovou kartu.

Více o instalaci ovladačů a softwaru se dozvíme v kapitole o softwarovém vybavení. Proto se jí zde dále nebudeme zabývat.

3.4.8 Volba síťové karty

Z předcházejících parametrů síťové kary můžeme snadno vybrat variantu, kterou budeme instalovat do počítačů v síti. Jelikož je naše síť typu Ethernet, volíme kartu s portem RJ-45 a tomu odpovídající kabeláž. Důležité je, aby bylo možné síťovou kartu instalovat do slotu PCI na základní desce. Funkce Wake-On a vzdálené bootování nejsou pro naše výukové účely nutné. Jelikož budou počítače připojeny ke switchi, tak by naše karta měla podporovat duplexní režim.

3.5 Switch

Switch nebo-li přepínač je aktivní síťový prvek, propojující jednotlivé segmenty sítě. Pracuje na druhé (linkové) vrstvě OSI modelu, rozhoduje se tedy podle MAC adresy. Pojem switch se používá pro různá zařízení v celé řadě síťových technologií. Obecnou vlastností switchů je, že analyzují procházející pakety a podle informací v nich obsažených (adres, identifikátorů apod.) rozhodují, kam paket předat dál. U přicházejících rámců čte zdrojovou MAC adresu a vytváří v paměti tabulku MAC adres a portů odkud pochází. Tabulka se označuje jako **CAM** (Content Addressable

Memory) tabulka. Pokud nemá pro cílovou MAC adresu záznam, tak rámec odešle na všechny porty mimo příchozího, jinak pokud má v tabulce cílovou MAC adresu, tak rámec pošle pouze na daný port.

Switch tedy slouží k propojení či oddělení segmentů, snižuje velikost kolizní domény a broadcasty se posílají všude. Switch pracuje rychle a je to základní prvek pro hvězdicovou topologii.

Obrázek 11 - Switch ASUS GigaX 1024i

Kvůli hledání kompromisu mezi zpožděním a spolehlivostí existuje několik metod nebo-li modů switche. Dnes se běžně používají tři módy.

1. Koncepčně pracují způsobem **Store-and-Forward**. Paket z jednoho rozhraní přijmou, uloží si do vyrovnávací paměti, prozkoumají jeho hlavičky a následně odvysílají do příslušného rozhraní.

2. Současné switche ale tento proces často optimalizují, takže k analýze hlaviček dochází jakmile dorazí začátek paketu. Ani s vysíláním do cílového rozhraní se nečeká, až dorazí celý paket, ale zahajuje se co nejrychleji, aby zpoždění paketu ve switchi bylo minimální. Této metodě se říká **Cut-Through**.

3. Existuje ještě třetí metoda **Fragment-Free** (Modified Cut-Through), což je takový kompromis, nejprve načte prvních 64 bytů (včetně hlavičky) a pak přeposílá paket dál.

Dále si popíšeme základní vlastnosti a dělení switchů. Na základě těchto informací se nakonec pokusíme vybrat jeden switch z aktuální nabídky na našem trhu.

3.5.1 Počet portů

Počet portů na switchi se pohybuje v různém rozmezí. Minimální počet bývá 5 portů a maximální 24 portů. Počet portů volíme tak, aby nám zbyla ještě nějaká rezerva pro případné pozdější rozšíření sítě. Pokud ovšem zaplníme všechny porty, můžeme připojit další switch a počet portů si tak třeba zdvojnásobit.

3.5.2 Typ portů

Typ portu je závislý na použité kabeláži a použitých konektorech. Běžné jsou porty RJ-45 pro kroucenou dvojlinku. Dříve se používali BNC konektory a s nimi se připojoval tenký koaxiální kabel. Poslední typ je port pro připojení optického kabelu.

Pokud budeme propojovat dva switche, měli bychom použít kříženou kroucenou dvojlinku, ale dnešní switche již zvládají i propojení přímým kříženým kabelem. Slouží k tomu port RJ-45 označen jako **Uplink**.

Tato zásuvka má již překřížení vodičů provedeno. Může pak použít obyčejný patch kabel. Port Uplink můžeme najít obvykle jako první nebo poslední port na switchi a jeho křížení se může zapínat přepínačem.

Nové switche již mají automatickou detekci překřížení a ta se značí jako **AutoMDI** (Auto Medium Dependent Interface). Detekce je aktivní na všech portech a tak jako Uplink můžeme použít jakýkoliv port. Switch již sám automaticky rozpozná, zda se jedná o překřížený či přímý kabel.

3.5.3 Provedení

Switche se vyrábějí ve dvou provedeních.

- **Desktop** - určené pro položení mimo rack
- **Rack** - switch určený do racku

3.5.4 Přenosová rychlost

Rychlost může být různá. Možnosti jsou následující: 10 Mb/s, 100 Mb/s nebo 1000 Mb/s. Při volbě rychlosti musíme brát v úvahu rychlosti použitých síťových karet v síti.

3.5.5 Světelné indikátory

Každý port má sadu světelných diod, obvykle bývají dvě. Diody indikují činnost portu. Zpravidla ukazuje jedna světelná dioda připojení portu k síťové kartě. Jelikož síťová karta může pracovat na různých přenosových rychlostech, tak se ještě používá rozdílná barva. Druhá dioda obvykle ukazuje aktivitu na přenosovém médiu.

3.5.6 Volba switche

Dostáváme se k výběru switche pro naší síť. V dnešní široké nabídce síťových komponent není jednoduché vybrat switch, který by vyhovoval naším podmínkám. Ale pokud si předem ujasníme vlastnosti, které by měl náš switch zvládat, tak se nám výběr dosti usnadní a už budeme hledat jen kompromis mezi cenou a výkonem.

Kladené požadavky na optimální switch pro naší síť jsou následující.

- Ethernetový switch pracující s minimální přenosovou rychlostí 100 Mb/s
- Dostatečný počet portů - nejlépe 24 portů
- Funkce VLAN (Virtual Local Area Network)
- Funkce TRUNKING
- Web management - centralizovaná správa switche
- Stohovatelný switch
- Určený do racku
- Nastavování jednotlivých portů
- Regulace šířky pásma
- Kontrolovaný přenos na portech

Switch s přenosovou rychlostí alespoň 100 Mb/s není žádný problém. Dnes switche pracují již běžně i na 1000 Mb/s rychlosti. Ani switch se 24 porty není překážka.

Výběr nám zúží až třetí požadavek na náš switch a to aby podporoval funkci **VLAN** (Virtual Local Area Network). Funkce VLAN slouží ke sdružování portů do virtuálních sítí. To znamená, že na jednom switchi můžeme provozovat více nezávislých sítí. Tuto funkci si podrobně probereme v poslední kapitole na ukázkovém příkladě pro výuku.

Funkce **TRUNKING** znamená, že můžeme několik portů sdružit do jednoho přenosového kanálu a násobit tak přenosovou rychlost. Tato funkce ale není pro naše výukové účely až tak důležitá.

Web management, tedy centrální správa switche, je naopak velmi důležitá vlastnost, kterou náš switch musí splňovat. Díky této funkci můžeme switch nastavovat z libovolného počítače v síti. Stačí když známe přihlašovací jméno a heslo. Přes webové rozhraní pomocí internetového prohlížeče, tak můžeme switch spravovat a nastavovat další parametry sítě napojené na switch. Můžeme regulovat šířku přenosového pásma pro jednotlivé porty, zakazovat či povolovat porty, kontrolovat přenos na portech atd.

Celkem novou vlastností switchů bývá, že jsou **stohovatelné**. To znamená, že můžeme mezi sebou propojit dva a více switchů. Pak také dochází k jednodušší správě switchů. Například když máme čtyři propojené switche a počítač připojen na první z nich, můžeme spravovat switch číslo čtyři aniž bychom vstali od stolu a museli přepojovat kabely mezi switchi.

Po delším hledání jsem zúžil výběr na dvě možnosti a to **Switch D-Link DGS-1216T** a **Switch ASUS GigaX 1024i**.

Switch D-Link DGS-1216T

Tento „inteligentní“ switch vyhovuje téměř všem našim požadavkům a ještě navíc má velmi dobrou podporu na webových stránkách firmy D-Link. Na těchto stránkách se nachází i **emulátor** switche, tedy jeho web managementu. Student si tak může úkoly vyzkoušet i mimo počítačovou učebnu.

Nevýhodou tohoto switche je ovšem cena, která je dvakrát vyšší než u druhé zvolené varianty. A jako druhou menší nevýhodu vidím počet portů, kterých je pouze 16. Ale v našem návrhu je právě 16 počítačů a tak ani to by neměl být problém.

Switch ASUS GigaX 1024i

Druhá varianta je opět „inteligentní“ switch. Ten již má 24 portů pracujících na rychlosti 1000 Mb/s. Vyhovuje všem požadavkům popsaných výše.

Výhodou je jeho příznivá cena, která nadmíru splňuje náš požadavek nízká cena za kvalitní výkon.

Z finančních důvodů bych právě volil druhou variantu a to **Switch ASUS**. V našem návrhu sítě počítáme se čtyřmi switchi a tak se výhoda ceny projeví ve větší míře. Také má přehledný manuál a elegantní konfiguraci přes web management.

3.6 Počítače

Výběr počítače vhodného do naší počítačové sítě pojmeme velmi obecně, jelikož to není hlavní účel této práce. Na začátek ještě dodejme, že budeme používat jenom počítače PC kompatibilní.

Počítače používané v naší síti mohou být staršího data výroby, jelikož na nich nebude provozován žádný speciální software náročný na výkon. V podstatě se na nich bude pracovat v příkazové řádce a v internetovém prohlížeči při správě switchů. Jelikož počítáme s instalací operačních systémů Windows XP a Linux Debian, tak by tomu měl i odpovídat výkon počítače.

Co se tedy týče hardwaru počítače, nemusíme se držet dnešní špičky v nabídce. Možná by bylo i dobré využít nějaké již existující počítačové učebny, kde již jsou starší počítače. Výhodou pro naše účely je počítač se základní deskou s již integrovanou síťovou kartou, ale ani to není podmínkou, jelikož budeme počítače rozšiřovat o druhou síťovou kartu.

Výhodou by byla přítomnost dvou pevných disků a to z důvodu instalace dvou operačních systému, ale jak víme, tak je možné instalovat dva operační systémy na jeden pevný disk, tak ani toto by nebylo překážkou.

4 Softwarové vybavení počítačů

Od hardwaru sítě se dostáváme k softwaru pro naší síť. V této kapitole se hlavně zaměříme na vybrané operační systémy, které budeme provozovat na koncových stanicích. V návrhu naší sítě počítáme se dvěma operačníma systémy a to Windows XP a Linux Debian.

Windows XP volíme, protože je to stále ještě standard na dnešních počítačích a dovoluje nám dobrou a kvalitní práci se sítí. Je také finančně výhodnější než novější Windows Vista. Pokud by v budoucnu v naší síti přibil i server, byla by možnost na něj instalovat síťový operační systém do firmy Microsoft Windows 2003 Server nebo dnes zcela nový Windows 2008 Server. Ale pro tuto chvíli se s těmito systémy nebudeme zabývat.

Distribuci **Linuxu Debian** přidáváme jako druhý operační systém. Důvod je jasný, dnešní servery ve velkých sítí běží právě na UNIXových systémech a tak je dobré studenty seznámit se správou sítě i v tomto systému. Výhodou je také, že distribuce Debianu je volně šiřitelná a tedy zdarma, pokud dodržíme licenční ujednání GNU / GPL (GNU is Not UNIX / General Public License).

Pokud máme na jednom počítači nainstalovány dva či více operačních systémů, nazýváme je jako *multi-boot* počítače. Abychom si mohl vybrat při startu počítače jeden z operačních systémů, musíme mít nainstalován boot manažer. Windows obsahují **NT** (New Technology) **boot manažer**, který nastavujeme pomocí souboru boot.ini v kořenovém adresáři aktivního spouštěcího oddílu na pevném disku. U Linuxu si můžeme vybrat ze dvou nejpopulárnější zaváděcích manažerů a to buď **LILO** (LInux LOader) nebo **Grub**. Oba můžeme zavést přímo do MBR (Master Boot Record) na pevném disku.

Instalací samotných systémů se zde zabývat nebudeme. Pouze si popíšeme jak pracovat se sítí v jednotlivých systémech.

4.1 MS Windows XP Professional

Na začátek dodejme, že popis práce s tímto systémem vychází z verze MS Windows XP Professional se Service Packem 2.

Práci se síti v systému MS Windows XP můžeme shrnout do následujících tří kroků:

1. Nejprve musíme mít nainstalovány ovladače k síťové kartě.
2. Poté proběhne instalace klienta sítě, nakonfigurujeme síťové protokoly a případně vytvoříme pracovní skupiny.
3. Nastavíme sdílení složek a definujeme případná přístupová práva.

Jen popis těchto tří kroků by nám mohl zabrat několik desítek stránek a tak se budeme snažit vybrat jen to nejdůležitější s čím se budeme potkávat při nastavování počítačové sítě a co poté bude moci využít při řešení cvičných úloh v poslední kapitole.

4.1.1 Ovladače síťové karty

Ovladače síťové karty se nám většinou načtou automaticky díky metodě **Plug and Play**. Poté mohou nastat tři varianty.

1. Ovladač síťové karty je známý pro Windows.
2. Ovladač Windows neznají a je nutné jej doinstalovat prostřednictvím *Průvodce nově rozpoznaným hardwarem*.
3. Ovladač karty a další software instalujeme pomocí instalačního programu.

První případ je ideální. Budeme pouze informováni o průběhu instalace a již se nemusíme o nic starat.

V druhém případě, kdy Windows ovladače síťové karty neznají, tak jej musíme ručně doplnit. K tomu slouží právě *Průvodce nově rozpoznaným hardwarem*. Okno tohoto průvodce se objeví o instalaci karty. Nejběžnější postup je ten, že máme ovladače připravené na nějakém přenosovém médiu jako je CD a pak tedy volíme buď *Instalovat software automaticky* a nebo *Instalovat ze seznamu či daného umístění*, pokud víme přesné umístění ovladačů na médiu.

Dále pokračujeme podle pokynů na obrazovce a neměl by nastat žádný větší problém. Více se věnovat instalaci ovladačů nebudeme.

Na závěr snad jen zkontrolujeme, že se instalace síťové karty zdařila a to tak, že ve *Vlastnostech systému*, které nalezneme v *Ovládacích panelech*, zvolíme záložku *Hardware* a zde tlačítko *Správce zařízení*. Zde bychom po správné instalaci

měli vidět položku Síťové adaptéry a po jejím rozbalení i naší nainstalovanou síťovou kartu. Pokud u ní není černý vykřičník ve žlutém kolečku nebo červený křížek, proběhla instalace v pořádku.

4.1.2 Síťový klient a jeho protokoly

Práci se síťovými klienty a protokoly je věnováno okýnko *Síťové připojení*. Vstoupit do něj můžeme například opět přes *Ovládací panely*. V oknu *Síťová připojení* můžeme vidět ikony reprezentující jednotlivá síťová připojení. Nás nejvíce bude zajímat ***Připojení k místní síti***. Jelikož máme nainstalovány dvě síťové karty, bude tam tato ikona zobrazená dvakrát a také očíslovaná.

Pokud na ikonku ťukneme pravým tlačítkem a dáme položku *Vlastnosti*, dostaneme se do *Připojení k místní síti - vlastnosti* a zde se budeme hlavně věnovat záložce *Obecné*. Jsou zde všechny součásti potřebné ke konfiguraci sítě. Ty sem po instalaci síťové karty doplní Windows XP automaticky.

My ale tyto součásti můžeme odebírat či přidávat, ale co je nejdůležitější, také měnit. Pojďme se na ně podívat blíže.

Práce s klientem

Pro práci v síti peer-to-peer je potřebný Klient sítě Microsoft. Ten se instaluje automaticky spolu s ovladačem síťové karty. Klienta můžeme přidat či odebrat, ale to asi nebudeme potřebovat. K tomu nám slouží tlačítka *Nainstalovat* a *Odinstalovat*.

Síťové protokoly

K dispozici máme následující protokoly: **NetBEUI**, **IPX/SPX** a **TCP/IP**. Pro malou síť můžeme použít kterýkoliv z nich, ale my už jsme se předem rozhodli pro protokol TCP/IP. Ten se opět instaluje automaticky. Také ho můžeme *Nainstalovat* či *Odinstalovat*, ale to provádět nebudeme, protože ho budeme hojně využívat, jak to si popíšeme dále.

4.1.3 Konfigurace protokolu TCP/IP

Pokud v oknu P*řipojení k místní síti - vlastnosti* označíme právě položku *Protokol sítě Internet (TCP/IP)* a ťukneme na tlačítko *Vlastnosti*, dostaneme se do nejdůležitějšího okna a to ***Protokol sítě Internet - vlastnosti***.

V kartě *Obecné* můžeme vidět dva rámečky. Jeden pro nastavení **IP adresy** a druhý pro nastavení **DNS serverů**. U obou těchto variant můžeme zvolit, buď zadat automaticky nebo ručně. *Získat adresu IP ze serveru DHCP automaticky* my používat nebudeme a ani nemáme server v naší síti, který by nám tuto službu zajišťoval. Logicky tedy ani nezaškrtneme *Získat adresu serveru DNS automaticky.*

Vybereme tedy rámeček *Použít následující adresu IP*, kde nastavujeme nejdůležitější údaje o naší identifikaci v síti a to:

- ***Adresa IP***
- ***Maska podsítě***
- ***Výchozí brána***

U rámečku *Použít následující adresy serverů DNS* můžeme vyplnit adresy DNS serverů. Po zmačknutí tlačítka *Upřesnit*, ještě můžeme systému podat nějaké upřesňující informace, ale těmi se tady zabývat nebudeme.

4.1.4 Pracovní skupiny a jména počítačů

V síti je velmi důležitá identifikace počítače. Každý počítač tedy musíme pojmenovat a přiřadit do určité pracovní skupiny. Pracovních skupin může být jedna či více. Pokud je skupin více, je možné mezi nimi přepínat. My pro začátek volíme pracovní skupinu s názvem HOME.

Pojmenování počítače je také snadné. V *Ovládacích panelech* zvolíme ikonku *Systém* a dostaneme se do okna *Vlastnosti systému*. Přejdeme na záložku *Název počítače* a zde můžeme vidět políčka *Popis počítače* a *Úplný název počítače*. Pro nás je stěžejní *Úplný název počítače*. Ten můžeme i s pracovní skupinou změnit pomocí tlačítka *Změnit...* například na počítač PC23 v pracovní skupině HOME.

Tyto základní nastavení, jméno, skupina, adresa, maska, brána provedeme u každého počítače v síti a máme tak síť pro začátek funkční a nastavenou pro další práci v síti.

4.1.5 Zjednodušené sdílení souborů

Síť tedy máme vytvořenou a teď se dostáváme k tomu, proč to všechno děláme. Chceme mezi uživateli sdílet soubory, adresáře, tiskárny, atd. Musíme tedy určit jaké složky budeme chtít sdílet a stanovit podmínky jejich sdílení.

Pravidla pro sdílení složek vychází ze souborového systému, který používáme. Souborový systém se stará o organizaci a ukládání souborů na disk. U každého souboru si také zaznamenává informace o délce souboru, datu vzniku, ale také o přístupových právech k souboru.

Dnes se u systému Windows můžeme setkat v podstatě s dvěma souborovýma systémy. Starší je **FAT** (File Allocation Table) a novější **NTFS** (New Technology System). Souborový systém FAT nás dost omezuje u použití oprávnění k souborům, kdežto mezi hlavní přednosti NTFS patří právě práce s oprávněními a tím i spojené sdílení souborů. Je tedy možné přesně definovat, kdo bude moci se složkou či souborem pracovat a co mu povolíme. Nadále se budeme věnovat jenom souborovému systému NTFS, jelikož je výchozí pro Windows XP.

Teď je také vhodná chvíle dodat, proč jsme si vybrali edici **Professional**. Ve zkratce si popíšeme její výhody oproti edici **Home**.

Windows XP Home

Tato edice je navržena hlavně pro domácnosti a do malých síti. Pracuje ve zjednodušeném režimu sdílení, který je méně náročný na správu, ale také méně zabezpečen. V sítích peer-to-peer může ke sdíleným složkám přistupovat kdokoliv ze sítě. Windows XP Home také nemohou být začleněny do domény.

Windows XP Professional

V síti peer-to-peer také pracují ve zjednodušeném režimu sdílení, ale můžeme je začlenit do domény, což přináší vyšší zabezpečení. To vyplývá z používání uživatelských účtů při práci s operačním systémem, větší či menší oprávnění, úplná práce se skupinami, možnost centrální správy v doméně atd. Také lze ověřovat přístupy ze sítě. Vnější uživatel musí mít vlastní účet, nebo vstupovat prostřednictvím účtu **Guest**.

Jak tedy na sdílení souborů? Je to poměrně jednoduché. Prvým tlačítkem ťukneme na složku, kterou chceme sdílet, a vybereme položku *Sdílení a zabezpečení...* Dostaneme se tak do okna *Vlastností* té dané složky a na záložku *Sdílení*. Nyní máme na výběr buď *Nesdílet tuto složku* nebo *Sdílet tuto složku*. Pokud ji chceme sdílet, vybereme druhou variantu. Můžeme pozměnit název sdílené položky a také ji okomentovat. Co je ale důležité, pokud jsme vlastníkem dané složky můžeme jí nastavit i omezující oprávnění pro ostatní uživatele a to tím, že zvolíme tlačítko *Oprávnění*. Zde můžeme přidávat a odebírat jak skupiny

uživatelů, tak samotné uživatele a nastavovat jim různá práva pro *čtení*, *změnu* nebo *úplné řízení složky.*

Nyní se podíváme na to, jak pracovat se síťovým nastavením v operačním systému Linux.

4.2 Linux Debian Sarge 3.1 s jádrem 2.6.12.3

Než se pustíme do popisu práce se systémem v síti, dodejme že budeme používat **jádro Linuxu 2.6.22-14**. Na trhu už je i verze Debianu 4.0, ale kvůli stabilitě systému zatím zůstaneme u staršího jádra.

Ještě malá poznámka k výběru distribuce. Distribucí Linuxu je celá řada, ale vybral jsem právě Debian, jelikož s touto distribucí pracuji nejdéle a tak s ní mám největší zkušenosti a je také má nejoblíbenější a to kvůli jejímu systému založeném na balíčkách **.deb**. Dá se také snadno rozšířit o grafickou nástavbu **KDE** (K Desktop Enviroment) nebo **Gnome**.

4.2.1 Start systému

Při startu Linuxu je do paměti zavedeno **jádro**, které zajišťuje uživatelům i programům všechny základní služby. Jádro Linuxu je modulární, to znamená, že pro ovládání nejrůznějších vstupně - výstupních zařízení stačí zavést za běhu příslušný modul či ovladač. Jádro samo zajišťuje nejzákladnější služby, a proto jsou doplňky zajišťovány tzv. *démony* nebo uživatelskými aplikacemi. Démony jsou programy, které se spustí při startu systému a pak až do jeho vypnutí poskytují své služby.

V Linuxu se často pracuje v příkazovém řádku neboli **shellu**. Dnes je ale již možné také pracovat v grafickém uživatelském prostředí, kde si lze spustit libovolné množství programů a shellů. Terminálů pro práci v příkazové řádce máme v linuxu několik na rozdíl od Windows, kde je pouze `command.com` a jen jedno grafické prostředí.

4.2.2 Uživatelské účty

Abychom se mohli přihlásit do Linuxu, musíme mít vytvořen uživatelský účet a případně skupinu, do které uživatel patří. Databázi uživatelů nalezneme v souboru

`/etc/passwd`, kde je na každém řádku záznam o jednom účtu. Skupiny jsou definovány podobně jako uživatelé v souboru `/etc/group`. Tyto soubory lze upravovat ručně nebo využívat různá grafická rozhraní.

Každý uživatel je členem alespoň jedné skupiny, kterou označujeme jako primární. Pokud bude uživatelské jméno uvedeno v souboru `/etc/group` u dalších skupin, bude po přihlášení uživatel člen všech těchto skupin. Primární skupinu lze měnit pomocí příkazu `$ newgrp`.

Hesla pro vstup do systému měníme pomocí príkazu `passwd`. Při změně hesla nejdřív musíme zadat staré heslo a poté dvakrát heslo nové.

Největší práva má v Linuxu a Unixu obecně superuživatel nazývaný **root**. Heslo roota zadáváme při instalaci systému. Root má neomezená práva v systému a proto bychom se na něj měli přihlašovat obezřetně, protože sebemenší chyba může poškodit systém. Jako root můžeme měnit přístupová práva k souborům, zakládat a mazat uživatele, měnit jejich hesla, instalovat programy, atd.

4.2.3 Přihlášení do systému

Máme-li vytvořen účet v systému, můžeme se na něj přihlásit. Nejjednodušší způsob přihlášení je v textovém režimu přímo na **konzoli**. Konzole je počítač se systémem u kterého přímo sedíme. Po vložení přihlašovacího jména hesla se spustí vybraný shell a uživatel tak může začít pracovat v příkazové řádce nebo si dále pustit grafické uživatelské prostředí.

Další možnost přihlášení je, že se k systému přihlásíme pomocí počítačové sítě. Tomu říkáme **terminálový přístup**. Základním způsobem je přihlášení pomocí terminálové emulace, kdy získáme podobný přístup jako u textové konzole. Pro terminálový přístup můžeme použít program **Telnet**, který je i součástí Windows jako `telnet.exe` nebo využít šifrovaného spojení pomocí protokolu **SSH** (Secure SHell). Ve Windows můžeme také použít volně šiřitelný klient jak pro šifrované spojení SSH tak pro Telnet nazývaný **PuTTY**.

4.2.4 Síťové rozhraní

Po přihlášení do systému můžeme začít se síťováním v Linuxu. Linux se hodí jako **WWW server** (World Wide Web), **router**, **poštovní server**, **FTP server** (File Transerf Protocol), **DNS server** (Domain Name Server), **SQL server** (Structured

Query Language), **firewall** atd. Protokol pro komunikaci se svými sousedy je TCP/IP.

O **síťovém rozhraní** mluvíme, máme-li v počítači s Linuxem síťovou kartu. Síťové rozhraní nemusí být ale jenom fyzické, může být i virtuální. Virtuální síťové rozhraní může být tzv. *loopback* nebo *aliasy*, které umožňují přiřadit jednomu síťovému rozhraní více různých IP adres.

Síťová rozhraní jsou pojmenována zkratkou, za níž následuje číslo. Číslo značí pořadí detekce v systému. Například když máme v počítači dvě síťové karty budou označeny názvy `eth0` a `eth1`. Příkazem pro výpis souboru `cat /proc/net/dev` si můžeme zjistit síťové karty přítomné v počítači. Vždy je zde také uvedeno zařízení pro **loopback**, které se označuje zkratkou `lo`.

Loopback je povinné zařízení pro všechny implementace protokolu TCP/IP a přiděluje se mu adresa 127.0.0.1 a maska 255.0.0.0. O adresách a maskách se dozvíme více v poslední kapitole.

Může se stát, že máme v počítači nainstalovanou síťovou kartu, ale systém ji nerozpozná. Obvykle je to způsobeno tím, že jádra jsou v jednotlivých distribucích kompilována co nejmenší a všechny ovladače jsou k dispozici jako moduly, které zavádíme za běhu systému jen v případě potřeby. Moduly nalezneme v adresáři `/lib/modules`. Moduly jsou zde systematicky rozčleněny do adresářů a tak zde také najdeme nejčastěji používané moduly pro běžné síťové karty.

Příkazem `$ lspci` si můžeme vypsat informace o zařízeních na PCI sběrnici a tak zjistíme i název síťové karty. Například pokud máme síťovou kartu RealTek RTL8139, tak použijeme modul `8139too` nebo když máme síťovou kartu 3com905, použijeme modul `3c59x`.

Pro **ruční zavádění modulů** do paměti se používá příkaz `$ modprobe`. Pro výpis zavedených modulů použijeme `$ lsmod` a pro odstranění modulu z paměti příkaz `$ rmmod`. Pokud je zařízení používáno, nelze modul odstranit a musí nejdříve zařízení deaktivovat příkazem `$ ifconfig eth0 down`.

Jestli bylo ruční přidání modulu úspěšné, zjistíme vypsáním souboru `cat /proc/net/dev`, případně pomocí příkazu `$ dmesg`, který vypíše poslední hlášení jádra Linuxu na obrazovku.

4.2.5 Konfigurace sítě

Dostáváme se k nejdůležitější části a to konfigurace síťového rozhraní pro komunikaci s protokolem TCI/IP. Než ale začneme, potřebujeme znát několik údajů pro připojení do sítě. Ty většinou získáme od správce sítě a nebo mohou být stanicím předány automaticky pomocí protokolu **DHCP** (Dynamic Host Configuration Protocol).

Pro nastavení konfigurace většinou používáme konfigurační nástroje dodávané s tou danou distribucí. My si však ukážeme, jak nastavit systém ručně, zkontrolovat ho nebo najít chybu.

Síťové rozhraní nastavujeme příkazem `$ ifconfig`. Použijeme-li tento příkaz samotný bez dalších parametrů, vypíše se přehled již nastavených síťových rozhraní a jejich parametry. Příkazem `$ route -n` lze zobrazit aktuální směrovací tabulku. Parametr `-n` použijeme pokud chceme místo jmen počítačů vidět IP adresy.

Dejme tomu, že máme od správce sítě údaje pro připojení do sítě.

- IP adresa - 10.0.0.3
- Maska - 255.255.255.0
- Brána - 10.0.0.1

Tak pak pro nastavení síťové karty použijeme následující příkazy.

```
$ 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
```

V prvním řádku nastavujeme speciální rozhraní `lo` (loopback). Jak už jsme si řekli, je povinnou součástí implementace TCP/IP protokolu. Toto rozhraní reprezentuje vždy náš vlastní počítač. Loopback je smyčka a proto se vždy připojíme ke stejnému systému, na kterém pracujeme, pokud se pokusíme s touto adresou spojit.

Deaktivace síťového rozhraní se provádí pomocí příkazu `$ ifconfig eth0 down`. Současně s deaktivací rozhraní jsou odstraněny i příslušné záznamy z směrovací tabulky.

Pokud bychom chtěli místo IP adres používat jména počítačů, je třeba nastavit i **DNS** (Domain Name Server). Nejprve ověříme, zda máme správně nastaveny údaje v několika souborech. Základní soubor pro převod jmen na IP adresy je `/etc/hosts`, ve kterém můžeme vyjmenovat IP adresy a k nim přiřadit odpovídající jména. Do tohoto souboru se vkládají vždy alespoň dva záznamy. Je to adresa loopbacku a vlastní IP adresa počítače. Není-li IP adresa v tomto souboru, snaží se systém získat jméno další dostupným způsobem a to dotazem na **DNS server**.

IP adresu DNS serveru musíme uvést v souboru `/etc/reslov.conf`. Na začátku řádku v souboru je nejprve klíčové slovo, pak mezera a poté příslušná hodnota. Nejčastěji se setkáme s názvy `nameserver`, `domain` a `search`. **Nameserver** definuje IP adresu DNS serveru. Pokud jich chceme uvést více, je třeba zadat více záznamů, každý na jeden řádek. **Domain** určuje doménu, ve které se počítač nachází. **Search** umožňuje předdefinovat seznam domén, ve kterém se bude příslušné jméno počítače hledat. Pokud tedy nelze zadané jméno počítače převést na IP adresu, jsou k němu postupně přidávány záznamy z direktivy search.

Poslední soubor je `/etc/nsswitch.conf`. Na začátku řádku definujeme klíčovým slovem `hosts:` pořadí, ve kterém se bude převod odehrávat. Například, pokud bude soubor obsahovat zápis `hosts: files dns`, tak se převod nejprve provede podle souboru `/etc/hosts` a v případě selhání tohoto pokusu se provede dotaz na DNS server podle údajů v souboru `/etc/resolv.conf`.

4.2.6 Ověření síťové komunikace

Jako první zkontrolujeme připojení do počítačové sítě. Ověříme, jestli je kabel správně zapojen a jestli svítí signalizační diody na síťové kartě. Příkazem `$ ifconfig` zkontrolujeme, zda je správně nastavena IP adresa. Pomocí příkazu `$ route` ověříme správnost záznamů ve směrovací tabulce.

Ping

Jako další krok zkusíme vyslat IP datagram z počítače do sítě a budeme čekat na odpověď. K tomu nám slouží kontrolní **ICMP** (Internet Control Message Protocol) zpráva nazývaná **ping**. Spouští se příkazem `$ ping` a jako parametr jí hlavně předáme IP adresu síťového prvku, na který posíláme paket. Nejčastěji se pokoušíme vyslat IP datagram na bránu v síti. Když jsme úspěšní volíme další

lokality, jako jiný počítač ve stejné síti, IP adresu serveru, DNS serveru pokud je to vzdálený DNS server a nebo až samotnou internetovou adresu vně naší sítě.

Ping zobrazuje jak došlé odpovědi, tak i dobu odezvy a na závěr i statistické údaje. Na rozdíl od Windows příkaz $ ping je prováděn v nekonečné smyčce a zastavíme ho pomocí kombinace kláves CTRL+C.

Příklad použití příkazu `$ ping`.

```
$ ping -c 4 -s 1440 10.0.0.1
----------------------------
PING 10.0.0.1 (10.0.0.1) 1440(1468) bytes of data.
1448 bytes from 10.0.0.1: icmp_seq=1 ttl=225 time=4.58 ms
1448 bytes from 10.0.0.1: icmp_seq=2 ttl=225 time=1.57 ms
1448 bytes from 10.0.0.1: icmp_seq=3 ttl=225 time=1.64 ms
1448 bytes from 10.0.0.1: icmp_seq=4 ttl=225 time=1.60 ms

--- 10.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2998ms
rtt min/avg/max/mdev = 1.574/2.351/4.589/1.293 ms
```

Parametr `-c` nám udává počet opakování a parametr `-s` nám zajistí vysílání delších datagramů než je obvyklé, konkrétně 1 440 B velkých. Můžeme tak ještě lépe otestovat kvalitu sítě a schopnost přenášet i delší zprávy. Hojně se využívá u bezdrátového spojení.

Traceroute

Další nástroj pro ověřování funkčnosti sítě je příkaz `$ traceroute`. Ten zobrazuje všechny routery na cestě k cílovému počítači. Jako parametr mu tedy zadáme nějaký vzdálenější počítač, abychom zjistili, kam až naše spojení se světem funguje. Zápis příkazu může vypadat takto:

```
$ traceroute www.yahoo.com
--------------------------
traceroute to www.yahoo.com (87.248.113.14), 30 hops max, 40 byte packets
 1 10.0.0.1 (10.0.0.1) 1.172 ms 1.870 ms 2.426 ms
 2 ...
```

4.2.7 Samba

Soubory v Unixových systémech, tedy i Linuxu, se sdílejí pomocí **NFS** (Network FileSystem). Ale tento způsob není obvyklý na počítačích s operačním

systémem MS Windows. Mezi těmito počítači se používá **Sdílení v sítích Microsoft**, které je založené na **SMB** (Server Message Block) protokolu. A právě z této zkratky pochází i název **Samba**. Samba je název pro projekt, který umožňuje sdílet soubory umístěné na Linuxovém počítači či serveru takovým způsobem, jako by na něm běžel operační systém Windows.

Konfigurace Samby

Nastavení Samby je uloženo v souboru `/etc/samba/smb.conf`. Soubor se dá upravovat buď ručně, což je docela nepohodlné a nebo pomocí nástroje **Swat** a internetového prohlížeče. Jelikož pracujeme v příkazovém řádku, tak se smíříme s ručním upravováním souboru.

Pokud vypustíme rozsáhlé komentáře, sdílení tiskáren a CD-Romů, mohl by konfigurační soubor vypadat takto:

```
[global]
      workgroup = linux
      guest account = nobody
      keep alive = 30
      os level = 2
      security = share
      printing = bsd
      printcap name = /etc/printcap
      load printers = yes
      character set = ISO8859-2
      client code page = 852
[write]
      path = /home/write
      comment = write
      read only = no
      browseable = yes
      public = yes
      create mode = 0750
```

Nás zajímá hlavně sekce `[write]`. Je to název pro naší sdílenou složku, což můžeme vidět na řádce s parametrem `patch`. Cesta ke sdílené složce je tedy `/home/write`. Parametr `comment` je komentář ke složce, zde je stejný jako název složky. Dále se dozvíme, že složka není jenom pro čtení ale i pro zápis (parametr `read only`) a že jí můžeme libovolně procházet (parametr `browsaeble`). Parametr `public` nám říká, že je to veřejná složka.

5 Praktické příklady pro výuku

V této kapitole se budeme věnovat praktickým příkladům pro výuku v síti, kterou jsme si navrhli v předchozích kapitolách. Popíši zde několik příkladů. První tři příklady však na sebe budou navazovat a naučíme se tak kompletní nastavení sítě. Poté budou následovat cvičné příklady menšího rozsahu, které již budou spíše zaměřené na teoretickou část výuky.

Vždy si uvedeme zadání příkladu. Poté bude následovat jeho řešení a případné upozornění na možné chyby nebo problémy, které mohou s daným příkladem nastat. Příklady se pokusím dostatečně okomentovat, aby byly srozumitelné i pro úplné začátečníky, co se síťové správy týče. K tomu nám také snad pomůže dostatečné množství obrázků, které mnohokrát řeknou více, než stránka textu.

Než se pustíme do řešení, nastíníme si, co nás čeká.

- V prvním příkladu si určíme, jakou IP adresu bude mít náš počítač. Také určíme IP adresy ostatních počítačů v síti a to podle zadaných pravidel.

- Ve druhém příkladě již budeme znát potřebné údaje pro konfiguraci síťové karty. Vyzkoušíme si tedy nakonfigurovat síťový protokol a síťovou kartu v obou operačních systémech.

- V poslední řadě nastavíme switch, tak aby se počítače viděli na síti a vyzkoušíme si nějaké pokusy s omezením přenosových rychlostí, nastavení VLAN a další funkce, co nám switch umožňuje.

5.1 IP adresa a maska sítě pro náš počítač

Na začátek nás čeká nezbytný úkol a to přiřadit každému počítači v síti nějakou tu IP adresu. Připomeňme si, že v síti máme 16 počítačů, které jsou číslované podle řad a pořadí v řadě.

Například počítač ve druhé řadě na třetím místě má identifikační číslo 23 a je připojen ke switchi B. Celé schéma nalezneme v kapitole 2.5.1 Návrh naší sítě a Obrázek 1.

5.1.1 Zadání úlohy

V síti máme 16 počítačů. Přiřaďte počítačům neveřejné IP adresy třídy C, tak abychom měli co největší masku sítě. Adresu sítě zvolte první možnou. Jakou adresu bude mít první a poslední počítač a jaká bude adresa broadcastu?

5.1.2 Řešení úlohy

Jak jsme se již dozvěděli, neveřejné IP adresy ve třídě C mají rozsah od **192.168.x.0 až 192.168.x.255**. Ty se tedy nepoužívají v Internetu a můžeme je právě použít pro naší lokální síť aniž by došlo k nějakým kolizím. Standardní maska pro třídu C je **255.255.255.0**. My si ze voleného rozsahu vybereme první možnou kombinaci a tak dostaneme výchozí adresu **192.168.0.0**.

Pokud si IP adresu a masku sítě napíšeme binárně pod sebe, uvidíme přesně, jaká část je určená pro síť a jaká zbývá na samotné počítače v sítě. Připomeňme si, že jedničky v masce reprezentují síť a nuly počítač.

```
IP adresa D:      192   .  168   .   0    .   0
IP adresa B:    11000000.10101000.00000000.00000000

Maska D:          255   .  255   .  255   .   0
Maska B:        11111111.11111111.11111111.00000000
```

Pozn.: D značí dekadickou soustavu, B značí binární soustavu.

Pro síť máme tedy první tři bajty (24 bitů) podbarvených šedě a poslední bajt (8 bitů) nám zbývá pro počítače. Jelikož jsme v binární soustavě, tak základ je 2. Máme 8 bitů pro počítače, tedy 2^8 je 256 počítačů. V takovéto síti s touto maskou může být 256 počítačů. To není až tak úplně pravda, protože musíme odečíst 2 adresy pro adresu sítě a adresu broadcastu. Zbude nám adresový prostor **254 počítačů**.

Adresa sítě je ta, která v části určené pro počítače má samé nuly (podbarveno šedě). Naopak **adresa broadcastu** má samé jedničky v binárním tvaru.

```
Adresa sítě D:    192   .  168   .   0    .   0
Adresa sítě B:  11000000.10101000.00000000.00000000

Broadcast D:      192   .  168   .   0    .   255
Broadcast B:    11000000.10101000.00000000.11111111
```

Naše síť má ale jen 16 počítačů a tak by nám mohl stačit menší počet bitů. Můžeme se tedy položit otázku, do které mocniny dvojky se vejde 16? Ta se vejde do čtvrté mocniny. $2^4 = 16$ počítačů. Ale jak jsme se dozvěděli před chvílí, musíme odečíst adresu sítě a broadcastu. Tak by nám zbyl prostor pouze pro **14 počítačů** (16 - 2). To je o dva méně, než potřebujeme. Musíme tedy mocninu zvýšit na 5 a tak dostaneme 2^5 kombinací, což je 32 permutací jedniček a nul, pokud se budeme pohybovat v binárních číslech.

Opět odečteme od 32 adresu sítě a broadcastu a dostáváme končený nejnižší adresový prostor pro **30 počítačů**, tedy i pro našich 16 počítačů v síti.

V takovémto případě můžeme posunout masku sítě o 3 bity doprava. Rozdíl opět vidíme na šedě podbarvených částech.

```
Původní maska D:   255   .  255   .  255   .   0
Původní maska B: 11111111.11111111.11111111.00000000

Nová maska D:      255   .  255   .  255   .  224
Nová maska B:    11111111.11111111.11111111.11100000
```

Nová maska sítě tedy je **255.255.255.224** a říká nám, že v síti může být 30 počítačů.

A pokud si zvolíme první možnou adresu sítě **192.168.0.0**, tak první počítač bude mít IP adresu **192.168.0.1** a poslední 16. počítač bude mít IP adresu **192.168.0.16**. Adresa broadcastu bude **192.168.0.32**.

```
Adresa síťe D:    192   .  168   .   0    .   0
Adresa síťe B:  11000000.10101000.00000000.00000000

Broadcast D:      192   .  168   .   0    .   32
Broadcast B:    11000000.10101000.00000000.00011111

Adresa PC11 D:    192   .  168   .   0    .   1
Adresa PC11 B:  11000000.10101000.00000000.00000001

Maska PC11 D:     255   .  255   .  255   .  224
Maska PC11 B:   11111111.11111111.11111111.11100000
```

Masku sítě můžeme také zapisovat jako dekadické číslo za IP adresu. První počítač by tedy měl adresu s maskou **192.168.0.1/27**. Číslo 27 značí počet bitů pro síť z IP adresy.

5.2 Konfigurace síťové karty a protokolu

Abychom mohli provádět konfiguraci síťových prvků, musíme znát údaje které budeme nastavovat. V předchozím příkladě jsme si spočítali IP adresu počítače a jeho síťovou masku. K úplnosti nám ještě chybí výchozí brána pro počítač a případné adresy DNS serverů.

5.2.1 Zadání úlohy

Nakonfigurujte síťový protokol TCP/IP, tak aby odpovídal následujícím údajům.

- Název počítače: PC14
- Pracovní skupina: HOME
- IP adresa počítače: 192.168.0.4
- Maska sítě: 255.255.255.224
- Výchozí brána: 192.168.0.1
- DNS server: 192.168.0.1

Konfiguraci si vyzkoušejte jak v operačním systému Windows, tak i Linux. Podmínkou je samozřejmě, mít správně nainstalovanou síťovou kartu.

5.2.2 Řešení úlohy pro Windows

Kontrola ovladačů síťové karty

Nejprve se tedy přesvědčíme, zda je síťová karta správně nainstalována. To provedeme tak, že si otevřeme okno *Vlastnosti systému*. To můžeme udělat několika způsoby.

- Buď ťukneme pravým tlačítkem myši na *Tento počítač* a zvolíme položku *Vlastnosti*.

- Nebo přes tlačítka *Start* - *Nastavení* - *Ovládací panely* si otevřeme okno *Ovládací panely* a zde volíme ikonku *Systém*.

- Nebo poslední možnost, která je nejjednodušší, že stiskneme kombinaci kláves Levý WIN + Pause/Break.

Pokud na ploše nemáme ikonky *Tento počítač* a *Místa v síti*, tak si je tam přidáme následujícím způsobem. Budeme je i dále potřebovat. Na ploše stiskneme pravým tlačítkem a dáme *Vlastnosti*, zde si vybereme záložku *Plocha*, stiskneme tlačítko *Vlastní nastavení plochy*. V záložce *Obecné* a rámečku *Ikony* na ploše zatrhneme položky *Tento počítač* a *Místa v síti* a vše potvrdíme *OK*.

Nyní jsme ve *Vlastnostech systému* a přepneme se na záložku *Hardware*. V rámečku *Správce zařízení* ťukneme na tlačítko *Správce zařízení*. Dostaneme se tak do okna *Správce zařízení*, kde můžeme vidět veškerý hardware nainstalovaný v počítači.

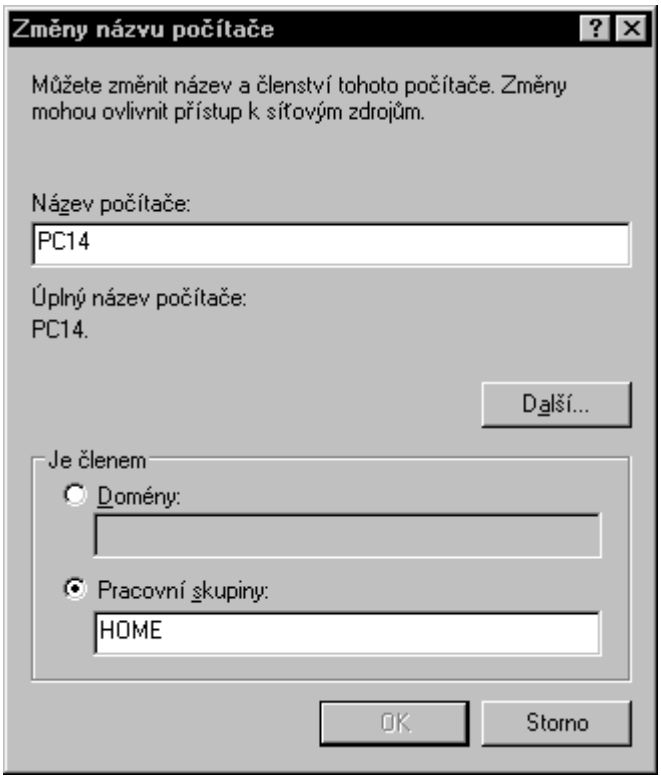
Obrázek 12 - Okno Správce zařízení

Pokud si rozbalíme *Síťové adaptéry,* můžeme vidět naší nainstalovanou síťovou kartu. Pokud u ní není nakreslena žádná značka, vše je v pořádku. Pokud by u ní byl červený křížek, tak je v systému zakázaná. To může být z několika důvodů. Můžeme tak mít nastaven hardwarový profil nebo třeba mít síťovou kartu zakázanou v **BIOS**u (Basic Input Output System).

Pokud by u ní byl zobrazen černý vykřičník ve žlutém kolečku, znamená to, že nemáme nainstalované ovladače nebo jsou nainstalované ovladače s chybou. Například když použijeme ovladače od jiné síťové karty, která není s tou naší kompatibilní.

Změna názvu počítače a pracovní skupiny

Pokud je vše v pořádku, můžeme okno zavřít a vrátit se do *Vlastností systému*. Zde se přepneme do záložky *Název počítače*. Zde můžeme vyplnit *Popis počítače*, ale ten pro nás není důležitý. Poté ťukneme na tlačítko *Změnit...* a objeví se nám okno *Změny názvu počítače*. Tady do *Názvu počítače* vyplníme **PC14**. V rámečku *Je členem* a políčku *Pracovní skupiny* vyplníme **HOME**. Potvrdíme vše *OK*.



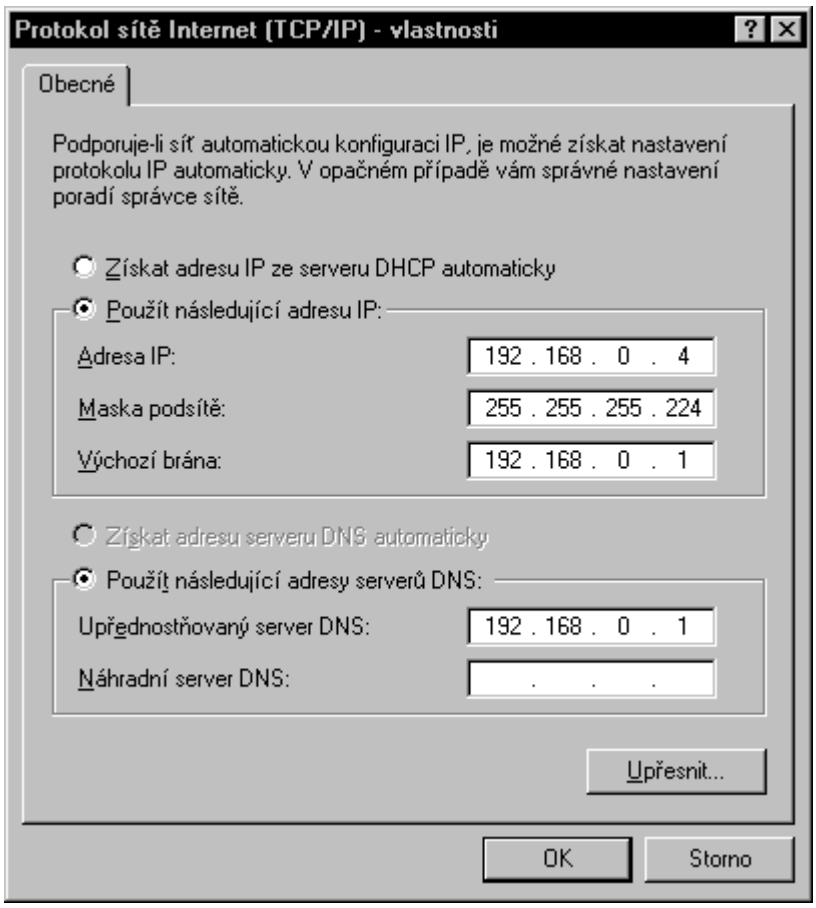
Obrázek 13 - Změny názvu počítače

Nastavení vlastností protkolu TCP/IP

Stiskneme pravým tlačítkem na *Místa v síti* a vybereme *Vlastnosti*. Otevře se nám okno *Síťová připojení*. Druhý způsob je možný opět přes *Ovládací panely* a ikonu *Síťová připojení*. Nalezneme zde ikonu *Připojení k místní síti*. Těchto ikon zde může být více, podle počtu sítových karet v systému. Vybereme si tu, která patří k síťové kartě, kterou chceme konfigurovat a opět přes pravé tlačítko dáme *Vlastnosti*. Otevře se nám okno *Připojení k místní síti - vlastnosti*. Nás zajímá

prozatím záložka *Obecné* a v ní vidíme nejméně jednoho klienta. To jsme si již popsali v kapitole 4 Softwarové vybavení učebny.

My se ale zaměříme na položku *Protokol sítě Internet (TCP/IP)*. Označíme si ho a ťukneme na tlačítko *Vlastnosti*. Konečně se dostáváme do okna, kde nás čeká již samotná konfigurace protokolu. Okno se jmenuje *Protokol sítě Internet (TCP/IP) - vlastnosti*. Jediná záložka *Obecné* nám nabízí dva rámečky. První se nás ptá, jestli chceme získat adresu IP se serveru DHCP automaticky a nebo jestli chceme použít následující IP adresu.



Obrázek 14 - Vlastnosti TCP/IP protokolu

Vybereme *Použít následující adresu IP* a můžeme začít s vyplňováním naši údajů. Do políčka *Adresa IP* zadáme **192.168.0.4**, do *Maska podsítě* vložíme **255.255.255.224** a do *Výchozí brány* zadáme **192.168.0.1**.

Ve druhém rámečku volíme *Použít následující adresy serverů DNS* a vyplníme *Upřednostňovaný server DNS* hodnotou **192.168.0.1**.

Pokud ťukneme na tlačítko *Upřesnit*, můžeme přidávat další IP adresy, brány a DNS servery. To se hodí pokud například počítač připojujeme často do jiných sítí a systém si pak volí vhodné hodnoty, podle toho v jaké je síti.

My ale všechno potvrdíme tlačítkem OK a máme konfiguraci hotovou. Pokud máme nakonfigurován i další počítač v síti, můžeme ověřit spojení v síti pomocí příkazu `ping` v *Příkazové řádce*.

5.2.3 Řešení úlohy pro Linux

Kontrola ovladačů síťové karty

Pomocí příkazu `$ lspci` zkontrolujeme jestli systém nalez síťovou kartu a příkazem `$ cat /proc/net/dev` zjistíme, jestli jí bylo přiřazeno síťové rozhraní. Ještě můžeme zkontrolovat, jestli se v systému nachází modul naší síťové karty pomocí příkazu `$ lsmod`, ale není to nutné, protože Linux se stará o zavádění modulů při startu systému. Další kontrolu můžeme provést příkazem `$ dmesg`, ten nám vypíše poslední hlášení jádra.

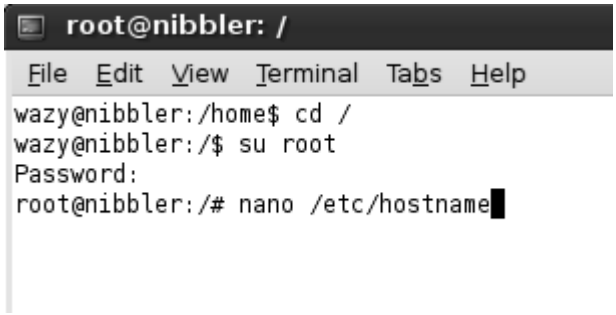
Příkaz **`$ cat`** čte textové soubory, které mu předáme jako parametr.

Změna názvu počítače

Abychom změnili název počítače v distribuci Debian, musíme změnit dva textové soubory a to **`hostname`** a **`hosts`**. Oba soubory jsou v adresáři `/etc` a tak musíme být přihlášeni jako **root**. Pracovní skupina v tomto systému nemá význam.

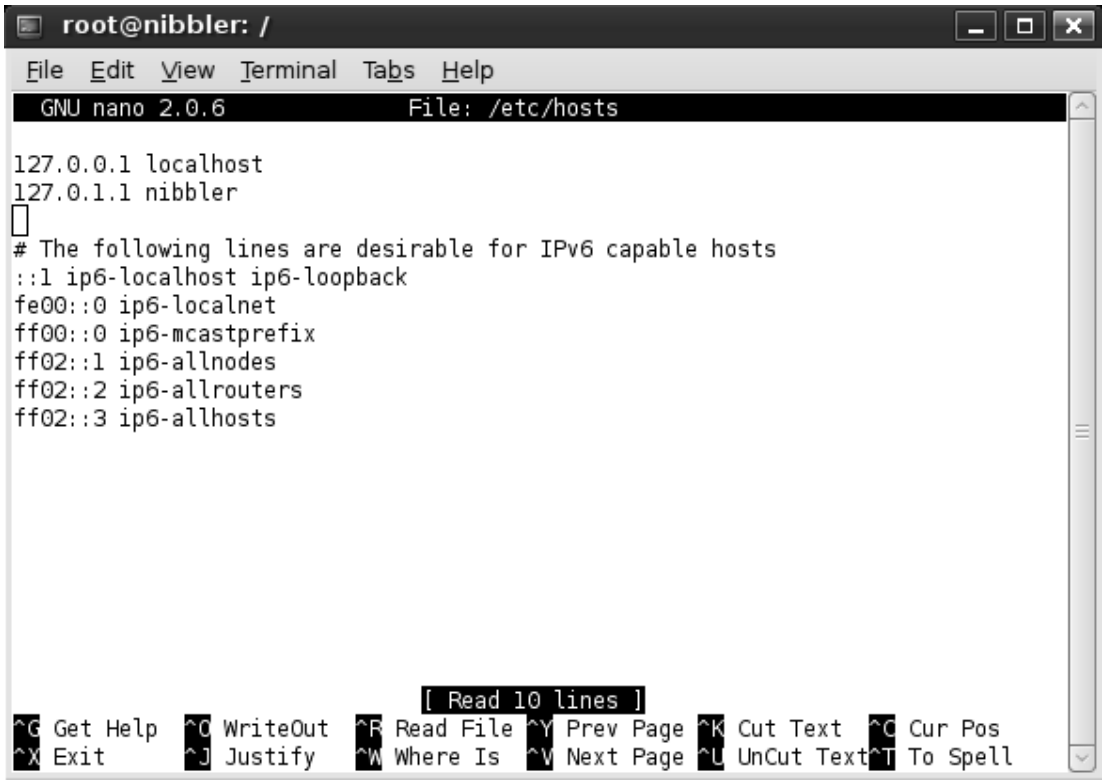
V shellu tedy zadáme příkaz `$ cd /`, ten nás přesune ve stromové struktuře do kořenového adresáře celého systému. Nyní se musíme přepnout do superuživatelského účtu. To provedeme příkazem `$ su root` a budeme vyzváni k zadání rootovského hesla.

Po správném vyplnění hesla již pracujeme v systému jako root a proto musíme být velmi opatrní a každou změnu v systému dobře uvážit.



Obrázek 15 - Zápis příkazů v shellu

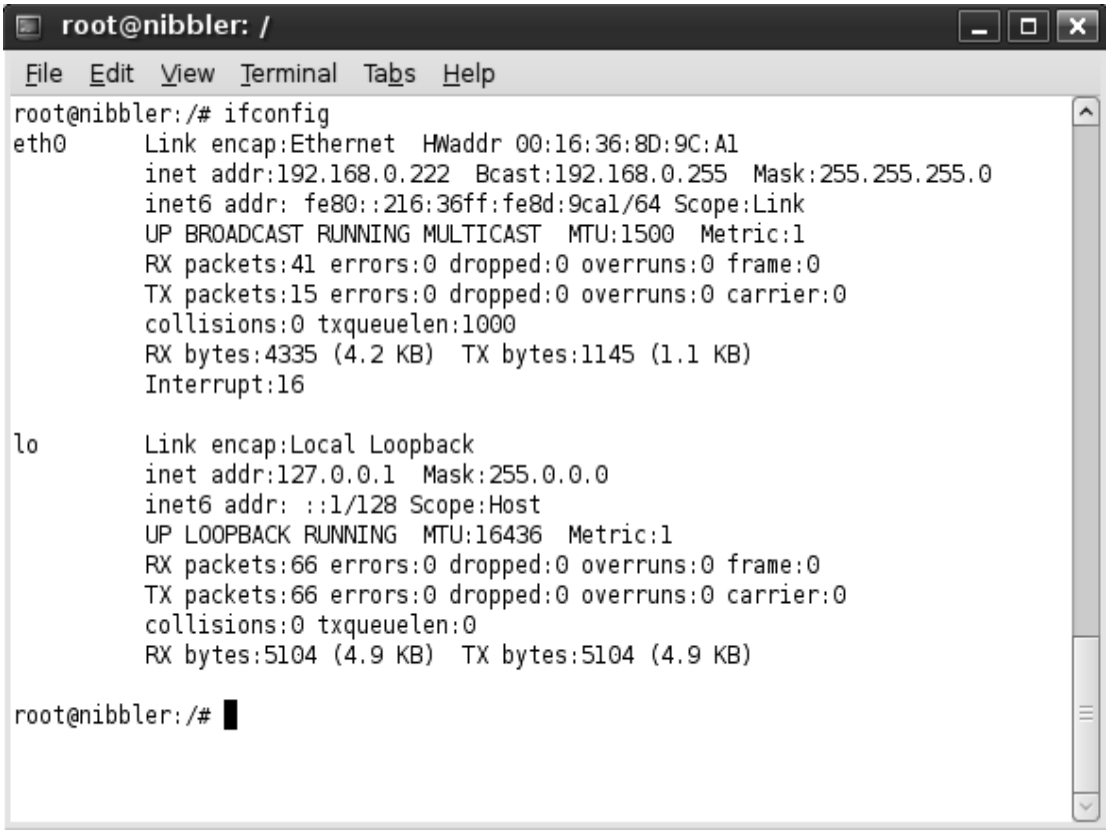
Na editaci textových souborů budeme používat program **nano**. Zadáme tedy příkaz `$ nano /etc/hostname` a otevře se nám uživatelské prostředí daného editoru. Přepíšeme původní název počítače na náš nový název **PC14** a pomocí klávesové kombinace Ctrl + O a následným stiskem klávesy ENTER soubor uložíme. Editor `nano` zavřeme kombinací kláves Ctrl + X. Totéž zopakujeme se souborem `/etc/hosts`, kde změníme jméno ve druhém řádku.



Obrázek 16 - Obsah souboru hosts

Nastavení vlastností protkolu TCP/IP

Konfiguraci síťového rozhraní provádíme příkazem `$ ifconfig` s různými parametry. My ale tento příkaz nejprve použijeme bez parametrů a tak se nám vypíšou aktivní síťová rozhraní. Můžeme vidět, že již máme dvě síťová rozhraní nastavená. Ukončit je můžeme příkazem `$ ifconfig eth0 down` a `$ ifconfig lo down`.



Obrázek 17 - Výpis příkazu $ ifconfig

Nastavení provedeme následujícími příkazy:

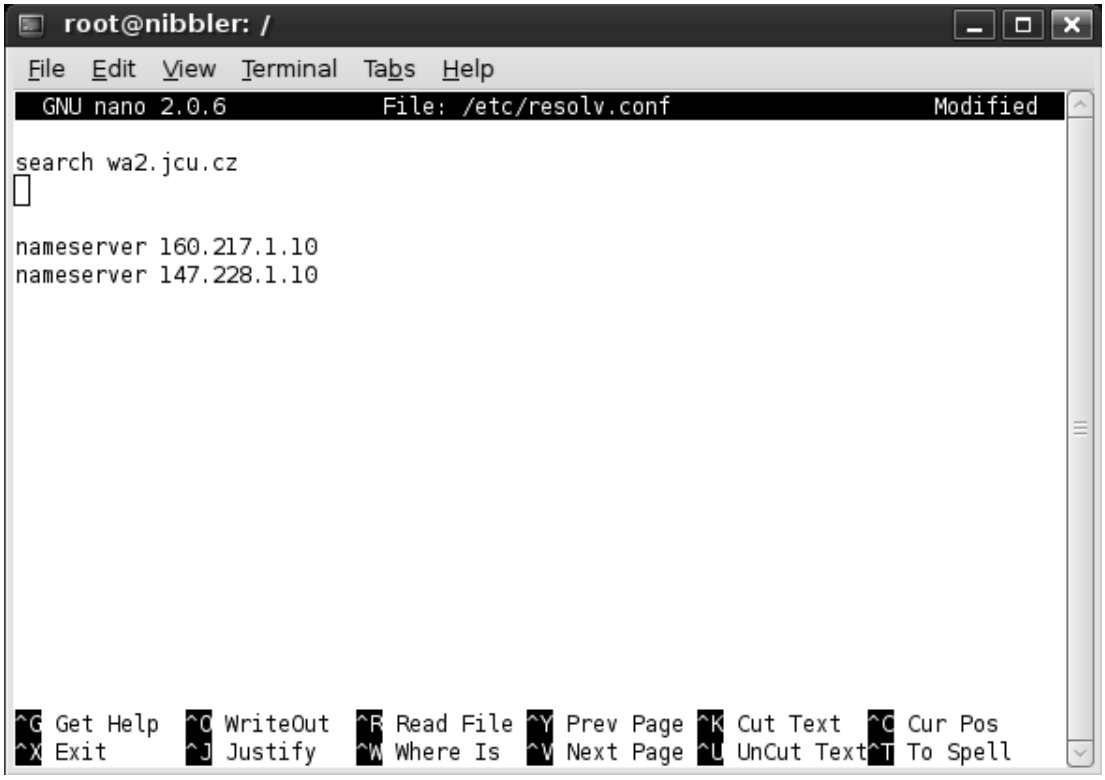
```
$ ifconfig lo 127.0.0.1 netmask 255.0.0.0 broadcast 127.255.255.255

$ ifconfig eth0 192.168.0.4 netmask 255.255.255.224 broadcast 192.168.0.32

$ route add default gw 192.168.0.1
```

První řádek nastavuje smyčku loopback. Na druhém řádku nastavíme IP adresu **192.168.0.4** síťovému rozhraní `eth0`, masku podsítě **255.255.255.224** a broadcast v síti. Třetí řádek nastavuje výchozí bránu pro počítač **192.168.0.1**.

Ještě nám zbývá nastavit DNS server. To provedeme změnou souboru `/etc/resolv.conf`. Postup je obdobný jako při změně jména počítače. Opět musíme být režimu root a příkazem `$ nano /etc/reslov.conf` editujeme textový soubor. Vyhledáme v něm řádek začínající `nameserver` a napíšeme za něj náš DNS server **192.168.0.1**. Řádek v souboru nemusí být vůbec, tak ho tam nově vytvoříme. Nakonec soubor uložíme.



Obrázek 18 - Obsah souboru resolv.conf

Alternativní nastavení vlastností protkolu TCP/IP

Ještě bych chtěl podotknout, že příkaz $ ifconfig je už starší a dnes je nahrazován příkazem $ ip. Zápis příkazu ip se poněkud liší a tak uvádím i zápis této alternativy.

```
$ ip address add 192.168.0.4/27 brd + dev eth0

$ ip link set eth0 up

$ ip route add default via 192.168.0.1
```

Prvním řádkem nastavíme IP adresu, masku a broadcast. Druhý řádek nám toto rozhraní zapne a na třetím řádku nastavíme výchozí bránu.

Všechna takto provedená nastavení jsou platná do restartu stroje. Má-li být nastavení trvalé, musíme přímo editovat soubor `/etc/rc.d/rc.inet1.conf` a `/etc/hostname`.

5.3 Nastavení VLAN sítí na switchi ASUS

Nyní když máme připravené počítače na propojení v síti, tak nám zbývá nastavit samotný switch, kterým jsou jednotlivé stanice propojené. Berme v úvahu, že síťová kabely jsou již správně zapojeny a síťové protokoly v počítačích správně nastaveny.

Pracovat budeme se switchem **ASUS GigaX 1024i**. Anglický manuál je přiložen k této práci jako příloha.

5.3.1 Zadání úlohy

Vyvolejte restart switche do továrního nastavení a poté nastavte heslo ze základního 0x2379 na 0x1234. Počítače PC11 a PC12 propojte v jedné virtuální síti VLAN#01 a počítače PC13 a PC14 propojte do druhé virtuální sítě VLAN#02. Uložte nastavení konfigurace switche do souboru.

5.3.2 Řešení úlohy

Berme v úvahu, že již máme počítače propojené se switchem a na počítači, ze kterého budeme konfigurovat switch máme připravený i software, který slouží ke konfigurace switche.

Dejme tomu, že budeme pracovat na počítači **PC11**. U switche ASUS GigaX 1024i je to software **CNM** (Centralized Network Management) a musí být nainstalován v operačním systému Windows XP. Počítače se switchem musí být v jedné síti.

Restart switche

Pokud chceme switch z nějakého důvodu nastavit do výchozí konfigurace switche, musíme učinit několik následujících kroků.

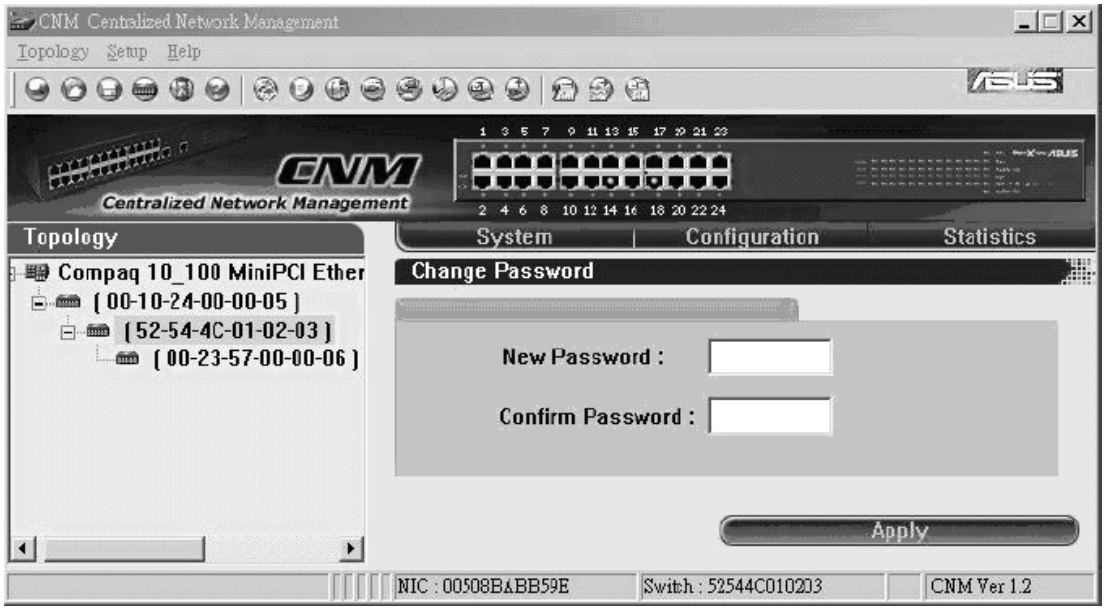
- Odpojíme všechny síťové kabely ze switche a připravíme si jeden patch kabel.
- Switch vypneme a opět zapneme.
- Během 20 vteřin po zapnutí switche musíme propojit port 1 a port 2 připraveným patch kabelem. Vytvoříme tak smyčku mezi těmito porty.
- Aby došlo k restartu switche musíme takto propojené porty nechal po dobu kolem jedné minuty.
- Pak teprve bude bude konfigurace switche nastavena na tovární hodnoty.
- Nakonec odpojíme patch kabel a opět vypneme a zapneme switch. Nyní již můžeme switch spravovat se základním heslem, které je **0x2379**.

Pokud bychom chtěli restartovat pouze heslo, tak zvolíme stejný postup, pouze s tím rozdílem, že patch kabelem propojíme port 3 a port 4.

Nastavení hesla

Na počítači **PC11** si pustíme z plochy CNM. První co musíme udělat je vyplnit základní heslo 0x2379. Prefix 0x značí, že jde o hexadecimální číslo a tak do políčka vypíšeme pouze **2379**.

Pokud se zdaří přihlášení na switch, přepneme se do záložky `System`. Zde vybereme `Change Password`. Vyplníme dvakrát nové heslo **0x1234** a stiskneme `Applay`. Budeme dotázáni dialogovým boxem, zda si přejeme uložit naší topologii sítě. Tu vidíme v levém rámci. Opět potvrdíme a změna hesla je dokončena.



Obrázek 19 - Změna hesla v CNM

Nastavení VLAN sítí

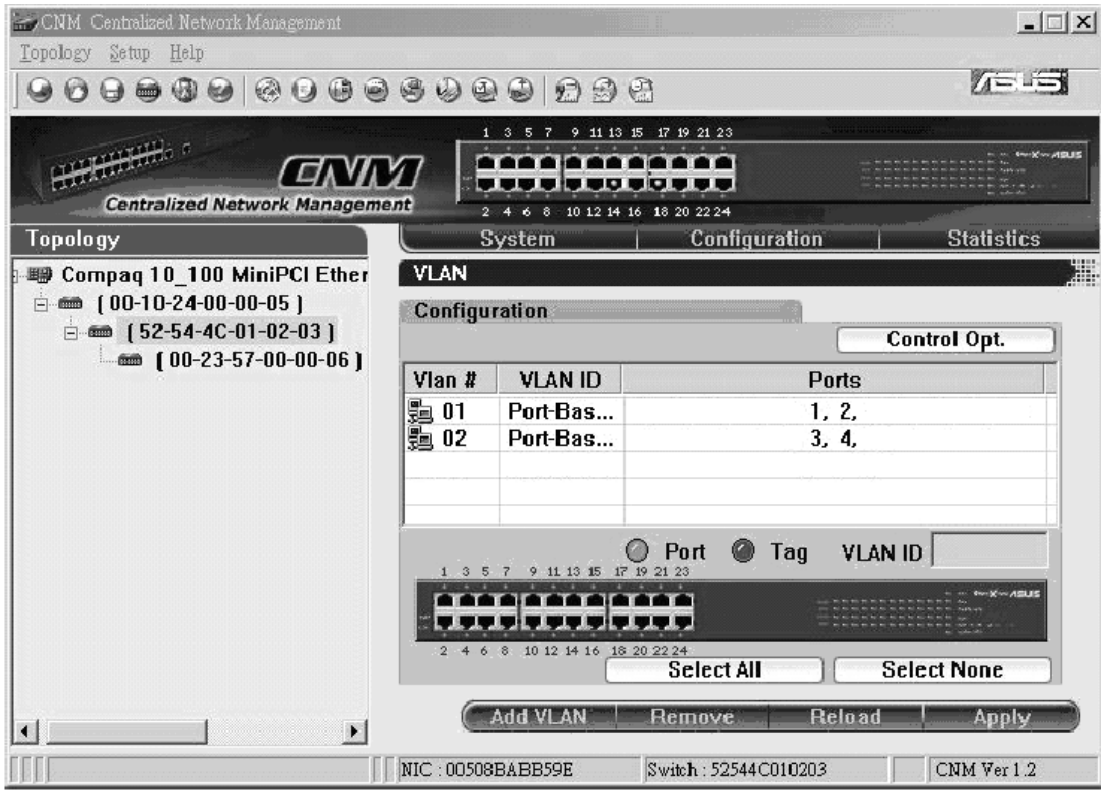
Pokud jsme tak ještě neučinili, propojíme zbylé počítače **PC12**, **PC13** a **PC14** se switchem. Můžeme použít například porty 1, 2, 3 a 4.

Nastavení VLAN se provádí v záložce `Configuration`. VLAN je jednoduše konfigurovatelný a dovoluje administrátorovi oddělit jednotlivé sítě mezi sebou. Postupovat budeme následovně.

- Vybereme tedy, že chceme konfigurovat VLAN.
- VLAN bude založená na portech. Označíme tedy tlačítko `Port`.
- Na obrázku switche označíme porty, které chceme přidat do první sítě VLAN#01.
- Označíme tedy `port 1` a `port 2`.
- Poté ťukneme na tlačítko `Add VLAN`, které VLAN síť přidá do tabulky VLAN sítí.

- Pokud chceme vytvořit síť VLAN#02, tak zopakujeme dva předešlé kroky.

- Nakonec stiskneme tlačítko Apply, kterým potvrdíme konfiguraci.



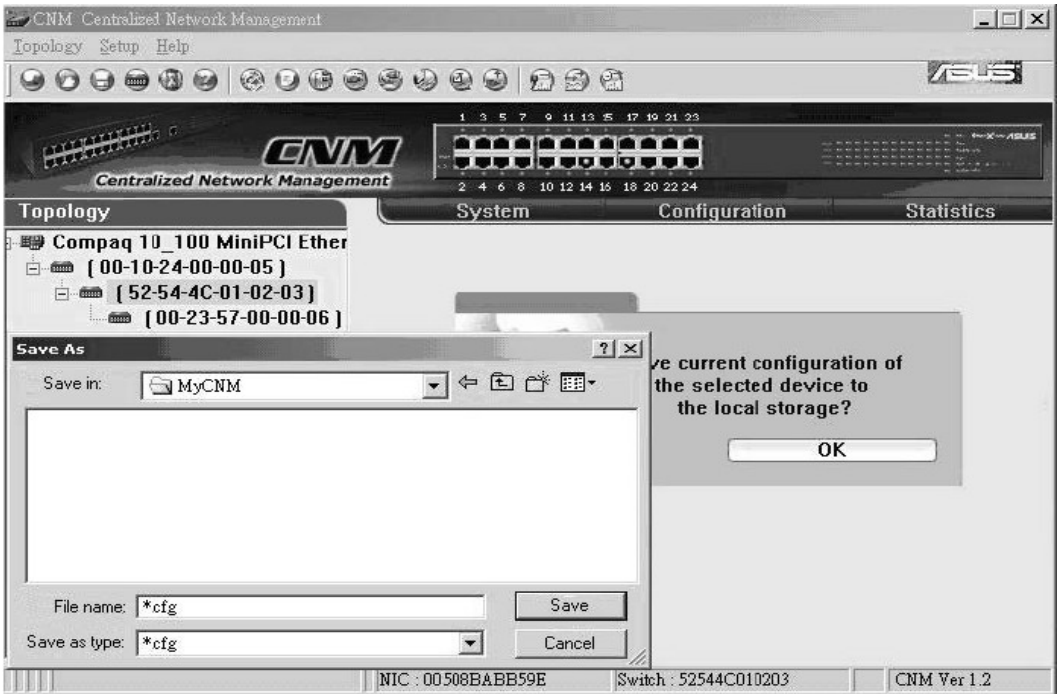
Obrázek 20 - Konfigurace VLAN sítí v CNM

Jak můžeme vidět i na obrázku 20, je zde ještě důležité tlačítko `Control Opt.`, kterým se provádí další nastavení VLAN sítí. Tyto nastavení platí pro všechny nakonfigurované sítě. Pokud otevřeme `VLAN Control Options` okno, tak na prvním místě můžeme vidět položku `VLAN function`. Tu musíme přepnout na `Enable`, aby nám sítě fungovaly a potvrdíme tlačítkem `Apply`. Ostatníma položka se prozatím zabývat nebudeme.

Obrázek 21 - Volby pro sítě VLAN

Uložení nastavení konfigurace switche do souboru

Přepneme se zpět do záložky `System` a volíme `Save`. Přes dialogové okno si vybereme kam soubor s uloženou konfigurací uložíme. Potvrdíme tlačítkem `Save`.



Obrázek 22 - Uložení nastavení switche do souboru

Takto uloženou konfiguraci si můžeme v budoucnu kdykoliv zase načíst. Tím jsme ukončili práci se switchem a můžeme začít s pokusy pomocí příkazu `ping`, jestli se vidí počítač PC11 s počítačem PC13 atd. Příkaz `ping` by mohl vypadat následovně: `ping -t 192.168.0.3`.

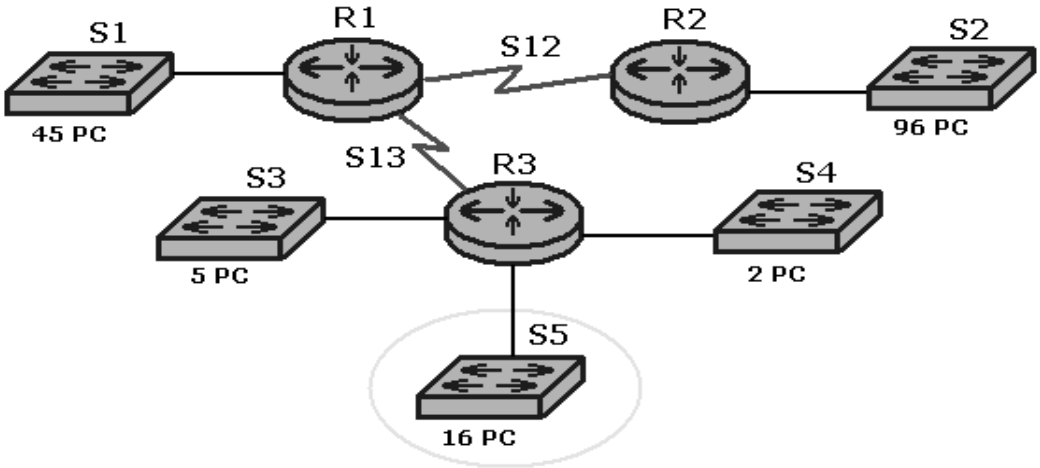
Manuál ke Switchi ASUS GigaX 1024i je přiložen k této práci jako elektronická příloha v podobě PDF na CD.

5.4 Výpočet proměnné délky síťové masky

Proměnná délka síťové masky **VLSM** (Variable Lenght Subnet Mask) je metoda pro přidělování IP adres a to takovým způsobem, aby byl co nejlépe využitý adresový prostor. Docílíme toho tak, že pro jednotlivé sítě budeme měnit jejich délku masky a to na základě jejich rozsahu.

Abychom mohli používat VLSM technologii musí routery v síti umět pracovat se směrovacími protokoly OSPF (Open Shortest Path First), EIGRP (Enhanced Interior Gateway Routing Protocol), RIPv2 (Routing Information Protocol) a IS-IS (Intermediate System to Intermediate System). V naší síti routery nemáme obsaženy a tak příklad probereme pouze teoreticky.

5.4.1 Zadání úlohy



Obrázek 23 - Schéma propojení sítí

Pozn.: Písmeno „S“ značí síť a „R“ označuje router. Routery se starají o směrování paketů a případný překlad adres.

Dejme tomu, že naše počítačová síť o 16 stanicích je připojena na jeden ze tří routerů podle obrázku 23.

Navrhněte optimální adresování s proměnnou délkou masky pro všechny sítě a určete IP adresy pro počítače v naší síti S5. Rozsah adres od poskytovatele je **192.168.11.0/24** a žádné adresy zatím nebyli přiděleny.

5.4.2 Řešení úlohy

Ke správnému návrhu adresování sítě musíme znát počet podsítí a minimální počet bitů, které potřebujeme na adresování stanic v každé podsíti. Z obrázku 23 je vidět je **podsítí je 7** (S1, S2, S3, S4, S5, S12, S13).

S počtem bitů určujícím stanici jsme se již setkaly v první úloze. Tak již jen krátce. Naše síť má 16 stanic, to je čtvrtá mocnina dvou. Ale když započítáme ještě adresu podsítě a její broadcast, tak nám již rozsah nestačí a musíme volit mocninu o jedničku vyšší, tedy 5. Adresový prostor tedy bude **32 IP adres pro síť S5**.

Zde si ale ještě musíme uvědomit, že musíme vyšetřit jednu IP adresu pro samotný router. Podíváme-li se na síť S4, která má 2 stanice, tak bychom mohli učinit závěr, že by nám měl stačit rozsah adres $2^2 = 4$. Ale po přičtení adres pro síť, broadcast a rozhraní routeru, se nám požadovaný rozsah zvýšil až na **5 IP adres pro síť S4**. A tak volíme rozsah 8 IP adres, tedy 2^3. Obdobně postupujeme i u dalších sítí.

Podsíť	Rozsah
S1	64 (2^6)
S2	128 (2^7)
S3	8 (2^3)
S4	8 (2^3)
S5	32 (2^5)
S12	4 (2^2)
S13	4 (2^2)
Celkem	**248**

Tabulka 5 - Podsítě a jejich adresový rozsah

Celkový rozsah, který požadují sítě dohromady je **248 IP adres**. Pokud by počet překročil 256 adres, již by nemohlo dojít ke správnému rozdělení adres pro podsítě, jelikož poskytovatel nám dal prostor právě pro 256 IP adres. To plyne ze zadané adresy a masky **192.168.11.0/24**.

Bez použití metody VLSM

Pokud bychom v našem případě nemohli využít proměnnou délku masky dostali bychom se do velkých problémů. Maska bez použití VLSM musí být konstantní a počet bitů pro lokální část je 8 bitů (1 bajt). Můžeme tedy vytvořit pouze jednu síť o rozsahu 256 IP adres, tedy 253 počítačů. Tu bychom například mohli využít pro největší síť S2, ale zbylé sítě bychom již nemohli realizovat.

Pro více sítí tedy využijeme metodu VLSM.

S použitím metody VLSM

U konstantní masky v předchozím případě jsme měli jeden blok o dané velikosti, určený pro počítače. Pokud použijeme VLSM, můžeme si těchto bloků vytvořit hned několik a jejich velikost se může lišit. Bloky se ovšem nesmí překrývat a tak zajistíme, že každý počítač bude mít unikátní IP adresu.

Na největší rozsah 128 IP adres sítě S2 musíme použít 7 bitů pro lokální část adresy. Můžeme tedy posunout masku o jeden bit doprava a tak nám vznikne adresa sítě **192.168.11.128/25 pro síť S2**. Síťová maska nám tedy určuje rozsah adres **192.168.11.128 až 192.168.11.255**. A jeden bit nám bude určovat **počet sítí 2**. Máme dvě stejně velké sítě o rozsahu 128 adres.

```
První síť D:        192   .  168   .   11   .   0
První síť B:     11000000.10101000.00001011.00000000

Druhá síť D:        192   .  168   .   11   .   128
Druhá síť B:     11111111.10101000.00001011.10000000

Maska D:            255   .  255   .  255   .   128
Maska B:         11111111.11111111.11111111.10000000
```

První z těchto sítí můžeme použít pro další sítě. Její rozsah adres je 192.168.11.0 až 192.168.11.127.

V dělení pokračujeme obdobně jako u sítě S2 s tím rozdílem, že nyní začínáme s maskou 25. Druhá největší síť je S1 s rozsahem 64 adres. Potřebujeme tedy 6 bitů. Máme jich ale 7 k dispozici, tak opět jeden bit můžeme uvolnit na určování podsítí. Adresa sítě **S1 je 192.168.11.64/26**. Zbytek použijeme pro další dělení.

```
První síť D:       192   .  168   .   11   .   0
První síť B:    11000000.10101000.00001011.00000000

Druhá síť D:       192   .  168   .   11   .   64
Druhá síť B:    11111111.10101000.00001011.01000000

Maska D:           255   .  255   .  255   .   192
Maska B:        11111111.11111111.11111111.11000000
```

Přichází na řadu naše síť S5, protože je další největší. Požaduje 32 adres tedy 5 bitů na adresaci. Pro adresování máme 6 bitů a tak nám opět jeden zbude na podsítě. V posledním bajtu tedy bude binárně 001xxxxx pro síť a 000xxxxx pro zbytek sítí. Přepsáno do dekadické podoby má **S5** adresu **192.168.11.32/27**.

Rozsah adres pro naší síť **S5** je tedy 1**92.168.11.32/27 až 192.168.11.63/27**. Pro počítače použijeme například IP adresy 192.168.11.33 až 192.168.11.49.

Následují dvě stejně velké sítě S3 a S4, každá o rozsahu 8 adres. Stačí jim tedy pouhé 3 bity na adresaci. K dispozici teď ovšem máme o 2 bity více. Na podsítě nám tedy nezbývá jeden, ale dva bity. A to se nám teď velmi hodí, jelikož potřebujeme jednu adresu na další podsítě a dvě adresy pro sítě S3 a S4.

Nastává nám tedy nová situace. Máme čtyři kombinace binárních prefixů pro sítě a to 00000xxx, 00001xxx, 00010xxx a 00011xxx.

```
První síť D:       192   .  168   .   11   .   0
První síť B:    11000000.10101000.00001011.00000000

Druhá síť D:       192   .  168   .   11   .   8
Druhá síť B:    11111111.10101000.00001011.00001000

Třetí síť D:       192   .  168   .   11   .   16
Třetí síť B:    11000000.10101000.00001011.00010000
```

```
Čtvrtá síť D:       192   .  168   .   11   .   24
Čtvrtá síť B:    11111111.10101000.00001011.00011000

Maska D:            255   .  255   .  255   .  248
Maska B:         11111111.11111111.11111111.11111000
```

Například třetí síť bude **S3** s rozsahem **192.168.11.16/29 až 192.168.11.23/29** a čtvrtá síť bude **S4** s adresami **192.168.11.24/29 až 192.168.11.31/29**. Druhá síť zůstane nepřidělena. Adresy 192.168.11.8/29 až 192.168.11.16/29 zůstanou nevyužity.

Zbývají nám dvě malé podsítě, které slouží k propojení rozhraní routerů. Postup je stejný jako předchozí se dvěma stejně velkými sítěmi. U každé potřebujeme 2 bity a máme k dispozici ještě 3 bity z první sítě výše. Kombinace jsou následující 00000000, 00000001, 00000010 a 00000011. Použijeme například dvě poslední a adresy tedy budou **192.168.11.2/30 pro S12** a **192.168.11.3 pro S13/30**.

5.4.3 Alternativní řešení pomocí čtverců

Jednotlivé bloky přiřazené jednotlivým sítím může znázornit i graficky. Přináší to větší přehlednost a také se dá celý návrh adresace udělat pomocí této metody dělení čtverců. Celý čtverec má rozměry 16x16 a tak se tam vejde všech 256 možných IP adres. Takto by vypadal čtverec rozdělený podle našeho zadání.

Obrázek 24 - Metoda VLSM pomocí čtverců

5.5 Fragmentace IP datagramu

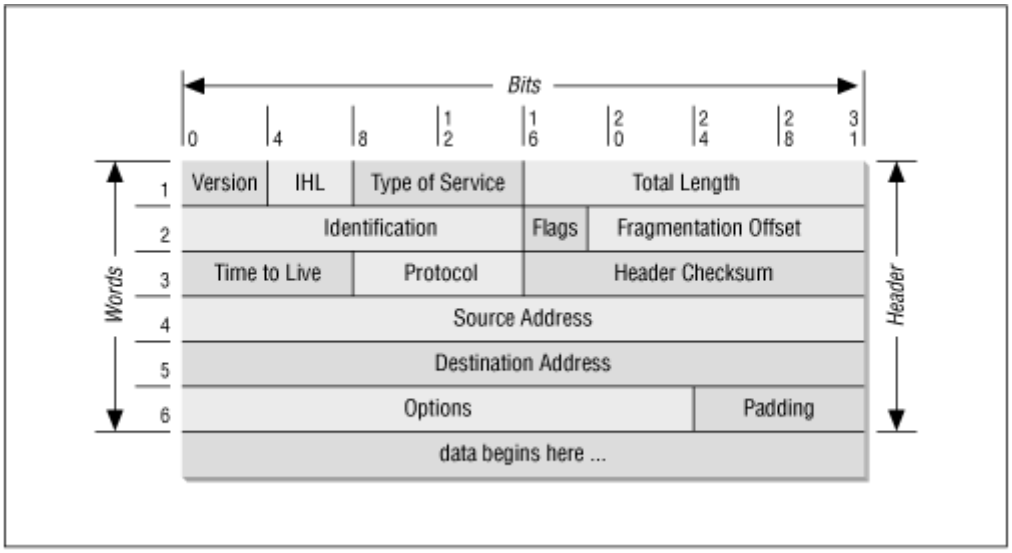
Fragmentace IP datagramu obecně

Než se pustíme do fragmentace, budeme potřebovat trochu teorie, abychom úlohu mohli vyřešit. Fragmentace je rozdělení datagramu na několik částí. Datagram rozdělujeme podle parametru **MTU** (Maximum Transmission Unit) pro danou síť. MTU nám udává maximální velikost paketu, kterou je síť schopna akceptovat a pustit paket dále do sítě. Proto paket musí mít maximální velikost takovou, aby byla rovna nebo byla menší než nejnižší MTU v celé síti, kudy bude paket procházet.

IP (Internet protokol)

Pakety jsou spojené s Internet protokolem, který najdeme na 2. síťové vrstvě TCP/IP modelu. Je založen na architektuře, která je nespolehlivá a nespojovaná. Spolehlivý přenos dodává až TCP na vyšší 3. transportní vrstvě TCP/IP modelu. Nespojovaný znamená, že není jenom jedna linka pro různé části datagramu v různý čas a tak každý paket je směrován nezávisle. **Účel protokolu** IP je směrovat pakety v sítích. Definovat datovou přenosovou jednotku a její strukturu. Také dává pravidla pro routery jak přenášet datagram.

Formát IP datagramu



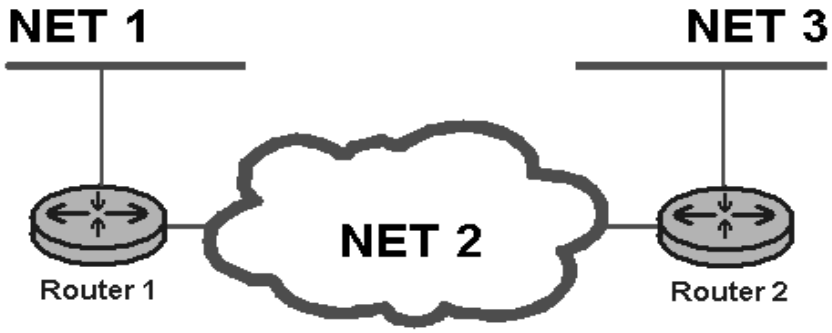
Obrázek 25 - Obsah IP datagramu

- **Header** – hlavička – minimální velikost 20B
- Version – číslo verze IP (binarně 0100 pro verzi 4)
- IHL - Header Lenght – délka hlavičky (min 20B = 5x32 bitů, max. 60B = 15x32 bitů, běžně 24B)
- Type of service – typ služby => určí jak použít datagram
- Total lenght – celková délka včetně záhlaví
- Identification – identifikace – unikátní číslo, které pomáhá při sestavování datagramu (fragmentaci)
- Flags - příznaky – M x D, kde M = more fragment a D = don't fragment
  a) pokud se M = 1, tak víme, že následují další fragmenty
  b) pokud se D = 1, tak víme, že je zákaz další fragmentace, jinak je povolená fragmentace

D	*M*	
1	0	zákaz fragmentace a dál se fragmentovat nebude
1	1	tento případ nemůže nastat
0	1	povolená fragmentace a následují další fragmenty
0	0	povolená fragmentace, ale nenásledují fragmenty
- Fragment offset – o co je daný fragment posunutý vzhledem k začátku datagramu - využívá násobky 8 Byte, tzv. oktety (ang. octets)
- Time to leave (TTL) – jedná se o dobu životnosti datagramu a když životnost vyprchá, tak je datagram zahozen
- Protocol – pro jaký protokol je datagram určen na vyšší vrstvě - protokol je reprezentován číslem: UDP - 17, TCP - 6, ICMP - 1, IGRP - 88 a OSPF - 89
- Header checksum – kontrolní součet pro hlavičku – pokud nesouhlasí je datagram zahozen
- Source address – IP adresa odesílatele
- Destination address – IP adresa adresáta
- Options - volitelné položky
- Padding – případná výplň, která dorovná délku hlavičky na násobek 4 Byte
- **Data** – surová data

5.5.1 Zadání úlohy

Rozdělte IP datagram na menší pakety tak, aby bylo možné jeho poslání přes **NET 2** na obrázku 26.



Obrázek 26 - Schéma sítě

Víme, že náš datagram má tyto hodnoty:

- **IHL**: délka hlavičky je 20 B
- **Total lenght**: 1424 B
- **Identification**: 56
- **Flags**: D = 0, M = 0 (výchozí příznak)
- **Fragment offset**: 0 (výchozí)

5.5.2 Řešení úlohy

Hlavička 20 B	Aplikační data 1404 B
Id = 56 **D = 0, M = 0** **FO = 0**	**552** **552** **300**
Id = 56 **D = 0, M = 1** **FO = 0**	**552** (576 – 20 = 556; 556 / 8 = 69,5) (69 * 8 = 552)
Id = 56 **D = 0, M = 1** **FO = 69**	**552**
Id = 56 **D = 0, M = 0** **FO = 138** (2 x 69 = 138)	**300** (1404 – 2 * 552 = 300)

Obrázek 27 - Fragmentace IP datagramu

Obrázek 27 ukazuje, jak datagram rozdělíme. Postupovat budeme takto:

1) Víme, že celá délka datagramu je **1424 B** a že hlavička má velikost **20 B**, když tedy odečteme 20 B od 1424 B, dostaneme tak velikost samotných dat v datagramu.

2) Také víme, že síť NET 2 propustí paket o maximální velikosti **576 B** a tak musíme datagram fragmentovat, jelikož má větší velikost.

3) Z celkového datagramu vytvoříme 1. fragment, který bude schopen projít i sítí **NET 2**.

4) Pokud od MTU = 576 B pro NET 2 opět odečteme hlavičku 20 B, zjistíme, že můžeme poslat **556 B** dat.

5) To ale není úplně tak pravda, protože můžeme posílat jenom násobky osmi, tedy tzv. oktety.

6) A tak data 556 B podělíme 8 a vyjde nám **69,5**.

7) Můžeme tedy reálně poslat 69 oktetů, což je v bytech **552 B** (69 x 8 B).

8) Do hlavičky 1. fragmentu tedy zapíšeme, že se bude dále **fragmentovat** (M = 1), jelikož nám ještě zbyla data z celkového datagramu.

9) Také v hlavičce nastavíme o co je náš 1. fragment posunutý od začátku datagramu a jelikož je to první fragment, tak se **FO = 0**.

10) Parametry **ID = 56** a **D = 0** zůstanou nezměněny.

11) Stejný postup volíme i pro další fragmenty, dokud máme nerozdělená data.

12) U posledního fragmentu vložíme celý zbytek dat, v našem případě **300 B**, jelikož už jsme 2x poslali 552 B.

13) Důležité je u posledního fragmentu nastavit v hlavičce příznak **M = 0**, tedy že již nebude následovat další fragment.

14) Také si můžete všimnout, že příznak FO pro poslední fragment je **138**, což je 2 x 69, tedy posunutí o 2 předchozí fragmenty.

6 Závěr

6.1 Shrnutí

Téma počítačových sítí je velmi obsáhlé. Snažil jsem se proto vybrat jen ty části, které se přímo dotýkaly mojí práce a to vytvoření malé počítačové sítě pro výuku počítačových sítí.

Postupoval jsem od obecného určení pojmů až k praktické realizaci sítě. Rozhodoval jsem jak o topologii, tak o normě pro síť, její velikosti a účelu. Síť je v podstatě celkem jednoduchá a to je zapříčiněno i absencí serveru. Ale i kdyby jsme měli finanční prostředky na zakoupení serveru, tak by bylo nemožné dodržet rozsah práce v kladených mezích.

Jelikož ale provozujeme v síti počítače i s operačním systémem Linux, můžeme si dočasně z jednoho osobního počítače vytvořit i slabší server. Vyzkoušet si instalaci Samby, Webového serveru, FTP serveru, SQL serveru atd.

V práci se také podrobně věnuji použitému hardwaru a to hlavně tomu, který přímo souvisí s provozem sítě. Uvádím zde poznatky z praxe. Správné vedení kabelů, výběr kategorie kabelu, krimpování koncovek RJ-45, propojování kabeláže ke switchům pomocí patch panelu a zásuvek.

Také se věnuji v práci dvoum operačním systémům, které bychom měli provozovat na počítačích v učebně. Zde si myslím, že je dobrá volba použít druhý alternativní operační systém Linux. Z finančního hlediska projekt sítě nezatíží a dnes většina serveru běží právě pod operačními systémy UNIX. Proto je dobré, když se student seznámí i s takovýmto operačním systémem, pokud se v budoucnu chce starat o správu sítě.

Aby měla vytvořená počítačová učebna nějaký účel, tak jsem také na závěr uvedl pár příkladů, které je možné realizovat v dané síti. Student si vyzkouší výpočet adresového prostoru pro počítače. Dále podrobně popisuji, jak nastavit protokol TCP/IP v obou operačních systémech. Také se věnuji popisu konfigurace Switch ASUS GigaX 1024i, na kterém si studenti můžou vyzkoušet moderní způsob administrace chytrého switche.

6.2 Zhodnocení

Myslím, že se mi celkem podařilo z nepřeberného množství informací o počítačových sítí vybrat ty důležité a hlavně ty, které bezprostředně souvisí se zadaným tématem.

Některé teoretické části jsou delšího rozsahu, ale určitě se bez nich při návrhu sítě neobejdeme. Tak jsem se je alespoň snažil podat čtivou formou a pokud možno je doplňovat častými obrázky nebo tabulkami.

Práci nerozděluji na část teoretickou a praktickou, ale snažím se tyto dvě části prolínat v průběhu celé práce. Nejprve vždy nastíním možnosti, které by pro nás připadali v úvahu a poté obhajuji ten jeden konkrétní případ, který použijeme v naší počítačové síti. Tato metodika se mi zdála být nejvhodnější i kvůli rozsahu práce a i z důvodu navazování jednotlivých kapitol.

Kapitoly jsem rozdělil do větších celků. Na začátku jsem se snažil nastínit co nás v kapitole čeká. Na konci kapitoly neuvádím celkové shrnutí, jelikož bych akorát opakoval úvodní informace a práce by tak dále nabývala na rozsahu.

Abych mohl práci zkompletovat, musel jsem nastudovat několik zdrojů literatury. Ovšem mojí největší výhodou je, že jsem již prošel krátkou praxí ve firmě, která se zabývá bezdrátovými počítačovými sítěmi a tak některé zkušenosti jsem mohl uplatnit i v této práci. Také jsem absolvoval tři semestry kurzů CISCO a proto jsem se také rozhodl pro toto téma práce.

Přínos práce vidím za prvé ve výběru informací pro stavbu malé počítačové sítě. Dále nabízím řešení jak počítačovou síť zrealizovat a případně rozšiřovat o další prvky. Dávám návod, jak volit síťové kabely pro počítačovou sít, ale hlavně jak je vést a jaké výhody to přináší. Velký přínosem také mohou být ukázkové příklady a to hlavně pro studenty, který se chtějí seznámit se správou počítačových sítí od úplného začátku.

Ukázkové příklady v této práci jsou také prezentovány v podobě HTML stránek. Ty jsou přiloženy jako elektronická příloha k práci na CD.

Literatura

[1] Horák, J., Keršláger, M. *Počítačové sítě pro začínající správce.* Brno: Computer Press, 2006

[2] Hucaby, D. *Konfigurace směrovačů Cisco*. Praha: Computer Press, 2004

[3] Kállay, F., Peniak, P. *Počítačové sítě LAN / MAN / WAN*. Praha: Grada, 2003

[4] Kostroun, A. *Stavíme si malou síť*. Praha: Grada, 2001

[5] Shinder, D., L. *Počítačové sítě*. Brno: Softpress, 2002

[6] Sportack, M., A. *Směrování v sítích IP.* Praha: Computer Press, 2004

[7] Teare, D. *Návrh a realizace sítí Cisco*. Praha: Computer Press, 2003

[8] Urbiš, M. *Zásady návrhu síťové infrastruktury* [online]. [cit. 2008-02-26]. Dostupné z WWW: <http://www.svetsiti.cz/view.asp?rubrika=Tutorialy&temaID=231&clanekID=232>

[9] Velte, A., T., Velte, T., J. *Síťové technologie Cisco - Velký průvodce*. Praha: Computer Press, 2003

Přílohy

- Anglický manuál - Switch ASUS GigaX 1024i
- Webové stránky s ukázkovými příklady