Univerzita Hradec Králové

Přírodovědecká fakulta

Katedra informatiky

Výuka počítačových sítí na základních a středních školách

Bakalářská práce

Autor:	Michael Mňuk
Studijní program:	B1801 Informatika
Studijní obor:	Informatika se zaměřením na vzdělávání Tělovýchovné a sportovní aktivity zaměřením na vzdělávání
Vedoucí práce:	Ing. Jiří Jelínek, Ph.D.
Odborný konzultant:	Libor Filip

Hradec Králové duben 2015

Prohlášení:

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně a že jsem v seznamu použité literatury uvedl všechny prameny, z kterých jsem vycházel.

V Hradci Králové dne 27. 4. 2015 Michael Mňuk

Poděkování

Děkuji vedoucímu práce Ing. Jiřímu Jelínkovi, Ph.D. za cenné připomínky, rady a hlavně čas, který mi věnoval při konzultacích a vedení práce.

Anotace

Mňuk, M. *Výuka počítačových sítí na základních a středních školách*. Hradec Králové, 2015. Bakalářská práce na Přírodovědecké fakultě Univerzity Hradec Králové. Vedoucí práce Jiří Jelínek. 68 s.

Cílem bakalářské práce je zaměřit se na problematiku praktické výuky počítačových sítí na základních a středních školách. Práce bude obsahovat přehled postupů jak vést praktickou výuku na základních a středních školách, v prostředí běžné počítačové učebny a v prostředí specializované učebny vybavené počítači s administrátorským oprávněním a vybranými síťovými prvky (přepínače, routery, analyzátory provozu sítě atp.). Výstupem práce mohou být návody pro budoucího pedagoga nebo návody na přípravu pedagogů v prostředí Přírodovědecké fakulty.

Klíčová slova

Počítačové sítě, výuka počítačových sítí, síťové protokoly, síťové topologie, směrování, PSImulator, vizualizace sítí

Anotation

Mňuk, M. *Teachingofcomputernetworking on elementary and highschools.* Hradec Králové, 2015. Bachelor thesis atFacultyof Science University of Hradec Králové. Thesis Supervisor Jiří Jelínek. 68 s.

The goal of this thesis is to focus on the issues with practical teaching of networking on elementary and high schools. Thesis will include outline procedures for how to conduct a practical classes on elementary and high schools in environment of ordinary komputer class and in environment of specialized komputer laboratoř equipped with administrator rights and selected network elements (switches, routers, network tradic analysers etc.). Out come of this thesis could become an instructions for future teachers or instructions for preparation of colleagues in the environment of Faculty of Science.

Key words

Computer network, teaching of computer networking, network protocols, network topology, routing, PSImulator, network virtualization

Obsah

Seznam obrázků

Seznam tabulek

Úvod

Problematika výuky počítačových sítí je jistě velmi obsáhlé téma, které se na odborných středních školách může vyučovat prakticky po celou dobu studia žáků. Je tedy třeba velmi zásadně rozlišovat přístup k výuce dle úrovně školy a úrovně znalostí žáků a studentů.

Výuka počítačových sítí by měl být zařazena nejenom na odborných středních a vysokých školách, ale měla by být i součástí výuky na školách základních.
Z různých, hlavně časových, důvodů není možné a nemá smysl probírat počítačové sítě více do hloubky. Cílem takové výuky by mělo být pouze navození základních představ žáků o fungování počítačových sítí, včetně nejznámější síť dnešní doby, Internetu.

S Internetem se žáci budou setkávat pravděpodobně po celý svůj život a bylo by tedy vhodné, aby i žáci, kteří následně jako svůj další obor studia na středních školách zvolí jiné zaměření, než je informatika, měli alespoň základní představu o fungování této sítě. Bez základních znalostí počítačových sítí však není možné žákům vysvětlit princip funkce internetu.

Na středních školách je situace odlišná, žáci na školách odborného zaměření mají k dispozici často velmi dobře vybavené síťové laboratoře, jenž dobře poslouží při výuce. Je zde již mnohem větší časový prostor pro výuku a předpokládá se také větší odbornost učitelů.

Cílem této práce je uvedení některých možností, jak by mohla probíhat výuka na základních a středních školách. Jsou zde popsány základy nutné pro pochopení principu funkce počítačových sítí, které mohou posloužit jako teoretický základ pro výuku. Práce také obsahuje praktické úkoly jak pro základní, tak střední školy a jejich řešení. Tato práce tak může posloužit pedagogům, jako jedna z možností výuky pro výuku počítačových sítí.

1 Počítačové sítě

Síť Internet, tzv. síť sítí, je bezesporu fenoménem dnešní doby. Je však chybou si pod pojmem počítačová síť představit pouze síť Internet. Pojmem počítačová síť se rozumí technické prostředky, díky kterým mohou dva počítače navzájem komunikovat, tedy zasílat mezi sebou informace.

Tyto informace, které si síťové prvky vyměňují, se nazývají *rámce.* K jejich šíření využívají fyzickou kabeláž, nebo je šíří bezdrátově. Celý provoz řídí síťové protokoly, které určují, jak se budou aktivní i pasivní prvky sítě chovat při vzájemné komunikaci. O tom všem i dalším se dozvíme v následujících kapitolách. Toto vše a další vysvětlují následující kapitoly.

Počítačové sítě umožňují sdílení například souborů nebo tiskáren mezi 2 nebo více počítači, umožňují zasílat zprávy, nebo také propojit do jedné sítě i jiná zařízení než jen počítače. Jsou to například televizory, mobilní telefony a tablety, herní konzole a jiné.

„Domácí sítě už ani neslouží výhradně počítačům. Do takové sítě lze zapojit televizi i systém domácího kina, takže si můžete užívat digitální hudbu, video, i obrázky na velké obrazovce a s prostorovým zvukem. Také videohry, ať už na PC nebo na herních konzolích těží z domácí sítě: jako rodina můžete hrát proti sobě nebo společně proti vzdáleným protivníkům.“ (Soper, 2005 str. 22).Je tedy nezbytné také rozlišovat různé druhy sítí, kromě domácích a podnikových je dále dělíme dle jejich topologie, velikosti a funkce aktivních prvků.

2 Síťové prvky

Počítačové sítě se skládají z jednotlivých částí. Pro správné pochopení fungování sítí je důležité znát jednotlivé prvky a jejich funkci. Základní rozdělení síťových prvků je na aktivní a pasivní.

2.1 Aktivní síťové prvky

Aktivní prvky jsou základním stavebním pro přenos informací mezi dalšími částmi sítě, jako jsou např. klienti, datová úložiště nebo třeba servery a slouží také pro spojení jednotlivých počítačových sítí. Jejich úkolem je převést informaci z média (optický, metalický kabel…) a poté zaslat tuto informaci za pomocí fyzického média k cíli. Mezi aktivní prvky tak patří směrovače, opakovač, přepínač, síťové karty, přístupový bod, brána, tedy prvky, které se aktivně podílejí na přenosu informací.

Opakovač (anglicky Repeater) je zařízení na obnovení signálu zeslabeného útlumem. „Jak elektrické signály cestují kabely, degradují a jsou zkreslovány. Tento efekt se nazývá *útlum*. Jak narůstá délka kabelu, efekt útlumu se zhoršuje. Je-li kabel příliš dlouhý, útlum nakonec znemožní rozpoznatelnost signálu a vzniknou tak datové chyby v síti. Instalace opakovačů umožňuje, aby signály cestovaly dále pomocí obnovení signálu sítě a jejich novým odesláním na další úsek kabelů.“ (Bigelow, 2004 str. 52)

Rozbočovač (anglicky Hub) je aktivní prvek v síti, který rozděluje signál mezi klienty a umožňuje tak jeho větvení. Umožňuje tedy připojení více klientů k jednomu zdroji, ale neumí signál cíleně směřovat a veškerá data, která přijímá např. ze zdroje, odešle všem klientům, čímž zbytečně vytěžuje síť.

Přepínač (anglicky Switch) je zařízení, které postupně nahradilo rozbočovače, jeho výhodou je cílené směřování dat. Pokud si jeden klient vyžádal od serveru konkrétní data, přepínač je odešle pouze na port, který je spojen s konkrétním klientem. Značně tím omezuje provoz v sítí a tím šetří vytížení sítě. Přepínače se využívají ke spojení v jedné místní síti.

Most (Bridge) je v oblasti počítačových sítích označení pro zařízení, které umožňuje oddělit provoz různých částí sítě. Most také, na rozdíl od opakovače nebo rozbočovače, směřuje svá data přímo tam, kam jsou určena. Díky jeho vlastnostem může mít i více využití. „Most může fungovat jako opakovač k prodloužení efektivní délky síťového kabelu. Most má však větší „inteligenci" a může rozdělit síť pro izolování nadměrného provozu nebo problematických dat. „Mosty mohou pracovat v lokální síti a propojovat její segmenty, ale může jít také o propojení vzdálených sítí (ať už homogenních nebo heterogenních) přes páteřní síť (WAN)." (Vavrečková, 2010)

Pokud například svazek z jednoho či dvou počítačů (nebo jednoho oddělení) zaplavuje síť daty a zpomaluje tak její činnost, může most tyto počítače (nebo oddělení) izolovat umístěním do jejich vlastní části kabelu." (Bigelow, 2004 str. 53). Most pracuje na linkové vrstvě ISO/OSI modelu (směruje rámce dat podle fyzické, MAC adresy). Výhoda mostu je snižování provozu v síti, pokud posílá data pouze tam, kam má, nikoliv všemi porty, jako hub.

Most, který se nově připojí do sítě, se postupně „učí" topologii sítě, tím, že si uloží adresu každého síťového prvku, se kterým komunikuje, do směrovací tabulky (uloží si jeho MAC adresu a port, kterým s daným prvkem komunikuje). Když most přijme rámce dat, zjistí z nich MAC adresu cíle, pokud není uložena ve směrovací tabulce, odešle rámce všemi porty, vyjma toho, kterým rámec přijal a pokud najde cíl, uloží ho do své tabulky. Pokud však MAC adresa je již uložena ve směrovací tabulce, most zjistí, jestli se nachází ve stejné části sítě. Rámce posílané v rámci jedné části most vyřazuje a dále neposílá. Tím se šetří provoz v síti. Rámce, určené pro jinou část sítě, most směřuje normálně dál.

Směrovač (Router) je zařízení, které dokáže spojit např. místní síť (LAN) k internetu a řídit veškerý provoz. „Ten si již uvědomuje topologii celé sítě, a díky tomu je pak schopen rozhodnout, kudy vede cesta do nějakého vzdáleného uzlu. Přijme-li nějaký blok dat, umí se rozhodnout, kterým směrem jej poslat dál, aby se nakonec (po případném průchodu dalšími mezilehlými uzly) dostal až ke svému konečnému adresátovi." (Peterka, 2011)

Pro porovnání s přepínačem, dalším síťovým zařízením, můžeme použít přirovnání přepínače k cestám spojujícím města v rámci jednoho státu, zatímco směrovač by v takovém případě znamenal hraniční přechod mezi celými státy. Směrovač totiž řídí provoz mez dvěma sítěmi, zatímco přepínač pouze v rámci jedné sítě. (Rukovanský, a další, 2009)

Pracuje na 3., tedy síťové vrstvě ISO/OSI modelu (směruje pakety dat podle IP adresy v nich uložené) a pro data přenášená směrovačem je používán pojem paket. Paket je rozdělen do dvou částí – řídící data (metadata) a uživatelská data, kdy v řídících datech jsou uloženy informace o odesílateli a příjemci dat apod., které jsou uloženy v hlavičce a na konci paketu.

Při odesílání se tedy data rozdělí na pakety (v Ethernetu běžně o velikosti 46 - 1500 bytů), do řídících dat se uloží informace o zdroji a cíli a zabalí se na tzv. rámce. O správné doručení rámců se pak stará směrovač za využití síťových protokolů. Výhodou takového rozdělení dat je skutečnost, že směrovač může pro každý rámec vybrat jinou trasu a využít redundance (nadbytečnosti) spojů v síti.

2.2 Pasivní síťové prvky

Pasivním prvkem počítačových sítí jsou takové části sítě, které se fyzicky účastní při přenosu informací, ale nemohou je přímo měnit. Jsou to tedy kabely, konektory, spojky, zásuvky a podobně. I přes to, že cíleně nemohou pasivní prvky ovlivňovat informace, které přenáší, je jejich vhodné použití důležité pro správné fungování. Nedostačující kabeláž použitá v síti může negativně ovlivňovat rychlost sítí a celý provoz brzdit.

Dnes běžně používanou kabeláž můžeme rozdělit na metalickou (nejčastěji stíněná/nestíněná kroucená dvojlinka) a optickou. Liší se svou přenosovou rychlostí, útlumem signálu na jednotku vzdálenosti a možností využití. Optické kabely jsou totiž náchylné na ohyby, proto se využívají spíše v páteřních sítích ve venkovním prostředí na větší vzdálenosti.

2.2.1 Metalická kabeláž

U metalické kabeláže je dnes nejrozšířenější kroucená dvojlinka a koaxiální kabel. Liší se v provedení a tím i v jejich využití. Kabeláž se dále rozděluje do několika kategorií (standardů), určujících jejich využití. Celkem 7 kategorií (některé ještě rozdělené na podkategorie) postupně přicházelo s vývojem technologií. Například kategorie 1 je určena převážně k telefonním rozvodům, přenosová rychlost takové kabeláže je do 1Mbit/s. V počítačových sítích se dříve využívala kategorie 3, s maximální rychlostí 10Mbit/s (10BASE-T), dnes to jsou kategorie 5, 6 a 7.

Koaxiální kabel je tvořen vodičem, který je obalen dielektrikem (izolace), na dielektriku je dále naneseno stínění (vodivé opletení) překryté další izolační vrstvou. Stínění vnitřního vodiče má význam hlavně v jeho odstínění a tím snižování vlivu vnějšího rušení. V počítačových sítích využíván hlavně pro propojení Wi-Fi adaptéru s externí anténou.

„Vyrábí se v tloušťkách od 4mm až po 10, 8mm a z různých materiálů. Rozhodujícím prvkem je však především materiál, ze kterého je vyroben vnitřní prut v kabelu a také opletení, které by mělo být vždy z mědi. Dalším důležitým faktorem je útlum na metr (označuje, kolik dB se ztratí při průchodu signálu na 1m kabelu). Platí, že čím nižší hodnota, tím lépe. A také to, že čím je kabel užší, tím má

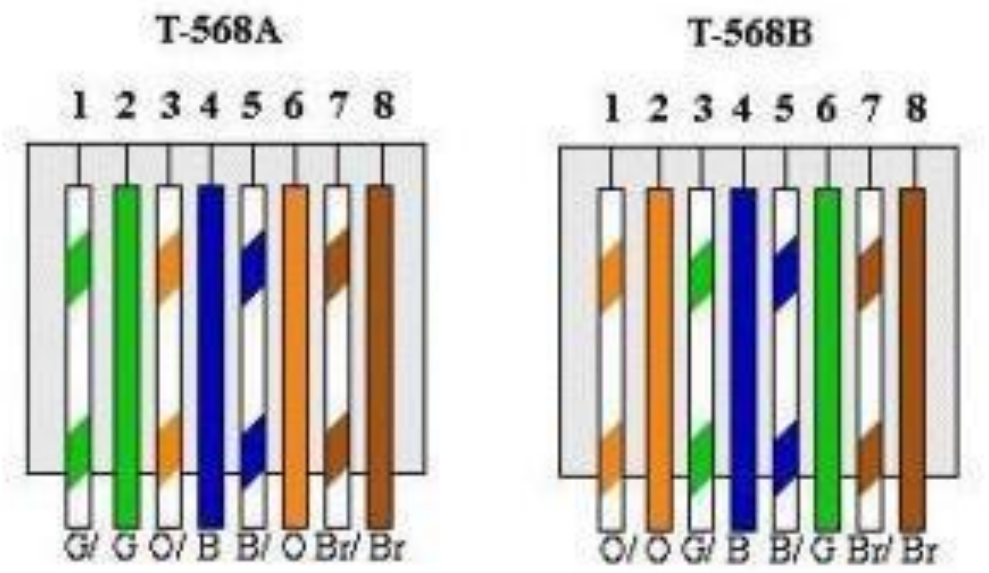
zpravidla větší útlum.“ (Rukovanský, a další, 2007 str. 69). U koaxiálních kabelů se využívá různých konektorů, nejčastěji N konektor, poté RSMA a TNC.

Kroucená dvojlinka je v současné době nejrozšířenějším řešením v oblasti lokálních počítačových sítí, a to prakticky bez ohledu na velikost – velmi dobře odvede svou službu jak při propojení dvou počítačů, tak ve firemním prostředí se stovkami strojů. (Malina, 2003)V počítačových sítích je nejčastěji tvořen 8 vodiči, tedy 4 páry, od sebe barevně odlišených. Tvoří ji páry vodičů, které jsou navzájem zkrouceny po celé své délce, navíc jsou mezi sebou navzájem zkrouceny páry vodičů.

Potřeba minimalizovat vzájemnou interakci mezi vodiči kroucené dvoulinky a jejím okolím se ovšem týká i opačného směru - tedy vyzařování z kroucené dvoulinky směrem ven, do jejího vnějšího okolí. Zde je nutné si vzpomenout na jednu ze základních pouček fyziky, která říká, že každé dva souběžně vedoucí vodiče se chovají jako anténa: pokud je jimi přenášen nějaký střídavý signál, vyzařují do svého okolí elektromagnetické vlny. Konkrétní efekt takovéhoto vyzařování samozřejmě závisí na mnoha faktorech (frekvenci signálu, fyzickému provedení souběžných vodičů atd.), ale při přenosových rychlostech dnešních počítačových sítí efekt vyzařování již není zdaleka zanedbatelný.

„Efekt „vyzařující antény" lze ale výrazně snížit, a to tím že se oba vodiče pravidelně zkroutí. Vyzařování se tím sice neodstraní úplně, ale sníží se na takovou míru, která již může být přijatelně nízká (v tom smyslu, že ani neohrožuje lidské zdraví, ani neovlivňuje jiná zařízení či jiné přenosové cesty). V praxi ovšem může záležet na konkrétních fyzických dispozicích a dalších požadavcích, ale i na normách či legislativních úpravách, a výsledná míra vyzařování kroucené dvoulinky bez dalšího stínění může stále být ještě příliš vysoká. Pak musí být místo tzv. nestíněné kroucené dvoulinky (UTP) použita dvoulinka stíněná (STP), která díky svému stínění vykazuje nižší míru vyzařování.“ (Peterka, 2011)

Oproti koaxiálnímu kabelu neumožňuje vytvářet tzv. „odbočky“, umožňuje pouze dvoubodové spoje. Největší možná vzdálenost na spojení kroucenou dvojlinkou je zhruba 100 metrů. Konektor pro zapojení je RJ – 45. Rozlišujeme dále dva typy možných zapojení – přímý a křížený. Křížený kabel se využívá pro propojení mezi dvěma počítači, přímý se využívá pro spojení mezi klientem a aktivním síťovým prvkem. Rozdílem je různé zapojení jednotlivých vodičů, kdy u kříženého kabelu je rozmístění vodičů na obou koncích kabelů rozdílné (dle normy T – 568), u přímého kabelu je jejich rozmístění stejné na obou koncích kabelu.



Obrázek 1 Zapojení kříženého kabelu, dostupné z http://www.cablinginstall.com/articles/2011/03/differences-between-t568a-and-t568b-explained.html

V praxi jsou nejčastěji používané 2 typy kroucené dvojlinky – UTP a STP. UTP je nestíněná kroucená dvojlinka. Jedná se o typ, kde jsou vodiče mezi sebou vzájemně zkrouceny, ale nejsou nijak více izolovány a jejich elektromagnetické záření je proto vyšší. Výhodou může být menší šířka a větší ohebnost. STP, stíněná kroucená dvojlinka, se odlišuje od UTP pouze tím, že má lepší stínění. Mezi zkroucenými vodiči a izolací je ještě vrstva kovové fólie, nebo mohou být stíněny jednotlivé páry. Silnější stíněný bývá využíván více v průmyslu, nebo tam, kde by mohlo dojít k velkému rušení. Nevýhodou STP je větší šířka a menší ohebnost.

2.2.2 Optická kabeláž

Optické vlákno je technologie, která pro šíření informací nevyužívá impulsy elektrické, ale světelné, ve vláknech složených z plastu nebo křemičitého skla. Optická vlákna jsou využívána převážně na velké vzdálenosti, hlavně kvůli minimálnímu útlumu při přenosu, a navíc vlákna nemohou být rušena elektromagnetickým zářením. Jsou nevodivá a nehořlavá.

Rozlišují se 2 druhy optických vláken – jednovidová a mnohavidová. Jednovidová optická vlákna používají pouze jeden zdroj světla, vláknem se tedy šíří pouze jeden paprsek (vid). Využívá se na delší vzdálenosti (řádově kilometry) s poměrně malým útlumem a vysokou přenosovou rychlostí. Jádro optického vlákna má pouhých 9μm a pro přenos je nutné použít kvalitnější (dražší) zařízení (zdroje a detektory světla).

U mnohavidových vláken, jak již název napovídá, se využívá k přenosu informací více paprsků (vidů), jádro má mnohem větší průměr 50 – 60μm. Používají se na kratší vzdálenosti s menšími nároky na použité zařízení i vlákna, proto jsou i levnější, než jednovidová vlákna. Při průchodu vláknem se každý paprsek odráží pod jiným úhlem a k detektoru doráží paprsky s určitým zpožděním mezi sebou, proto dochází k postupnému zkreslení, které se postupně zvětšuje při použití na větší vzdálenost.

„Princip vedení světla je jednoduchý - světelný paprsek dopadá na rozhraní dvou prostředí s rozdílnou optickou hustotou a tedy s rozdílným indexem lomu, kde se zčásti láme a prostupuje z jednoho prostředí do druhého, a z části se odráží a vrací se zpět do prostředí, ze kterého přichází. Nakolik se paprsek odrazí zpět do prostředí, ze kterého pochází, záleží na úhlu, ve kterém paprsek do vlnovodu přichází. Pro každé optické rozhraní však existuje mezní úhel odrazu. Pokud světlo dopadá pod tímto (nebo menším úhlem) dochází k tzv. totálnímu odrazu, kdy se 100% světla odráží a neopouští prostředí, ze kterého přichází. Právě tento princip "vnitřních odrazů" využívají optická vlákna.“ (Plexo, 2008).

3 Dělení počítačových sítí

Rozdělení počítačových sítí není jednoznačným krokem, počítačové sítě totiž můžeme dělit hned podle několika kritérií:

- Velikost
- Topologie
- Funkce prvků v síti
- Využití

3.1 Dělení sítí dle velikosti

Rozdělení počítačové sítě podle její velikosti je jedním ze základních dělení. Dle tohoto kritéria dělíme sítě na PAN, LAN, MAN a WAN.

PAN („osobní síť“) je síť nejmenšího rozsahu, pro potřeby často jednotlivce, nebo velmi malé skupiny uživatelů, která slouží k propojení mobilních telefonů, PDA, notebooků a podobných zařízení, často při využití Wi–Fi, Bluetooth nebo přes USB.

LAN („místní síť“) je síť, která se nachází v ohraničeném objektu, často mluvíme o jedné učebně, nebo budově, která sdílí jednu síť, ale může také spojovat několik budov, vždy ale blízkých (obvykle několik stovek metrů).

MAN („metropolitní síť“) je síť většího rozsahu, propojující navzájem sítě LAN, často v rámci jednoho města, nebo oblasti. Spojuje na vzdálenosti do několika desítek kilometrů.

WAN je síť největšího rozsahu, která spojuje sítě LAN a MAN, které se nachází například na území jednoho státu, nebo i kontinentu. Počítačová síť Internet je sítí typu WAN.

3.2 Rozdělení sítí podle topologie

Rozdělení podle topologie sítě se přímo řídí tím, jak jsou jednotlivé prvky síťového provozu uspořádány. Jejich pojmenování obvykle přímo vychází z toho, jak výsledné zapojení sítě vypadá. Každé zapojení má svoje výhody i nevýhody a jejich použití se tedy může lišit dle konkrétních situací.

Topologie Hvězda je centralizované zapojení, kdy jsou všechny prvky zapojeny do jednoho, centrálního, který celý „provoz“ v síti řídí. Výhodou takového zapojení je jeho snadné rozšíření, jeho odolnost vůči chybám (díky vyhrazenému spojení mezi prvky), poměrně snadné hledání závad a také fakt, že výpadek jedné části sítě neznamená problémy pro zbytek sítě. Pokud však vypadne centrální prvek (switch, hub apod.), celá síť přestane fungovat. Dalším problémem může být velký nárok na kabeláž.

Topologie sběrnicová je takové síťové uspořádání, kde jsou všechny počítače a ostatní síťové prvky připojeny na společnou sběrnici (přenosové médium), přes kterou prochází veškerý síťový provoz. Výhodou této topologie, je jednoduchost zapojení a nízké náklady, nevýhodou však je případná porucha sběrnice, která vyřadí mimo provoz kompletní síť, navíc nelze běžně využít jako kabeláž kroucenou dvojlinku, kvůli nemožnosti na ní dělat odbočky. Další nevýhodou je nemožnost vysílání data z více, než jednoho počítače (klienta). Tato nevýhoda je však vyřešena programově tzv. CSMA (systém náhodného přístupu). Problematický je také výkon sítě, který při použití více klientů klesá. Topologie je proto vhodná spíše pro malé sítě.

„Kruhová topologie se podobá sběrnicové topologii v tom, že každý počítač je propojený s dalším počítačem. Místo ukončení obou konců jsou však tyto spojeny dohromady ve formě kruhu. Toto propojení způsobuje, že signály cestují cyklicky od jednoho počítače k dalšímu a nakonec se vrátí k počátečnímu bodu. Ve většině případů je kruhová topologie striktně logickou konstrukcí, a ne fyzickou, protože kabely se v kruhové topologii připojují k rozbočovači a tvoří spíše hvězdici.“ (Bigelow, 2004 str. 67)Datový tok v této topologii je vždy zesílen v každém počítači, který přijme a zase odešle data (fungují tedy jako repeater, opakovače signálu). Pokud však dojde k výpadku jednoho klienta, může to mít za následek výpadek celé sítě. Dalšími komplikacemi může být nesnadné rozšiřování.

Další z možných topologií jsou kombinace několika z nich. Jako příklad můžeme uvést kombinaci hvězdicové a sběrnicové topologie.“Hvězdicová a sběrnicová je metodou, kterou můžete použít k rozšíření velikosti sítě LAN o více než jednu hvězdici. Síť LAN rozšíříte spojením několika hvězdicových sítí se samostatným segmentem sběrnicového kabelu pro vzájemné propojení jejich rozbočovačů.“ (Bigelow, 2004 str. 66)

Další možnou kombinací je tzv. stromová. Jedná se o topologii, která rozšiřuje možnosti topologie hvězda, kdy v podstatě spojuje aktivní síťové prvky a vytváří tak spojení několika menších sítí (několika hvězd). Využívá se často ve velkých firmách pro spojení např. několika oddělení.

3.3 Rozdělení dle funkce prvků v síti

Dle funkce prvků zapojených v síti je můžeme dělit na sítě peer-to-peer a klient-server. Rozdíl v obou typech je velký, stejně tak se liší jejich využití. Sítě klient-server jsou sítě s centrální jednotkou, zpravidla serverem, který se stará o síťový provoz a účastní se na veškerém datovém toku v síti. Na rozdíl od toho sítě peer-to-peer nemají žádný přímo centralizovaný prvek, komunikace probíhá přímo mezi klienty.

Síť Klient-server má tedy centralizované řízení, o které se stará vyhrazený server. „Vyhrazený server je počítač, který funguje pouze jako server poskytující soubory a správu prostředků – není používán jako klient nebo pracovní stanice. Servery jsou optimalizovány pro rychlé zpracování požadavků od velkého počtu síťových klientů a zajišťují zabezpečení souborů a adresářů. Díky tomu se sítě založené na serverech staly standardními modely pro moderní sítě společností. Sítě založené na serverech jsou známé také jako sítě *klient/server* (někdy označované jako dvouvrstvé architektury). Pamatujte si, že jde o operační systém a další síťový software, který definuje síť klient/server nebo peer-to-peer – propojení hardwaru a fyzické sítě je identické.“ (Bigelow, 2004 str. 46)

Komunikace tedy probíhá mezi klientem (například webový prohlížeč) a serverem (webový server). Klient zažádá o informaci server, který žádost o informace vyhodnotí a zašle je na klienta. Z toho vyplívá, že čím více je klientů v jedné síti, kteří potřebují komunikovat se serverem, tím více ho budou zahlcovat a bude

postupně klesat rychlost komunikace. S rostoucími nároky sítí také vznikaly nové, specializované druhy serverů podle jejich určení. Rozlišujeme tedy mimo jiné servery: souborové, databázové, poštovní, aplikační, komunikační, audio/video, chat-servery, FTP, brány, firewall a proxy, webové a Telnet servery.

Sítě peer-to-peer se liší od sítí klient-server v tom, že provoz síti není přímo centralizován a komunikují mezi sebou přímo klienti, všichni na stejné úrovni. „Nejsou zde žádné vyhrazené servery a mezi počítači neexistuje žádná hierarchie. Protože jsou si všechny počítače rovné, označují se *peer* (druzi). Každý počítač slouží jako klient i server a není žádný administrátor odpovědný za celou síť – uživatel každého z počítačů stanovuje, jaká data se budou sdílet v síti. Všichni uživatelé mohou sdílet jakýkoli ze svých prostředků způsobem, který si sami zvolí." (Bigelow, 2004 str. 45)

Problémem těchto sítí bývá zabezpečení, které vlivem neřízeného datového toku není zajištěno. Výhodou pak je skutečnost, že s rostoucím počtem klientů v sítí roste přenosová rychlost mezi klienty. Pokud například jeden klient požaduje určitá data, vyšle do sítě požadavek a data. Pokud se v síti nachází více klientů s požadovanými daty, bude klient požadující data přijímat z více zdrojů a vše proběhne rychleji.

3.4 Rozdělení sítí dle využití

Počítačové sítě můžeme dle využití rozdělit na 2 následující podmnožiny – podnikové a domácí. Ve firmách se počítačové sítě využívají na sdílení tiskáren, na ukládání dat na společný pevný disk, na rychlé sdílení informací a podobně. V domácnostech se využití pochopitelně trochu liší i přesto, že umožňují prakticky stejné využití. Hlavním rozdílem bude složitost, respektive jednoduchost počítačové sítě v domácnosti. Domácí počítačové sítě jsou výrazně menší, skládají se většinou jen z několika málo počítačů, nebo zařízení.

4 Síťová architektura

Vytvořit velkou a funkční síť je poměrně složitý proces, proto se přistoupilo k rozdělení síťové komunikace na několik menších částí - vrstev. Pro lepší představu můžeme přirovnat komunikaci v rámci jedné sítě k fungování firmy, kde jsou úkoly také rozděleny, každý zaměstnanec má své úkoly a vše jako celek funguje. Podobně se tedy uvažuje u síťové architektury, která je návrhem sítě, jenž definuje počet vrstev a rozhoduje o tom, co bude mít jaká vrstva na starosti. Zahrnuje také přesnou představu o způsobu fungování každé z vrstev.

V odborné literatuře se můžeme setkat také s pojmem síťový model. Rozdíl mezi síťovým modelem a architekturou je v tom, že model zahrnuje představu o tom, na kolik vrstev bude síť rozdělena, co bude mít která vrstva na starosti. Nezahrnuje však představu o tom, jak bude každá vrstva své úkoly řešit. Přesné algoritmy pro řešení problémů obsahují až komunikační protokoly, které ale nejsou součástí síťových modelů. Ty implementuje až síťová architektura, kterou tak můžeme označit za komplexnější řešení.

4.1 Model ISO/OSI

Referenční model ISO/OSI se nazývá pouze modelem, ale můžeme o něm uvažovat i jako o síťové architektuře. Při jeho vzniku totiž vznikaly i komunikační protokoly pro každou z vrstev modelu. V praxi se však nepodařilo tyto protokoly prosadit, dnes se nevyužívají a síťový model ISO/OSI tak je abstraktním modelem reálné sítě, který uvádí pouze obecné principy sedmivrstvé architektury. Model se využívání při nastavování částí sítě, kde každá z částí představuje jinou vrstvu síťového modelu. Pod jednotlivými vrstvami si tak můžeme představit síťovou kartu, softwarový ovladač, aplikaci a podobně. Výhodou je možnost samostatně měnit jednotlivé části.

Síťový model ISO/OSI vyvinula Mezinárodní standardizační organizace (Internacional Organization for Standardization – ISO) již koncem 70. letech 20. století (v roce 1984 přijat jako standard pro návrh komunikačních systémů) s cílem sjednotit vývoj komunikačních sítí a zamezit vzniku proprietárních sítí, které si nechávaly budovat velké firmy. „Vytvoření standardu pro síťovou komunikaci je v základu pokus o definování široce přijatelného způsobu, jak

vytvořit vzájemnou komunikaci mezi systémy, o nastavení sítí a způsobech jejich propojení.“ (Palovský, 2010 str. 110)

„Model OSI představuje vhodný způsob, jak uvažovat o síťové struktuře, neboť pochopení toho, jak se nějaká daná funkce vztahuje na jiné síťové činnosti, je pak snadnější. Model OSI je hierarchický. Základní síťové funkce, jako jsou například stanovení fyzického média používaného sítí a dekódování rádiových signálů, probíhají na nižších vrstvách. Vyšší vrstvy řídí způsob, jakým jsou prováděny transakce, a nakonec stanovují pravidla pro konkrétní síťové aplikace, jako je například sdílení souborů, tisk, atd.“ (Brisbin, 2003 str. 28)

I přes svoje stáří se model ISO/OSI zachoval dodnes, ale je brán spíše jako abstraktní síťový model, než jako síťová architektura, protože protokoly, které navrhoval model ISO, se nepodařilo v praxi prosadit. Pokud tedy budeme řešit pouze model jako takový, celkem se skládá ze sedmi vrstev. Každá z vrstev má tedy svou jasně danou funkci, zodpovídá za určitý úkol. V rámci jednoho prvku (uzlu) síťového provozu mezi sebou mohou vrstvy komunikovat, jedná se ale pouze o vrstvy přímo sousedící. Třetí vrstva (relační), tedy bude moci komunikovat pouze s druhou (prezentační) a čtvrtou (transportní). V rámci komunikace mezi dvěma prvky (uzly) mezi sebou mohou komunikovat pouze vrstvy stejné úrovně.

V praxi však mezi uzly nekomunikují všechny vrstvy modelu, ale pouze jedna – fyzická. Všechny ostatní vrstvy přenášejí svůj požadavek na komunikaci s dalšími prvky v síti na nižší vrstvy, vždy svému „sousedovi“ pod sebou, až se požadavek dostane na fyzickou vrstvu, která odešle požadované informace. Pokud naopak nějaké informace obdrží, posílá je opačným směrem na zpracování. Komunikace mezi vrstvami probíhá skrze SAP – Service Access Points, čili „přechodové body“. Vrstvy 1 až 3 jsou orientované na přenos dat, vrstvy 5 až 7 jsou zase orientované na podporu aplikací. Vrstva číslo 4, transportní, je jakási přizpůsobovací.

1	**Fyzická vrstva**
2	**Linková vrstva**
3	**Síťová vrstva**
4	**Transportní vrstva**
5	**Relační vrstva**
6	**Prezentační vrstva**
7	**Aplikační vrstva**

Tabulka 1 Referenční model ISO/OSI

4.1.1 Fyzická vrstva

První vrstvou je tedy fyzická, která představuje fyzické propojení počítačů mezi prvky v síti. „Tvoří specifikace konektorů, vlastnosti kabelů, napěťové úrovně přenášené kabely, fyzikální vlastnosti připojovaných zařízení, jako jsou síťové adaptéry, opakovače, huby. Vytváří a udržuje fyzické spoje mezi koncovými body.“ (Palovský, 2010 str. 112)Dále se zabývá přímo přenosem jednotlivých informací – přijme požadavek na přenos dat („zabalených“ do rámců)od vyšších vrstev a obdržené informace převede do jednotlivých bitů a zajistí jejich odeslání.

4.1.2 Linková vrstva

Vrstva číslo 2, linková, někdy nazývána též datová, nebo spojová, připravuje pro přenos informace, které obdrží od vyšších vrstev, vytváří z nich tzv. rámce, které dále posílá na fyzickou vrstvu. Naopak přijímá data z fyzické vrstvy, „zabalí“ je do rámců a odesílá k dalším zpracování vyšším vrstvám. Linkovou vrstvu můžeme ještě rozdělit na dvě podvrstvy – MAC a LLC. MAC má na starosti řízení přístupu ke sdílenému médiu (například společná linka). Často by totiž bez řízení docházelo ke kolizím, kdy by na jednom médiu vysílalo najednou hned několik zařízení. LLC určuje způsob použití linky, řízení toku dat, synchronizaci rámců a kontrolu chyb.

„Podvrstva LLC je definována ve specifikaci IEEE 802.2 a podporuje služby bez spojení i se spojením používané protokoly vyšší vrstvy. Ve specifikaci je definován počet polí v rámcích datové vrstvy, které umožňují většímu množství protokolů vyšší vrstvy sdílet jeden fyzický datový spoj. Podvrstva MAC provádí správu

přístupu protokolu k fyzickému síťovému médiu. Obsahuje definici adres MAC, což umožňuje jedinečnou identifikaci různých zařízení v datové vrstvě.“ (Bigelow, 2004 str. 92)

Detekci a případnou opravu chyb provádí linková vrstva zasláním požadavku na opětovné zaslání poškozeného rámce, které mohou vzniknout při přenosu mezi fyzickými vrstvami, nijak se nezabývajícími kontrolou dat, jenž přijmou či odešlou. Navíc má tedy na starosti fyzické adresování za pomocí jedinečného identifikátoru – MAC adresy. Přenos rámců dokáže přímo zajistit pouze v případě přímého spojení s cílovým uzlem, čili může komunikovat pouze se svými „sousedy“.

4.1.3 Síťová vrstva

Pro komunikaci s uzly nepřímo sousedícími, se využívá další vrstva- síťová, poslední z vrstev orientovaných na přenos dat. Ta přebírá data od vyšších vrstev a vytváří z nich tzv. pakety a zaručuje jejich doručení až k cílovému síťovému prvku. Pro správné doručení je zapotřebí využít směrovač (router), který pracuje právě na této vrstvě.

„Prvotním úkolem síťové vrstvy je podpora výstavby přepojovacích sítí z dvoubodových a vícebodových spojů (v tom případě většinou lokálních sítí). Propojovacími prvky jsou směrovače (router), ty směrují pakety od odesílatele k adresátovi a opírají se přitom o síťové adresy.“ (Janeček, a další, 2003 str. 117)

„Umožňuje přenos přes jednu nebo více fyzických sítí. Síťová vrstva provádí směrovací funkce, také provádí fragmentaci dat v případě, že je to třeba, a také opětovné složení těchto fragmentovaných dat. Síťová vrstva dokáže přemostit různé přenosové technologie přenosu na fyzické úrovni. A měla by zabezpečit kvalitu služby, kterou po ní bude požadovat transportní vrstva.“ (Palovský, 2010 str. 113)

4.1.4 Transportní vrstva

Jak již bylo nastíněno v minulé kapitole, transportní vrstva přímo nepatří v síťovém modelu ISO/OSI do vrstev orientovaných na přenos ani do vrstev zaměřených na služby. Je jakousi mezivrstvou spojující tyto dvě části. Využívá služeb síťové vrstvy, která zajišťuje přenos paketů. Transportní vrstva se tak

zabývá pouze tzv. end-to-end komunikací (komunikace mezi koncovými účastníky). Cílem je poskytovat spolehlivý a transparentní přenos dat.

Rozlišujeme dva typy služeb, které může transportní vrstva nabízet – spojově orientované a nespojové. Spojově orientované spojení nabízí spolehlivost. Zaručuje, že komunikace bude probíhat v pořádku a bez chyb. K tomu se používá potvrzování příjmu všech rámců a ukončení spojení. Pokud by některé rámce nedorazily v pořádku, protokol na transportní vrstvě by si vyžádal jeho opětovné zaslání. Nevýhodou takového spojení je větší vytížení sítě. Příkladem spojově orientovaného protokolu je TCP.

Nespojově orientované protokoly transportní vrstvy oproti tomu neřeší, jestli vše přišlo v pořádku, nebo ne. Není zde žádná kontrola kvality, pouze jednoduché odeslání a příjem dat. Jako příklad můžeme uvést protokol UDP. Použití obou typů protokolů na transportní vrstvě tedy záleží na požadavcích, jestli je důležitější rychlost, jednoduchost a menší zatížení sítě, nebo je třeba dbát na kvalitu přenosu.

4.1.5 Relační vrstva

Název relační vrstvy pochází z jejího hlavního úkolu – navazování a ukončování relací (anglicky sessions) mezi koncovými účastníky. „*Relace* je řada souvisejících přenosů orientovaných na připojení mezi komunikujícími subjekty. Vytvoření relace může vyžadovat ověření uživatelského účtu a stanovení typu komunikace, která se uskuteční.“ (Bigelow, 2004 str. 94)Relační vrstva tedy řídí probíhající komunikace, pokud je to zapotřebí, může určovat, v jaký okamžik bude kdo vysílat a kdo pouze čekat a přijímat. Stejně tak následně spojení ukončuje.

4.1.6 Prezentační vrstva

Prezentační vrstva má za úkol zpracovat data pro vyšší aplikační vrstvu. Úkolem prezentační vrstvy je šifrování a dešifrování, případně i komprese dat, převod mezi znakovými sadami (převod mezi znakovými kódy EBDIC a ASCII) a rozšíření grafických prvků.

4.1.7 Aplikační vrstva

Poslední vrstvou v síťovém modelu ISO/OSI je aplikační. „Aplikační vrstva poskytuje aplikaci přístup ke komunikačnímu médiu. Interaguje přímo s uživatelskou aplikací, které po ní požaduje komunikační služby.“ (Palovský, 2010

str. 114)Tato vrstva je tak nejblíže uživateli, či koncové aplikaci. Vcelku logicky jde také o jedinou vrstvu, která nezajišťuje služby pro žádnou vyšší vrstvu. Příkladem protokolů fungujících na sedmé vrstvě ISO/OSI modelu jsou HTTP, SMTP nebo FTP.

4.2 TCP/IP

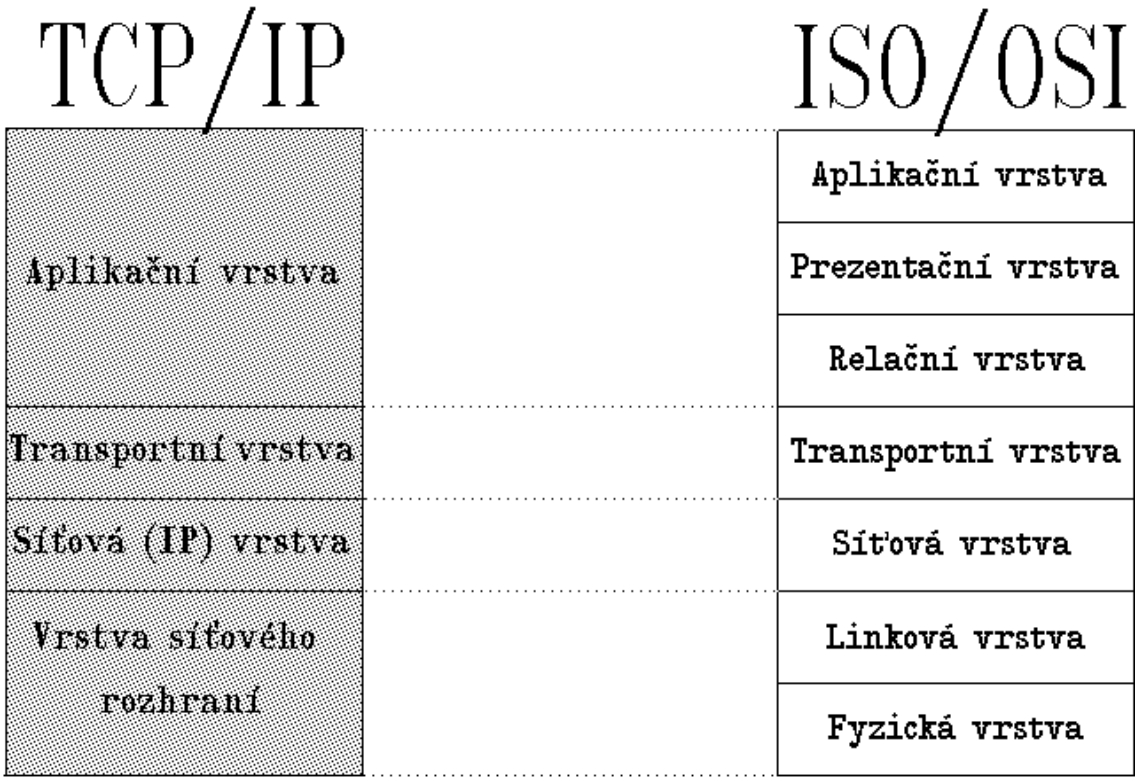
Dnes nejvyužívanější síťovou architekturou je TCP/IP. Protokoly TCP/IP využívá například dnes nejznámější síť Internet. Právě využití TCP/IP v síti Internet v praxi zamezilo globálnímu rozšíření referenčního modelu ISO/OSI. V době ustanovení modelu ISO/OSI už se využívala architektura TCP/IP a přechod by byl velmi nákladný a těžko proveditelný. Model ISO/OSI je totiž poměrně komplikovaný a až příliš obsáhlý.

4.3 Architektura TCP/IP

Architektura TCP/IP využívá, stejně jako model ISO/OSI rozdělení sítě na vrstvy. Nepoužívá však vrstev sedm, ale pouze čtyři. Velké odlišnosti v obou architekturách vznikaly již při jejich vývoji. Model ISO/OSI měl za cíl nabízet co nejvíce funkcí. Tím ale vznikají velké nároky na síť.

„Později se ale ukázalo, že například právě v otázce zajištění spolehlivosti to není nejšťastnější řešení – že totiž vyšší vrstvy nemohou považovat spolehlivou komunikační podsíť za dostatečně spolehlivou pro své potřeby, a tak se snaží zajistit si požadovanou míru spolehlivosti vlastními silami. V důsledku toho se pak zajišťováním spolehlivosti do určité míry zabývá vlastně každá vrstva referenčního modelu ISO/OSI.

Tvůrci protokolů TCP/IP naopak vycházeli z předpokladu, že zajištění spolehlivosti je problémem koncových účastníků komunikace, a mělo by tedy být řešeno až na úrovni transportní vrstvy. Komunikační podsíť pak podle této představy nemusí ztrácet část své přenosové kapacity na zajišťování spolehlivosti (na potvrzování, opětné vysílání poškozených paketů atd.), a může ji naopak plně využít pro vlastní datový přenos.“ (Peterka, 2011)



Obrázek 2 Porovnání TCP/IP a ISO/OSI; dostupné z http://www.earchiv.cz/a92/a231c110.php3

Určitá jednoduchost je patrná i z TCP/IP modelu, který má pouze čtyři vrstvy. V porovnání s ISO/OSI modelem zde dvě vrstvy obstarávají funkci více vrstev z modelu ISO/OSI. Nejnižší je vrstva síťového rozhraní. Jejím úkolem je ovládání přenosové cesty a přímé vysílání a příjem paketů. Vrstva se vždy liší dle použité technologie, proto není blíže specifikována. Nejčastější technologií je Ethernet, proto bývá označována jako Ethernetová vrstva.

Další vrstvou v pořadí je síťová, někdy označovaná také jako IP vrstva. Na této vrstvě tedy pracuje protokol IP. „Úkol této vrstvy je v prvním přiblížení stejný, jako úkol síťové vrstvy v referenčním modelu ISO/OSI – stará se o to, aby se jednotlivé pakety dostaly od odesílatele až ke svému skutečnému příjemci, přes případné směrovače resp. brány. Vzhledem k nespojovému charakteru přenosů v TCP/IP je na úrovni této vrstvy zajišťována jednoduchá (tj. nespolehlivá) diagramová služba.“ (Peterka, 2011)

Transportní vrstva, která následuje, se také označuje za TCP vrstvu. Důvodem je protokol TCP pracující na této vrstvě. Jejím úkolem je zajistit komunikaci mezi dvěma koncovými účastníky. V případě TCP/IP se jedná o entity vyšší vrstvy, tedy aplikační programy. Dále ovlivňuje tok dat oběma směry a zajišťuje spolehlivost. Na této vrstvě také pracuje protokol UDP, který lze označit za méně spolehlivý, ale rychlejší. Vyšší vrstva, přesněji řečeno protokoly vyšší vrstvy, pak můžou rozhodnout, který z protokolů bude využit.

Poslední vrstvou je aplikační. V porovnání s modelem ISO/OSI tato vrstva zastupuje také funkce prezentační a relační vrstvy, které v TCP/IP vůbec nenajdeme. V aplikační vrstvě jsou jako entity zastoupeny aplikační programy. Absencí prezentační a relační vrstvy musí tyto aplikační programy komunikovat přímo s transportní vrstvou a musí si zároveň zajistit jejich funkci samy. Příkladem aplikačních programů jsou FTP, HTTP nebo DHCP (Dynamic Host Configuration Protocol).

4.4 Protokoly TCP/IP

Přesto, že je zkratka složena z protokolů TCP a IP, které jsou základem v této architektuře, je nutné si pod tímto pojmem představit hned několik dalších protokolů, které se v síti Internet využívají. Proto se lze často setkat s pojmem „rodina TCP/IP protokolů“.

„V současném internetu máme obrovské množství protokolů. Některé z nich jsou v činnosti, pokud uživatel požaduje nějakou akci, jako je například protokol SMTP, který přenáší poštu mezi účastníky, protokol HTTP, který přenáší stránky WorldWide Webu nebo protokoly SIP a RTP, které se používají při navázání spojení a vlastním přenosu dat při telefonování přes internet. Jiné jsou v činnosti (po nastavení) automaticky bez přímého požadavku uživatele, jako NTP protokol umožňující časovou synchronizaci počítačů přes internet nebo DNS zprávy, které řeší překlad mezi lidmi používanými doménovými adresami a interně v síti používanými adresami IP protokolu.“ (Palovský, 2010 str. 21)

4.4.1 IP

Protokol IP je jedním ze síťových protokolů, který je základem pro další protokoly. Je také jedním z hlavních. „Protokol IP je založen na principu hostitelů a sítí.

Hostitel je jakékoli zařízení v síti, které je schopné odesílat a přijímat pakety IP. Hostiteli IP proto mohou být směrovače, pracovní stanice, servery či každé zařízení s adresou IPO skupině hostitelů sdílejících společnou strukturu adres se říká, že je ve stejné síti.“ (Bigelow, 2004 str. 102)Hostitelem jsou tedy aktivní síťové prvky, které se zapojují do komunikace v síti. Základním kamenem protokolu IP je možnost hostitelů, kteří jsou ve stejné místní síti (LAN), komunikovat navzájem přímo. Pokud jsou ale hostitelé každý v jiné síti, je nutné pro jejich komunikaci využít směrovač pro směrování mezi dvěma sítěmi.

„Když pochopíme základní pravidlo sítě IP, ihned je zřejmé, proč dva hostitelé sdílející společnou linku, ale odlišné síťové adresy, nebudou schopny komunikovat přímo mezi sebou. I v této konfiguraci by musel být využit směrovač. Skutečnost, že jsou na stejné fyzické lince, neznamená, že by zařízení mohla komunikovat přímo.“ (Bigelow, 2004 str. 102)

IP protokol provádí doručování paketů v síti. Zároveň definuje jeho přesný formát. Podobně jako pošta, která dopravuje obálky, je IP protokol zodpovědný za doručení paketů. K tomu využívá IP adres jako identifikátorů v místní síti. Po doručení paketů se již nestará o doručení potvrzení, vysílací klient tedy neví, jestli se data doručila, nebo ne. Stejně tak nezaručuje doručení ve správném pořadí.

„Definice IP protokolu v současnosti používané jsou dvě. IP protokol verze 4 – původní definice IP protokolu, používaná od 70 let, a IP protokol verze 6 definovaný v 90 letech. Ostatní verze protokolu byly pouze experimentální a nebyly zavedeny do praktického využití.“ (Palovský, 2010 str. 50)Problémem verze 4 se stal nedostatek IP adres. Tato problematika je detailněji popsána v kapitole IP adresy.

4.4.2 TCP

Protokol TCP (TransmissionControlProtocol) je dalším ze základních protokolů použitých v TCP/IP. Tento protokol navazuje v sítích duplexní (data lze posílat oběma směry nezávisle na sobě) spojení mezi dvěma aplikacemi. Zároveň se zajímá o správné doručení paketů a jejich případné znovu zaslání, pokud jsou poškozené, nebo nedorazí do cíle. Pracuje na transportní, tedy třetí vrstvě. Zatímco

protokol IP dopravuje pakety mezi klienty, TCP zajišťuje dopravu mezi dvěma konkrétními aplikacemi pracujícími na těchto klientech.

„TCP je protokol se spojením. Byl navržen speciálně pro nespolehlivou síť, tj. nespolehlivý přenos s možností ztráty či duplikace paketů. TCP rozděl zprávu do segmentů o max. délce 64 kbyte. Z každého segmentu vytvoří pak IP samostatný datagram. Celá zpráva je očíslována tak, že od počátku zprávy je každému bytu přiděleno pořadové číslo. Tato čísla se využívají v položkách TCP segmentu (pořadí a potvrzení).“ (Jandoš, 1995 str. 117)

Spolu s protokolem TCP musíme ještě zmínit protokol UDP, který je jakousi alternativou. Pracuje taktéž na transportní vrstvě, stejně tak vytváří spojení mezi dvěma aplikacemi. Rozdílem ale je, že nekontroluje stav paketů v koncovém zařízení, neřeší pořadí, v jakém data odesílá a zakládá si na jednoduchosti. Výhodou je tedy menší režie v síti.

4.4.3 ICMP

Posledním ze základních protokolů v TCP/IP je ICMP. Jedná se o řídící protokol, který umožňuje ohlašovat chyby a žádat o jejich řešení, sám je však neřeší. Obvykle takovou zprávu zasílá nějaký prvek uvnitř sítě systému, který odesílal data, a v ní jej informuje o něčem mimořádném. Třeba o tom, že byl nucen jeho paket zničit, nebo o tom, že správná cesta je jiným směrem. A je na odesílajícím systému, aby odpovídajícím způsobem reagoval. Protokol informuje odesílající systém o situacích, které jsou trvalejšího charakteru. Jsou to situace, které by opětovně nastaly, pokud by odesílající systém znovu odeslal stejný paket. (Palovský, 2010)

5 IP a MAC adresy

Stejně jako v jiných odvětvích lidské společnosti, je i v počítačových sítích pro správné přijímání a odesílaní důležité jednoznačně a unikátně odlišit každé zařízení, které se chce zapojit do provozu v síti. Těžko si lze představit počítačovou síť, kde by nebyl každý prvek odlišen od ostatních a neměl svou unikátní adresu, která jej také odliší.

5.1 IP adresa

IP adresa je, podobně jako MAC adresa, identifikátor zařízení připojených do počítačové sítě, nicméně je využíván jinými protokoly pracujícími na jiné vrstvě síťového ISO/OSI modelu. IP adresu má jak klient (může mít i více, pokud má více síťových karet), tak i aktivní síťové prvky, a je součástí správného doručování paketů, které využívá IP – Internet Protocol. V průběhu vývoje však nastal problém s nedostatkem těchto adres.

Nedostatek IP adres se stal s velkým rozmachem internetu značným problémem. Používaná verze IP protokolu – verze 4, umožňuje vytvořit „pouze“ 2^{32} adres. Vzhledem k faktu, že každý prvek v síti musí mít svou IP adresu, začalo volných IP adres ubývat. I přes všemožné snahy se nepodařilo ubývání zastavit. S úbytkem pomáhá například zmíněný DHCP protokol, funkce CIDR nebo NAT servery. Ty umožňují připojovat se celé LAN síti na Internet přes jeden port směrovače.

„Kvůli nedostatečnému globálnímu adresnímu prostoru protokolu IPv4 musejí hostitelé používat mechanismy, které dovolují překládat interní (privátní) adresní prostor IP na menší adresní prostor (nebo dokonce na jedinou IP adresu) s možností externího směrování. Díky překladu adres NAT může více zařízení v rámci jedné organizace používat lokální privátní adresy (RFC 1918) a přitom sdílet jednu nebo více globálních IPv4 adres k externí komunikaci. Technologie překladu adres NAT sice krátkodobě zpomalila vyčerpávání adresního prostoru IPv4, ale obecně komplikuje obousměrnou komunikaci mezi aplikacemi.“ (McFarland, a další, 2011 str. 22)

Různá řešení problémů s nedostatkem adres tedy pouze problém oddalovala, ale žádné ho nedokázalo vyřešit. Hlavním řešením problému bylo přestavení IP protokolu verze 6, která pracuje se 128 bity a umožňuje tedy mnohem větší rozsah adres. Nasazení nové verze však není tak jednoduché, protokol IPv6 není zpětně kompatibilní a zařízení, umožňující komunikaci pouze ve verze 4 nemohou samostatně komunikovat s verzí 6. Musí se tedy vyměnit všechna zařízení, která spolu v síti komunikují, nebo musí být použity poměrně složité techniky na překlad komunikace.

„Adresy počítačů v IP protokolu verze 4, což je současný nejvíce používaný protokol, jsou 32 bitové. Pro počítač jsou to homogenní 32 bitová čísla, nicméně pro používání lidmi zavedli autoři konvenci, kdy 32 bitové číslo se píše jako čtveřice 8 bitových čísel, oddělených od sebe tečkami a zapisovaných dekadicky.“ (Palovský, 2010 str. 50) Teoreticky tak existuje rozsah adres 0.0.0.0 až 255.255.255.255, ale spousta z těchto adres je rezervována.

5.1.1 Třídní a beztřídní logika IP adres

Z 32 bitového čísla pro IP adresu je vždy jedna část vyhrazena na adresu sítě a druhá část vyhrazena na adresu konkrétního uzlu. Pro příklad si můžeme uvést adresu domu, kdy část IP adresy pro konkrétní uzel představuje ulici a číslo domu a druhá část adresy pak bude určovat město, ve kterém se dům nachází. Celý adresní prostor IP se rozděluje na tzv. třídy adres, pak se jedná o třídní logiku. Dále existuje logika beztřídní.

O tom, jak velká bude část pro adresu sítě a jak velká bude pro adresy klientů, rozhoduje právě třída adres. „Každá adresa třídy A, B a C se navíc skládá ze dvou částí (pokud netvoříme podsítě), a sice ze síťové části a hostitelské části. Typ třídy určuje velikost obou částí, kterou můžeme explicitně určit také pomocí výchozí masky třídy: výchozí maska sítí třídy A je například 255.0.0.0 a má tedy 8 binárních nul, což znamená 8 bitů síťové části a 24 bitů hostitelské části.“ (Odom, a další, 2009 str. 113)

Třída skupina A tedy má 24 bitů volných pro adresy klientů a osm pro adresy sítí. Síť s adresami skupiny A tedy může mít 2^7 možných kombinací pro adresu sítě a 2^{24}-2 adres pro klienty. Dvě adresy jsou totiž v každé síti rezervované a nelze je použít jako adresu klienta. Jedná se o tzv. všesměrovou adresu označující celou síť jako celek. Třídy B a C mají vždy o osm bitů více pro adresy sítě, ve skupině adres typu C může být až 2^{21} adres pro sítě a 2^8 adres pro klienty.

V průběhu let, hlavně jako reakce na docházející IP adresy, se zavedla beztřídní logika. V takové logice neexistují žádné třídy adres a odstraňují hlavní nevýhodu třídního dělení – velké plýtvání. Ve většině případů totiž nebylo využito zdaleka všech adres, které poskytnutá třída nabízela. „Beztřídní dělení adres zobecňuje možnosti rozdělení adresy mezi část *adresa sítě* (network address) a část *adresa systému* (network address) ze tří možných hranic, které byly na hranicích jednotlivých bytů, na libovolnou hranici, která může být na libovolné bitové hranici.

Určení, kde tato hranice bude, se děje objektem nazývaným *síťová maska* (network mask, subnetmask) Síťová maska specifikuje, kde takové dělení nastává. Jeden ze způsobů zápisu je uvedení počtu bitů síťové části adresy (prefixu). Uvádí se jako číslo za lomítkem. Tento zápis se používá ve spojení s adresou sítě. Např. 146.102.194.0/23 znamená, že máme specifikovanou adresu sítě, a maska je na 23. bitu.“ (Palovský, 2010 str. 54)

Adresu IP musí mít každý z prvků síťového provozu, je proto potřeba adresu každému prvku nastavit, nebo využít služeb protokolu DHCP, který dokáže řídit přidělování IP adres novým prvkům. Adresy přidělené protokolem DHCP nazýváme dynamické, adresy pevně nastavené uživatelem zase statické. Výhodami dynamického přidělování adres jsou jednoduchost, obzvláště při použití u velkých sítí a také šetření IP adres. Ta se totiž klientovi pouze „propůjčí“ na určitý čas, poté je buď obnovena, nebo může být znovu použita pro jiného klienta.

5.2 MAC adresa

MAC adresa je jedinečná adresa, přiřazená každému aktivnímu prvku v síti při jeho výrobě. Využívá se při komunikaci v síti jako jednoznačný identifikátor, proto žádné prvky v síti nesmí mít stejnou adresu. Proto udělování MAC adres celosvětově řídí organizace IEEE a každý výrobce síťových prvků dostane přesné hodnoty, které může využít. Díky jedinečnosti MAC adres tak například lze na aktivním síťovém prvku nastavit určitá omezení pouze pro určité MAC adresy, tedy klienty. Můžeme tím omezit přístup určitým klientům třeba k internetu, cožje využíváno ve firmách, školách a podobně.

Fyzická adresa, jak se MAC adrese říká, protože je součástí každé síťové karty, se celkem skládá ze 48 bitů a obvykle je zapsána 3bajtovým hexadecimálním číslem (např. 21-A7-5E-F2-A0-FA). Maximálně je možné využít 2^{48} možných adres. První polovina fyzické adresy identifikuje výrobce, který používá stále stejné značení (velcí výrobci mají k dispozici několik adres). Druhá polovina je již přidělována přímo výrobcovým libovolným systémem, ale musí se dodržet jedinečnost adres.

I přes skutečnost, že MAC adresy byly původně koncipovány jako stálé, bez možnosti je jakkoliv upravovat, lze v dnešní době adresu změnit v nastavení síťové karty, což může pomoci při problému vzniklém výměnou staré síťové karty

v počítači za novou. Může se totiž stát, že poskytovatel připojení k Internetu zpřístupní pouze na jednu jedinou MAC adresu a změnou síťové karty se MAC adresa klienta změní. V takovou chvíli lze MAC adresu změnit a přepsat ji na adresu staré síťové karty. Pro zjištění MAC adresy můžeme v systémech Windows v Příkazovém řádku použít příkaz „*ipconfig /all*“, který vypíše seznam všech MAC adres spojených s klientem. Změna MAC adresy se také používá při obcházení zabezpečení sítě. Z toho důvodu se může v praxi stát, že budou mít v síti všechny zařízení unikátní MAC adresu a proto komunikace mezi nimi nemusí fungovat správně.

Rozlišujeme několik typů MAC adres – jednosměrová, všesměrová a vícesměrová. Jednosměrová adresa označuje pouze jedno konkrétní zařízení, je to tedy adresa jednoho prvku v dané síti. Všesměrová adresa se využívá, pokud chce některý z prvků sítě komunikovat se všemi prvky v lokální síti. Taková adresa má vždy stejnou hodnotu – FF-FF-FF-FF-FF-FF (nebo binárně samé jedničky).

„Vícesměrové rámce sítě Ethernet slouží ke komunikaci s potencionálně dynamickou podmnožinou zařízení v síti LAN. Nejčastěji se pomocí nich řeší vícesměrové vysílání IP. Jestliže má například určitá síť LAN 100 uživatelů, z nichž tři budou pomocí video aplikace postavené na vícesměrovém vysílání, sledovat jistý proud videa, může tato aplikace zasílat jediný vícesměrový rámec. Dotčená tři zařízení se na tento přenos připraví tím, že začnou naslouchat rámce zaslané na příslušnou vícesměrovou adresu sítě Ethernet a začnou je zpracovávat.“ (Odom, a další, 2009 str. 42)

6 Směrování v sítích TCP/IP

Pojmem směrování (anglicky routing) rozumíme způsob, jakým síťové protokoly zasílají IP pakety v síti. Při přenosu dat, o který žádá aplikace pracující na aplikační vrstvě síťového modelu ISO/OSI. Data se při zpracování protokoly v dalších vrstvách „zabalí“ do PDU (Prokolová datová jednotka) – základní označení pro data přenášená mezi entitami pracujícími ve stejné vrstvě. O doručení PDU se poté stará protokol IP.

„Směrování IP datagramů je velice podobné třídění dopisů na poště. Na poště mají třídící stůl s vyřezanými otvory. Pod každým otvorem je přivázán poštovní pytel. Nad otvorem jsou napsány názvy měst, kam je z místní pošty přímé poštovní spojení. Třídění probíhá tak, že úředník bere dopis za dopisem. Na každém dopisu si prohlédne adresu. Je-li adresát z Brna, pak dopis vhodí do otvoru Brno. Je-li adresát z Roztok u Prahy, pak dopis vhodí do otvoru Praha. Až poštovní úředník vytřídí všechny dopisy, pak pytel po pytli odváže z třídícího stolu. Každý pytel zaváže a přiváže k němu visačku, na kterou napíše název města, kam se má pytel odeslat. Poté se pytel naloží…“ (Dostálek, a další, 2008 str. 187)

V počítačových sítích si na pozici úředníka pošty můžeme představit směrovač (router), který podobným způsobem třídí IP datagramy. Datagramy pak nehází do pytlů, ale rozhoduje, kterému ze svých sousedů, a tedy kterým svým portem, datagramy odešle. Takto musí směrovač usměrnit každý datagram, který byl do sítě vyslán.

Důležité v problematice směrování je rozlišit, zda se cílový klient nachází ve stejné síti, jako zdrojový (vysílající) klient. Pokud tomu tak je, mohou si data „zabalená“ v datagramech zaslat přímo. Jedná se o přímé směrování. Zda cílový klient leží ve stejné síti, pozná zdrojový klient podle IP adresy cíle. Takové směrování je jednoduché, má nízkou režii. Často je však potřeba směrovat data do jiné sítě.

Pokud klient zjistí, opět z IP adresy, že jeho cílový klient je v jiné síti, odešle datagramy na směrovač spojující tyto dvě sítě. Takový směrovač se nazývá branou – spojuje dvě sítě, je hraničním bodem těchto sítí. Zaslaný datagram tedy obdrží brána a zdrojový klient se dále o doručení nestará. Je tedy úlohou směrovače, aby zajistil doručení datagramu. Nastat může také situace, kdy bude cílový klient

dostupný pouze cestou přes několik směrovačů – bran. V tom případě směrovač vždy volí nejlepší cestu, odešle datagram na sousední směrovač. Zajímá se vždy pouze o přímého souseda, v angličtině nazýváno „hop“. Pokud datagram na cestě projde celkem přes tři brány, bude cesta „dlouhá“ tři hopy.

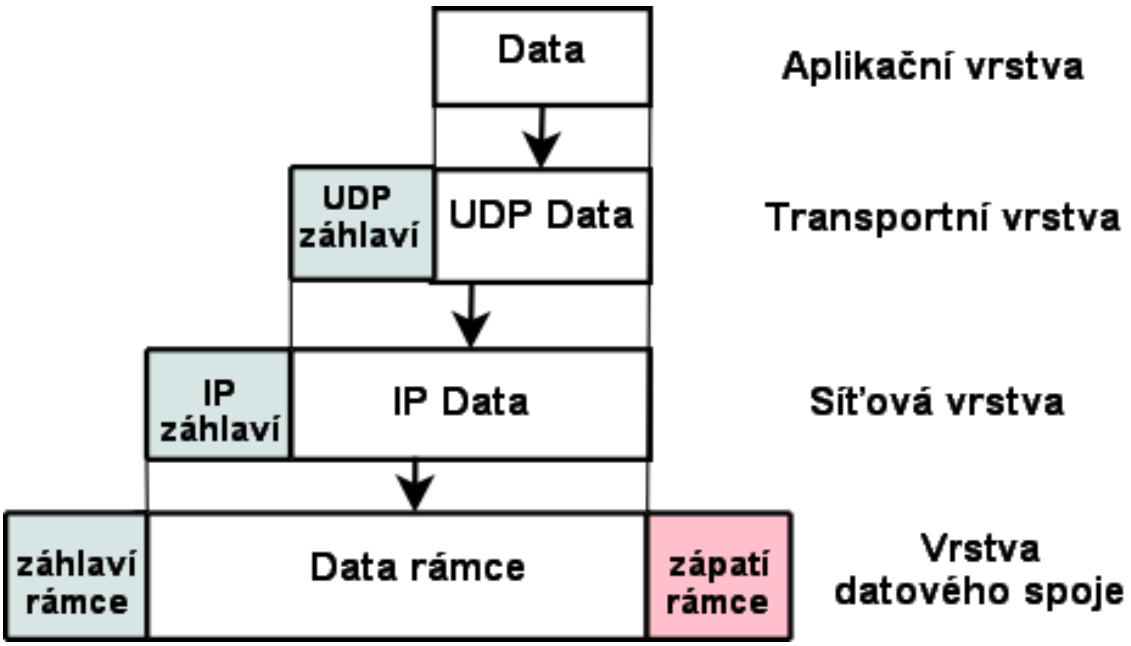
Směrovač při výběru ideální trasy pro datagram zohledňuje právě počet hopů, nemusí to však jediným faktorem pro vhodný výběr trasy. Lépe řečeno je na směrovacích protokolech, které určují, jakým stylem bude výběr trasy probíhat. Například vývojově velmi starý, ale přesto stále občasně, pro svojí jednoduchost využívaný, protokol RIP zohledňuje právě pouze počet hopů. Tento protokol omezuje maximální počet hopů na 15, jakékoliv překročení tohoto počtu je nežádoucí a datagram je smazán. Novější a modernější směrovací protokoly zohledňují mnohem více faktorů, jako je například šířka pásma nebo zpoždění.

Při prvním zapojení směrovače do komunikační sítě, nemá ve své paměti uloženy žádné informace o topologie sítě. K ukládání používá tzv. směrovací tabulku. Do ní si ukládá veškeré informace potřebné ke směrování. Data jsou uložena v řádcích a seřazena od nejkonkrétnějších adres po nejobecnější. Při příjmu datagramu směrovač přečte cílovou adresu a porovná ji se svojí směrovací tabulkou. Pokud najde shodu, pošle datagram svým příslušným portem cílovému zařízení, nebo častěji, pokud se nenachází ve stejné síti, ho odešle sousednímu směrovači, který je na cestě k cíli. Stejným způsobem fungují všechny směrovače v cíli, vždy řeší pouze své přímé sousedy a další směrování nechávají přímo na nich.

6.1 Datové jednotky

Dalším důležitým pojmem jsou datové jednotky. Datovou jednotkou rozumíme nejmenší možnou jednotku, přenášenou v síti. PDU obsahuje vždy, kromě samotných přenášených dat, také informace potřebné k jeho doručení a informace o odesílajícím. Označení pro protokolovou datovou jednotku se vždy liší podle protokolu, který datovou jednotku vytvořil. Rozlišujeme tak několik pojmů, které musíme rozlišovat pro správné pochopení síťového provozu.

Uvažujme o datových jednotkách v sítích TCP/IP. V takové síti vzniknou na aplikační vrstvě data, která vyžaduje konkrétní aplikace zaslat cílové aplikaci na jiném klientovi v síti. Aplikační vrstva data doplní o aplikační hlavičku a zašle je nižší vrstvě – transportní. Ta v případě nutnosti data rozdělí na části a přidá hlavičku TCP nebo UDP dle využitého protokolu. Na síťové vrstvě, kde pracuje IP protokol, se doplní IP hlavnička a vznikne IP paket. Poslední je vrstva síťového rozhraní, která doplní ethernetovou hlavičku na začátek a tzv. *trailer* na konec. V něm je obsažen kontrolní součet (viz obrázek 2 – zapouzdření dat při využití UDP protokolu). Výsledkem je ethernetový rámec. Celý tento proces se nazývá zapouzdřování (encaplsulace) a probíhá vždy od nejvyšší vrstvy směrem dolů.



Obrázek 3 Zapouzdření dat v TCP/IP; dostupné z https://is.mendelu.cz/eknihovna/opory/download.pl?objekt=447

Zapouzdřování se provádí při odesílání dat k jinému klientovi v síti. Na opačné straně probíhá proces přesně opačný. Ve chvíli, kdy cílový klient přijme rámec, začne postupně s jeho zpětným rozbalováním (deencapsulace), vždy od nejnižších vrstev (vrstva datového spoje) po vrstvu nejvyšší (aplikační). Na konci procesu rozbalení zůstanou pouze data, která byla cílem přenosu a jsou zpracována cílovou aplikací.

Názvy datových jednotek se rozlišují dle protokolů, které je vytvoří. Postupně tedy vzniká na každé vrstvě síťového modelu jiná datová jednotka. Názvy jednotlivých datových jednotek tedy rozlišujeme na:

- Zprávy – aplikační vrstva
- Segmenty – transportní vrstva
- Pakety – síťová vrstva
- Rámce – linková vrstva
- Datové „proudy“ (anglicky streams) – fyzická vrstva

7 Výuka počítačových sítí

Výuku počítačových sítí můžeme rozdělit na dvě části – praktickou a teoretickou. Její rozdíl je zřejmý. V teoretické části žáky a studenty seznámíme s problematikou a teorií, v praktické části si mohou zkusit fyzické zapojení síťových prvků a jejich nastavení. Vzhledem k obsáhlosti tématu počítačových sítí se můžeme setkat se středními školami, které mají počítačové sítě jako své oborové studium. Je tedy těžké určit, jak moc by se měli studiu počítačových sítí věnovat studenti jiného zaměření středních škol a žáci základních škol.

7.1 Výuka počítačových sítí na základních školách

Žáci na základních školách by jistě měli přijít s počítačovými sítěmi a jejich výukou do styku. Sítě a hlavně Internet jsou součástí jejich života a je vhodné, aby měli alespoň představu o jejich fungování. Je ale pravdou, že celá výuka předmětu informatika je téma obsáhlé a při poměrně malé časové dotaci, kterou tento předmět na základních školách dostává, není ani možné věnovat počítačovým sítím mnoho prostoru. Žáci si musí osvojit samotné základy ovládání PC, pochopit základní princip jeho fungování nebo například základy práce s textovými a tabulkovými editory.

Při náhledu do školních vzdělávacích programů některých základních škol si myslím, že výuce sítí je věnován poměrně dostatek času a pokud nebude zvýšena časová dotace na předmět informatika, není vhodné zařazovat výuku počítačových sítí na úkor jiných témat. Žáci ve výuce přicházejí do styku se základem Internetu, jeho využívání, možných rizicích, používání vyhledávačů a práce s nimi a základní seznámení s dalšími funkcemi, jako je e-mail.

Jiná situace nastává v případě volitelných, zájmových kroužků. Žáci základních škol se mohou dobrovolně zapsat a navštěvovat zájmové kroužky zaměřené na konkrétní předměty. V těchto kroužcích je více prostoru pro výuku informatiky a možnost probrat učivo konkrétněji. Také se zde počítá se zvýšeným zájmem žáků, kteří dobrovolně navštěvují tyto hodiny. Bohužel, ne každá ze základních škol má ve své nabídce kroužky informatiky.

Na tomto zájmovém, či povinně volitelném kroužku by bylo pro žáky jistě přínosné dozvědět se o počítačových sítích více a zkusit si i praktické zapojení. Otázka teoretické části je zřejmá, žáci by byli poučeni o fungování počítačových sítí obecně (popis síťových prvků, pojmy IP adresa, paket, směrování, síťový protokol, případně další dle časové dotace). Bohužel horší situace nastává v otázce praktické části. Vybavení základní školy není zpravidla nijak připraveno na takto pokročilou výuku a v prostředí běžné počítačové učebny není možné, aby žáci vytvořili a nastavili fyzickou počítačovou síť.

7.1.1 Síťové simulátory

Jedinou možností, kterou lze provozovat i v prostředí základní školy, tak zůstává využití programů, které simulují počítačové sítě. Tyto simulátory umožňují programově zapojovat síťové prvky, vytvořit tak vizualizaci sítě a některé z nich umožňují i detailnější nastavení a je možné je provozovat v prostředí běžné počítačové učebny. Jsou vhodným doplňkem pro pochopení alespoň základních principů funkcí počítačových sítí.

Funkce a možnosti simulátorů se liší dle jejich zaměření, určení a třeba i ceny. Některé z nich jsou kompletně zdarma, jiné jsou pouze pro použití v rámci nějaké konkrétní výuky a některé jsou placené. Pro využití v rámci základních a středních škol nás budou zajímat pouze programy, jejichž použití není omezené ani zpoplatněné. Nabídka je relativně velká, jako příklady můžeme uvést Omnet++, PacketTracer, ns-3, GNS3 nebo PSImulator, vyvinutý na ČVUT v Praze.

Zajímavou volbou by byl program PacketTracer, je poměrně jednoduchý na základní ovládání a přehledný. Jeho použití je však zdarma pouze pro studenty Cisco Networking Academy. Ze zbývajících volně dostupných simulátorů lze doporučit využívat PSImulator, který je dostupný pod licencí GNU GPL v3 a je tedy pro využití ve školní výuce k dispozici zdarma. Byl vyvinut pro výuku počítačových sítí na ČVUT a je zaměřen na začátečníky a mírně pokročilé uživatele.

Vzhledem k zaměření programu je jeho ovládání jednoduché a rychle pochopitelné. Jeho další výhodou je možnost spustit ho na operačních systémech Windows, Mac OS i Linux. V následující části je obsažena jednoduchá ukázka, která

by mohla posloužit jako podklad pro výuku na základních školách nebo středních školách a gymnáziích s jiným než IT zaměřením.

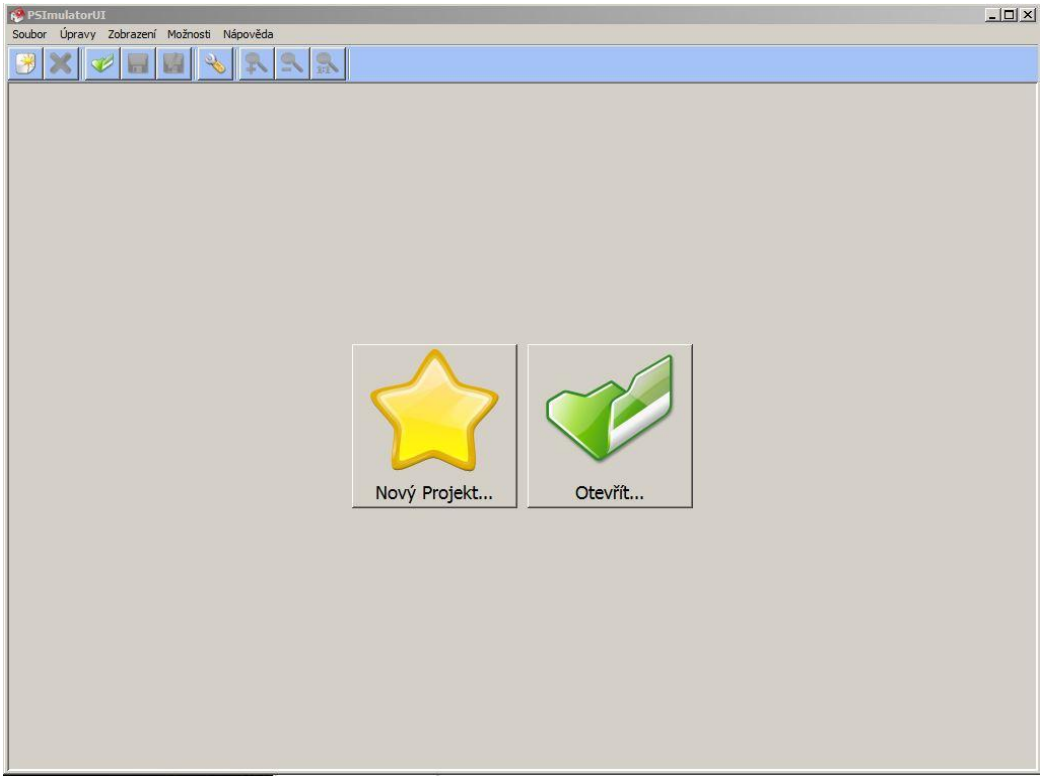
7.1.2 Zadání praktických úkolů

Příklad č. 1 - vytvořte model sítě, který bude obsahovat:

- jeden přepínač (switch)
- čtyři klienty
- klienty vzájemně propojte s přepínačem
- projekt uložte jako *Mala_sit*

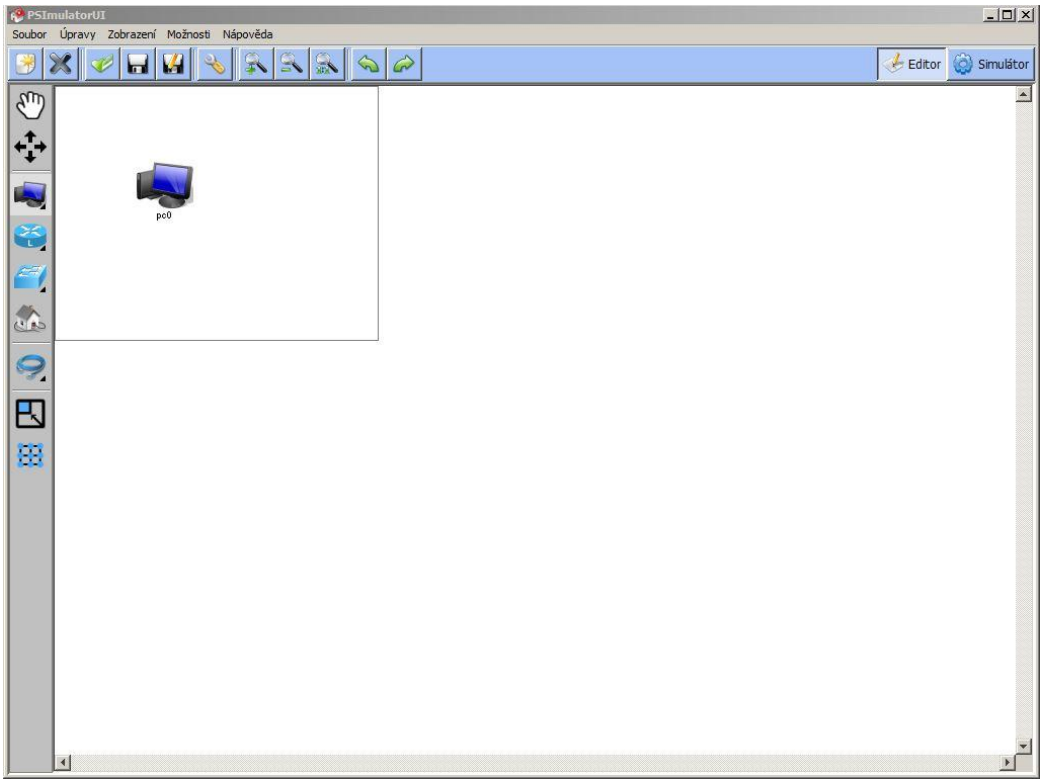
Postup řešení:

- Spustíme aplikaci PSImulator, zvolíme možnost Nový Projekt…



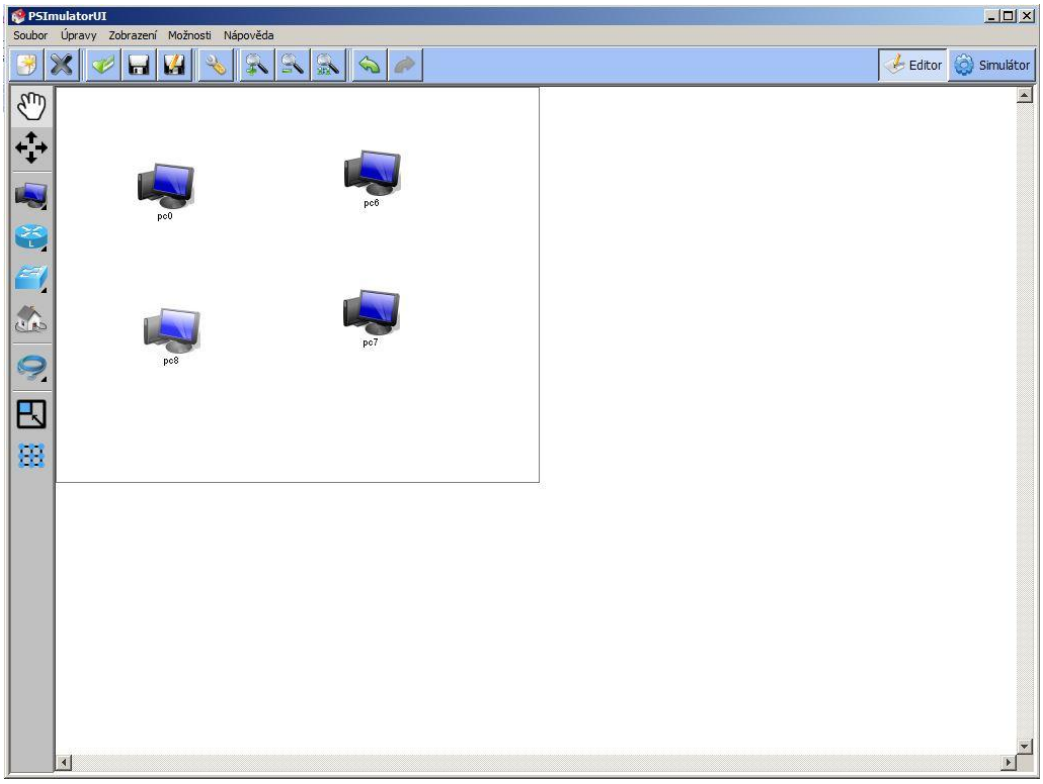
Obrázek 4 Řešení příkladu č. 1

- V novém okně na levém okraji vybereme z panelu síťových prvků ikonku počítače, která reprezentuje síťového klienta. Na ikonku klikneme levým tlačítkem myši a poté znovu levým tlačítkem libovolně do pracovní plochy.



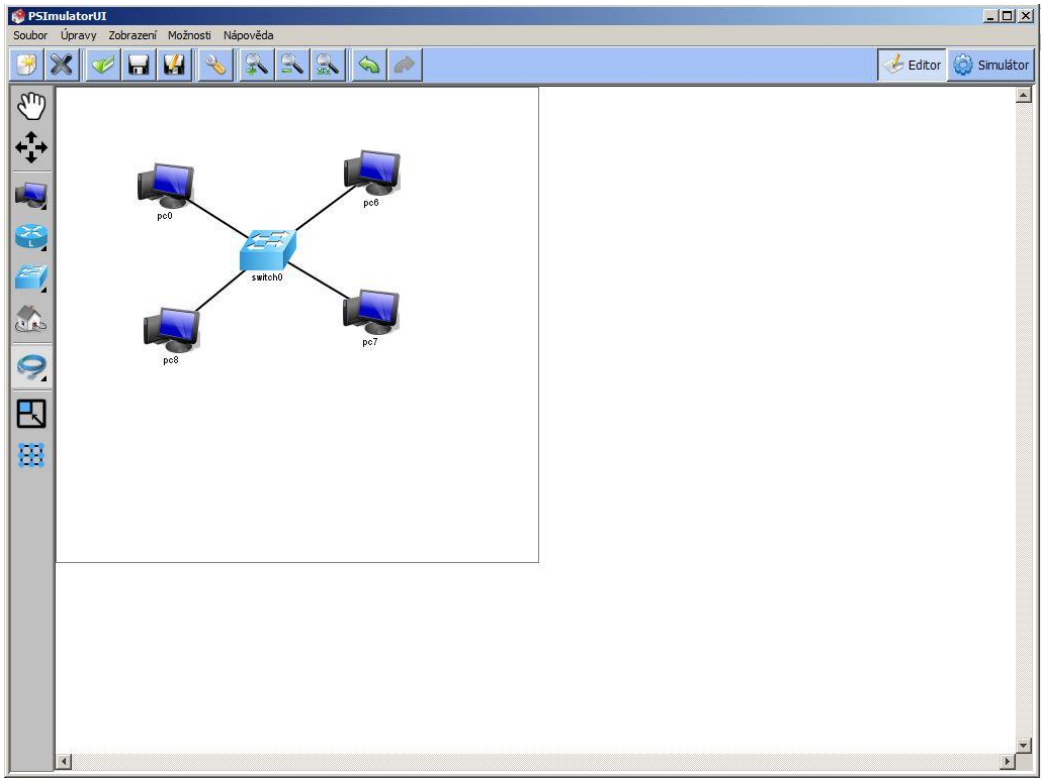
Obrázek 5 Řešení příkladu č. 1

- Stejným způsobem přidáme do naší virtuální sítě další tři klienty. Rozmístění prvku můžeme ještě upravovat nástrojem Ruka v levém menu.



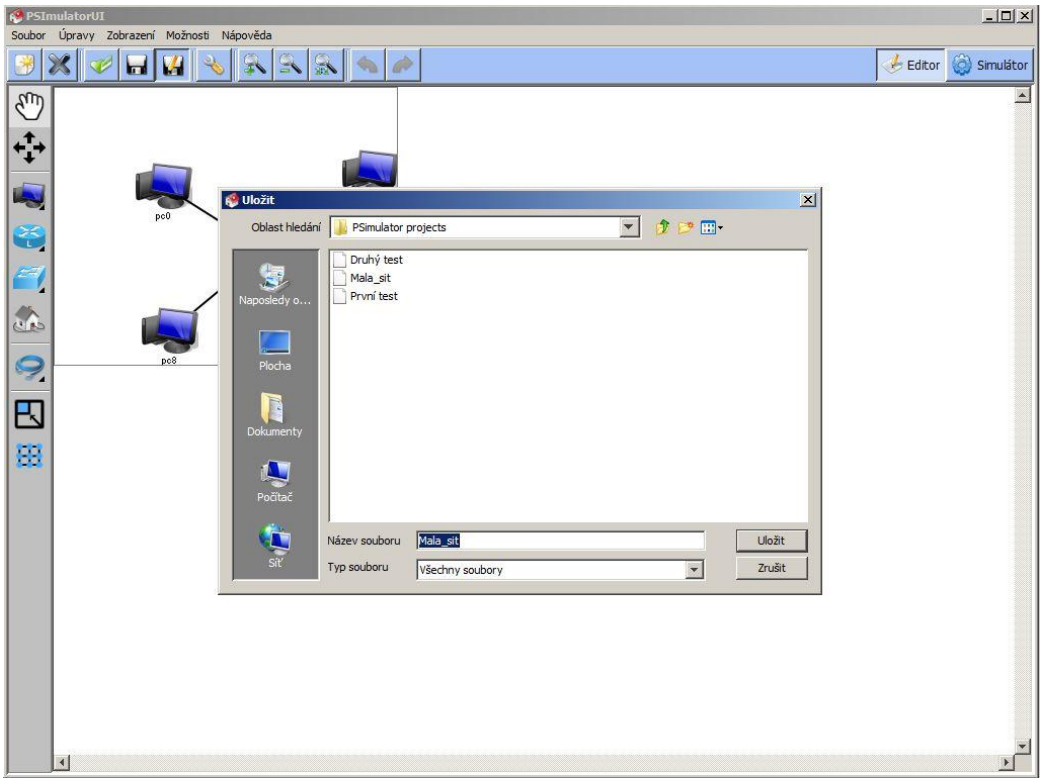
Obrázek 6 Řešení příkladu č. 1

- Následně do sítě přidáme přepínač (switch). Přepínač umístíme na pracovní plochu a následně klienty propojíme s přepínačem. V levém menu vybereme položku Ehternetový kabel, klineme levým tlačítkem myši na jednoho z klientů a poté na přepínač.



Obrázek 7 Řešení příkladu č. 1

- Vytvořenou síť uložíme pomocí tlačítka Uložit Jako… v horním menu. Vybereme adresář, do kterého projekt uložíme, do Názvu souboru napíšeme *Mala_sit*a projekt uložíme.



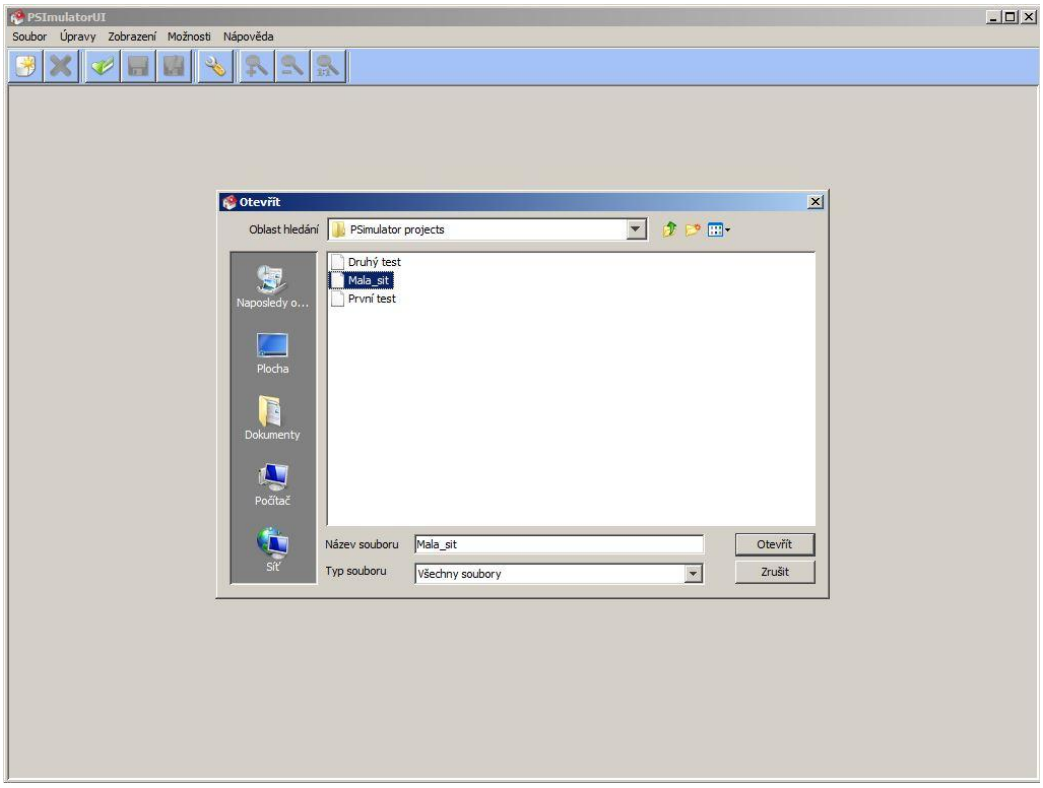
Obrázek 8 Řešení příkladu č. 1

Příklad č. 2 –vytvořte celkem tři sítě, které:

- Obsahují každá čtyři klienty a jeden přepínač
- Alespoň jedna ze sítí musí obsahovat alespoň jeden notebook
- Sítě vzájemně propojte s využitím směrovače (router) – musí být značky Cisco
- Využijte vytvořený projekt z Příkladu č. 1

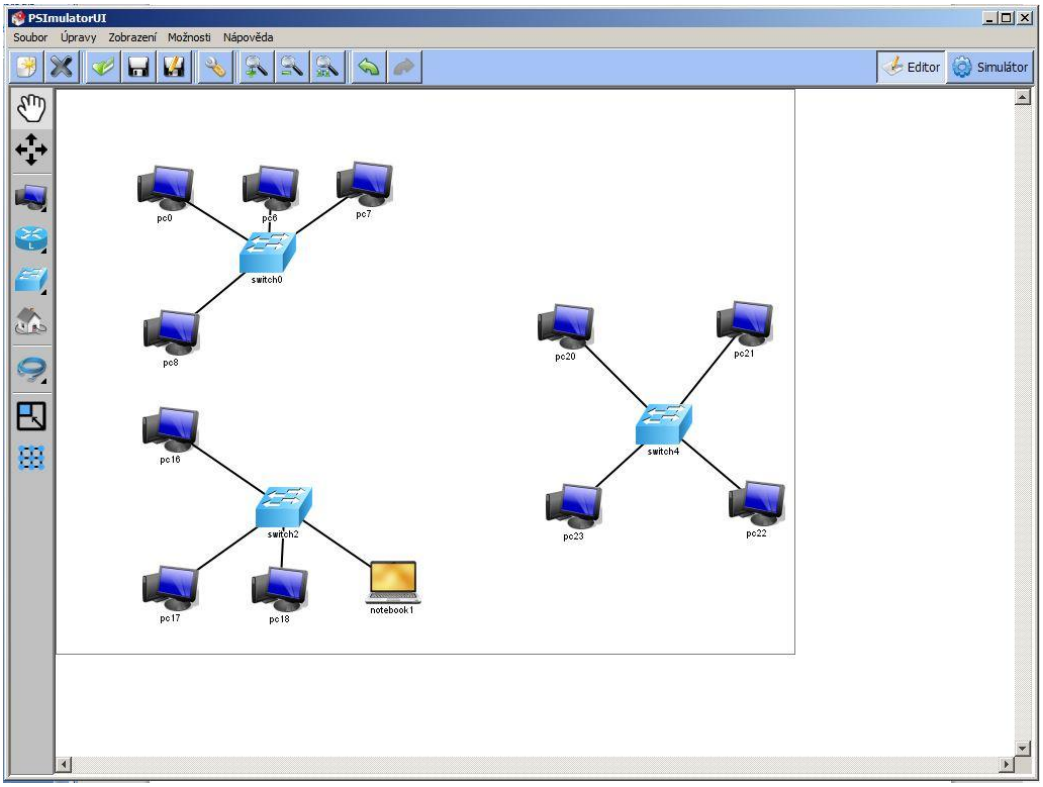
Postup řešení:

- Spustíme program PSImulator, klikneme na ikonku Otevřít..., v adresáři vybereme soubor *Mala_sit*



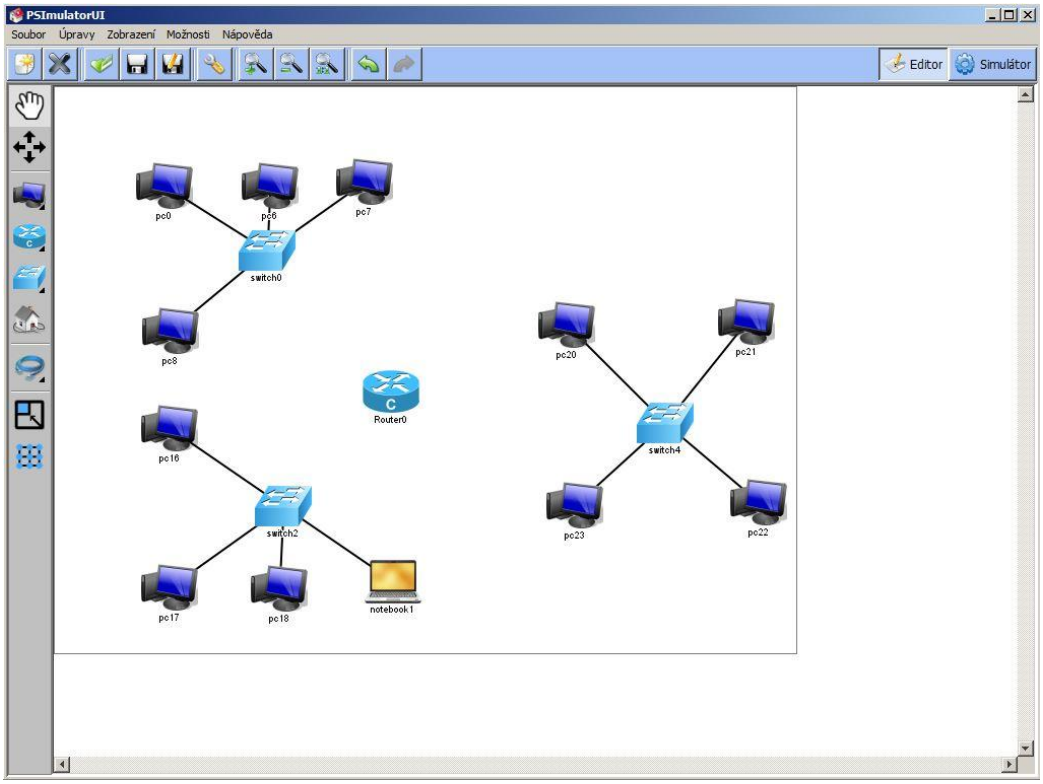
Obrázek 9 Řešení příkladu č. 2

- Vytvoříme další síť o čtyřech klientech a jednom přepínači. Při vkládání klientů klikneme pravým tlačítkem na ikonku počítače v levém menu a vybereme možnost Notebook – Rozhraní: 1. Následně levým klikem myši na pracovní plochu vložím notebook do sítě a opět zapojíme klienty s příslušným přepínačem. Stejným způsobem vytvoříme třetí síť. Výběr klientů je již libovolný.



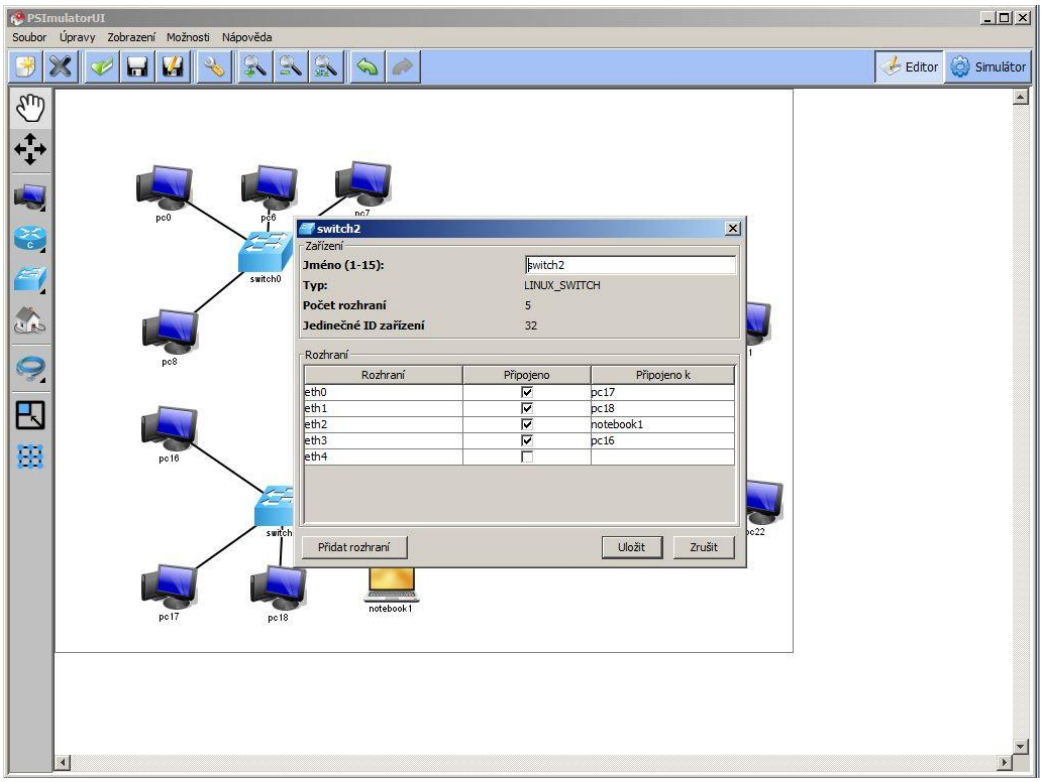
Obrázek 10 Řešení příkladu č. 2

- Do sítě vložíme směrovač (router), při jeho výběru opět klikneme na ikonku směrovače pravým tlačítkem a zvolíme možnost Cisco router – Rozhraní: 4. Kliknutím levého tlačítka do pracovní plochy ho vložíme do sítě.



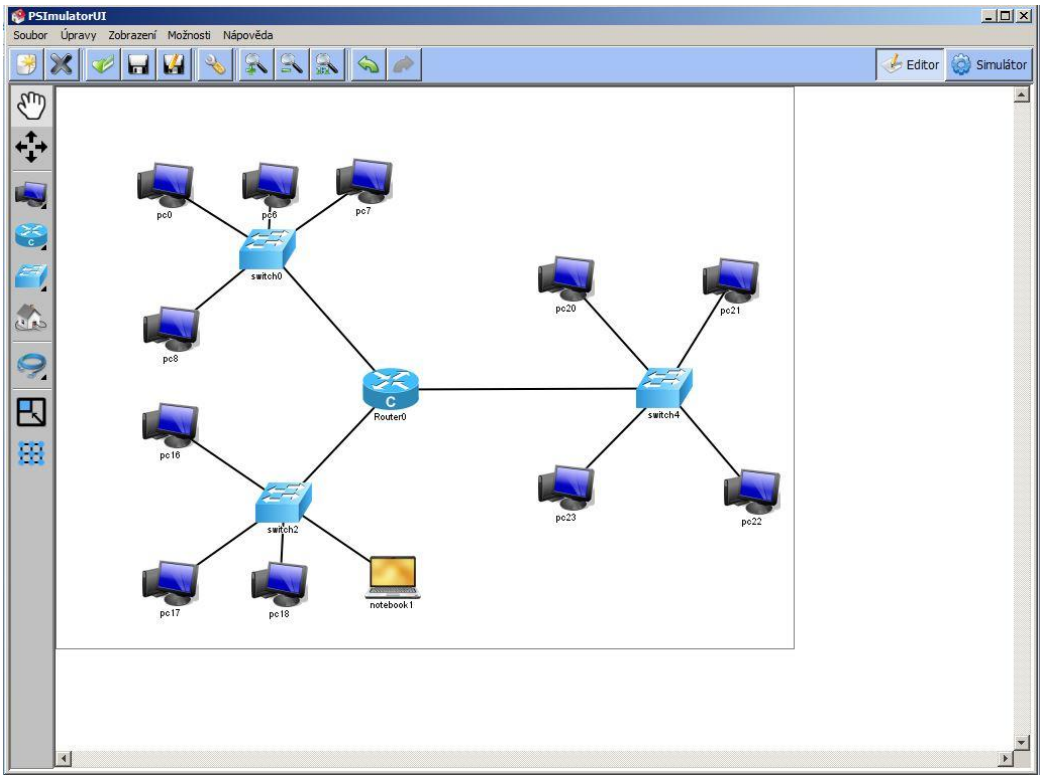
Obrázek 11 Řešení příkladu č. 2

- Následně musíme rozšířit počet rozhraní přepínačů, které jsou již zaplněné. Přepneme se do režimu Ruka, pravým tlačítkem klikneme na jeden z přepínačů a zvolíme Vlastnosti. V levém dolním rohu zvolíme možnost Přidat rozhraní a uložíme. Stejně to provedeme u všech dalších přepínačů.



Obrázek 12 Řešení příkladu č. 2

- Následně provedeme propojení aktivních prvků sítě. Tímto krokem je zadání splněno.



Obrázek 13 Řešení příkladu č. 2

7.2 Výuka počítačových sítí na středních školách

Na středních školách je situace již poněkud odlišná. Jistě se budu velmi lišit dle zaměření dané školy. Na středních průmyslových školách se zaměřením na informatiku bude jistě mnohem větší časová dotace i lepší prostředky pro výuku počítačových sítí, než na gymnáziích či odborných učilištích. Na školách, které nejsou zaměřeny na informatiku, je situace často podobná té na základních školách – pro větší část výuky počítačových sítí není dostatečný prostor.

Není to samozřejmě chybou, výuka počítačových sítí není na takových školách prioritní. Mělo by se jí nicméně alespoň okrajově věnovat pro pochopení principu funkce, obdobně jako na základních školách, ale s přihlédnutím k vyššímu věku žáků, jejich větším znalostem a zkušenostem, které by mělo umožnit probrat téma více odborně a do hloubky. Praktická část výuky by mohla probíhat podobně, jako na základních školách – využitím programů na simulaci chování počítačových sítí. Pro výuku tedy postačí běžná počítačová učebna.

Na středních školách s obory zaměřenými na informatiku, jako jsou průmyslové školy a obchodní akademie, se již předpokládá vyšší časová dotace i lepší vybavení. Některé vybrané střední školy mají poměrně pokročilé laboratoře, kde mohou žáci zapojovat a programovat různé síťové prvky a vytvářet tím větší počítačové sítě. V takových laboratořích nechybí směrovače a přepínače profesionální úrovně. Škola je často obdrží jako sponzorský dar od spolupracujících firem, které často tyto směrovače vyřazují a nahrazují novějšími modely.

Výhoda takovýchto laboratoří je samozřejmě možnost skutečného zapojení a nastavení sítě, možnost sledovat provoz a chování sítě v provozu. Taková praxe je velkou výhodou pro žáky a studenty v jejich osobním rozvoji a je i vhodnou praxí v budoucí kariéře. Některé vybrané střední školy se zapojují do celosvětového programu Cisco Networking Academy společnosti Cisco, která umožňuje studentům získat i mezinárodně uznávané certifikáty.

Tyto certifikáty jsou v oboru síťových a informačních technologií žádané a absolventi s tímto certifikátem jistě najdou uplatněný v tomto oboru. Firma Cisco založila tuto akademii v roce 1997 s cílem zvýšit počet kvalifikovaných absolventů připravených se zapojit ihned po absolvování škol do oboru komunikačních sítí. Po

celém světě se do Cisco Networking Academy zapojuje více než 9000 škol a institucí nabízejících možnost získání certifikátu. V Hradci Králové nabízí možnost výuky a certifikátu například Střední škola a Vyšší odborná škola aplikované kybernetiky, nebo Fakulta informatiky a managementu Univerzity Hradec Králové.

Pro ostatní školy, kde není specializovaná učebna využitelná pro výuku, můžeme k praktické výuce použít opět simulátory počítačových a komunikačních sítí, nebo vytvářet malé sítě s využitím relativně dostupných směrovačů (router) a počítačů v běžné počítačové učebně. K těmto praktickým úkolům potřebujeme:

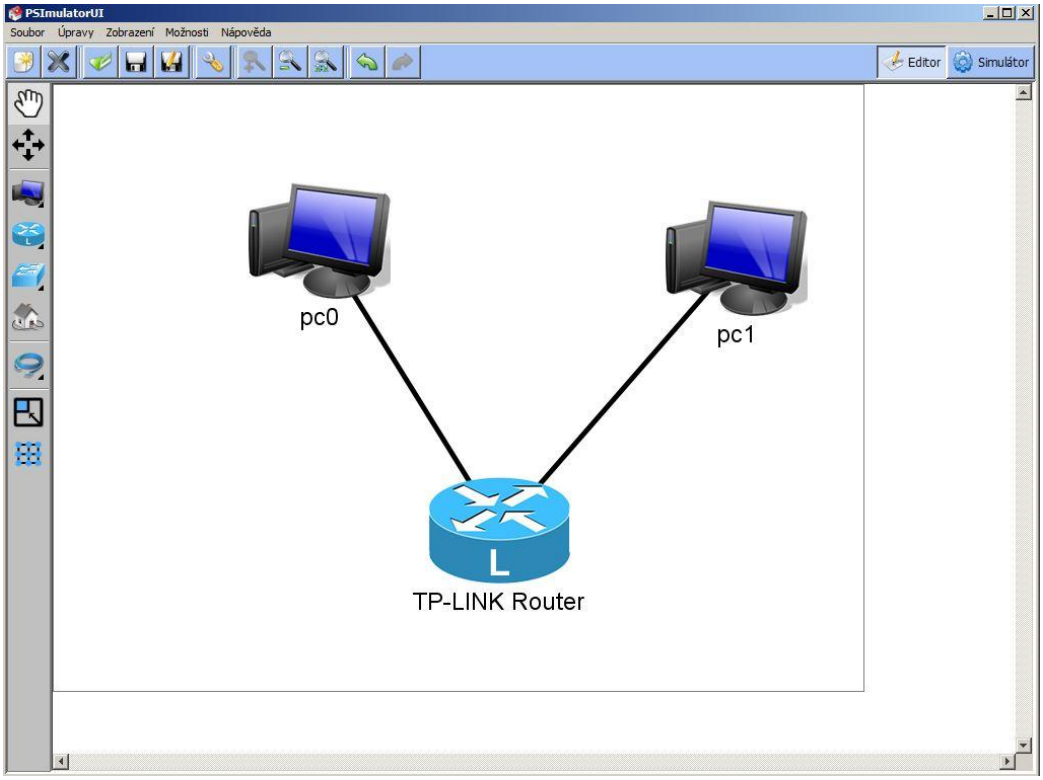
- Alespoň dva počítače (klienty)
- Jeden aktivní síťový prvek
- Síťové kabely s koncovkou RJ – 45

Následující praktická úloha tedy vyžaduje odborné vybavení, bez kterého není možné úlohu realizovat. Pokud není možnost požadované prvky koupit, či jinak zaopatřit, je vhodné provádět výuku pouze v simulačním prostředí na počítačích, které je k dispozici zcela zdarma. V našem případě jsme pro praktickou úlohu využili směrovač společnosti TP-LINK, model TL-WR1043ND. Důvodem výběru byl pouze fakt, že byl k dispozici a nebylo nutné kupovat, či jinak získat jakýkoliv jiný směrovač. Pro toto využití by jistě postačil libovolný směrovač z běžné nabídky na trhu.

7.2.1 Zadání praktických úkolů

Příklad č. 1 – vytvořte malou počítačovou síť s jedním aktivním prvkem a dvěma klienty. V této síti postupně nastavte:

- IP adresu směrovače na 192.168.1.1, masku podsítě na 255.255.255.0
- Statické IP adresy klientům:
  - PC0 – 192.168.1.2
  - PC1 – 192.168.1.3
  - Masku podsítě 255.255.255.0
- Ověřte funkčnost komunikace pomocí příkazu *ping*



Obrázek 14 Virtualizace zadání příkladu č. 1, vytvořeno v PSImulator

Postup řešení:

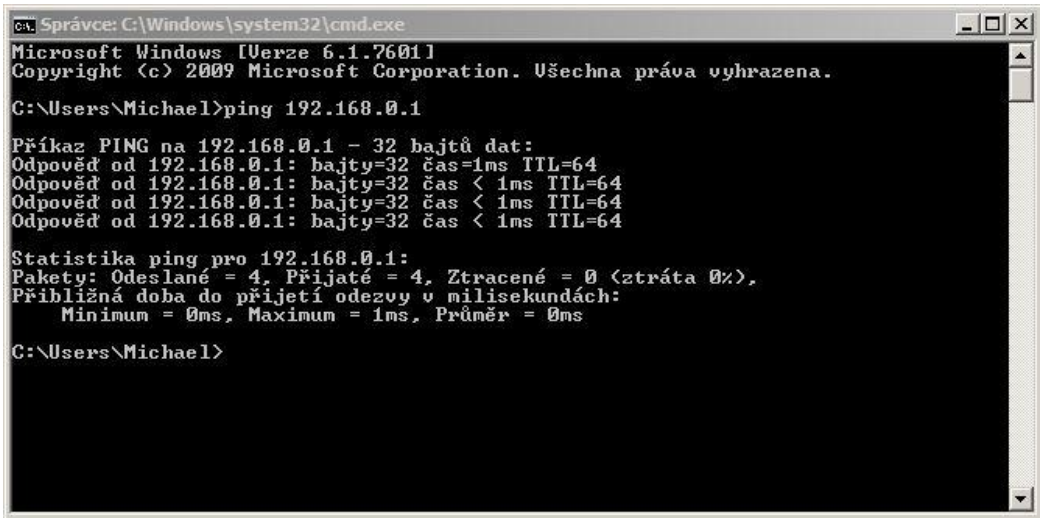
- Provedeme fyzické zapojení prvků. Využijeme kabeláž typu kroucená dvojlinka s koncovkou RJ – 45. Kabel může být typu UTP i STP. Zapojení provedeme vždy mezi počítačem (klientem) a směrovačem.

- K zapojení využijeme síťové porty počítačů a jeden z portů směrovače. V našem případě čtyři žlutě označené porty. O správném připojení informuje směrovač rozsvícením příslušné diody.

Obrázek 15 Konektory směrovače TP-LINK; dostupné z http://www.tp-link.cz/

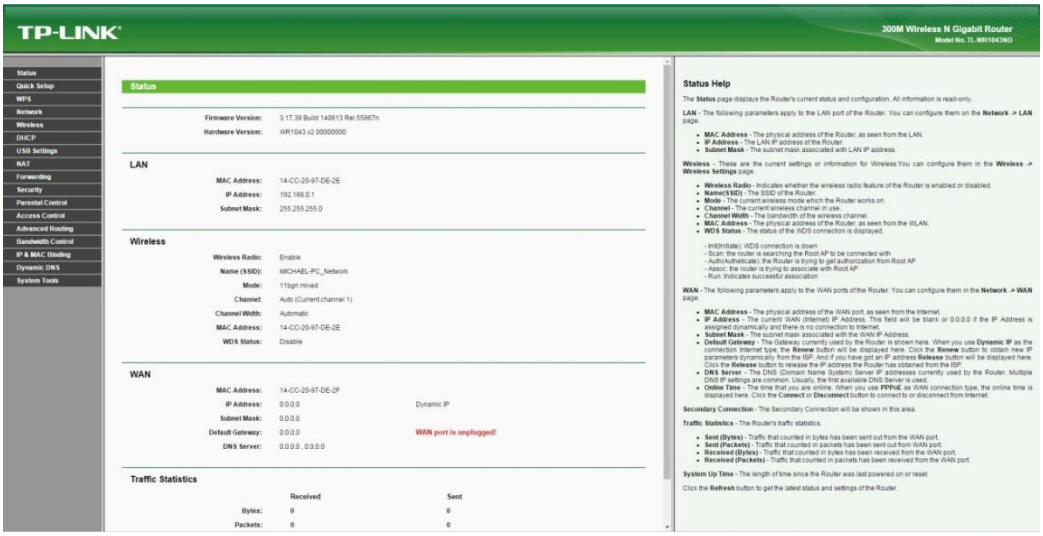
- Pro ověření správného zapojení v systému Windows v Příkazovém řádku použijeme příkaz *„ipconfig /all“,* který vypíše veškeré informace o síti, ve které se klient nachází. Zde zjistíme adresu směrovače (položka „Výchozí brána“).

- Příkazem *„ping 192.168.0.1“*, což je IP adresa směrovače, odešleme na směrovač dotaz a čekáme na odpověď. Pokud je vše zapojeno správně, dočkáme se od směrovače odpovědi, viz Obrázek 5. Příkaz použijeme i na druhém klientovi, který je připojen ke směrovači.



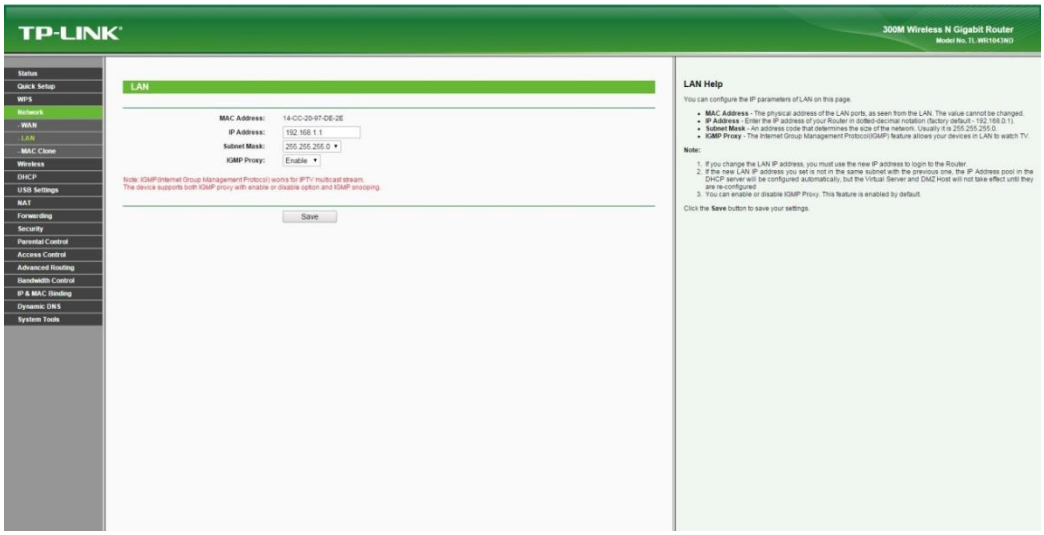
Obrázek 16 Příkaz *ping*

- Následně můžeme provést nastavení směrovače. To se provádí na v libovolném internetovém prohlížeči na klientech připojených ke směrovači. Do pole pro zadání adresy napíšeme http://tplinklogin.net. Následně vyplníme přihlašovací jméno a heslo. Při standardním nastavení je vždy jméno i heslo *admin.*



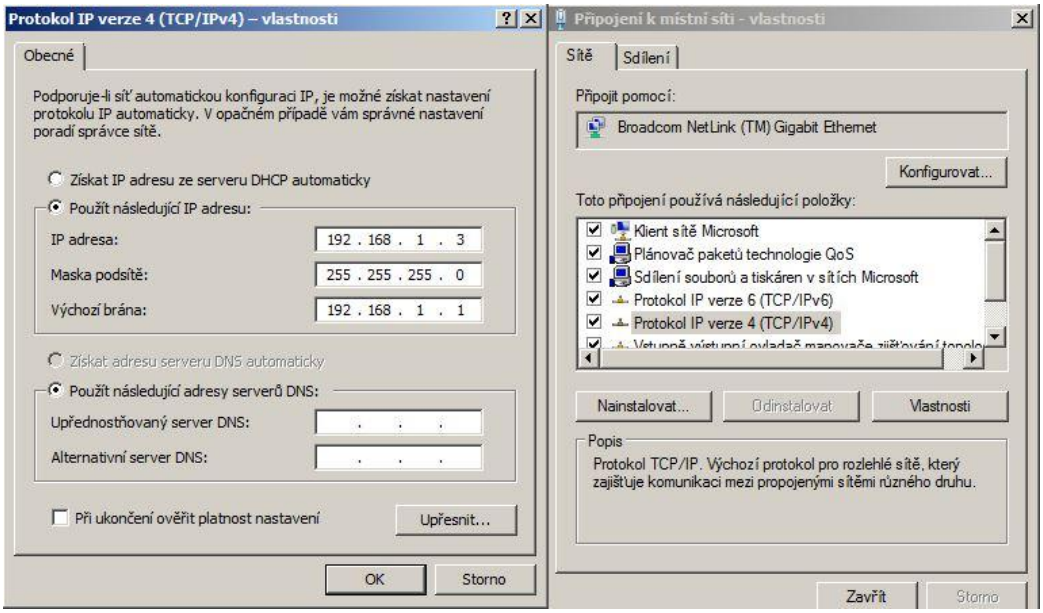
Obrázek 17 Prostředí pro správu a nastavení směrovače TP-LINK

- V prostředí pro správu a nastavení změníme IP adresu směrovače. To provedeme v sekci Network – LAN. Položku IP Address přepíšeme na 192.168.1.1, SubnetMask (Maska podsítě) přepíšeme na 255.255.255.0. Dále zde můžeme měnit nastavení sítě, ručně přiřazovat MAC adresy klientů k jejich IP adresám, omezovat přístup klientů na Internet, nastavovat zabezpečení, umožňuje nahlédnout do směrovacích tabulek a podobně. Pro naše potřeby v tomto úkolu však není žádné z těchto nastavení třeba.



Obrázek 18 Změna IP adresy směrovače

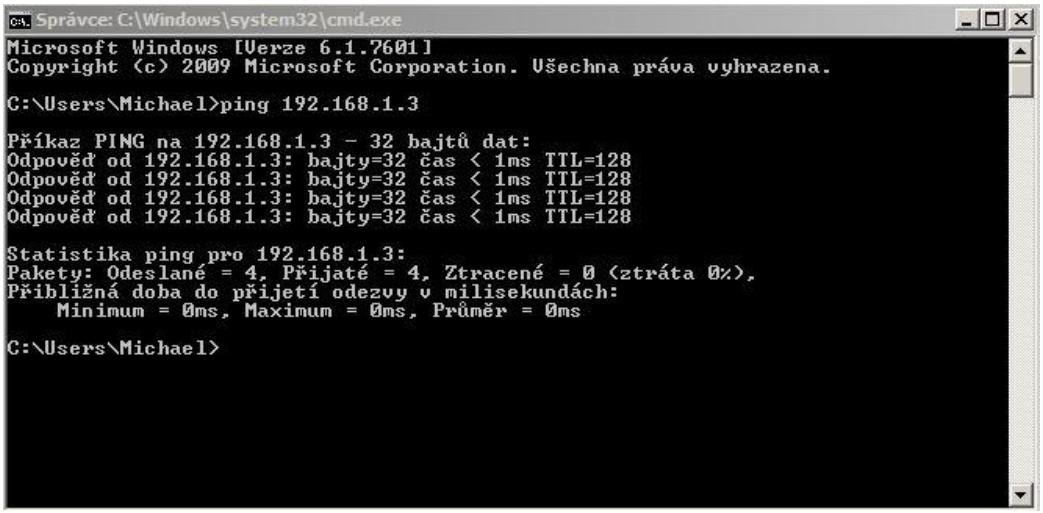
- Pro nastavení IP adres na klientech v operačním systému Windows 7 si otevřeme Ovládací panely – Centrum síťových připojení a sdílení – Připojení k místní síti. Zde pokračujeme přes Vlastnosti – Protokol IP verze 4 (TCP/IPv4) – Vlastnosti – Použít následující IP adresu. Vyplníme požadovanou IP adresu dle zadání, masku podsítě a výchozí bránu. Výchozí bránou je pro nás IP adresa směrovače. Stejné nastavení provedeme i na druhém klientovi.



Obrázek 19 Nastavení IP adresy klienta

- Z důvodu změny nastavení síťových adres provedeme opět zkoušku komunikace mezi klienty a směrovačem za pomocí příkazu *ping 192.168.1.1*. Pokud vše proběhne v pořádku (směrovač zašle zpět odpověď na zaslané dotazy), je vše nastaveno správně

- Posledním krokem je test komunikace mezi klienty navzájem. Tu provedeme opět příkazem *ping* a otestujeme ji na obou klientech. Cílová IP adresa je vždy IP adresa druhého klienta. Pokud komunikace proběhne v pořádku, je zadání splněno.



Obrázek 20 Komunikace mezi klienty v síti

Závěr

Výuka počítačových sítí je téma velice obsáhlé a dokáže plně vytížit studenty oborů počítačových sítí na celou dobu jejich studia. Proto je těžké najít ideální rozsah výuky sítí i tam, kde to není hlavním studijním oborem. Vzhledem k rozšířenosti počítačových sítí v dnešní době, by však měli všichni studenti přijít s výukou sítí do styku.

Je třeba rozlišovat, o jaké obory studia a jaký stupeň se jedná. Na základních školách prvního i druhého stupně, bych doporučil výuku počítačových sítí pouze okrajově a teoreticky, hlavně s ohledem na malou časovou dotaci a obsáhlost ostatních probíraných témat. Není tak v praxi moc možné probrat více, než jsou základy.

Více času mohou nabídnout hodiny volitelné informatiky na základních školách. V těchto hodinách je prostor k dalším možnostem a pravděpodobně i větší zájem samotných žáků, ne každá základní škola ale tyto hodiny žákům nabízí. Jako vhodným doplňkem pro názorné ukázky, se mi jeví využití simulátorů síťové komunikace, kterých je zdarma k dispozici poměrně velké množství.

Z teoretické části je vhodné do výuky zahrnout obecně rozbor síťových prvků aktivních i pasivních, rozbor síťového modelu ISO/OSI, základní popis a funkci vybraných síťových protokolů, způsob doručování dat v sítích a rozbor sítě Internet, který je a bude součástí života mladých žáků a studentů.

Velice podobné je to u studentů středních škol, kde není jejich zaměřením informatika. Není příliš v silách vyučujících, aby mohli studenty nějak více zaujmout v oblasti počítačových sítí, vzhledem k často nízkým časovým dotacím. Navíc to, s přihlédnutím k jiným zaměřením studia, nemá velký smysl. Obecné jednoduché základy by však měli znát i tito studenti.

Na středních školách se zaměřením na informatiku je již situace odlišná. Na výuku je zde většinou dostatek prostoru, stejně tak často nechybí ani kvalitní vybavení v dobře zařízených laboratořích. Další zajímavostí je často možnost získání uznávaného certifikátu Cisco Networking Academy společnosti Cisco. Dle všeho je výuka na středních školách odborného zaměření zajištěna dobře.

Výuka na odborných středních školách by měla probíhat celkově, po stránce teoretické i praktické. Teoretická výuka by měla zahrnovat výuku síťových topologií, rozbor aktivních i pasivních síťových prvků, rozbor MAC adres, rozbor a počítání IP adres v sítí při znalosti libovolné IP adresy a prefixu (určení adresy sítě, celkové rozsahu adres a podobně), znalosti o směrování paketů, TCP/IP, Ethernetu a další. Pod pojmem počítačových sítí se skrývá spousta informací a jejich důsledná výuka zabere velké množství času.

V praktické části výuky by bylo vhodné testovat fyzické zapojení a nastavování sítí. Studenti tak uplatní získané znalosti a lépe je využijí. I v tomto případě můžeme doporučit využití simulátorů počítačových sítí, a to hlavně na začátku výuky v prvních ročnících, nebo jako vizualizace zadání a tedy sestavení jakéhosi plánu. Hlavní část by však měla být věnována fyzickému vytváření a nastavování sítí. K tomu je však zapotřebí vybavení, které rozhodně není pro školu levnou záležitostí a je tak často odkázána na různé partnerské programy, nebo sponzorské dary.

Seznam použitých zkratek:

ISO/OSI	Internacional Organization for Standardization/Open Systems Interconnection
MAC	Media Access Control
LAN	Local Area Network
PAN	Personal Area Network,
MAN	Metropolitian Area Network
WAN	Wide Area Network
RSMA	Reverse SubMiniature version A
TNC	Threaded Neill–Concelman
UTP	UnshieldedTwisted Pair
STP	Shielded Twisted Pair
CSMA	Carrier Sense Multiple Access
FTP	File Transfer Protocol
SAP	Service Access Points
MAC	Media Access Control
LLC	Logical Link Control
TCP	TransmissionControlProtocol
UDP	User Datagram Protocol
EBDIC	Extended Binary Coded Decimal Interchange Code
ASCII	American Standard Code for Information Interchange
HTTP	HyperText Transfer Protocol
SMTP	Simple Mail Transfer Protocol

FTP	File Transfer Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
DHCP	Dynamic Host Configuration Protocol
SIP	Session Initiation Protocol
RTP	Real-time Transport Protocol
NTP	Network Time Protocol
DNS	Domain Name Systém
ICMP	Internet Control Message Protocol
CIDR	Classless Inter-Domain Routing
NAT	Network Address Translation
IEEE	Institute of Electrical and ElectronicsEngineers
PC	Personal Computer
PDU	Protocol data unit
RIP	Routing Information Protocol
ČVUT	České vysoké učení technické v Praze

Citovaná literatura

Bigelow, Stephen J. 2004. *Mistrovství v počítačových sítích.* Brno : Computer Press, 2004. ISBN 80-251-0178-9.

Brisbin, Shelly. 2003. *Postavte si svou vlastní wi-fi síť.* Praha : Neocortex, 2003. ISBN 80-86330-13-3.

Dostálek, Libor a Kabelová, Alena. 2008. *Velký průvodce TCP/IP a systémem DNS.* Brno : Computer Press, 2008. ISBN 978-80-251-2236-5.

Jandoš, Jaroslav. 1995. *Komunikační systémy a služby.* Praha : VŠE, 1995.

Janeček, Jan a Bílý, Martin. 2003. *Lokální sítě.* Praha : ČVUT, 2003.

Malina, Patrik. 2003. *Budujeme malou počítačovou síť.* Praha : PC WORLD, 2003.

McFarland, Shannon, a další. 2011. *IPv6 Kompletní průvodce nasazením v podnikových sítích.* Brno : Computer Press, 2011. ISBN 978-80-251-3684-3.

Odom, Wendell, Healy, Rus a Mehta, Naren. 2009. *Směrování a přepínání sítí.* Brno : Computer Press, 2009. ISBN 978-80-251-2520-5.

Palovský, Radomír. 2010. *Informační a komunikační sítě.* Praha : Vysoká škola ekonomická v Praze, 2010. ISBN 978-80-245-1729-2.

Peterka, Jiří. 2011. Archiv článků a přednášek Jiřího Peterky. *eArchiv.* [Online] 2011. http://www.earchiv.cz/.

Plexo. 2008. PCTuning. *PCTuning.* [Online] 22. 1 2008. http://pctuning.tyden.cz/.

Rukovanský, Imrich a Kratochvíl, Oldřich. 2007. *Bezdrátové počítačové sítě.* Kunovice : Evropský polytechnický institut, 2007. ISBN 978-80-7314-112-7.

Rukovanský, Imrich, Kratochvíl, Oldřích a Kavka, Jaroslav. 2009. *Computer Networks.* Kunovice : Evropský polytechnický institut, 2009. 978-80-7314-175-2.

Soper, Mark Edward. 2005. *Malé počítačové sítě.* Praha : Grada Publishing, 2005. ISBN 80-247-1391-8.

Vavrečková, Šárka. 2010. *Počítačové sítě a decentralizované systémy.* Opava : Slezská univerzita, 2010.