INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Vzdělávání pedagogů pomocí tabletů

CZ.1.07/1.3.00/51.0005

Tento studijní text slouží pouze jako doplňující výukový materiál k prezenčnímu Workshopu 1 (školení) v rámci klíčové aktivity A3 – Metodik ICT ve škole.

Obsahuje 2 bloky:

- První je zaměřen na vybrané kapitoly z oblasti **hardware**,
- druhý blok je orientován na problematiku vybraných kapitol **počítačových sítí**.

Bc. Tomáš Vyjídák

HARDWARE A POČÍTAČOVÉ SÍTĚ

VYBRANÉ KAPITOLY

Obsah

Vybrané kapitoly Hardware

Počítač lze jednoduše chápat jako stroj na zpracování informací. Přesněji řečeno se jedná o elektronické zařízení, které zpracovává data pomocí předem vytvořeného programu.

Počítač se fyzicky skládá z technického vybavení (**hardware**), které zahrnuje části počítače (procesor, klávesnice, monitor atd.) **a software**, který zahrnuje programové vybavení počítače (souhrnný název pro veškeré programy, které mohou na počítači pracovat – např. operační systém a především aplikační programy). (1)(2)(3)

Programem rozumíme algoritmus zapsaný prostřednictvím nějakého programovacího jazyka (jinak řečeno, jedná se o posloupnost instrukcí). Každý program je vytvořen za nějakým účelem a podle toho je možné dělit je na **systémový software**, který zajišťuje chod samotného počítače a jeho styk s okolím (operační systémy, pomocné programy pro správu systému - utility, překladače programovacích jazyků) a **aplikační software**, který představuje programy umožňující řešení specifických problémů uživatele (textové editory, tabulkové procesory, databázové systémy, grafické editory, počítačové hry aj.).

Počítač je ovládán uživatelem, který zadává instrukce ke zpracování dat prostřednictvím vstupních zařízení (klávesnice, myš, scanner aj.) **a počítač výsledky prezentuje pomocí výstupních zařízení** (monitor, tiskárna aj.).

NĚKTERÉ POJMY, KTERÉ JE NUTNÉ PŘED DALŠÍM STUDIEM ZNÁT:

bit: 1 bit (binary digit - dvojková číslice) je základní jednotka informace. Poskytuje množství informace potřebné k rozhodnutí mezi dvěma možnostmi. Jednotka bit se označuje **b** a může nabývat pouze dvou hodnot – 0 nebo 1.

Byte: Jednotka informace, která se označuje B a platí 1B = 8b.

Paměť: Zařízení, které slouží pro uchování informací (konkrétně binárně kódovaných dat). Množství informací, které je možné do paměti uložit, se nazývá kapacita paměti a udává se v bytech. Protože byte je poměrně malá jednotka, používá se často následujících předpon: **kilo, mega, giga, tera.**

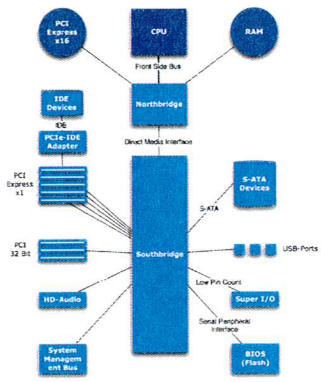
Dále se zaměříme na pojmy jak z oblasti HW, tak systémového SW, které mají rozhodující úlohu pro HW konfiguraci počítače.

1 Základní deska a BIOS

Základní deska (angl. mainboard či motherboard) je základním hardware většiny počítačů, který umožňuje připojit jednotlivé komponenty, a to jak mechanicky, tak jim poskytnout elektrické napájení.

Jednotlivé komponenty se k základní desce připojují pomocí **rozšiřujících slotů** nebo kabelů. Na základní desce je umístěna energeticky nezávislá **paměť typu ROM** (FLASH paměť), ve které je uložen **BIOS**.

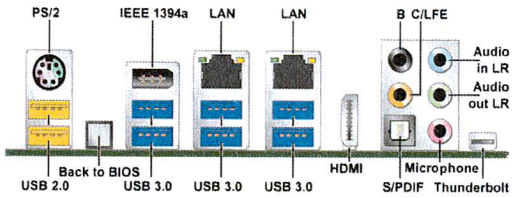
Základní deska obsahuje dále tzv. **chipset** – v oblasti počítačů je tento termín používán k označení specializovaných čipů. Fyzicky se může jednat buď o jeden čip, nebo dva (v tom případě se označují jako **northbridge** a **southbridge**). Čipová sada rozhoduje, jaký procesor a operační paměť je možné k základní desce připojit, stará se vlastně o komunikaci mezi procesorem, sběrnicemi, sloty, řadiči a dalšími součástmi na základní desce.



*Úloha **Chipset** na základní desce*[1]

[1] Zdroj: http://cs.wikipedia.org/wiki/%C4%8Cipov%C3%A1_sada

Vybrané konektory na nákladní desce



Porty na nákladní desce[2]

OTÁZKY:

K jakému účelu se používají jednotlivé konektory nebo chcete-li porty na obrázku výše?

Které porty na obrázku výše postrádáte?

1.1 BIOS

Základní deska je součástí, která spojuje všechny díly počítače. Jednotlivé prvky základní desky (procesor, disky, sběrnice, integrované periférie, vstupní a výstupní porty,...) se mezi sebou musí domluvit. Pro tento účel funguje **BIOS**.

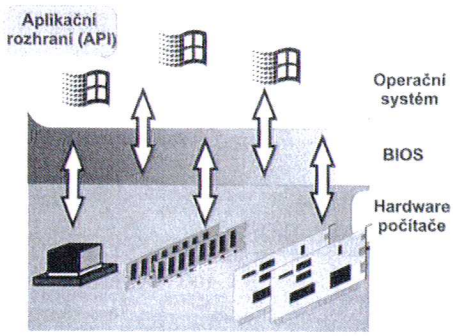
BIOS desku oživí a vzájemně přizpůsobí parametry jejích komponent. Desky tak mohou spolupracovat s hardwarem různých výrobců v odlišných konfiguracích. (5)

BIOS zpracovává signály základní desky a předává je vyšší vrstvě PC – **operačnímu systému** (OS).

Příklad:

Díky BIOSU „vidí" OS disk jako úložiště dat, umí sem ukládat data a číst, ale nemusí se zajímat o konkrétní parametry disku (počet hlav, povrchů, stop, sektorů atd.) V samotné podstatě je BIOS tvořen sadou ovladačů základních komponent systému. Na tom, jak budou pracovat mezi sebou jednotlivé díly počítače závisí celý výkon počítače.

[2] Zdroj: http://www.anandtech.com/show/3736/news-just-in-gigabyte-announces-usb3-miniitx-h55-motherboard-



Princip činnosti BIOSU

1.1.1 VRSTVY BIOSU

Fyzicky je BIOS uložen ve vlastním **integrovaném obvodu** zasunutém do patice základní desky. Jde o paměť *Flash ROM*, z níž lze jen číst (ale i přepsat za pomocí speciálního programu).

Integrovaný obvod s BIOSem

Kromě vlastního BIOSU jsou zde zapsány i informace o možných komponentách základní desky. Tyto informace jsou dostupné po startu počítače. Systém si tak dokáže detekovat druh paměti, druh procesoru, ...).

Druhou vrstvu BIOSu tvoří nastavení, které provede obsluha PC programem *Setup* – ten je součástí každého BIOSu a slouží ke konfiguraci HW. (5)

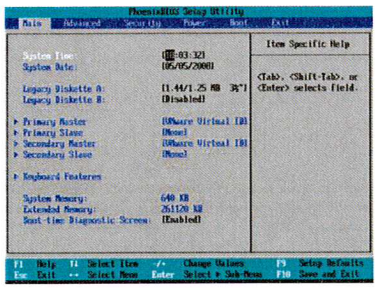
Všechny komponenty základní desky (integrované i rozšiřující) nesou informace samy o sobě ve vlastních pamětech ROM, tzv. *firmware*. Při startu systému se načtou jejich ovladače a vytvoří se tak **třetí vrstva** BIOSu.

Princip je následující:

BIOS vytvoří tzv. *Application Programming Interface* (API), tvořené různými příkazy a funkcemi. Při rozdílných konfiguracích HW je tak vždy zaručeno standardní rozhraní pro operační systémy.

V praxi to znamená, že se programy nemusí starat, jak a kam mají uložit soubory nebo jak tisknout atd. Aplikace předá příkaz API a to zajistí vše potřebné pro provedení tohoto příkazu. Komunikace mezi komponentami počítače se tak zjednodušuje, protože aplikace komunikují pouze s operačním systémem, nikoli s HW.

1.1.2 Program SETUP



Okno programu SETUP

Program Setup umožňuje definovat hodnoty BIOSu. Jeho prostřednictvím můžeme zvolit HW, se kterým bude deska spolupracovat, nastavovat parametry jednotlivých prvků.

SETUP jak známo nespouštíme z operačního systému, ale během startu počítače. Informace o tom jak SETUP otevřít najdeme vždy při startu počítače na monitoru nebo v manuálu základní desky.

1.1.3 Baterie a paměť CMOS

BIOS má k dispozici paměť **CMOS**, kam si ukládá vytvořené **API**, svá nastavení atd. **CMOS je trvale zálohována baterií.**

Vybitím či výměnou baterie dojde většinou ke ztrátě dat, která byla v paměti CMOS zapsána. Programem SETUP tak musíme sjednat nápravu. **Každý SETUP dokáže nastavit konfigurační hodnoty automaticky**.

1.1.4 Start BIOSu

1. Nejdříve BIOS prohlédne všechny sloty (PCI, PCIe, AGP, patice procesoru, pamětí,...) a z jejich pamětí ROM přečte informace, z nichž vytvoří API. Aby to nemusel dělat při každém startu, ukládá si tyto údaje (tzv. ESCD) do paměti CMOS.
2. BIOS spustí testy *POST*, jimiž zjistí, jaký je v počítači HW. Jestliže narazí na problém, informuje nás o něm (hlášením či kódem BEEP). Po úspěšném provedení testů POST se na monitoru může objevit (nemusí – podle nastavení) seznam HW prvků počítače.
3. Pokud jsou POST v pořádku, vyhledá BIOS na základě nastavení programu SETUP **zaváděč OS**. Po nalezení načte zaváděč OS a ten dále všechny ovladače potřebné pro komunikaci s API.

2 Procesor

Procesor (též CPU, z angl. *Central Processing Unit* = Centrální Výpočetní Jednotka) **je základní součástí počítače, která je složena z mnoha elektronických prvků** (prvky jsou integrovány – dnešní procesory obsahují cca 1.000.000.000 tranzistorů).

Procesor funguje zjednodušeně řečeno tak, že čte z paměti strojové instrukce a na jejich základě vykonává program. Jelikož by byl procesor vykonávající program zapsaný v některém z vyšších programovacích jazyků příliš složitý, má každý procesor svůj vlastní jazyk - tzv. **strojový kód** (1).

2.1.1 Součásti procesoru

- **aritmeticko-logická jednotka** (ALU - Arithmetic-Logic Unit) – probíhají v ní všechny logické a aritmetické výpočty (sčítání, násobení, negace, bitový posuv atd.).
- **řadič** - společně s ALU vytváří základní řídící jednotku procesoru. Zajišťuje řízení činnosti procesoru v návaznosti na povely programu.
- **registr procesoru** - slouží k ukládání mezivýsledků a dočasných hodnot. Přístup k registrům je mnohem rychlejší než přístup do operační paměti, a proto se dá jeho funkce přiřadit k jakési rychlé vyrovnávací paměti. Registr procesoru dělíme na tři základní typy - registry *uživatelské*, *systémové* a *vnitřní*.
- **numerický koprocesor** - operuje s čísly, které mají plovoucí desetinnou čárku.

Je nutno dodat, že současné procesory obsahují zpravidla mnoho dalších rozsáhlých funkčních bloků, jako třeba paměť **cache**[3], a různých periferií, které z ortodoxního hlediska nejsou součástí procesoru. Proto se setkáváme s pojmem „**jádro procesoru**" – rozlišuje se tedy mezi vlastním procesorem a integrovanými periferními obvody (současné procesory obsahují většinou několik jader).

2.1.2 Typy procesorů

1) **Dělení podle délky operandu v bitech**
   - ✓ **4bitové a 8bitové** – používají se pro velmi jednoduché aplikace (kalkulačky, mikrovlnné trouby),
   - ✓ **16bitové procesory** – používají se pro středně složité aplikace (mobilní telefony, PDA, herní konzoly),
   - ✓ **32 bitové procesory** – použití ve starších počítačích, tiskárnách,

[3] Paměť **cache** může mít v informace více podob. Pokuste se sami nalézt a prostudovat její význam.

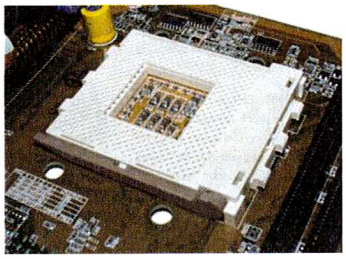
   - ✓ **64 bitové procesory** – většinou se jedná o vícejádrové procesory, použití v dnešních počítačích.

2) **Podle vnitřní architektury**
   - ✓ **RISC** (Reduced Instruction Set Computer) - v překladu počítač s redukovanou instrukční sadou. Vychází ze skutečnosti, že většina programů prováděných na počítačích využívá pouze malou část ze všech dostupných strojových instrukcí procesoru. Z uvedeného vyplývá, že složitější operace efektivněji vykoná posloupnost jednodušších instrukcí, které lze provádět s vyšší frekvencí.
   - ✓ **CISC** (Complex Instruction Set Computer) - procesor s velkou sadou strojových instrukcí (cca stovky) a relativně malým počtem registrů. (1)

3) **Dělení podle počtu jader**
   a) **Jednojádrové** – obsahují pouze jedno jádro.
   b) **Vícejádrové** – v jediném čipu procesoru je integrováno více jader. Tento trend můžeme pozorovat u procesorů pro osobní počítače. Integrací většího počtu jednodušších jader lze dosáhnout na stejné ploše křemíku mnohem vyšší výpočetní výkon, než použitím jediného složitého jádra.

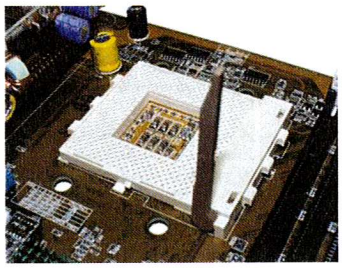
2.1.3 Montáž procesoru - obecně

Montáž procesoru na základní desku je činnost, se kterou jste se možná měli možnost setkat, možná ji provádíte běžně a možná Vás to jednou bude čekat. Níže se podíváme na zjednodušený postup. (7)



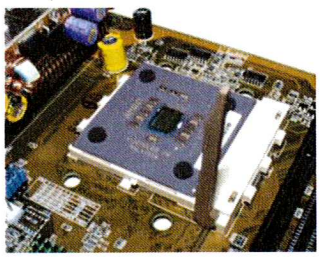
Patice pro procesor – socket

U patice je malá páčka (někdy je z plastu, někdy kovová). Tu pomalu a hlavně **nenásilně zvedneme**.



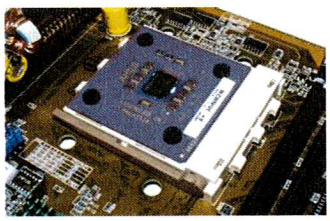
Nadzvednutí páčky

Poté opatrně vezmeme procesor a **zasadíme jej do patice skoseným rohem ke skosenému rohu**. Pozor - procesor se nevkládá silou - socket je typu ZIF (Zero Input Force - zasouvání nulovou silou).



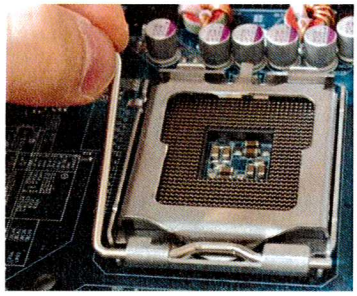
Procesor vložený v patici

Pokud máme, tak páčku vrátíme opět na místo. Procesor by měl držet. Poté ho **natřeme teplovodivou pastou**. Není potřeba se až tak bát a rovnoměrně natřeme jádro procesoru.

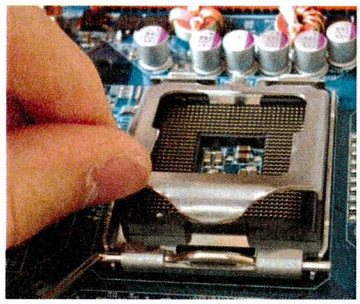


Patice s nainstalovaným procesorem

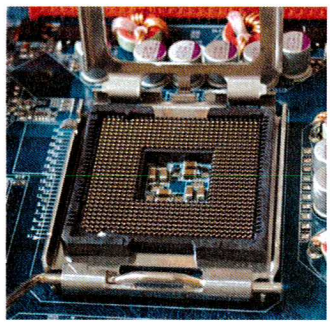
Dnes se u základních desek setkáváme nejčastěji s paticemi LGA. Ty neobsahují otvory, do nichž by zapadly nožičky (piny) procesoru, ale kontakty, na něž dosedají protější kontaktní plošky procesorů nové generace. Montáž je však obdobná a zachycuji ji následující obrázky.



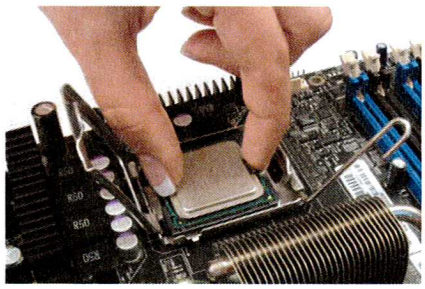
Otevřeme zajišťovací mechanismus patice – páčku



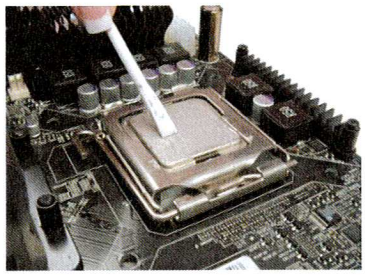
Odklopení přítlačné desky procesoru



Patice přichystaná pro montáž procesoru



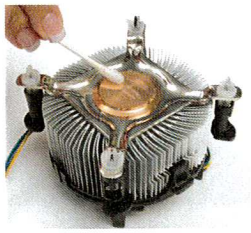
Osazení patice procesorem



Nanesení teplovodivé pasty

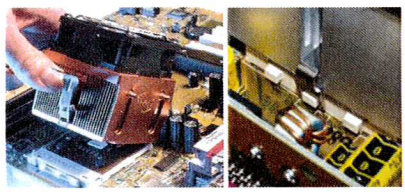
2.1.4 Montáž chladiče procesoru

Na procesor s nanesenou teplovodivou pastou nasadíme opatrně **chladič** (ten můžeme taktéž natřít pastou). Chladiče se vyrábějí v různých provedeních. **Zpravidla se jedná o kombinaci pasivního chlazení (hliníkové žebrování) a aktivního chlazení (ventilátorek).** U novějších počítačů se můžeme setkat i s kapalinným chlazením. (7)



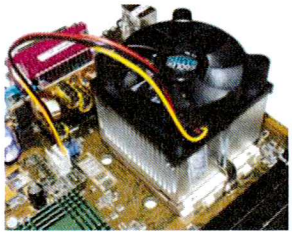
Natření teplovodivou pastou

Chladič upevňujeme za paticí (u starších typů) nebo za "čtverce kolem patice" - toto je u nových procesorů. Vše musí dobře docvaknout a je hotovo. Nepoužívejte násilí.



Přítlačnou pružinu na jedné straně zahákneme za plastový úchyt

Po mechanickém nainstalování chladiče je nutné ještě připojit kabel od ventilátoru ke konektoru na základní desce.

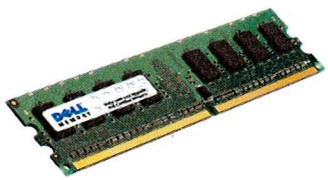


Připojení konektoru

3 Operační paměť

Operační paměť je „nejbližším" spolupracovníkem procesoru. Její kapacita a rychlost podstatně ovlivňují výkon počítače. **Po spuštění programu dojde nejdříve k jeho zavedení do operační paměti RAM** (Random Access Memory) **a teprve odtud jej dokáže procesor vykonávat.** Je důležitá pro rychlý chod počítače. Pokud se její kapacita v daný okamžik zaplní, zpracovávaná data se začnou zapisovat na pomocné úložiště - několikanásobně pomalejší harddisk (1).

Operační paměť RAM je určena pouze ke krátkodobému uložení informací. Pokud totiž počítač vypneme, je její obsah vymazán (na rozdíl od pevného disku, flashdisku či DVD).



Paměťový modul DDR2

Nedostatek operační paměti se projeví snížením rychlosti, případně vede i k havárii celého systému. Velikost operační paměti vychází z požadavků OS a spuštěných aplikací.

Např. **Microsoft** udává, že min. velikost operační paměti pro **Windows Vista** je 512 MB, ovšem pro běžnou práci je potřeba uvažovat o min. **2 GB**. Pro **Windows 7** je situace obdobná, ovšem vzhledem k propracovanějšímu jádru tohoto OS je využití velikosti operační paměti efektivnější. V rámci **Windows 8.1** se udává 1 GB (pro 32bitová verze) nebo 2 GB (64bitová verze). U serverových OS (např. Windows Server 2012) je situace více závislá na úlohách daného serveru.

Pokud se podíváme dále např. **na OS Linux Ubuntu**, tak v případě desktopové verze začínají min. požadavky na paměť RAM od 512 MB, v případě serverové verze je uváděno jen 192 MB.

3.1 Využití Operační paměti a Stránkovací paměť

Má-li OS málo operační paměti, použije k simulaci OP **prostor na pevném disku**. Do souboru na disk si ukládá momentálně nepotřebný obsah paměti RAM. Tento soubor se nazývá *stránkovací* (virtuální paměť, swapovací soubor). Jde o skrytý soubor *pagefile.sys*. Stránkovací soubor se vytváří automaticky během instalace.

3.1.1 Nastavení parametrů stránkovacího souboru

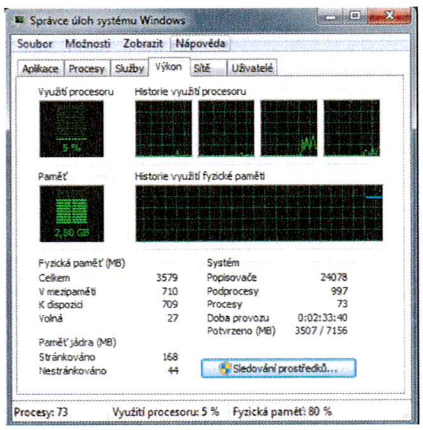
Pokud se Vám zobrazují upozornění, že virtuální paměť je malá, je třeba zvětšit minimální velikost stránkovacího souboru. Operační systém Windows nastaví počáteční minimální velikost stránkovacího souboru na hodnotu odpovídající velikosti paměti RAM (random access memory) instalované v počítači, plus další trojnásobek paměti RAM instalované v počítači. Pokud se při těchto doporučených úrovních zobrazují upozornění, je třeba zvětšit minimální a maximální velikost stránkovacího souboru.

Postup – např. pro Windows 7:

1. Otevřete okno Systém kliknutím na Start, kliknutím pravým tlačítkem myši na položku Počítač a kliknutím na tlačítko **Vlastnosti**.
2. V levém podokně klikněte na položku Upřesnit nastavení systému. Pokud vás systém vyzve k zadání nebo potvrzení hesla správce, zadejte heslo nebo proveďte potvrzení.
3. Na kartě Upřesnit klikněte v části Výkon na možnost Nastavení.
4. Na kartě Upřesnit v části Virtuální paměť klikněte na příkaz Změnit.
5. Zrušte zaškrtnutí políčka Automaticky spravovat velikost stránkovacího souboru pro všechny jednotky.
6. Ve skupinovém rámečku Jednotka [Jmenovka] klikněte na jednotku obsahující stránkovací soubor, který chcete změnit.
7. Klikněte na možnost Vlastní velikost. Do polí Počáteční velikost (MB) nebo Největší velikost (MB) zadejte novou velikost v megabajtech, klikněte na příkaz Nastavit a potom na tlačítko OK.

3.1.2 Správce úloh a OP

Ve *Správci úloh* (CTRL – ALT – DELETE) můžeme podrobně sledovat obsazení operační paměti na kartě **Výkon**:



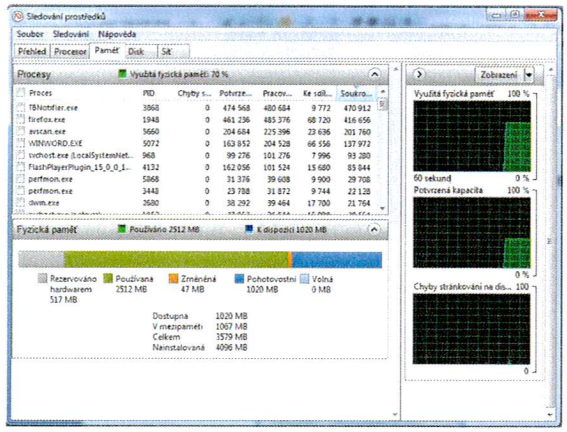
Správce Úloh systému Windows 7

Přehled o využití OP podává okénko **Fyzická paměť** (kB) – údaje se týkají skutečné fyzické paměti, tedy kapacity v paměťových modulech:

- **Celkem** – je celková fyzická velikost OP nainstalované v počítači;
- **K dispozici** – představuje velikost volné paměti, kterou je možné využít;
- **Mezipaměť systému** – množství paměti RAM, kterou si Windows vyhradily pro uložení naposledy použitých programů;
-

Okno **Paměť jádra** informuje o velikosti paměti obsazené jádrem OS a ovladači zařízení:

- **Stránkováno** představuje množství paměti jádra, které je mapováno na stránky ve virtuální paměti;
- **Nestránkováno** představuje velikost **rezidentní paměti**, která nemůže být zkopírována do stránkovacího souboru;

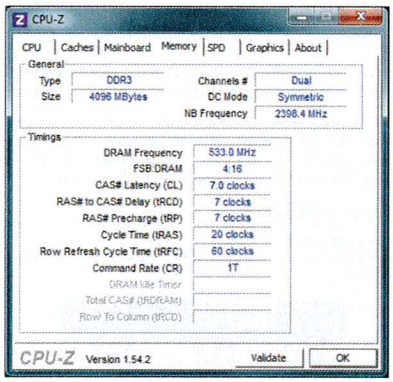


Sledování prostředků paměti

JAKÝ TYP PAMĚŤOVÉHO MODULU MÁM V POČÍTAČI?

Toť otázka ☺. Paměťových modulů existuje celá řada typů, od DIMM, přes DDR až po moderní RDRAM. Rychlou informaci o typu paměťových modulů instalovaných ve Vašem počítači (bez nutnosti jej hledat v OS), včetně dalších informací o procesoru, základní desce či grafické kartě nám řekne velmi jednoduchý program CPU-Z[4].

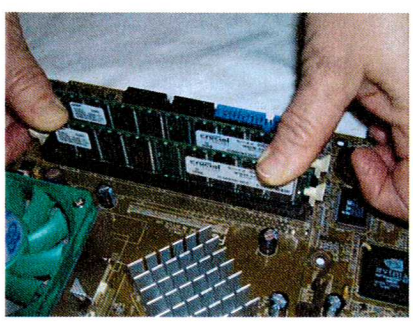
[4] http://www.cpuid.com/softwares/cpu-z.html

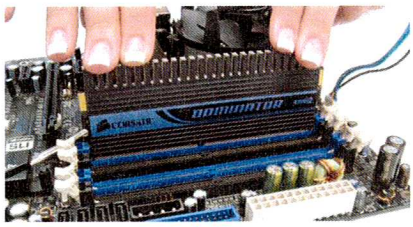


Program CPU-Z

3.2 Montáž operační paměti

Opět to není nic těžkého. Vybereme slot, ten bývá většinou v blízkosti procesoru. Uvidíme tam dvě páčky. **Páčky odklopíme a vložíme modul.** Modul má zářezy, proto není možné se splést. Na modul seshora zatlačíme, dokud "nezacvakne" a páčky se samy nepřiklopí. (7)





Montáž paměťového modulu

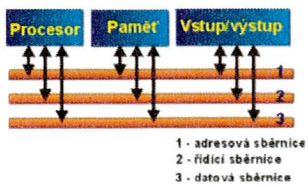
4 Sběrnice

Je-li procesor „srdcem" počítače, základní deska je „kostrou" počítače, pak sběrnici lze označit „páteří". Její úlohou je přenášet data a veškeré signály mezi jednotlivými částmi počítače. (7)

Pod pojmem sběrnice obecně rozumíme soustavu vodičů, pomocí kterých mezi sebou jednotlivé části počítače komunikují a přenášejí data. Sběrnice podporuje modularitu systému (je možné relativně jednoduše přidávat či ubírat další moduly - části počítače). Sběrnice je po mechanické stránce vybavena konektory uzpůsobenými pro připojení dalších komponentů.

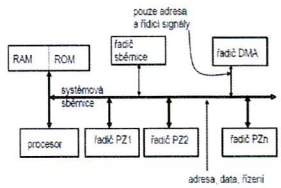
Sběrnici lze rozdělit na tři základních skupin:

- datová sběrnice (přenos dat),
- řídící sběrnice (rozhodování o přidělení sběrnice pro následující datovou fázi),
- adresová sběrnice.



Zobrazení sběrnic

Procesor, koprocesor, cache paměť, operační paměť, řadič cache paměti a operační paměti a některá další zařízení jsou propojena tzv. **systémovou sběrnicí (CPU bus)**.

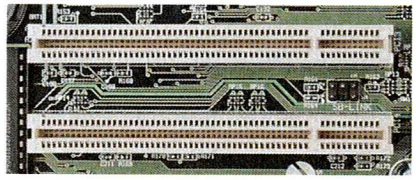


Osobní počítače jsou navrženy tak, aby se daly snadno rozšířit o další zařízení (síťové karty, grafické karty, zvukové karty, řadiče disků apod.). To umožňuje tzv. **rozšiřující sběrnice** počítače (častěji označované pouze jako sběrnice), na kterou se jednotlivá zřízení zapojují. Tato rozšiřujíci sběrnice a zapojovaná zařízení musí tedy splňovat určitá pravidla. **Pojem sběrnice je obvykle chápán jako**

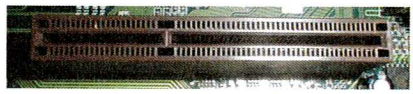
standard, dohoda o tom, jak vyrobit zařízení (rozšiřující karty), která mohou pracovat ve standardním počítači.

Nejpoužívanější typy sběrnic (7):

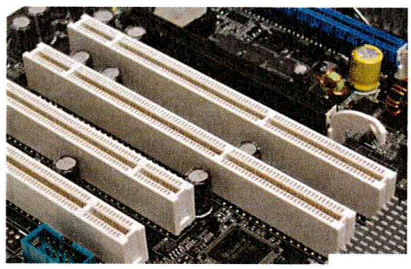
- **PCI** (Peripheral Component Interconnect) – starší sběrnice, používá paralelní přenos dat (šířka 32 nebo 64 bitů). Dnes již v podstatě nahrazena PCI Express.



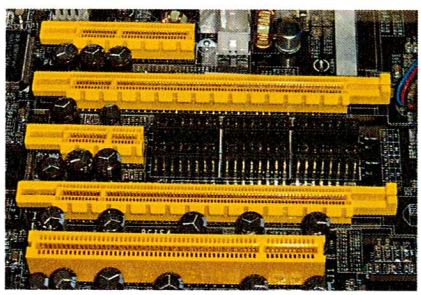
- **AGP** (Accelerated Graphics Port) - jednoúčelová sběrnice určená pro připojení grafické karty k systému. Rovněž nahrazena PCI Express.



- **PCI-X** - zpětně kompatibilní rozšíření sběrnice PCI, nenahradila ji však, protože se dostatečně nerozšířila. Nástupcem sběrnice PCI tak byla až sběrnice PCI-Express.

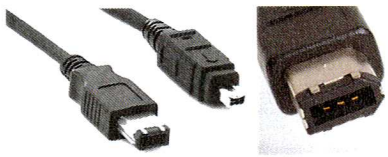


- **PCI-Express** (PCIe) - byl standard systémové sběrnice, který byl vytvořen jako náhrada za starší standardy PCI, PCI-X a AGP. Vyrábí se v několika variantách: PCI-E 16× (pro grafické karty pro PCI-E), PCI-E 8×, 1× a 4× (pro zvukové karty, řadiče pevných disků a další zařízení).



- **USB** (Universal Serial Bus) - sériová polyfunkční sběrnice, možnost připojování Plug & Play bez nutnosti restartování počítače, 2 diferenciální datové vodiče + 2 napájecí vodiče, široké použití. (1)

- **FireWire** (označované jako i.Link nebo IEEE 1394) - sériová polyfunkční sběrnice, používá se pro připojení digitálních videokamer, externích disků a optických mechanik, čteček paměťových karet ad. Poskytuje vyšší přenosovou rychlost než USB, ale díky nižším cenám zařízení se více rozšířila právě USB (1).



4.1 Rozšiřující karty

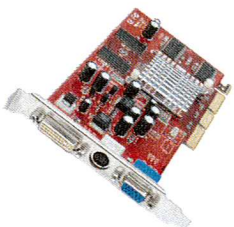
Následně si probereme pouze základní informace k jednotlivým rozšiřujícím kartám.

4.1.1 Grafická karta

Grafická karta (ang. graphics card, video card, video adapter, graphics-accelerator card nebo display adapter) **převádí signál z počítače do monitoru.** Může být i integrována na základní desce nebo ve formě rozšiřující karty připojena prostřednictvím slotu (většinou PCI-Express slot) k základní desce.

Základní parametry grafických karet:

- **Druh chlazení** – aktivní vs. pasivní.
- **Velikost paměti.**
- **Rychlost grafického jádra udávána v Mhz a Ghz.**
- **Rychlost paměti.**
- **Spotřeba** – moderní grafické karty mají nejvyšší spotřebu ze všech počítačových komponent.



Grafická karta (rozšiřující karta)

4.1.2 Síťová karta

Síťová karta (angl. network interface card, network adapter, network interface controller, zkratka NIC) **slouží ke vzájemné komunikaci počítačů v počítačové síti.** Můžeme se s ní setkat ve dvou variantách – integrované na základní desce anebo v podobě karty, která se zasune do slotu (PCI, PCI-e) základní desky.

Každá síťová karta má od výrobce přidělen jedinečný 48-bitový identifikátor, který se nazývá **MAC** adresa[5] (též známá jako fyzická nebo hardwarová adresa).

Základní parametry grafických karet:

- **Typ média** – bezdrátový přenos, kroucená dvojlinka, koaxiální kabel, optické vlákno.
- **Typ sítě** – Ethernet, Token Ring atd.
- **Rychlost** - 100Mbit/s, 1Gbit/s, 10Gbit/s, ...

Síťová karta pro připojení kabelem (kroucená dvojlinka)

4.1.3 Zvuková karta

Zvuková karta (sound card) je rozšiřující karta počítače pro vstup a výstup zvukového signálu. Provádí digitálně-analogový převod nahraného nebo vygenerovaného digitálního záznamu. Tento signál je přiveden na výstup zvukové karty (lze připojit reproduktory nebo sluchátka). Dále lze připojit mikrofon. Na některých kartách nalezneme také MIDI a GamePort konektor.

Barvené značení konektorů zvukové karty

Zelený – Linkový výstup, Sluchátka nebo Přední reproduktory.

Růžový – vstup mikrofonu.

Světle modrý – stereo linkový vstup.

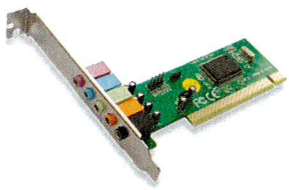
Oranžový – výstup pro subwoofer

Černý – zadní reproduktory (surround)

Šedý – prostřední reproduktory

Zlatý – Game port

[5] **MAC adresa** (Media Access Control) je jedinečný identifikátor síťového zařízení. Je přiřazována síťové kartě NIC bezprostředně při její výrobě a proto se jí také někdy říká **fyzická adresa**, nicméně ji lze dnes u moderních karet dodatečně změnit. MAC adresa se skládá ze 48 bitů a podle standardu by se měla zapisovat jako tři skupiny čtyř hexadecimálních čísel (např. 0123.4567.89ab), mnohem častěji se ale píše jako šestice dvojciferných hexadecimálních čísel oddělených pomlčkami nebo dvojtečkami (např. 01-23-45-67-89-ab nebo 01:23:45:67:89:ab).

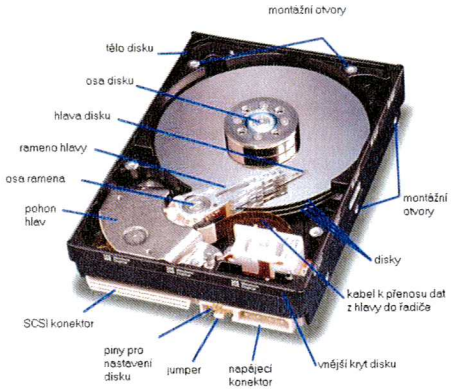


5 Pevný disk

Pevný disk (angl. hard disk drive, HDD) **je zařízení sloužící k trvalému uchovávání většího množství dat.** Funguje na principu magnetismu – data jsou ukládána pomocí zmagnetování míst na discích z magneticky měkkého materiálu.

5.1 Fyzická struktura

Každý disk je složen z několika **ploten** (kotoučů), které se při chodu disku otáčejí určitými otáčkami. Dnes běžně 7200, příp. 10000 ot./min. Na každé straně plotny je *magnetická vrstva* kam se ukládají data (1). Nad každou stranou plotny se pohybuje jedna **magnetická hlava**, která čte a zapisuje data (2).

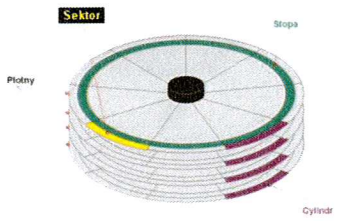


Pevný disk[6]

Magnetický povrch ploten je rozdělen na **stopy** (soustředné kružnice), do kterých se údaje zapisují. Každá stopa je navíc příčně rozdělena na **sektory**. Hlavy pevného disku jsou umístěny na společném rameni. Pokud řadič posune jednu hlavu nad určitý sektor dané stopy svého povrchu – ostatní hlavy

[6] Zdroj: http://puny-hw.wz.cz/hw/harddisk.html

se taktéž posunou nad daný sektor svých povrchů. Díky společnému rameni se tedy hlavy vždy vznášejí nad stejnou stopou všech povrchů. Stejným stopám na různých površích se říká **cylindr**. (1)



Rozdělení disku na logické části[7]

5.2 Rozhranní pevného disku

- EIDE -

Každý disk má svoji řídící elektroniku, která komunikuje se sběrnicí. Na druhém konci sběrnice musí být elektronický obvod – **řadič** (součást základní desky), který komunikaci s diskem zprostředkovává. Jedním z těchto řadičů je **EIDE**, které je pokračovatelem staré normy **IDE** (EIDE se často zapisuje v programu SETUP stále jako IDE). Řadič EIDE je integrován na základních deskách počítačů, je tedy součástí BIOSu a jeho vlastnosti určujeme přes program **SETUP**.

EIDE má **2 kanály,** na každém z nich může pracovat dvojice zařízení. Jedno z nich musí být označeno **MASTER** (hlavní, řídící) a druhé **SLAVE** (podřízené). V SETUP proto najdeme 4 řádky pro konfiguraci zařízení EIDE.

Pozn. Jako MASTER se zapojuje vždy rychlejší z obou zařízení pracujících na jednom kanálu. Nastavení součásti jako MASTER nebo SLAVE se provádí přímo na daném zařízení pomocí speciální propojky zvané jumper.

Pro komunikaci mezi řadičem a diskem jsou z hlediska BIOSu důležité následující vlastnosti:

1. Adresování diskových bloků

Pevný disk musí být schopen určit přesnou polohu dat, která jsou na něm uložena. Rovněž řadič, který s diskem komunikuje, musí umět definovat požadavek, s kterými daty chce pracovat. Obě zařízení tedy musí používat stejnou metodu pro adresování dat.

[7] Zdroj: http://www.banan.cz/serialy/Jak-funguje/Jak-funguje-harddisk-HDD

Dnes se používá zejména metoda **LBA** (Logical Block Addressing), která nahradila starší metody CHS a XCHS. Zpočátku LBA používala 28bitovou adresu odkazující na sektor disku (každý sektor má tedy svoji adresu).

2. Rychlost přenosu dat

Přenos dat mezi diskem a operační pamětí může probíhat dvěma způsoby:

PIO (Programmed Input/Output) – programovaný vstup/výstup je řízen procesorem počítače. Jeho základní nevýhodou je vytěžování procesoru při zápisu či čtení z disku. V režimech PIO dnes pracují pouze některé optické mechaniky.

DMA (Direct Memory Access) – vylepšená verze **Ultra DMA**. Pro přímou komunikaci mezi řadičem a pamětí se používá *Busmastering*. Ten spočívá v tom, že přesun dat je řízen řadičem, nikoli procesorem. Procesor jednoduše zadá příkaz k přenosu dat a o vše ostatní se postará řadič disku.

- SATA -

Sériové rozhraní má proti klasickému paralelnímu rozhraní (EIDE) několik výhod:

- K jednomu zařízení (např. disku SATA) vede pouze jeden kabel, disk je vždy MASTER a odpadají tak časové prodlevy nutné při přepínání mezi dvěma disky EIDE. Navíc max. délka kabelu může být až 1m.
- Přenosová rychlost Seriál ATA je 150 MB/s.
- Díky navržení vnějšího provedení sběrnice a konektorů je možné připojení a odpojení disků za chodu počítače.

- SCSI -

Rozhraní **SCSI** (Small Computer Systems Interface). Cílem SCSI bylo vytvořit standardní rozhraní poskytující sběrnici pro připojení dalších zařízení. SCSI dovoluje připojit ke své sběrnici až 8 různých zařízení, z nichž jedno musí být vlastní SCSI rozhraní. Mezi další velké výhody patří možnost připojení nejen interních zařízení, jako tomu bylo u všech předchozích rozhraní, ale i zařízení externích. SCSI není pevně vázáno na počítač řady PC, ale je možné se s ním setkat i u jiných počítačů (např.: MacIntosh, Sun, Sillicon Graphics).

5.3 Smazané soubory

Mazání souborů probíhá v rámci MS Windows ve **dvou krocích**. Nejdříve se smazané soubory přemístí do *Koše*, a pokud jsou odstraněny i odsud, považujeme je za skutečně smazané. Ve skutečnosti se o souborech vyjmutých z koše zruší záznamy v logické struktuře, ale **fyzicky jsou stále uloženy v sektorech disku** (4). K jejich úplnému vymazání dojde až zápisem nových dat do sektoru. Z toho plynou 2 poznatky:

- ✓ Jestliže chceme data z disku smazat tak, aby nemohly být obnoveny (bez formátování) musíme zapsat data nová.

- ✓ Jestliže data smažeme a později je chceme obnovit, máme šanci, že se nám to podaří.

5.4 Obnova smazaných dat

Jak již bylo řečeno, mazáním se data z disku neodstraňují, pouze se alokační jednotky (v nichž jsou data uložena) označí za volné. Pokud tedy nedošlo k jejich přepsání, můžeme data obnovit. Je k tomu určen speciální SW. Jako příklad můžeme uvést program *PC Inspector File Recovery*.

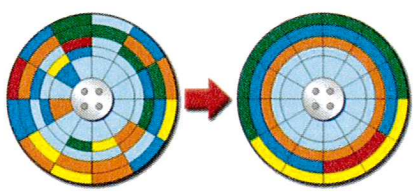
5.5 Defragmentace disku – co a proč

Soubory na disku jsou uloženy v malých alokačních jednotkách. Je zřejmé, že většina souborů se do jedné alokační jednotky nevejde a je rozložena do více clusterů. Pokud jsou všechny alokační jednotky seřazeny za sebou, je vše v „pořádku". Jestliže však alokační jednotky souboru na sebe nenavazují, skládá se soubor z několika částí – **fragmentů**, je fragmentován (6).

Fragmentace je nežádoucím jevem, protože:

- pokud je fragmentovaný soubor rozložen mezi více cylindrů, musí magnetické hlavy pevného disku přeskakovat mezi stopami, což způsobuje zpomalení práce disku a následně celého systému;
- ještě větší problém je způsoben tím, že v sousedních alokačních jednotkách může být umístěno několik fragmentovaných souborů. Dojde-li pak k chybě byť jen malé části disku, bývá postiženo více souborů.
- rovněž obnova fragmentovaných souborů je velmi problematická;

Např. ve Windows 7 je **Defragmentace** nastavena, aby se pravidelně automaticky spouštěla v pozadí a to s minimálním dopadem na naši práci. To vše zajistí, že data na disku budou efektivně umístěna a systém tak bude moci neustále poskytovat rychlou odezvu na vzniklé požadavky. V rámci Windows 7 může být více disků defragmentováno zároveň, bez dalšího čekání na to, než se defragmentuje předchozí disk. K dispozici jsou rovněž free SW produkty pro defragmentaci.



Defragmentace disku zjednodušeně

5.6 Vyčištění disku

Vyčištění disku je zaměřeno na **odstranění různých typů dočasných souborů**. Dočasné (temporary) soubory si vytvářejí programy, ukládající sem prozatímní údaje a po skončení práce by měla aplikace dočasný soubor smazat.

Integrovaný program **Vyčištění disku** ve Windows.

Program disk prohlédne a nabídne přehled souborů, které je možné smazat. Jde většinou o tyto soubory:

- ***Stažené soubory programů*** – ze sítě stažené programové soubory (ovládací prvky ActiveX a applety Java).
- ***Temporary Internet Files*** – dočasné soubory, které se ukládají na disk při načítání www stránek z Internetu (obrázky, videa, cookie).
- ***Ladící informace*** – soubory, v nichž jsou uloženy informace o ladění některých programů.
- ***Koš*** – seznam dříve smazaných souborů.
- ***Dočasné soubory*** – dočasné soubory se ukládají do složky TEMP. Zde se jich pravidelně hromadí velké množství.
- ***Komprese starých souborů*** – Windows automaticky komprimují dlouho nepoužívané, staré soubory a šetří tak místo na disku.
- ***Katalogové soubory pro službu Indexování*** – služba indexování vytváří indexy obsahu a vlastností dokumentů na pevném disku a na sdílených síťových jednotkách. Pokud se na disku nalézají soubory starých indexů, *Vyčištění disku* je najde a odstraní.

6 Optická mechanika (CD, DVD, Blu-ray)

Optické mechaniky (angl. optical disc drive - ODD) **pracující na principu laserového světla, nebo elektromagnetických vln blízkých světelnému spektru.** Tyto mechaniky slouží k ukládání dat na optické disky (CD, DVD, Blu-ray, HD DVD) - některé však mohou data jenom číst.

Hlavní částí mechaniky je optická hlava, jež se skládá z polovodičového laseru, čočky pro usměrnění laserového paprsku a fotodiody, která zachycuje odražené světlo z povrchu disku (7).

Na disky pro optické mechaniky je možné data zapsat pouze jednou (CD-R, DVD-R, BD-R) nebo vícekrát (CD-RW, DVD-RW, DVD+RW, DVD-RAM, BD-RE, HD DVD-RW). Jednou zapisovatelný disk funguje na následujícím principu: na vrstvě zlata má nanesenou organickou vrstvu, která je krytá polykarbonátovým základem. Při zápisu pak laserový paprsek projde polykarbonátem a propálí organickou vrstvu až k vrstvě zlata a tím vznikne důlek (pit).

U přepisovatelných médií je možné předešlý záznam smazat a nahradit novým. To je umožněno díky materiálům, které mohou měnit svoji strukturu z krystalické na amorfní a zpět. Pokud se tento materiál ohřeje laserovým paprskem na teplotu přes 600°C, dojde po ochlazení ke změně struktury – na amorfní. V případě, že se ohřeje méně (cca 200°C), vrátí se do původního stavu. Při čtení se paprsek laseru odrazí od místa s amorfní strukturou méně než od místa s fází krystalickou. To umožňuje rozlišit dva stavy – jedničku a nulu.

Optická mechanika

7 Počítačová skříň

Počítačová skříň (angl. *computer case*) **slouží k mechanickému upevnění a ochraně všech ostatních vnitřních dílů a částí počítače.** Nosné části jsou kovové, na krycí části bývají použity plasty. Skříně mají standardizované rozměry tak, aby byly kompatibilní s jednotlivými částmi počítačů (základní deska, harddisk atd.).

Nepoužitá skříň má na přední straně ovládací tlačítka, zaslepené otvory pro „dvířka" mechanik, čteček apod. a na zadní straně zaslepené otvory pro konektory a přídavné karty.

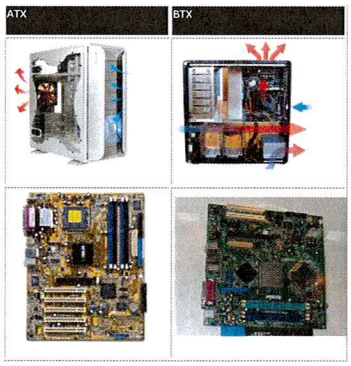
Skříň má odnímatelné víko nebo boční stěny, které po odstranění odhalí samotné šasi.

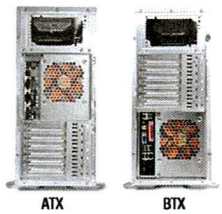
Existuje několik typů počítačových skříní:

desktop – skříň je na stole umístěna naležato a na ní je postaven monitor. V desktopu jsou rozšiřovací karty umístěné svisle vůči vodorovně umístěné základní desce.

tower – skříň je umístěna nastojato (leží na své nejmenší stěně a tím zabírá nejméně místa). Může být umístěna i na zemi pod stolem. Tower je dnes nejpoužívanějším typem skříně. Základní deska je položena svisle a rozšiřovací karty jsou do ní uloženy vodorovně.

V současnosti se setkáváme s dvěma standardy skříní **ATX** (Advanced Technology eXtended) a **BTX** (Balanced Technology eXtended), které se liší prouděním vzduchu uvnitř skříně. BTX je díky plynulému průtoku skříní určena pro výkonnější počítače – zajišťuje kvalitnější chlazení (7).





Napájecí zdroj počítače (angl. *Power Supply Unit – PSU*) je zařízení sloužící úpravě střídavého napětí odebíraného ze sítě (u nás 230V/50Hz). Dochází k transformaci hladiny napětí na nižší, které je vhodné k napájení elektronických obvodů počítače. Jednotlivé komponenty se ke zdroji připojují prostřednictvím napájecích vodičů.

8 Počítačové periferie

8.1 Monitor

Monitor je základní počítačová periferie sloužící k zobrazování textových a grafických informací. Propojuje se s grafickou kartou.

Monitory můžeme podle používaných technologií rozdělit na několik skupin:

- **CRT** (klasická vakuová obrazovka) - velmi vysoký kontrastní poměr, výborné zobrazení barev, avšak velké rozměry a váha, taktéž větší spotřeba elektrické energie než u LCD displejů.
- **LCD** (tekuté krystaly) – jsou kompaktní, lehké, mají nízko spotřebu, nemají žádné elektromagnetické vyzařování, avšak mají malý kontrastní poměr.
- **LED** – nejnovější technologie, přibližně o 40 % elektrické energie méně, než běžný monitor podobné velikosti. (7)

Velikost monitoru se udává jako vzdálenost mezi protilehlými rohy obrazovky (tzv. úhlopříčka - používanou jednotkou jsou palce).

Rozlišením (angl. resolution) monitoru rozumíme počet pixelů, které může být zobrazeno na obrazovce. Uvádí se jako počet sloupců (horizontálně, „X"), které se uvádí vždy jako první, a počet řádků (vertikálně, „Y"). Nejpoužívanějšími rozlišeními jsou: 1024×768 (XGA/XVGA, eXtended), 1280×800 (WXGA, Wide XGA, hlavně u notebooků), a 1600×1200 (UXGA, Ultra-eXtended).

Dalším sledovaným parametrem u monitoru je **obnovovací frekvence** (jednotka Hz) – jako ergonomické minimum pro CRT monitory je uváděno 85–100 Hz, u LCD monitorů je tento parametr nepodstatný.

Odezva se udává v jednotkách milisekund a je to doba, za kterou se bod na LCD monitoru rozsvítí a zhasne.

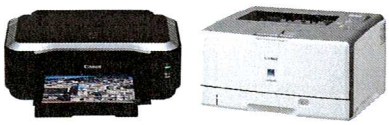
LCD monitor

8.2 Tiskárny

Tiskárny jsou dnes naprosto běžnou součástí počítačového pracoviště. **Jedná se o výstupní zařízení, které slouží k přenosu dat uložených v elektronické podobě na papír** (případně obdobné médium – např. samolepky, kompaktní disk). (6)

Tiskárny se připojují k počítači pomocí USB portu, síťového kabelu nebo bezdrátově. Podle technologie tisku je možné je členit do kategorií:

- *jehličkové* - jsou srovnatelné s obyčejným psacím strojem, kdy řada 9 nebo 24 jehliček vyťukává přes barvicí pásku na papír jemné body, ze kterých se skládají písmena a obrázky. Často se používá nekonečný papír, především ve firmách.
- *inkoustové* (angl. ink-jet printer) - tisková hlava tryská z několika desítek mikroskopických trysek na papír miniaturní kapičky inkoustu.
- *laserové* (angl. laser printer) - pracují na stejném principu jako kopírky - laserový paprsek vykresluje obrázek na světelném válci, na povrch tohoto válce se pak nanáší toner, který se pak uchytí jen na osvětlených místech. Válec s tonerem se poté obtisknou na papír a toner se na konec papíru tepelně fixuje (zažehlí).



Inkoustová a laserová tiskárna

8.3 Skener

Skener je zařízení, které slouží k převedení obrázků a textů z papírové (nebo obdobné) podoby do podoby počítačového souboru. Jeho použití je např. při archivaci papírových dokumentů (faktur, objednávek, knih, projektů...), pro převedení textových dokumentů do podoby textových souborů (tzv. OCR – Optical Character Recognition, optické rozpoznávání textů), odesílání papírových dokumentů elektronickou poštou, při počítačovém zpracování fotografií, filmů a jiné grafiky a pro celou řadu jiných použití.

8.4 Záložní zdroj

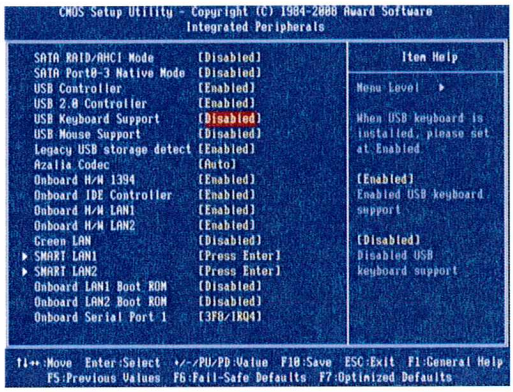
Záložní zdroj (angl. Uninterruptible Power Supply (Source) – „nepřerušitelný zdroj energie" - UPS) **je zařízení, které zajišťuje dodávku elektřiny do počítače, a to i při neočekávaném výpadku el. sítě.**

Tento zdroj funguje na principu akumulátoru - jestliže není dodávka elektřiny z primárního zdroje přerušena, je udržován v nabitém stavu. Jakmile dojde k přerušení dodávky elektrické energie, napájí počítač až do svého vybití (příp. obnovení dodávky). Doba, po kterou UPS udrží zařízení v chodu, je dána kapacitou akumulátorů. Zpravidla ale máme dostatečnou dobu na uložení rozpracovaných dokumentů, aniž bychom o ně přišli.

VĚDĚLI JSTE, ŽE?

Asi dnes všichni víme, že současné klávesnice a myši se připojují pomocí sériového rozhraní USB. Nicméně stalo se Vám někdy, např. po pádu OS, že naběhla obrazovka zavádění OS s požadavkem akce – **Spustit systém běžným způsobem** a klávesy Vaší USB klávesnice nereagovaly?

V případě, že máte doma ve skříni ještě starší PS/2 klávesnici mohli jste tento problém vyřešit jejím dočasným oživením. Nicméně Váš problém s USB klávesnicí je v nastavení **BIOS**, kde je zakázán **USB keyboard Support**.



BIOS – USB Keyboard Support

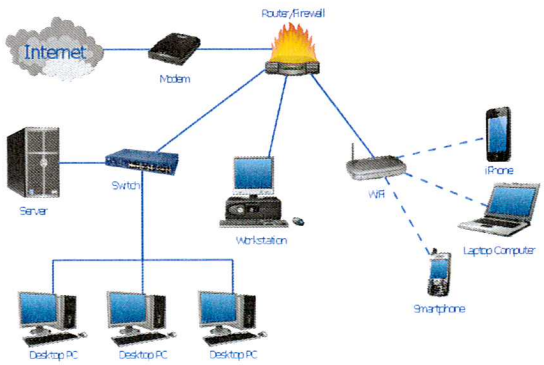
Závěr bloku Hardware

První blok byl zaměřen na vybrané kapitoly Hardware, následuje blok věnovaný Počítačovým sítím. Další informace k problematice Hardware lze čerpat buď přímo z odborné literatury, nebo na specializovaných portálech.

Vybrané kapitoly Počítačových sítí

Pojmem **počítačová síť** se obvykle rozumí propojení více počítačů tak, aby mohly navzájem sdílet své prostředky. **Přitom je jedno zda se jedná o prostředky hardwarové nebo softwarové.**

Po formální stránce je počítačová síť skupina počítačů popř. periferií, které jsou mezi sebou propojeny tak, aby zajistily vzájemnou komunikaci libovolného uživatele s programem na libovolném počítači, dvou programů mezi sebou nebo dvou libovolných uživatelů mezi sebou, a to při vysoké spolehlivosti komunikace. (8)

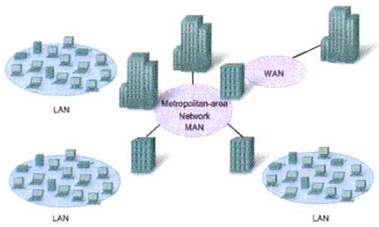


Síť[8]

[8] Zdroj: http://www.conceptdraw.com/mosaic/draw-the-system-diagram-for-this-solution

9 Členění počítačových sítí

9.1 Členění podle rozlehlosti



LAN, MAN, WAN [9]

9.1.1 PAN

Osobní sítě, zvané též **PAN** (původem v anglickém ***Personal Area Network***), jsou sítě s nejmenší rozlehlostí. Jsou používané pro propojení osobních elektronických zařízení. Osobní počítačové sítě si nekladou za cíl co nejvyšší přenosovou rychlost, ale spíše odolnost proti rušení, nízkou spotřebu elektrické energie nebo také třeba snadnou konfigurovatelnost. Mají velmi malý dosah, obvykle jen několik metrů.

9.1.2 LAN

Menší sítě např. v rozsahu jedné budovy (např. školy) se označují jako lokální sítě (LAN z anglického Local Area Network). **Většina moderních sítí LAN podporuje širokou škálu počítačů a jiných zařízení.** Každé zařízení musí používat vlastní fyzické protokoly a protokoly datového spojení pro konkrétní síť a všechna zařízení, která chtějí komunikovat se všemi ostatními v síti, musí používat stejný komunikační protokol. (10)

Ačkoliv jednotlivé sítě LAN jsou co do rozsahu omezeny, mohou být propojeny do větších celků. Podobné sítě LAN se propojují pomocí **mostů** (bridge), které slouží jako body přenosu mezi sítěmi. Rozdílné sítě LAN se spojují bránami (gateways), které přenášejí data a zároveň je konvertují podle protokolů používaných síti příjemce (8).

9.1.3 MAN

Síť, která svou rozlohou pojímá např. celé město, pracující vysokou rychlostí a schopná přenášet data na vzdálenost až 80 km.

[9] Zdroj: http://somelearning.com/concepts-of-computer-networks-network-types

9.1.4 WAN

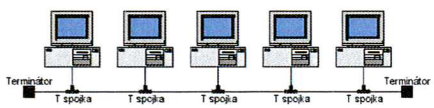
Jedná se o celosvětovou síť, která v podstatě vzniká propojením menších sítí LAN a MAN. Síti WAN je internet.

9.2 Fyzická topologie počítačových sítí

Topologie sítě úzce souvisí s aplikacemi, přenosovou rychlostí, přenosovými prostředky a mnohonásobným přístupem k nim. **Je třeba rozlišovat mezi fyzickou a logickou topologií. Fyzická topologie** popisuje fyzická propojení, tj. vedení přenosových prostředků. Logická topologie popisuje způsob toku signálu.

9.2.1 Sběrnicová topologie

Sběrnicová topologie je také označována jako lineární sběrnice. Jde v podstatě o nejjednodušší způsob propojení počítačů do sítě. Skládá se z jediného kabelu, který v jedné linii propojuje všechny počítače v síti (9)



Síť se sběrnicovou topologií

Komunikace ve sběrnicové topologii

Počítače v síti komunikují tak, že adresují data konkrétnímu počítači a posílají tato data po kabelu ve formě elektrických signálů. Abyste pochopili, jak počítače ve sběrnicové topologii komunikují, musíte se seznámit se třemi pojmy (9):

- posílání signálu
- vracející se signál
- terminátor

Posílání signálu

Data v síti ve formě elektrických signálů jsou posílána všem počítačům v síti, nicméně informaci přijme pouze ten počítač, jehož adresa odpovídá adrese zakódované v počátečním signálu. **V daný okamžik může zprávy odesílat vždy pouze jeden počítač.**(9)

V síti se sběrnicovou topologií může v daném okamžiku data posílat vždy pouze jeden počítač, proto závisí výkon sítě na počtu připojených počítačů. Čím více počítačů, tím více počítačů bude čekat, aby mohly poslat data po sběrnici, a tím bude síť pomalejší.

Sběrnicová topologie je pasivní topologií. Počítače ve sběrnicové síti pouze poslouchají, zda jsou v síti posílána nějaká data. Neodpovídají na přesun dat z jednoho počítače na druhý. Pokud jeden počítač selže, neovlivní to zbytek sítě. V aktivní topologii počítače obnovují signály a přesunují data dále po síti. (9)

Vracející se signál

Vzhledem k tomu, že data jsou posílána po celé síti, putují z jednoho konce kabelu na druhý. Kdyby mohl signál pokračovat bez přerušení, neustále by se vracel tam a zpět podél kabelu a zabránil by tak ostatním počítačům v odesílání jejich signálů. Proto je potřeba signál, co měl možnost dosáhnout cílové adresy, zastavit. (9)

Terminátor

Aby se zastavilo vracení signálu, umístí se na oba konce kabelu terminátor, který pohlcuje volné signály. Pohlcování vyčistí kabel tak, aby mohly data posílat i další počítače. (9)

Výhody

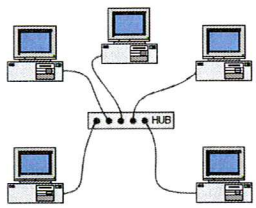
- ✓ Snadná realizace a snadné rozšíření již stávající sítě.
- ✓ Nevyžaduje tolik kabeláže jako např. hvězdicová topologie.
- ✓ Vhodná pro malé nebo dočasné sítě, které nevyžadují velké rychlosti přenosu.

Nevýhody

- Nesnadné odstraňování závad.
- Omezená délka kabelu a také počtu stanic.
- Pokud nastane nějaký problém s kabelem, celá síť přestane fungovat.
- Výkon celé sítě rapidně klesá při větších počtech stanic nebo při velkém provozu.

9.2.2 Hvězdicová topologie

Ve hvězdicové topologii jsou počítače propojeny pomocí kabelových segmentů k centrálnímu prvku sítě, nazývanému **přepínač** (SWITCH). Dříve rozbočovač (HUB. Signály se přenáší z vysílacího počítače přes switch k příjemcům. Tato topologie pochází z počátků používání výpočetní techniky, kdy bývaly počítače připojeny k centrálnímu počítači mainframe. Mezi každými dvěma stanicemi musí existovat jen jedna cesta! (9)



Síť s hvězdicovou topologií

Hvězdicová topologie nabízí centralizované zdroje a správu. Protože jsou však všechny počítače připojeny k centrálnímu bodu, vyžaduje tato topologie při instalaci velké sítě velké množství kabelů. Selhání switche ve hvězdicové topologii způsobí "spadnutí" sítě u stanic k němu připojených. Je proto vhodné ho chránit před výpadkem záložním zdrojem. (9)

Pokud ve hvězdicové síti selže jeden počítač nebo kabel, který ho připojuje k přepínači, pouze tento nefunkční počítač nebude moci posílat nebo přijímat data ze sítě. Zbývající část sítě bude i nadále fungovat normálně.

Výhody

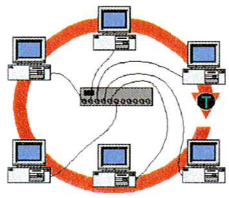
- ✓ Pokud selže jeden počítač nebo kabel nebude fungovat spojení pouze pro jednu stanici a ostatní stanice mohou vysílat i přijímat nadále
- ✓ Dobrá výkonnost v porovnání se sběrnicovou topologií. To souvisí s tím, že na jednom kabelu je připojen pouze jeden počítač a tudíž jednak nedochází ke kolizím mezi pakety a také může současně přenášet data více počítačů.
- ✓ Snadno se nastavuje a rozšiřuje
- ✓ Závady se dají snadno nalézt

Nevýhody

- U větších sítí vyžadováno velké množství kabelů - ke každému počítači jeden.
- Potřeba extra hardware v porovnání se sběrnicovou topologií.
- V případě selhání centrálního síťového prvku přestane fungovat celá síť.

9.2.3 Kruhová topologie

Kruhová topologie propojuje počítače pomocí kabelu v jediném okruhu. Neexistují žádné zakončené konce. Signál postupuje po smyčce v jednom směru a prochází všemi počítači. Narozdíl od pasivní sběrnicové topologie funguje každý počítač jako **opakovač**, tzn., že zesiluje signál a posílá ho do dalšího počítače. Protože signál prochází všemi počítači, může mít selhání jednoho počítače dopad na celou síť. (9)



Síť s prstencovou topologií

Předávání známky

Jeden způsob přenosu dat po kruhu se nazývá předávání známky. Známka (token) se posílá z jednoho počítače na druhý, dokud se nedostane do počítače, který má data k odeslání. Vysílající počítač známku pozmění, přiřadí datům elektronickou adresu a pošle ji dál po okruhu.

Data procházejí všemi počítači, dokud nenaleznou počítač s adresou, která odpovídá jim přiřazené adrese. Přijímací počítač vrátí vysílacímu počítači zprávu, že data byla přijata. Po ověření vytvoří vysílací počítač novou známku a uvolní ji do sítě.

Může se zdát, že oběh známky trvá dlouho, ale ve skutečnosti se přenáší přibližně rychlostí světla. Známka proběhne kruhem o průměru 200m asi 10 000krát za sekundu.

Výhody

- ✓ přenos dat je relativně jednoduchý, protože packety se posílají jedním směrem
- ✓ přidání dalšího uzlu má jen malý dopad na šířku pásma
- ✓ nevznikají kolize
- ✓ minimální zpoždění (v bitech podle počtu uzlů)
- ✓ průchodnost sítě je z výše uvedených důvodů ze všech ostatních topologií nejvyšší
- ✓ snadná možnost implementace záruk na množství přenesených dat za jednotku času
- ✓ množství kabelů může být menší, než u hvězdicové topologie
- ✓ Závady se dají snadno nalézt

Nevýhody

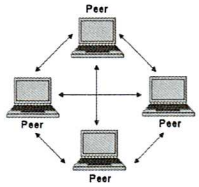
- vstup a výstup (zapnutí a vypnutí) stanice je logicky a implementačně komplikovaná operace
- data musí projít přes všechny členy kruhu, což zvyšuje riziko poruchy
- přerušením kruhu vzniká problém (Při vyřazení jedné stanice další stanice přestávají pracovat)
- při přidání nového uzlu je nutné dočasně kruh přerušit (u Token ringu jen na zanedbatelný okamžik)

9.3 Členění podle postavení uzlů

Peer-to-peer nebo též **peer to peer**, **rovný s rovným** či **P2P**, je typ sítě, ve které jsou si všechny počítače, resp. uzly, v síti rovny. Každá stanice v síti může vyčlenit některý svůj prostředek (tiskárnu, úložné médium, adresář) ke sdílení. Jiná stanice může tyto prostředky používat, pokud si sdílený prostředek připojí a její uživatel zná případné heslo. Sdílení a hesla mohou být kdykoliv změněna nebo zrušena uživatelem, který u stanice pracuje. Tento typ sítě v podstatě nelze centrálně spravovat. Příkladem může být sdílení souborů a systémových prostředků v různých operačních systémech a souborů v internetových sítích. (10) (11)

Klient-server je typ sítě, ve které je jeden počítač (server) nebo více počítačů (několik serverů) nadřazen jinému počítači (klientovi) či několika počítačům (několika klientům). Server poskytuje služby „běžným" stanicím – klientům.

Serverů může být více typů podle poskytovaných služeb (**souborový server**, **tiskový server**, **poštovní server**, **WWW server**, **FTP server** atd.). Nemusí platit, že server = jeden počítač, u malých sítí plní úlohu několika typů serverů jeden „fyzický" počítač, u velkých sítí může např. jeden „fyzický" počítač plnit pouze úlohu tiskového serveru.



10 Síťové prvky

10.1 Aktivní síťové prvky

Aktivní síťové prvky jsou všechna zařízení, která slouží ke vzájemnému propojení v počítačových sítích. Aktivní síťový prvek je všechno to, co nějakým způsobem aktivně působí na přenášené signály – tedy je zesiluje a různě modifikuje. Mezi aktivní prvky se řadí především:

- opakovač,
- hub,
- switch,
- bridge,
- router.

10.1.1 Opakovač

Repeater nebo též **opakovač** či **zesilovač** je elektronický aktivní síťový prvek, který přijímá zkreslený, zašuměný nebo jinak poškozený signál a opravený, zesílený a správně časovaný ho vysílá dále. Tak je možné snadno zvýšit dosah média bez ztráty kvality a obsahu signálu. Opakovače patří do první (fyzické) vrstvy referenčního modelu OSI, protože pracují přímo s elektrickým signálem.

10.1.2 Hub

Hub nebo též **rozbočovač** je prvek, který umožňuje její větvení a je základem sítí s hvězdicovou topologií. Chová se jako opakovač. To znamená, že veškerá data, která přijdou na jeden z portů (zásuvek), zkopíruje na všechny ostatní porty, bez ohledu na to, kterému portu (počítači a IP adrese) data náleží. To má za následek, že všechny počítače v síti „vidí" všechna síťová data a u větších sítí to znamená zbytečné přetěžování těch segmentů, kterým data ve skutečnosti nejsou určena. Hub je velmi jednoduché aktivní síťové zařízení. Nijak neřídí provoz, který skrz něj prochází. Signál, který do něj vstoupí, je obnoven a vyslán všemi ostatními porty.

10.1.3 Switch

Switch nebo též **přepínač** je prvek propojující jednotlivé segmenty sítě. Switch obsahuje větší či menší množství portů (až několik stovek), na něž se připojují síťová zařízení nebo části sítě. Pojem switch se používá pro různá zařízení v celé řadě síťových technologií. Pracuje na druhé (linkové) vrstvě OSI modelu. Vedle vyššího výkonu (stanice připojené k různým rozhraním switche navzájem nesoutěží o datové médium) znamená přínos i pro bezpečnost sítě, protože médium již není sdíleno a data se vysílají jen do rozhraní, jímž je připojen jejich adresát (9) .

10.1.4 Bridge

Bridge nebo též **most** je zařízení, které spojuje dvě části sítě na druhé (linkové) vrstvě referenčního modelu ISO/OSI. Most je pro protokoly vyšších vrstev transparentní (neviditelný), odděluje provoz různých segmentů sítě a tím zmenšuje i zatížení sítě. Most odděluje provoz dvou segmentů sítě tak,

že si ve své paměti RAM sám sestaví tabulku MAC (fyzických) adres a portů, za kterými se dané adresy nacházejí. Leží-li příjemce ve stejném segmentu jako odesílatel, most rámce do jiných částí sítě neodešle. V opačném případě je odešle do příslušného segmentu v nezměněném stavu (týká se pouze tzv. Unicast rámců, které jsou určeny jedinému příjemci).

10.1.5 Router

Router nebo též **směrovač** je zařízení, které procesem zvaným routování přeposílá datagramy směrem k jejich cíli. Routování probíhá na třetí (síťové) vrstvě referenčního modelu ISO/OSI. Obecně jako router může sloužit jakýkoliv počítač s podporou síťování a pro routování v menších sítích se často dodnes používají běžné osobní počítače, do vysokorychlostních sítí jsou však jako routery používány vysoce účelové počítače obvykle se speciálním hardwarem, optimalizovaným jak pro běžné přeposílání (forwarding) diagramů. (9)

10.2 Pasivní síťové prvky

Mezi pasivní prvky se řadí především datové rozvaděče, které fyzicky přenášejí data do počítače.

10.2.1 Strukturovaná kabeláž

- *Kroucená dvojlinka* je druh kabelu, který je tvořen páry vodičů, které jsou po své délce pravidelným způsobem zkrouceny a následně jsou do sebe zakrouceny i samy výsledné páry . Oba vodiče jsou v rovnocenné pozici (i v tom smyslu, že žádný z nich není spojován se zemí či s kostrou), a proto kroucená dvojlinka patří mezi tzv. symetrická vedení (dvojice spirálově stočených vodičů v kabelu).

- *Koaxiální kabel* je asymetrický elektrický kabel s jedním válcovým vnějším vodičem a jedním drátovým nebo trubkovým vodičem vnitřním. Vnější vodič nazýváme často stíněním a vnitřní vodič jádrem. Vnější a vnitřní vodič jsou odděleny nevodivou vrstvou (dielektrikum).

- *Optické vlákno* je skleněné nebo plastové vlákno, které prostřednictvím světla přenáší signály ve směru své podélné osy. Optická vlákna jsou široce využívána v komunikacích, kde umožňují přenos na delší vzdálenosti a při vyšších přenosových rychlostech dat než jiné

formy komunikace. Vlákna se používají místo kovových vodičů, protože signály jsou přenášeny s menší ztrátou a zároveň jsou vlákna imunní vůči elektromagnetickému rušení.

10.3 Standardy síťového hardwaru

V předchozí kapitole jsme se podívali na některé části síťového HW a dále bychom si měli objasnit, zdali existují nějaké standardy, které definují požadavky na technické provedení sítí. Normalizaci provádí organizace IEEE, tudíž jednotlivé normy nesou její označení. (10)

Např.:

IEEE 802.3	Standardy sítě ETHERNET
IEEE 802.11	Standardy bezdrátové sítě

Z praktického hlediska nás nejvíce zajímají tyto standardem definované vlastnosti:

- Přístupová metoda,
- Topologie sítí,
- Typ kabelu, jeho délka, způsob připojení stanic,
- Rychlost přenosu dat.

Dnes je nejvíce používaným standardem Ethernet. Problematika s tímto svázaná je poměrně rozsáhlá a my se jí zde věnovat nebudeme, nicméně je záhodno, abyste si jí více prostudovali z jiných zdrojů uvedených např. v seznamu doporučené literatury na konci tohoto bloku.

11 Síťové modely a protokoly

Počítačové sítě zpočátku vyvíjelo více firem, ale jednalo o uzavřené a vzájemně nekompatibilní systémy. Vznikla tak potřeba stanovit určitá pravidla pro přenos dat v síti a mezi nimi.

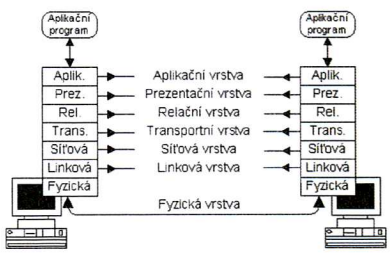
11.1 Referenční model ISO/OSI

Model ISO/OSI je referenční komunikační model označený zkratkou slovního spojení "International Standards Organization / Open Systen Interconnection" (Mezinárodní organizace pro normalizaci / propojení otevřených systémů). Jedná se o doporučený model, který rozděluje vzájemnou komunikaci mezi počítači v síti do sedmi souvisejících vrstev. Zmíněné vrstvy jsou též známé pod označením *Sada vrstev protokolu*.

Úkolem každé vrstvy je poskytovat služby následující vyšší vrstvě a nezatěžovat vyšší vrstvu detaily o tom jak je služba ve skutečnosti realizována. Než se data přesunou z jedné vrstvy do druhé, rozdělí se do **paketů**. V každé vrstvě se pak k paketu přidávají další doplňkové informace (formátování, adresa), které jsou nezbytné pro úspěšný přenos po síti. (8)(9)

Paket – v rámci sítě LAN se data přenášejí tak, že jsou rozdělena na malé balíčky – pakety. Paket je tedy množina dat uzpůsobená k přenosu. (Soubor kopírovaný z jednoho PC na druhý je tedy nejprve rozdělen na pakety, přenesen a pak zpětně složen.)

Uvedený model obsahuje následující vrstvy (každá vyšší vrstva využívá funkce vrstvy nižší.



Referenční model ISO/OSI[10]

[10] Zdroj: http://zam.opf.slu.cz/botlik/CD-0x/1.html

Fyzická vrstva

Úkolem této vrstvy je umožnit přenos jednotlivých bitů mezi příjemcem a odesilatelem prostřednictvím fyzické přenosové cesty, kterou tato vrstva bezprostředně ovládá. K tomu je ovšem třeba vyřešit mnoho otázek převážně technického charakteru - např. jakou úrovní napětí bude reprezentována logická jednička a jakou logická nula, jak dlouho "trvá" jeden bit, kolik kontaktů a jaký tvar mají mít konektory kabelů, jaké signály jsou těmito kabely přenášeny, jaký je jejich význam, časový průběh apod. (8)

Linková vrstva

Linková vrstva má za úkol zajistit bezchybný přenos celých bloků dat (velikosti řádově stovek bytů), označovaných jako **rámce** (**frames**). Jelikož fyzická vrstva nijak neinterpretuje jednotlivé přenášené bity, je na linkové vrstvě, aby správně rozpoznala začátek a konec rámce, i jeho jednotlivé části.

V rámci sítě může docházet k nejrůznějším poruchám, v jejichž důsledku jsou přijaty jiné hodnoty bitů, než jaké byly původně vysílány. Jelikož fyzická vrstva se nezabývá významem jednotlivých bitů, rozpozná tento druh chyb až linková vrstva. Ta kontroluje celé rámce, zda byly přeneseny správně (podle různých kontrolních součtů, viz 3. díl našeho seriálu). Odesilateli potvrzuje přijetí bezchybně přenesených rámců, zatímco v případě poškozených rámců si vyžádá jejich opětovné vyslání. (8)

Síťová vrstva

Linková vrstva zajišťuje přenos celých rámců, ovšem pouze mezi dvěma uzly, mezi kterými vede přímé spojení. Co ale dělat, když spojení mezi příjemcem a odesilatelem není přímé, ale vede přes jeden či více mezilehlých uzlů? Pak musí nastoupit síťová vrstva, která zajistí potřebné **směrování** (**routing**) přenášených rámců, označovaných nyní již jako **pakety** (**packets**). Síťová vrstva tedy zajišťuje volbu vhodné trasy resp. cesty přes mezilehlé uzly, a také postupné předávání jednotlivých paketů po této trase od původního odesilatele až ke konečnému příjemci. Síťová vrstva si tedy musí "uvědomovat" konkrétní topologii sítě (tj. způsob vzájemného přímého propojení jednotlivých uzlů). (8)(10)

Transportní vrstva

Síťová vrstva poskytuje transportní vrtsvě služby, zajišťující přenos paketů mezi libovolnými dvěma uzly sítě. Transportní vrstvu proto zcela odstiňuje od skutečné topologie. Transportní vrstvě díky tomu stačí zabývat se již jen komunikací koncových účastníků (tzv. **end-to-end** komunikací) - tedy komunikací mezi původním odesilatelem a konečným příjemcem. Při odesílání dat zajišťuje transportní vrstva sestavování paketů, do kterých rozděluje přenášená data, a při příjmu je zase z paketů vyjímá a sestavuje do původního tvaru. (8)

Relační vrstva

Úlohou relační vrstvy je navazování, udržování a rušení **spojení** mezi účastníky výměny informací. Při navazování relace si relační vrstva vyžádá na transportní vrstvě vytvoření spojení, prostřednictvím kterého pak probíhá komunikace mezi oběma účastníky relace. Pokud je třeba tuto komunikaci nějak řídit (např. určovat, kdo má kdy vysílat, nemohou-li to dělat oba účastníci současně), zajišťuje to

právě tato vrstva, která má také na starosti vše, co je potřeba k ukončení relace a zrušení existujícího spojení. (8)

Prezentační vrstva

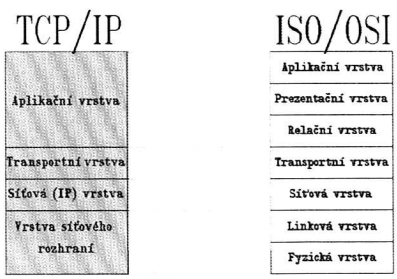
Informace přenášené prostřednictvím sítě mohou být textové, číselné či obecnějších datových struktur. **Potřebné konverze přenášených dat má na starosti prezentační vrstva**. V rámci této vrstvy bývá také realizována případná komprese přenášených dat, eventuálně i jejich šifrování. (8)

Aplikační vrstva

Prostřednictvím aplikační vrstvy mohou uživatelé nebo aplikace vidět výsledky služeb zajišťovaných všemi nižšími vrstvami. Jde o vrstvu nejbližší uživateli, která na rozdíl od ostatních nezajišťuje služby pro vyšší vrstvu (žádnou již nemá). Příklady funkcí zajišťovaných touto vrstvou jsou:

- souborové přenosy,
- sdílení zdrojů,
- přístup k databázím,
- prohlížení webových stránek,
- ovládání programů, apod.

11.2 Model TCP/IP



Porovnání modelů [11]

Zatímco referenční model ISO/OSI vymezuje sedm vrstev síťového programového vybavení, reálný model TCP/IP počítá se čtyřmi vrstvami.

Spolehneme-li se opět na slova Jiřího Peterky, popis jednotlivých vrstev je následující (8):

[11] Zdroj: http://www.earchiv.cz/a92/a213c110.php3

Vrstva síťového rozhraní

Vrstva síťového rozhraní (**Network Interface Layer**) (někdy též: **linková vrstva** resp. **Link Layer**) má na starosti vše, co je spojeno s ovládáním konkrétní přenosové cesty resp. sítě, a s přímým vysíláním a příjmem datových paketů. V rámci soustavy TCP/IP není tato vrstva blíže specifikována, neboť je závislá na použité přenosové technologii. **Funkce na této vrstvě zahrnují mapování IP adres na fyzické adresy.**

Vzhledem k velmi častému připojování jednotlivých uzlů na lokální sítě typu Ethernet je vrstva síťového rozhraní v rámci TCP/IP často označována také jako **Ethernetová vrstva** (**Ethernet Layer**). (8)

Síťová vrstva

Síťová vrstva již není závislá na konkrétní přenosové technologii. V TCP/IP označovaná jako **Internet Layer** (volněji: vrstva vzájemného propojení sítí), nebo též **IP vrstva** (**IP Layer**) podle toho, že je realizována pomocí **protokolu IP**. Tato vrstva se stará v základu o to, aby se jednotlivé pakety dostaly od odesílatele až ke svému skutečnému příjemci, přes případné směrovače resp. brány. Vzhledem k nespojovanému charakteru přenosů v TCP/IP je na úrovni této vrstvy zajišťována jednoduchá (tj. nespolehlivá) datagramová služba. (8)

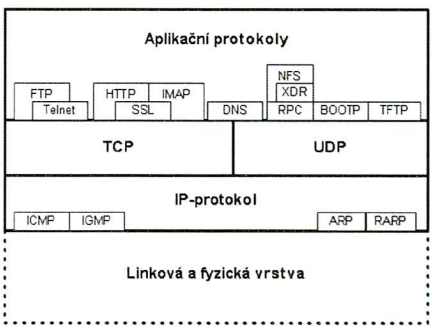
Transportní vrstva

Třetí vrstva TCP/IP je označována jako **transportní vrstva** (**Transport Layer**), nebo též jako **TCP vrstva** (**TCP Layer**), neboť je nejčastěji realizována právě protokolem TCP (Transmission Control Protocol). Hlavním úkolem této vrstvy je zajistit přenos mezi dvěma koncovými účastníky, kterými jsou v případě TCP/IP přímo aplikační programy (jako entity bezprostředně vyšší vrstvy). Podle jejich nároků a požadavků může transportní vrstva regulovat tok dat oběma směry, zajišťovat spolehlivost přenosu, a také měnit nespojovaný charakter přenosu (v síťové vrstvě) na spojovaný. (8)

Aplikační vrstva

Nejvyšší vrstvou TCP/IP je pak vrstva **aplikační** (**Application Layer**). Jejími entitami jsou jednotlivé aplikační programy, které na rozdíl od referenčního modelu ISO/OSI komunikují přímo s transportní vrstvou. Případné prezentační a relační služby, které v modelu ISO/OSI zajišťují samostatné vrstvy, si zde musí jednotlivé aplikace v případě potřeby realizovat samy. (8)

11.3 Základní síťové protokoly



Protokoly v rámci vrstev [12]

Nedílnou součástí síťového SW jsou síťové protokoly. Jak už asi víme, protokol definuje komunikační pravidla, jimiž se řídí výměna dat v síti. U sítí LAN se fakticky používá pouze sada protokolů TCP/IP.

11.3.1 Internet Protokol

IP protokol pracuje v síťové vrstvě modelu TCP/IP. Přenáší tzv. IP-datagramy mezi vzdálenými počítači. Každý IP-datagram ve svém záhlaví nese adresu příjemce, což je úplná směrovací informace pro dopravu IP-datagramu k adresátovi. Takže síť může přenášet každý IP-datagram samostatně. IP-datagramy tak mohou k adresátovi dorazit v jiném pořadí, než byly odeslány.

Protokol IP je nespojový (před zahájením výměny dat nevytváří relaci) a „nespolehlivý" (předání paketů na místo určení není kontrolováno). Paket IP se tedy může ztratit, být doručen mimo pořadí, být zdvojen nebo zpožděn. Protokol IP neobsahuje prostředky pro zotavení z chyb tohoto typu. To vše musí zajistit nadřízená transportní vrstva – **protokol TCP**. (11)

11.3.2 Transmission Control Protocol

Protokol TCP a stejně tak protokol UDP odpovídají transportní vrstvě. Od aplikační vrstvy (prostřednictvím některého protokolu) přebere data, která rozdělí na **segmenty,** očísluje a seřadí podle toho, jak mají být postupně odeslány. **Před zahájením výměny dat zahájí relaci s transportní**

[12] Zdroj: http://dc352.4shared.com/doc/FrJCwiK-/preview.html

vrstvou protějšího počítače. Poté začne s vysíláním a potvrzováním jednotlivých datových segmentů. Vlastní odeslání už má na starosti IP protokol. (11)(12)

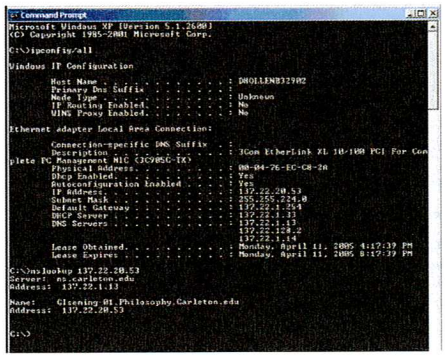
11.3.3 User Datagram Protocol

Protokol UDP má v podstatě stejnou úlohu jako TCP. Ovšem na rozdíl od TCP nevytváří před přenosem dat relaci a je tedy nespojový. To znamená, že ani nekontroluje, zda byly diagramy cílem vysílání přijaty. Protokol UDP je jednodušší, ale méně spolehlivý. Některé aplikace jej ale využívají pro rychlý a nenáročný přenos dat (např. stream media). (11)

11.3.4 Informace o nastavení protokolu TCP/IP

Pro zjištění základních informací o nastavení TCP/IP je ve Windows k dispozici příkaz IPCONFIG.

- Vyvoláme konzolu příkazového řádku (Win+ R) a v okně Spustit napíšeme zkratku cmd.
- Do příkazového řádku napíšeme příkaz ipconfig /all



Příkaz IPCONFIG

12 IP adresace

IP adresa verze 4 IPv4 je tvořena čtyřmi bajty. IP adresa se zapisuje notací, kde jednotlivé bajty se mezi sebou oddělují tečkou.

Rozeznáváme:

Dvojkovou notaci, kde jednotlivé bity každého bajtu se vyjádří jako dvojkové číslo, např.: 10101010.01010101.11111111.11111000

Desítkovou notaci - čtyři osmiciferná dvojková čísla se převedou do desítkové soustavy, tj. pro náš příklad: 170.85.255.248

Šestnáctkovou notaci - jednotlivé bajty IP adresy se vyjádří šestnáctkově (hexadecimálně), tj. naš příklad: aa.55.ff.f8

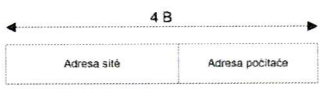
IP adresa se skládá ze dvou částí:

1. Adresy (lokální) sítě.
2. Adresy počítače (resp. uzlu) v (lokální) síti.

Problém je v tom jak zjistit, která část IP adresy je adresou sítě a která adresou počítače. Není ani zcela jasné co to znamená slovo síť, protože jeho význam se postupně měnil a kromě slova síť se zavedly pojmy subsíť a supersíť. (13)

12.1 Síť – první období

Toto období probíhalo od počátku Internetu až do roku 1993. V této epoše bylo slovo síť specifikováno normou RFC-796. Těchto dvanáct let je poznamenáno představou, že čtyři bajty na IP adresy musí stačit. (13)



Struktura IP adresy [13]

IP adresa se dělí na **adresu sítě** a **adresu uzlu** v rámci této sítě. Kolik bajtů z IP adresy tvoří adresu sítě určují počáteční bity prvního bajtu IP adresy. IP adresy se dělí do pěti tříd (nicméně dnes už se tím v podstatě neřídíme):

Třída A: používá první oktet adresy pro identifikaci sítě a zbývající tři oktety pro identifikaci rozhraní. **V třídě A máme 126 sítí** (0 a 127 mají zvláštní význam. V každé síti je 2^{24}-2 adres pro počítače (adresy tvořené samými nulami a samými jedničkami mají zvláštní význam).

[13] Zdroj: http://zam.opf.slu.cz/botlik/CD-0x/6.html

Třída B: používá první dva oktety adresy pro identifikaci sítě a zbývající dva oktety pro identifikaci rozhraní. Můžeme tedy mít celkem 2^{14} sítí a v každé síti 2^{16}-2 počítačů. Tyto adresy jsou již rozděleny většinou mezi národní a nadnárodní ISP providery.

Třída C: používá první tři oktety pro adresy pro identifikaci sítě a zbývající oktet pro identifikaci rozhraní. Adresy třídy C tak poskytují minimální prostor pro adresování stanic v síti (jen 254).

Třída D: zatímco třídy A-C adres sloužily k adresaci jednotlivých uzlů a sítí, třída D slouží pro adresaci skupinovou. Mezi speciální skupinové adresy patří:

- 224.0.0.1 – skupina všech stanic připojených k lokální podsíti,
- 224.0.0.2 – skupina všech směrovačů připojených k lokální podsíti.

Třída E: třída nejmenšího rozsahu adres sloužící jen pro experimentální účely. (10)

	Struktura adresy (S = síť, U = uzel)	Platné hodnoty prvního oktetu desítkově	Počet adres sítí v třídě	Počet stanic adresovatelných v rámci sítě
Třída A	S.U.U.U	1-126	126	2^{24} - 2
Třída B	S.S.U.U	128-191	2^{14}	2^{16} - 2
Třída C	S.S.S.U	192-223	2^{21}	254
Třída D	Skupinová	224-239	-	-
Třída E	experimentální	240-255	-	-

Všechny platné adresy v rámci jedné sítě (A – C) neoznačují stanice. Dvě adresy jsou rezervovány pro:

- Adresu sítě.
- Všeobecnou adresu v síti (**broadcast**) – (např. adresa 10.255.255.255 je broadcast pro síť 10.0.0.0, tj. všechny stanice připojené k této síti jsou touto adresou specifikovány.

12.1.1 Síťová maska

Síťová maska se používá pro určení adresy sítě. Adresa sítě je jak víme částí IP adresy. Síťová maska určuje, které bity v IP adrese tvoří adresu sítě. **Síťová maska je opět čtyřbajtové číslo.** Toto číslo vyjádřené v dvojkové soustavě má v bitech určujících adresu sítě jedničky a v ostatních bitech nuly.

Princip síťové masky se dobře pochopí, používáme-li dvojkovou notaci.

Jednotlivé třídy sítí používají jako adresu sítě různě dlouhou část IP adresy. Třída A používá pro adresu sítě první bajt. Čili standardní síťová maska pro adresy třídy A má v prvním bajtu samé jedničky a ve zbylých třech bajtech samé nuly (13):

11111111.00000000.00000000.00000000

což vyjádřeno v desítkové soustavě je:

255.0.0.0 (šestnáctkově ff.00.00.00)

Obdobně standardní síťová maska pro třídu B je desítkově:

255.255.0.0 (šestnáctkově ff.ff.00.00)

Konečně pro třídu C:

255.255.255.0 (šestnáctkově ff.ff.ff.00).

Síťové masky odpovídající třídám A, B a C se nazývají standardní síťové masky.

Síťová maska slouží k řešení úlohy: Jak určit adresu sítě, na které leží počítač o IP adrese:

170.85.255.248, tj. dvojkově 10101010.01010101.11111111.11111000

Řešení je jednoduché: Nejprve se podíváme do tabulky tříd IP adres a zjistíme, že naše adresa je třídy B. Používáme-li standardní síťovou masku, pak maska pro třídu B je:

11111111.11111111.00000000.00000000

Vynásobíme-li nyní IP adresu bit po bitu se síťovou maskou, pak získáme adresu sítě:

10101010.01010101.11111111.11111000

x 11111111.11111111.00000000.00000000

10101010.01010101.00000000.00000000

Výsledek převedeme do desítkové soustavy a zjistíme, že počítač leží na síti 170.85.0.0.

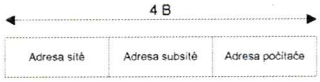
Tato metoda určení adresy sítě se může zdát až příliš komplikovanou v případě, že se používají standardní síťové masky. Může se zdát, že síťová maska je důležitá tak pro tvůrce operačního systému, nikoliv však pro správce. Význam síťové masky doceníme v následujícím historickém období. (13)

12.2 Síť – druhé období

V roce 1993 vyšly normy RFC-1517 až 1520. Tyto dnes již málo citované normy od základu změnily pohled na slovo síť, jak je chápáno v Internetu. **Přestalo se na sítě hledět přes třídy, ale výhradně přes síťové masky.** (13)

Ono to sice úplně nejde abstrahovat od sítí, takže v podstatě dělení IP adresy na adresu sítě a adresu počítače zůstalo, pouze část IP adresy dříve odpovídající adrese počítače se rozdělila na dvě části:

na dresu **subsítě** a adresu počítače.



Struktura IP-adresy [14]

Z hlediska síťové masky je adresa sítě i subsítě jeden celek. Ta část IP-adresy, kde jsou v masce jedničky je prostě síť. Jenže nyní dochází k nejednoznačnosti v terminologii. Jednou slovo síť označuje ve smyslu třídy (A, B, nebo C) a podruhé je sítí myšleno obecně část IP adresy, kde v odpovídající masce jsou jedničky. Pokud na čas zapomeneme na třídy a budeme používat libovolné masky, pak už nestačí mluvit o síti např. 192.168.0.0, ale vždy k ní musíme dopsat masku, abychom vyjádřili, co touto sítí míníme. Pokud bychom uvažovali třídně, pak se pro tuto síť použije vždy maska 255.255.255.0, protože se jedná o síť třídy C. Maska 255.255.255.0 pro síť 192.168.0.0 se nazývá standardní síťovou maskou.

Kromě subsítí se používají i **supersítě**, u kterých je počet jedniček masky menší než u standardní síťové masky.

Jako příklad je uvedeno dělení sítě 192.168.0.0 na subsítě s různými maskami (standardní maska je zobrazena tučně).

Příklad dělení sítě 192.168.0.0 na subsítě (13):

Maska	Počet jedniček v masce (zleva)	Síť je tvořena intervalem IP adres	Zkrácený zápis sítě (včetně masky)
255.248.0.0	13	192.168.0.0 až 192.175.255.255	192.168.0.0/13
255.252.0.0	14	192.168.0.0 až 192.171.255.255	192.168.0.0/14
255.254.0.0	15	192.168.0.0 až 192.169.255.255	192.168.0.0/15
255.255.0.0	16	192.168.0.0 až 192.168.255.255	192.168.0.0/16
255.255.255.0	**24**	**192.168.0.0 až 192.168.0.255**	**192.168.0.0/24**
255.255.255.252	30	192.168.0.0 až 192.168.0.3	192.168.0.0/30

[14] Zdroj: http://zam.opf.slu.cz/botlik/CD-0x/6.html

255.255.255.254	31	192.168.0.0 až 192.168.0.1 Pozor, takováto síť je nesmysl, protože má jen dvě IP-adresy, tedy adresu sítě samotné a adresu oběžníku, nedostávají se už adresy pro počítače na této síti.	192.168.0.0/31
255.255.255.255	32	Adresa samostatného počítače (host address) 192.168.0.0	192.168.0.0/32

Jelikož dvojkové vyjádření síťové masky je tvořeno zleva souvislou řadou jedniček, tak se místo vyjádření "síť 192.168.0.0 s maskou 255.255.255.252" častěji zkrácen na 192.168.0.0/30, kde číslo 30 vyjadřuje počet jedniček masky.

12.2.1 Vyhrazené adresy

Nejnižší adresa v síti (s nulovou adresou stanice) slouží jako označení celé sítě (např. „síť 192.168.24.0"), nejvyšší adresa v síti (adresa stanice obsahuje samé binární jedničky) slouží jako adresa pro všesměrové vysílání (broadcast), takové adresy tedy nelze použít pro normální účely.

Adresy 127.x.x.x (tzv. *localhost*, nejčastěji se používá adresa 127.0.0.1) jsou rezervovány pro tzv. loopback, logickou smyčku umožňující posílat pakety sám sobě.

Dále jsou vyčleněny rozsahy tzv. interních (**neveřejných**) IP adres (tzv. *privátní IP adresy*), které se používají pouze pro adresování vnitřních sítí (např. lokálních), na Internetu se nikdy nemohou objevit. Jako neveřejné jsou určeny adresy:

- **ve třídě A:** 10.0.0.0 až 10.255.255.255 (celkem 1krát 16 777 216 adres; tj. 16 777 216 adres, z nichž je použitelných jen 16 777 214)
- **ve třídě B:** 172.16.0.0 až 172.31.255.255 (celkem 16krát 65 536 adres; tj. 1 048 576 adres, z nichž je použitelných jen 1 048 544)
- **ve třídě C:** 192.168.0.0 až 192.168.255.255 (celkem 256krát 256 adres; tj. 65 536 adres, z nichž je použitelných jen 65 024)

12.2.2 IPv6

IPv6 je internetový protokol nové generace. Tento protokol má za svůj cíl v budoucnu nahradit protokol IPv4, který je dnes používán pro drtivou většinu aplikací na internetu.

Protokol IPv6 by natrvalo vyřešil problém adresového prostoru IP, protože jeho adresový prostor je prakticky nevyčerpatelný. IPv6 adresový prostor obsahuje celkem 2^{128} adres. Protokol IPv4 definuje adresový prostor pouze pro 2^{32} adres. A to je pro dnešní potřeby rozvoje komunikační dálnice velmi málo. Velká část z tohoto omezeného adresového prostoru je navíc vyhrazena pro speciální účely (například jako neveřejné adresy) a tím se volný počet IPv4 adres ještě snižuje.

Předpoklady přesného data vyčerpání adres protokolu IPv4 se sice posouvají stále do budoucnosti, ale je téměř jisté, že konec je neodvratný. Záchranou pro protokol IPv4 bylo zavedení a všeobecné

rozšíření techniky překladu adres označované zkratkou **NAT (Network Address Translation)**. Tato technika umožňuje skrýt i velmi rozsáhlou infrastrukturu s mnoha počítači za jednu společnou veřejnou IPv4 adresu. Nebylo již nutné žádat pro každý počítač nebo zařízení o přidělení samostatné veřejné IPv4 adresy.

NAT se stal brzy velmi populárním nástrojem pro připojování lokálních sítí (LAN) k internetu. Problémem překladu adres je však určité omezení využitelných služeb a komplikace při provozu některých typů aplikací. Typickým příkladem takto problémových služeb jsou protokoly pro tvorbu **VPN** (Virtual Private Network), **FTP** (File Transfer Protokol) nebo **VoIP** (Voice over IP). Postupem času bylo vyvinuto mnoho způsobů jak tato omezení obcházet a udržet použitelnou funkčnost aplikací i v tomto „nehostinném" prostředí. Určitým vykoupením je zvýšení pocitu bezpečí v síti připojené k internetu pomocí překladu adres. Počítače takové sítě totiž nemohou být přímo dostupné z internetu. Tento fakt klade menší nároky na konfiguraci a údržbu **firewallů**. Bezpečnost se stala jedním z nejdůležitějších argumentů ospravedlňujících použití techniky NAT. (10)(12)

Tvar IPv6 adresy

Adresy protokolu IPv4 jsou zapisovány obvykle jako čtveřice osmibitových čísel oddělených tečkami. IPv4 adresa může být například: **185.28.36.213**

Adresy protokolu IPv6 mají podstatně delší a komplikovanější zápis. IPv6 adresy se zapisují jako osm skupin čtyř hexadecimálních čísel oddělených dvojtečkami. Zápis adresy IPv6 může vypadat například takto: **2001:5c01:1507:9b00:2173:31ff:fe65:7b04**

13 Serverové služby nezbytné pro chod sítě

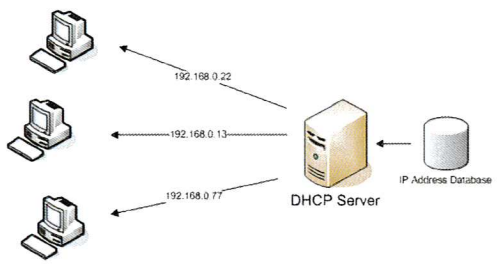
V této kapitole se podíváme na dvě základní služby DHCP a DNS. Obě jsou součástí sítí typu klient / server a jsou pro její činnost nezbytné.

13.1 DHCP

DHCP (Dynamic Host Configuration Protocol) je název protokolu z rodiny TCP/IP nebo označení odpovídajícího DHCP serveru či klienta. Používá se pro automatickou konfiguraci počítačů připojených do počítačové sítě. DHCP server přiděluje počítačům pomocí DHCP protokolu zejména IP adresu, masku sítě, bránu a adresu DNS serveru. Platnost přidělených údajů je omezená, proto je na počítači spuštěn DHCP klient, který jejich platnost prodlužuje.

13.1.1 Princip činnosti

Klienti žádají server o IP adresu, ten u každého klienta eviduje půjčenou IP adresu a čas, do kdy ji klient smí používat (*doba zapůjčení*, anglicky *lease time*). Poté co vyprší, smí server adresu přidělovat jiným klientům.



DHCP Server [15]

13.1.2 Možnosti přidělení IP adresy

IP adresa může být stanici přidělena několika způsoby:

Ruční nastavení

[15] Zdroj: http://www.windowsdevcenter.com/pub/a/windows/2007/06/12/implementing-and-understanding-dhcp.html

V tomto případě správce sítě nevyužívá DHCP serveru a konfiguraci jednotlivých stanic zapisuje jednotlivě přímo do konfigurace jednotlivých stanic.

Statická alokace

DHCP server obsahuje seznam MAC adres a k nim příslušným IP adres. Pokud je žádající stanice v seznamu, dostane vždy přidělenu stejnou pevně definovanou IP adresu.

Dynamická alokace

Správce sítě na DHCP serveru vymezí rozsah adres, které budou přidělovány stanicím, které nejsou registrovány. Časové omezení pronájmu IP adresy dovoluje DHCP serveru již nepoužívané adresy přidělovat jiným stanicím. Registrace dříve pronajatých IP adres umožňuje DHCP serveru při příštím pronájmu přidělit stejnou IP adresu.

V IPv6 sítích je automatickému nastavení stanice věnována vyšší pozornost, aby byla konfigurace počítačové sítě ještě jednodušší.

13.2 DNS

DNS (Domain Name System) je hierarchický systém doménových jmen, který je realizován servery DNS a protokolem stejného jména, kterým si vyměňují informace. Jeho hlavním úkolem a příčinou vzniku jsou vzájemné převody doménových jmen a IP adres uzlů sítě. Později ale přibral další funkce (např. pro elektronickou poštu či IP telefonii) a slouží dnes de facto jako distribuovaná databáze síťových informací.

Servery DNS jsou organizovány hierarchicky, stejně jako jsou hierarchicky tvořeny názvy domén. Jména domén umožňují lepší orientaci lidem, adresy pro stroje jsou však vyjádřeny pomocí adres 32bitových (IPv4) nebo 128bitových (IPv6). Systém DNS umožňuje efektivně udržovat decentralizované databáze doménových jmen a jejich překlad na IP adresy. Stejně tak zajišťuje zpětný překlad IP adresy na doménové jméno - PTR záznam.

Prostor doménových jmen tvoří strom s jedním kořenem. Každý uzel tohoto stromu obsahuje informace o části jména (doméně), které je mu přiděleno a odkazy na své podřízené domény. Kořenem stromu je tzv. kořenová doména, která se zapisuje jako samotná tečka. Pod ni se v hierarchii nacházejí tzv. *domény nejvyšší úrovně (Top-Level Domain, TLD)*. Ty jsou buď tematické (*com* pro komerci, *edu* pro vzdělávací instituce atd.) nebo státní (*cz* pro Českou republiku). (11)

Strom lze administrativně rozdělit do zón, které spravují jednotliví správci (organizace nebo i soukromé osoby), přičemž taková zóna obsahuje autoritativní informace o spravovaných doménách. Tyto informace jsou poskytovány autoritativním DNS serverem.

Výhoda tohoto uspořádání spočívá v možnosti zónu rozdělit a správu její části svěřit někomu dalšímu. Nově vzniklá zóna se tak stane autoritativní pro přidělený jmenný prostor. Právě možnost delegování pravomocí a distribuovaná správa tvoří klíčové vlastnosti DNS a jsou velmi podstatné pro jeho úspěch. Ve vyšších patrech doménové hierarchie platí, že zóna typicky obsahuje jednu doménu. Koncové zóny přidělené organizacím připojeným k Internetu pak někdy obsahují několik domén –

například doména *kdesi.cz* a její poddomény *vyroba.kdesi.cz*, *marketing.kdesi.cz* a *obchod.kdesi.cz* mohou být obsaženy v jedné zóně a obhospodařovány stejným serverem.

DNS Servery

DNS server může hrát vůči doméně (přesněji zóně, ale ve většině případů jsou tyto pojmy zaměnitelné) jednu ze tří rolí:

- ✓ **Primární server** je ten, na němž data vznikají. Pokud je třeba provést v doméně změnu, musí se editovat data na jejím primárním serveru. Každá doména má právě jeden primární server.
- ✓ **Sekundární server** je automatickou kopií primárního. Průběžně si aktualizuje data a slouží jednak jako záloha pro případ výpadku primárního serveru, jednak pro rozkládání zátěže u frekventovaných domén. Každá doména musí mít alespoň jeden sekundární server.
- ✓ **Pomocný (caching only) server** slouží jako vyrovnávací paměť pro snížení zátěže celého systému. Uchovává si odpovědi a poskytuje je při opakování dotazů, dokud nevyprší jejich životnost.

Odpověď pocházející přímo od primárního či sekundárního serveru je autoritativní, čili je brána za správnou. Z hlediska věrohodnosti odpovědi není mezi primárním a sekundárním serverem rozdíl, oba jsou autoritativní. Naproti tomu odpověď poskytnutá z vyrovnávací paměti není autoritativní. Klient může požádat o autoritativní odpověď, v běžných případech ale stačí jakákoli. (11)

14 Bezdrátové sítě Wi-Fi

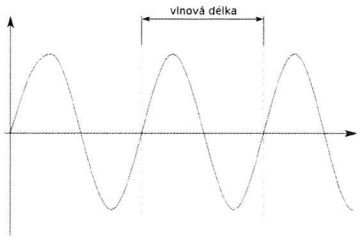
Wi-Fi – způsob komunikace mezi bezdrátovými zařízeními na základě určitého standardu (protokolu). Tato pravidla určuje organizace IEEE (Instititut of Electrical and Electronics Engineers).

WLAN – Tato zkratka ***Wireless Local Area Network*** označuje obecně jakoukoliv bezdrátovou síť a je vlastně ekvivalentní zkratce LAN. Jakákoliv bezdrátová síť kde figurují počítače se tedy odborně nazývá WLAN.

Obr. *Certifikováno WiFi Aliancí (WECA)*

14.1 Bezdrátová spektra

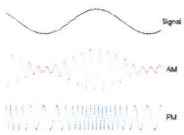
Signál se přenáší elektromagnetickým vlněním (vzduchem, vakuem), které vlastně nahrazuje metalické kabely. **Elmag. vlny** se liší vlnovou délkou (a frekvencí). Chceme-li od sebe odlišit jednotlivé přenosové linky, musíme pro každou z nich použít jinou frekvenci. (15)



Rádiové vysílání probíhá na určité základní frekvenci, které se říká nosná. Nosné frekvence jsou rozděleny do pásem. Jednotlivá pásma slouží konkrétním službám, např. rádiu a televizi. Vysílání v některých pásmech vyžaduje licenci, která může být udělena pro konkrétní frekvenci, nebo může pokrývat celé pásmo.

Wi-Fi využívá část volného spektra nelicencované frekvence **2,4 GHz** a frekvence **5 GHz**, které je ale určitým způsobem regulována pravidly. U nás se o tyto pravidla stará Český telekomunikační úřad.

Stejně jako u známých rádiových standardů AM a FM funguje přenos signálu přidáním (modulací) informací k šířícím se vlnám. **U různých standardů Wi-Fi existují různé typy modulace.**



Prohlédněte si tabulku pod odkazem pro rádiové vlny:

http://cs.wikipedia.org/wiki/Rádiové_vlny

Úkol: Do jakého frekvenčního pásma spadají frekvence 2,4 GHz a 5 GHz?

14.2 Přímá viditelnost

Jedním z nejdůležitějších aspektů při práci s bezdrátovými sítěmi je to, že přenos signálu by měl být realizován vzdušnou čarou, pokud možno **bez jakýchkoliv překážek**. Ideální je, když je jeden uzel sítě z druhého vidět – pak už výkon sítě závisí jen na výkonu vysílače.

Nejhorší jsou pevné překážky (zvlášť ty vodivé). Vzduch, sklo problémy nečiní. Ocel a další kovy ano – všechno ostatní je někde na pomezí. Hodně materiálů se na signálu podepíše *útlumem*. Sádrokarton a omítka tlumí středně, beton tvárnice hodně.

14.3 Antény

Antény zachycují elektromagnetické vlnění a jeho energii přeměňují na elektrický signál o téže frekvenci. Všechny informace které jsou v původním elektromagnetickém vlnění uložené, se tak zachovají pro nemodulační obvody přijímače. U bezdrátových sítí se pracuje s velice slabými signály, a tak musí být antény co nejúčinnější.

Antény mohou být **směrové** nebo **všesměrové**.

Směrové antény – slouží k propojení dvou bodů na delší vzdálenosti, jelikož září jen do jednoho bodu. Používají se dva typy: parabolické, které mají drátěné síto a ozařovač uprostřed, a tzv. antény **Yagi**.

Všesměrové antény – vysílají do všech stran, tzn., že pokryjí úhel 360°. Běžně se dodávají ke všem Wi-Fi výrobkům. Například přístupový bod připojuje klienty ze všech směrů nebo síť ad-hoc propojuje vzájemně počítače po celém bytě ze všech směrů. Jejich zisk je ovšem značně nižší.

Speciálním typem antén jsou antény **sektorové**.

Pokryjí jen určitý úhel od 30° do 180°. Jejich použití je vhodné tam, kde stačí pokrýt jen omezené území – například do rohu místnosti postačí anténa s 90° pokrytím. Můžete též s jejich pomocí zamezit šíření signálu (a potažmo možnosti přístupu do sítě) mimo žádané území.

Základní parametry antén

- Zisk
- Vyzařovací úhly
- Polarizace - udává rovinu, ve které se šíří rádiové vlny. Pro optimální spojení musí být na obou stranách antény se stejnou polarizací. V opačném případě dochází k velikým ztrátám a potlačení zisku antén až o 16–24 dB, což v důsledku znemožní přenos dat.

14.4 Standardy Wi-Fi

Standard bezdrátového Ethernetu **IEEE 802.11** definuje způsob komunikace zařízení po rádiových vlnách v rozptýleném spektru (DSSS, OFDM). Při tomto vysílání se data pohybují v malých, diskrétních blocích po různých frekvencích z jistého intervalu.

14.4.1 IEEE 802.11b

Standard nahrazovaný IEEE 802.11g a 802.11n.

- používá spektrum (frekvenci) 2,4 GHz
- maximální teoretická propustnost čili rychlost je 11Mbs
- zabezpečení: SSID, MAC filtr, šifrování WEP, WPA, WPA2
- kompatibilita: 802.11b
- režim komunikace: nahodilý, infrastruktura
- modulace: CCK/DSSS

14.4.2 IEEE 802.11g

Standard v pásmu 2,4 GHz.

- používá spektrum (frekvenci) 2,4 GHz
- maximální teoretická propustnost čili rychlost je 54Mbs
- zabezpečení: SSID, MAC filtr, šifrování WEP, WPA, WPA2
- kompatibilita: 802.11b, 802.11g
- režim komunikace: nahodilý, infrastruktura
- modulace: CCK/DSSS i CCK/OFDM

14.4.3 IEEE 802.11a

- používá spektrum (frekvenci) 5 GHz
- maximální teoretická propustnost čili rychlost je 54Mbs běžně 20Mbs
- zabezpečení: SSID, MAC filtr, šifrování WEP, WPA, WPA2
- kompatibilita: 802.11a
- režim komunikace: nahodilý, infrastruktura
- modulace: OFDM

14.4.4 IEEE 802.11n

Standard, který umožňuje dosahovat až rychlosti 600Mbs, obecně rychlosti vyšší než 100Mbs a to jak na frekvenci 2,4 GHz, tak i ve spektru 5 GHz. Využívá techniku modulace MIMO.

14.4.5 Další standardy

802.11e - rozšíření MAC pro **QoS** - Zkratka QoS označuje službu Quality of Service zajišťující vyrovnanou kvalitu služby důležitou například pro multimédia. Zjednodušeně řečeno je potřeba, aby když někdo v bezdrátové síti telefonuje nebo pořádá videokonferenci, aby trvalý tok jeho dat měl přednost před lidmi, kteří například jen stahují poštu a chvilkový výpadek naprosto nepoznají,

zatímco v hlasu nebo videu by byl hodně poznat. Toto upřednostnění určitých dat v bezdrátové síti přináší vrstva MAC, Medium Access Layer. Ta upřednostní hlasové a videopřenosy.

802.11i - zlepšení bezpečnosti v 802.11 bezdrátových sítích vylepšením autentifikačního a šifrovacího algoritmu.

14.5 Spektrum – Frekvenční pásmo

Evropa

2,4 GHz: 2,412 – 2,4872**Počet kanálů:** 1-13

Kanál	Frekvence v GHz
1	2,412
2	2,417
3	2,422
4	2,427
5	2,432
6	2,437
7	2,442
8	2,447
9	2,452
10	2,457
11	2,462
12	2,467
13	2,472
14	2,484

Česká republika (přidržujíc se konvence ETSI) má k dispozici v Evropě největší počet povolených kanálů. Jenže ani 13 není nijak moc. Bohužel to neznamená, že je k dispozici 13 plnohodnotných frekvenci, neboť technologie rozprostřeného spektra znamená, vysílání do frekvenčního rozsahu ***22 MHz***. Jenže odstup mezi kanály je pouze ***5 MHz***, tedy vysílání na jednom kanálu se překrývá s vysíláním na sousedních čtyřech kanálech. (14)(15)

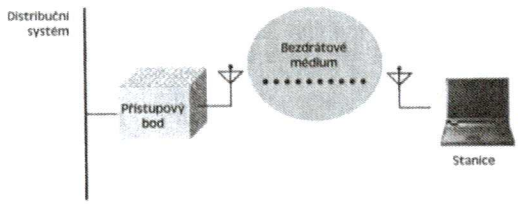
14.5.1 Princip funkce

Datový paket v bezdrátových sítích se skládá z 2 částí: **informační** a **datové** části. První část slouží jako upozornění celé síti, že bude následovat přenos dat pro nějakého účastníka sítě (preambule). Poté je zaslána hlavička, která příjemci sděluje, jak velká jsou přenášená data, a nakonec se přenesou data jako druhá část paketu.

Aby se více zařízení nerušilo, při odeslání preambule ví ostatní zařízení, že se budouci posílat nějaká data. Počkají si na sdělení, jak dlouho to bude trvat a poté budou opět komunikovat. To je základem přístupové metody **RTS/CTS**.

CCK – Obě části, informační a datová jsou modulovány pouze na jeden nosič. Což je nejjednodušší, ale zároveň nejpomalejší mechanismus.

14.6 Komponenty sítě Wi-Fi



Distribuční systém - v okamžiku, kdy má více přístupových bodů tvořit rozsáhlejší síť, musí spolu komunikovat a předávat si informace o pohybu mobilních stanic. Distribuční systém je logická komponenta standardu 802.11 používaná k přesměrování datového toku na stanici skutečného určení podle její aktuální polohy v síti. V naprosté většině komerčních systémů je distribuční systém řešen jako kombinace síťového mostu (bridge) a distribučního média, jímž je páteřní síť používána pro přenášení dat mezi přístupovými body. Téměř vždy je touto páteřní sítí Ethernet.

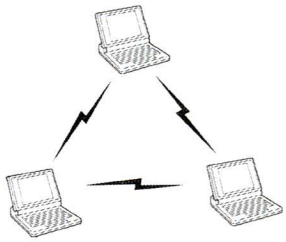
Přístupový bod (Access Point) představuje právě ono přemostění mezi kabelovou a bezdrátovou sítí, a ačkoliv přístupový bod poskytuje i celou řadu dalších funkcí, funkce *mostu* mezi bezdrátovou a kabelovou částí sítě je nejdůležitější.

Bezdrátové médium je pro sítě WLAN tímtéž, co kabeláž pro sítě kabelové - bezdrátové médium je nosičem dat při přesunu dat od stanice ke stanici. Mohli bychom říci, že tím médiem je vzduch, což je ovšem nesmysl (ostatně sítě WLAN fungují i ve vzduchoprázdnu). Bezdrátovým médiem rozumí 802.11 dvě radiové frekvence (2,4 a 5 GHz) a málo využívanou infračervenou fyzickou vrstvu.

Stanice - bezdrátové sítě se staví proto, aby bylo možné přenášet data mezi jednotlivými stanicemi. Stanicí může být obecně jakékoliv zařízení: počítač, notebook, tablet, mobil. Nikde není řečeno, že stanice v bezdrátové síti musí být mobilní a je mnoho sítí WLAN, které propojují počítače prakticky nepřenášené z místa například z důvodu nemožnosti instalace kabelového Ethernetu, z důvodu vytvoření dočasných sítí apod. V takových sítích pak odpadají některé problémy, kupříkladu se nemusí řešit problém mobility jednotlivých stanic.

14.7 Režim činnosti bezdrátové sítě

14.7.1 Nahodilý režim (Ad-Hoc)



Ad-hoc [17]

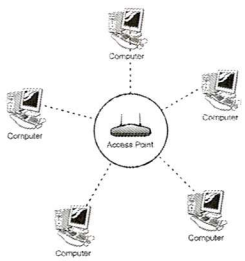
Nahodilý režim spočívá v komunikaci počítačů v režimu peer-to-peer. Idealní jsou pro malé nebo dočasně vytvářené sítě, např. v učebně či školní třídě.

[16] Zdroj: http://www.mgzps.estranky.cz/fotoalbum/schemy-zapojenia/wlan-schema.html
[17] Zdroj: http://engineersworld.wordpress.com/2011/07/11/how-to-transfer-data-through-a-adhoc-network/

Podstatnou výhodou je rychlá instalace. Umožňuje sdílení souborů a Internetu, tisk přes síť.

Nevýhodou je fakt, že všechna zařízení musí být v dosahu – každý musí vidět každého.

14.7.2 Režim infrastruktury



Režim infrastruktury [18]

Do bezdrátové sítě v režimu infrastruktury jsou jednotlivé uzly zapojeny přes bezdrátový **přístupový bod (AP)**, jenž tvoří také most do pevné části sítě.

Režim infrastruktury je vhodný pro firemní sítě a pro takové sítě, v nichž je potřeba sdílet specializované prostředky, jako je připojení k internetu a centralizované databáze.

14.8 Přístupový bod (AP)

Je základem bezdrátové sítě v režimu infrastruktury. Přístupový bod obsahuje rádiovou část – vysílač/přijímač a část kabelovou – zdířky RJ-45 pro připojení kroucené dvojlinky.

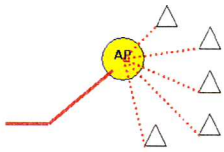
Zařízení může poskytovat vlastní **DHCP** server, možnost **NAT** (překladač veřejných IP na soukromé a opačně), předávání portů do vnitřní sítě (tzv. port forwarding), autentizace klientů proti RADIUS serveru, různé úrovně šifrování (viz níže) a podobně. Některé chybějící vlastnosti lze nahradit vhodně umístěným doplňujícím počítačem nebo dalším jednoúčelovým zařízením (router). AP router může fungovat také jako klient WISP.

Některé přístupové body je možno nakonfigurovat do režimu bezdrátových mostů:

- jednoduchý převod ethernetu na bezdrátové spojení,
- vyhrazený bezdrátový most (opakovač),

[18] http://etutorials.org/shared/images/tutorials/tutorial_112/15fig12.gif

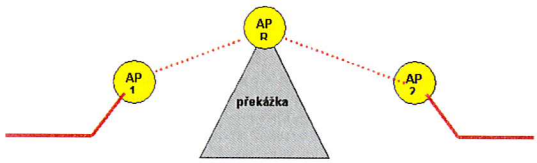
- kombinace bezdrátového mostu a přístupového bodu.



Režim AP – přístupový bod
Je základní režim ve kterém se přes AP připojují klientská zařízení (koncové stanice). AP obvykle slouží jako brána (gateway) do internetu.

Režim Opakovač
V tomto režimu funguje zařízení jako bezdrátový most. Je třeba nastavit MAC adresu proti zařízení, se kterými se bude komunikovat.

V tomto nastavení se mohou spojit jen dva určené přístupové body. Na zařízení AP1 je třeba nastavit (povolit) MAC adresu protějšího zařízení AP2 a naopak u AP2 je třeba nastavit MAC AP1. V režimu opakovač se nelze k AP1 ani AP2 připojit přes klientské zařízení.



V tomto případě je mezi AP1 a AP2 překážka, která brání spojení obou bodů. Do vhodného místa přidáme zařízení AP R. Na AP1 je nastavena MAC adresa AP R, na AP 2 je taktéž nastavena MAC adresa AP R. Na AP R jsou nastaveny dvě MAC adresy – AP1 a AP2. Opět – v tomto režimu se nelze k AP1, AP2 ani AP R připojit přes klientské zařízení.

Režim AP + Opakovač

V tomto režimu funguje zařízení zároveň jako bezdrátový most – bridge a zároveň se na něj mohou připojit i bezdrátoví klienti. Této funkce je možné použít v případě potřeby vykrytí určitého hluchého území.

AP1 je nastaveno do režimu bridge – a je na něm nastavena MAC zařízení AP2. AP2 je v režimu AP + Opakovač, a je nastaven MAC adresa zařízení AP1. V tomto nastavení se mohu klienti připojit k AP2, ale AP1 je pouze jako bezdrátový most.

14.8.1 Firewall

Mnoho výrobců integruje přímo do svých routerů (AP) firewall nebo funkce, které jsou firewallu podobné. Například možnost filtrovaní obsahu www serverů na základě databáze zvolených klíčových slov – podobná fce proxy serveru.

14.8.2 Co tedy dnes AP umí?

Překlad adres (NAT) a zabezpečení privátní sítě

Hlavním bezpečnostním prvkem většiny routerů je vnitřní překlad adres privátní sítě na jednu veřejnou adresu poskytnutou ISP. Tento překlad je po prvním zapojení zkonfigurován jako jednosměrný. Je tedy možné přistupovat z privátní sítě k internetu, ale opačně to „nelze" (viz. PORT Forwarding).

Pro většinu uživatelů je tato konfigurace naprosto dostatečná a nikdy nezatouží po změně. Je dobré ale zjistit jak široce lze vnitřní překlad adres konfigurovat. K základu by mělo patřit otevření libovolných portů pro provoz směrem do privátní sítě pro TCP a UDP protokol. Pokud chcete mít ve vnitřní síti VPN PPTP server (tedy třeba VPN server na MS Windows XP nebo 2003), tak je pro vás důležité aby váš router uměl do privátní sítě přeložit i libovolný jiný IP protokol (pro PPTP konkrétně IP protokol 47).

V tomto kontextu je hodně diskutovaná i UPNP funkcionalita u routerů. Jde o metodu, pomocí níž si sama aplikace běžící na počítači v privátní síti dokáže otevřít požadovaný port na routeru pro příchozí provoz. Na platformě MS Windows lze pozorovat pomalý nárůst popularity této služby, takže pokud ji váš router bude disponovat, není to od věci.

DHCP server

Automatické přidělování IP adres počítačům v privátní síti je opět základní vlastností téměř všech routerů. Přesto se v implementaci této funkce najdou velké rozdíly. Informujte se, zda vámi vybraný zařízení disponuje tzv. předrezervací. Tedy možností přidělit určité MAC adrese v privátní síti předem

vybranou IP adresu. Zamezí se tak změnám IP adres u méně často používaných počítačů v privátní síti.

Druhou zajímavou funkcí je možnost omezit rozsah (pool) IP adres, které router používá pro rozdělování. I tato funkce umožní přidělit některým počítačům v privátní síti statické IP adresy bez rizika, že dojde ke konfliktu s těmi automaticky přidělenými.

Tiskový server

Dostáváme se k vlastnostem, kterými zdaleka nedisponují všechny routery. Připojení tiskárny k jednomu počítači v síti a z něho ji sdílet není ideální řešení. Takový počítač musí být pak zapnout v každém okamžiku, kdy chcete tisknout. Opět šetříte náklady na elektřinu a nervy. Dávejte pozor, jakým portem (USB nebo LPT) router disponuje. Logicky musí odpovídat tomu, přes nějž se připojuje tiskárna. Samotná přítomnost daného portu na routeru ovšem nestačí. Router musí přímo nabízet funkci sdílení tiskárny. Každopádně je dobré si tuto funkci s vaší tiskárnou vyzkoušet, protože levné GDI tiskárny tento způsob připojení často nepodporují a fungovat nebudou.

Omezení rychlosti klientů

Sdílení čehokoliv vede i ke konfliktům. Takže je dobré možnost kapacitu připojení rozdělit podle pravidel a ne způsobem „co si kdo ukousne, je jeho". Možnosti limitovat jednotlivým připojeným klientům rychlost se říká **shaping** a malá část nových routerů jim už disponuje.

Sdílení souborů

Mnohé routery dnes umožňují připojení USB disku. Soubory z něho pak lze sdílet v privátní síti anebo k nim dokonce přistupovat přes internet. Záleží na tom jakou formou je tato funkce implementována. Přístup přes FTP je většinou nejjednodušší, ale pro stanice s Windows také nepříliš pohodlný.

VPN

Možná zatoužíte po propojení dvou privátních sítí (třeba doma a ve škole) mezi sebou nebo budete chtít do vaší sítě přistupovat přes internet i z cest. Pak je vaším cílem zřízení virtuální privátní sítě (VPN). **Implementace je velice různorodá, ale obecně jde o to, že tato funkce umožní počítačům nebo celé síti, které jsou samy o sobě připojeny k internetu, aby měli přístup k prostředkům, které jsou jinak dostupné jen v dané domácí síti.** Z notebooku připojeného přes wifi v internetové kavárně se tak dostanete na soubory na disku u vás doma. Hledejte zařízení, která disponují možností zakončení (terminace) VPN spojení. Většina dnešních zařízení umí jen VPN propustit (VPN pass-through), což je dostatečné pouze v tom případě, že pro zakončení VPN budete mít v síti další zařízení nebo stále spuštěný počítač.

Wake On LAN

Tato technologie má úzkou vazbu na předchozí bod. Když budete chtít přistupovat z cest k souborům na disku vašeho počítače doma budete potřebovat aby byl zapnutý. Není zrovna ekonomické nechávat počítač zapnutý stále. Wake on LAN (nebo také etherwake, magic packet apod.) je speciální síťový paket, který umí probudit vypnutý počítač. K tomu je potřeba uvnitř počítače propojit síťovou kartu kablíkem se základní deskou a povolit tuto funkci v BIOSu. Pak už potřebujete jen zařízení, které

„probouzecí" paket pro počítač vygeneruje. A je skvělé, když to může být přímo váš router a jde to ovládat přes www.

DNS server

Jako DNS server sítě za routerem je většinou nastaven právě router samotný. Ve většině případů ale funguje pouze jako předávací DNS server. Všechny požadavky na překlady DNS jmen předá DNS serveru vašeho poskytovatele internetu. Může být praktické mít možnost do tohoto procesu zasáhnout. Pak je možné si pojmenovat počítače a další zařízení ve vaší privátní síti a nemusíte si pamatovat jejich číselní IP adresy. Pomocí jednoduchého triku s přesměrováním na localhost je také možné odstavit reklamní servery, které přidávají reklamní proužky do www stránek.

14.8.3 Šifrování

WEP (Wired Equivalent Privacy) – šifrovací protokol, který byl uveden v roce 1999. Je založen na šifrovacím algoritmu RC4 s tajným klíčem o velikosti 40 nebo 104 bitů kombinovaným s 24 bitovým inicializačním vektorem (IV). Pro ověření správnosti používá metodu CRC-32 kontrolního součtu.

Takzvaný 64 bitový WEP je kombinace 40 bitového klíče a 24 bitového IV, 128 bitový WEP je 104 bitový klíč a 24 bitový IV. Někteří výrobci bezdrátových zařízení podporují i 256 bitový WEP.

WEP je díky zranitelnosti šifrovacího algoritmu RC4, délce klíče a kolizím IV lehce překonatelnou* ochranou a **jeho použití se dnes nedoporučuje ani pro domácnosti**.

**získat WEP klíč za použití speciálního software *airodump, aireplay, aircrack* je otázkou několika málo minut*

WPA (Wi-Fi Protected Access) – (rok 2002) náhrada za původní slabé zabezpečení WEP. Stejně jako WEP je použit šifrovací algoritmus RC4, ale se 128 bitovým klíčem a 48 bitovým inicializačním vektorem (IV). Zásadní vylepšení však spočívá v **dynamicky se měnícím klíči** – TKIP (Temporal Key Integrity Protocol). Je vylepšena také kontrola integrity (správnosti) dat - díky použití metody označující se jako MIC (Message-Integrity Check).

WPA nabízí více možností, jak síť zabezpečit a to buď pomocí autentizačního serveru (RADIUS), který zasílá každému uživateli jiný klíč (podnikové řešení) nebo pomocí PSK (Pre-Shared Key), kdy každý uživatel má stejný přístupový klíč (malé podnikové sítě nebo domácnosti).

Zvětšení velikosti klíče a IV, snížení počtu zaslaných paketů s podobnými klíči a ověřování integrity dělá zabezpečení WPA těžko prolomitelné (ale bohužel už i to lze).

WPA2 – (rok 2004) označující se také jako IEEE 802.11i. Je použit protokol CCMP (Counter-Mode/Cipher Block Chaining Message Authentication Code Protocol) se silným šifrováním AES (Advanced Encryption Standard), MAC (Message Authentication Code) dynamicky mění 128 bitový klíč, MIC pro kontrolu integrity a ochranu proti útokům snažící se zopakovat předchozí odposlouchanou komunikaci (replay). (16)

Existují další metody zabezpečení – EAP typy ověřování pod WPA/WPA2 Enterprise, určené pro silné zabezpečení podnikových bezdrátových sítí.

14.9 Obecné zásady zabezpečení

Oproti metalickým sitim je bezpečnost hůře zajistitelná. Základním nebezpečím při provozu je to, že signál se šíří do všech stran a provoz tak může kdokoliv odposlouchávat, či se do bezdrátove sitě zapojit.

Bezpečnostní zásady jsou v zásadě 2:

- Autentizace, kdy se kontroluje oprávněnost přiřazeni nove stanice do bezdrátove sitě.
- Šifrování, jímž jsou přenášená data kódována (aby se nedala vyluštit ani po jejich zachyceni).

1. Ihned změňte administrátorské jméno, heslo!!! **A TAKÉ STANDARTNÍ IP ADRESU**!!!
2. Vypněte vysilání SSID - ikdyž je jasné, že jsou programy které SSID bez problému odhali, je to první krok k ukryti Vaši sitě před amatéry.
3. Zapněte nejvyšši možnou podporu šifrování (64, 128, 256 bitů) - zvolte nejvyšši možnou, kterou podporuji všechny klientské karty. Je jasné že WEP lze prolomit, ale lepši malá ochrana než žádná. Pravidelně měňte klíč a distribuujte ho mezi klienty (nikoliv emailem ale jiným humánním způsobem, který je bezpečnější).
4. Některá zařízeni již mají podporu *WPA* (*WiFI Protected Access*) - je to nový bezpečnostni mechanismus ratifikovaný WiFI Alianci - využivá stejný šifrovaci mechanismus jako *WEP* (128 b) ale obsahuje dočasné *TKIP* (Temporal Key Integrity Protocol) klíče - ty se mění každých 10 000 paketů. POZOR! *WPA* musi podporovat všechna zařízeni v siti.
5. Filtrování MAC adres - odhalit MAC adresu nějakého zařízeni není zase tak jednoduché jako odhalit 64b WEP klíč, ale jde to. To ale není důvod, proč tuto funkci nezapínat, ale i tohle má své pro a proti. Filtrování MAC adres je dobré tam, kde nepoužíváte roaming nebo kde máte jen jedno AP - zde musite pořád udržovat platný seznam. Např. prodáte kartu tak ji musite smazat ze seznamu a přidat tam jinou kterou třeba koupite. To je ale jasné. Nevýhodou je, že při použiti roamingu již na dvou nebo třech AP musite udržovat aktuální seznam MAC adres – záleží také, jak často se například ve firmě (škole) mění HW atd. Pro použiti doma je to bezúdržbová záležitost :-).
6. *Denial of Service* (DoS) - tyto útoky sice nepatří v pravém slova smyslu mezi průniky do sitě, ale mohou se vysíláním nesmyslných požadavků postarat o výpadek sitě (vyřazeni sitě z provozu) - takže pokud Vaše AP má možnost zapnout ochranu před DoS - rozhodně ji zapněte!
7. Nikomu nesdělujte svá hesla, MAC adresy nebo šifrovací klíče. Pokud dovolíte vašemu kamarádovi, aby si na Vaši síť připojil notebook, po jeho odchodu změňte šifrovací klíč!!
8. ROZDĚLTE LAN A WLAN - pokud máte doma nebo spiše ve firmě sitě LAN a WLAN - pokud to jen jde, oddělte je od sebe. Máte zase vyšší jistotu, že ten kdo napadne bezdrát, nebude mit přistup k drátům.
9. Nic nepodceňte - mohu Vám říci, že pokud si takhle síť zabezpečíte, nikdo se na Vás nabourávat nebude. Pokud se útočník dostane přes jeden kopec .. čeká ho další ... nabouráni se do takové sitě není otázka pár minut, ale hodin, dnů ba i týdnů ... a věřte, že to nikoho nebude bavit jen pro to aby se k vám dostal kvůli internetu zadarmo ... takže taková síť je relativně hodně bezpečná a nikdo se do takové sitě nebude lámat, pokud nebude přesně vědět po čem jde ... přestane se o vaši síť zajímat a půjde zase o dům dál :o)
10. Řiďte se body 1 – 9

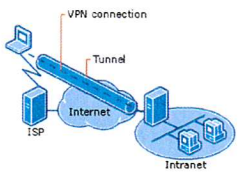
14.10 VPN

VPN je zkratka pro virtuální privátní síť *(Virtual Private Network)*. VPN slouží k virtuálnímu spojení více fyzicky vzdálených počítačů, takže se chovají, jako by byly přímo propojené jednou sítí. Umožňuje například spojeni sítí dvou poboček jedné firmy do sítě, která se chová jako jeden celek.

VPN je užitečná například při přistupu k síťovým službám, které jsou dostupné pouze z IP adres lokální sítě. Tímto způsobem může být omezen přístup k řadě placených informačních zdrojů pořizovaných pro uživatele. Dále se VPN používá ve velké míře i pro autentizaci a zabezpečení při připojení přes Wi-Fi síť. (14)

14.10.1 Jak funguje VPN?

Klient požádá server o vytvoření tunelu. Když server ověří jméno a heslo uživatele, klient i server vytvoří nová síťová rozhraní, která jsou *spojena* tunelem, který je šifrovaný a přes který jdou veškerá data. Servery po cestě tak vidí komunikaci mezi klientem a serverem šifrovaně a nejsou schopny ji přečíst. Cílový server potom data rozšifruje a pošle dál do internetu. Z venku to vypadá, že klient má počítač připojený přímo k serveru.



Virtual Private Network [19]

Realizace VPN serveru je postavená na protokolu **PPTP**.

- dynamické nastavování klienta (přidělování IP či adres DNS serverů)
- zabezpečení pomocí ověřování hesla (klient musí zadat správné heslo) nebo Challenge-handshake ověřování (server odešle otázku, na kterou klient musí správně odpovědět)
- kompresi dat, obě strany se dohodnou pomocí CCP (Compression Control Protocol) na algoritmu komprese dat
- šifrování dat, ve chvíli kdy je navázáno spojení se obě strany pomocí ECP (Encryption Control Protocol) dohodnou na formě šifrování dat.

[19] Zdroj: http://technet.microsoft.com/en-us/library/cc779919%28v=ws.10%29.aspx

Zdroje a literatura:

1. BROOKSHEAR, J. G. Informatika. Brno: Computer Press, 2013. ISBN 978-80-251-3805.
2. MEYER, M. Osobní počítač – názorný průvodce hardwarem, systémem a sítěmi. Brno: CP Books, 2005. ISBN 80-251-0834-1.
3. WINKLER, P. Velký počítačový lexikon. Brno: Computer Press, 2009. ISBN 978-80-251-2331-7.
4. HORÁK, J. Havárie počítače. Brno: Computer Press, 2006. ISBN 978-80-251-1451-3.
5. HORÁK, J. BIOS a Setup. Brno: Computer Press, 2004. ISBN 80-251-0148-7.
6. HORÁK, J. Hardware: Učebnice pro pokročilé. Brno: Computer Press, 2007. ISBN 978-80-251-1741-5.
7. DOSTÁL, J. Hardware moderního počítače. Studijní opora. Olomouc: Univerzita Palackého, 2011.
8. Archiv.cz: archiv článků a přednášek Jiřího Peterky. *Co je čím v počítačových sítích.* [online]. [cit. 2014-11-11]. Dostupné z: http://www.earchiv.cz/index.php3
9. Site.the.cz. *Počítačové sítě.* [online]. [cit. 2014-11-13]. Dostupné z: http://site.the.cz/index.php
10. PUŽMANOVÁ, R. *Moderní komunikační sítě od A do Z.* Brno: Computer Press, 2006. ISBN 80-251-1278-0.
11. HORÁK, J., KERŠLÁGER, M. *Počítačové sítě pro začínající správce.* Brno: Computer Press, 2008. ISBN 978-80-251-2073-6.

12. TRULOVE, J. *Sítě LAN.* Praha: Grada, 2009. ISBN 978-80-247-2098-2.
13. IP-adresa - dodatek pro správce sítí. [online]. [cit. 2014-11-11]. Dostupné z: http://zam.opf.slu.cz/botlik/CD-0x/6.html
14. KÖHRE, T. *Stavíme si bezdrátovou síť Wi-Fi.* Brno: Computer Press, 2004. ISBN 80-251-0391-9.
15. DAVIS, H. *Průvodce úplného začátečníka pro Wi-Fi bezdrátové sítě: není zapotřebí žádných předchozích zkušeností!* [přeložil Karel Voráček]. 1. vyd. Praha: Vydavatelství Grada, 2006. 334 s. ISBN 80-247-1421-3.
16. KLEMENT, M. *Bezdrátové sítě ve vzdělávání.* Studijní opora pro kurz projektu: Rozvoj ICT kompetencí pedagogických pracovníků Olomouckého kraje pomocí e-Learningu.

Obrázky:

Obrázky, u nichž není uveden zdroj v poznámce pod čarou, jsou čerpány z citované literatury výše nebo jsou vlastním dílem.