

Kapitola 2

Základní pojmy síťového softwaru

Kromě síťového hardwaru, jímž jsme se zabývali v předešlé kapitole, je dalším stavebním kamenem sítí software. Tím je hardware oživen a vznikne provozuschopná síť. Trh se softwarem počítačových sítí je ve srovnání s hardwarem podstatně užší. Setkáme se se sítěmi Microsoftu a Linuxem. Každému produktu bude věnována zvláštní část. Než se pustíme do detailního popisu jednotlivých síťových systémů, vysvětlíme si některé obecné pojmy, které potřebujeme při práci se síťovým softwarem znát.

Typy síťového softwaru

Základním kritériem, podle něhož rozdělujeme síťový software, je použití (či nepoužití) serveru. Z tohoto hlediska rozeznáváme síť peer-to-peer a klient-server.

Síť peer-to-peer (rovný s rovným)

Tato síť je tvořena jednotlivými síťovými stanicemi (počítači), které si jsou navzájem rovné. Znamená to, že počítače si mezi sebou nabízejí své služby. Například mohou být na počítači zpřístupněny určité složky, do nichž je povolen přístup jiným uživatelům, nebo můžeme dovolit tisk na jedné tiskárně více stanicím. Jako vše má takovéto řešení své přednosti a nedostatky:

- ◆ **Výhody:** Pro správu sítě nejsou třeba žádné velké znalosti. Jde o řešení levné, není nutné kupovat server ani žádné síťové operační systémy (peer-to-peer síť je obsažena ve Windows).
- ◆ **Nevýhody:** Při větším počtu počítačů je velmi obtížné udržet přehled o datech (na kterém počítači je to uloženo?). Data jsou jen málo chráněna proti zneužití. Konfigurace přístupových práv (kdo může co číst) je u peer-to-peer jednoduchá (a méně bezpečná), navíc se musí aplikovat (a dodržovat) na všech stanicích, což bývá téměř neuskutečnitelné.

Celkově lze říci, že síť peer-to-peer je vhodná pro propojení několika počítačů v malé firmě. Horní hranice provozuschopnosti sítě je někde u deseti stanic.

Síť klient-server

Filozofie tohoto řešení je jednoduchá. Soustředit vše (data, služby, údaje o uživatelích...) do jednoho bodu v síti. Ten důkladně zabezpečit a odsud nabízet služby všem síťovým stanicím. Počítač, kam údaje soustřeďujeme, nazýváme server (sluha). Protože musí obsluhovat mnoho požadavků

v krátkém čase je zde ukládáno mnoho dat, je nutné, aby to byl počítač kvalitní a rychlý. Navíc na něm musí být nahrán speciální program – síťový operační systém, který bude organizovat ukládání dat, přidělovat přístupová práva k složkám a souborům, vést evidenci o tom, kdo se může k serveru přihlásit a co bude moci na serveru dělat... Celkově lze síť klient-server charakterizovat takto:

- ◆ **Výhody:** Vysoká bezpečnost dat, přehlednost, snadná konfigurovatelnost.
- ◆ **Nevýhody:** Spočívají v nákladech na nákup serveru a síťového operačního systému, v nutnosti mít vysoce kvalifikovaného pracovníka, který bude umět obsluhovat síťový operační systém.

Pro většinu sítí je toto řešení nevyhnutelné, a proto je také značná část knihy věnována popisu nej-používanějších síťových operačních systémů. Nejrozšířenější síťové operační systémy pracující na serveru jsou pro síť LAN:

- ◆ Od firmy **Microsoft** to je Microsoft Windows Server 2008 a jeho předchůdci Microsoft Windows Server 2003 a Microsoft Windows 2000 Server.
- ◆ Různé distribuce **Linuxu**.

Server

To nejdůležitější a nejdražší v celé síti není žádný počítač, ale data (kvůli nimž síť budujeme). Nicméně je server tím místem, kde jsou data uložena, a proto se na něj podíváme blíže. Serverem může být teoreticky jakýkoliv počítač, na něj nahrajeme síťový operační systém. Víme však, že server je jádrem počítačové sítě, musí současně obsluhovat mnoho požadavků od síťových stanic, zaručit bezpečnost zde uložených dat, a tak na hardware serveru klademe daleko vyšší nároky než na obyčejnou stanici.

Hardwarové požadavky na server

Mikroprocesor

Ten samozřejmě požadujeme vždy co nejlepší. U levných serverů se používají vícejádrové desktopové procesory (Intel Core2, Intel Core i7, AMD Phenom). Daleko častější je však použití mikroprocesorů vyvinutých speciálně pro servery – Intel Xeon a AMD Opteron. U serverů určených do velkých sítí se používá multiprocessing – spolupráce několika mikroprocesorů na jedné základní desce.

Operační paměť

Musí být dostatečně velká pro soubory síťového operačního systému a ještě musí poskytnout prostor pro další aplikace vyžadované uživateli. Navíc je potřeba místo pro kešování pevných disků. Velikost paměti je tedy závislá na použitém operačním systému, počtu stanic v síti a na programech, které budeme ze serveru spouštět. U menších serverů je její spodní hranice zhruba 4 GB, ale často se používají paměti podstatně větší. Většinou se používají operační paměti v provedení *registered* a *ECC*.

Při charakteristikách paměti jsme se setkali s několika novými pojmy, které nemusí každý znát:

- ◆ **Kešování (cache):** Server musí velmi často číst data z disku, což je ve srovnání s čtením dat z operační paměti pomalá operace. Proto jsou dříve čtená data stále uchovávána v operační

paměti. Pokud přijde požadavek na čtení dat, hledají se nejdříve v rychlé operační paměti, a až když tam nejsou nalezena, jsou přečtena z pomalejšího pevného disku. Protože většina uživatelů sítě používá stejný program (uložený na serveru), je pravděpodobnost nalezení dat v operační paměti vysoká – podstatně se tak zrychlí práce serveru.

- ◆ **ECC (Error Checking and Correcting)** je samoopravný kód, který dokáže nejen zjistit, ale i opravit jednobitovou (nové systémy i dvoubitovou) chybu v paměti. ECC musí být podporován základní deskou i paměťovým modulem. ECC paměti jsou samozřejmě dražší, proto se používají převážně v serverech.
- ◆ **Registered** moduly se liší použitím speciálních vstupně-výstupních bufferů, které zvyšují stabilitu a spolehlivost přenosu dat. Také registrované moduly musejí být podporovány chipsetem základní desky a také ony jsou dražší než častěji používané moduly bez bufferů (unbuffered).

Pevné disky

Pevné disky, na něž se ukládají data z celé sítě, jsou další veledůležitou součástí serverů. Musejí mít dostatečnou kapacitu, která závisí na použitém programu a velikosti sítě. Spodní hranice velikosti disků je okolo 200 GB, většinou se však používají disky podstatně větší. Dalším požadavkem, uplatňovaným u serverů, jsou zvýšené požadavky na bezpečnost uložených dat – z tohoto důvodu se serverové disky sdružují do diskových polí *RAID*.

Dnes se setkáme u levnějších serverů s disky s rozhraním SATA (Serial ATA). Tato relativně nová technologie přenosu dat mezi pevným diskem a základní deskou je rovněž rychlá a je možné ji použít při sestavování disků do polí RAID. Ve srovnání s SCSI je znatelně jednodušší a především levnější.

U kvalitnějších (a dražších) serverů se používá diskové rozhraní SAS (*Serial Attached SCSI*). To je oproti paralelnímu SCSI rozhraní sériovým. SAS zachovává příkazy SCSI, ale je:

- ◆ univerzálnější: je možné k němu připojit více druhů i větší počet zařízení, a protože používá stejné kabely jako SATA, tak i disky SATA,
- ◆ rychlejší, přičemž se v brzké době předpokládá výrazné zvýšení rychlosti,
- ◆ duplexní, současně je možné data číst i zapisovat,
- ◆ je levnější než SCSI.

Disková pole

Jako velké sklady dat se v dražších serverech nepoužívají jednotlivé disky, ale disková pole. Jde o skupinu disků, která se navenek „tváří“ jako disk jeden. Server sem posílá požadavky na čtení a zápis dat a pole si samo organizuje, na který disk se data uloží (či odkud se přečtou). Pole mohou být umístěna ve skříni serveru i mimo ni. Účelem diskových polí je především zvýšení bezpečnosti dat. K organizaci dat používají některou z metod *RAID (Redundant Array of Inexpensive Disks)*. Vlastní problematika RAID je velmi složitá, pro naše účely postačí vysvětlit základní vlastnosti diskových polí. Vyšší bezpečnosti diskových polí je dosaženo díky nadbytečnosti (redundanci) dat. V principu jde o to, že se stejná data zapisují na více disků. Při havárii se pak z nadbytečných dat doplní chybějící údaje. Vyšší bezpečnost je vykoupěna snížením použitelného prostoru disku. RAID se dělí do několika skupin, které používají různé úrovně redundance dat. Podstatné znaky metod RAID použitých u serverů PC ukazuje tabulka:

Tabulka 2.1: Úrovně redundance dat

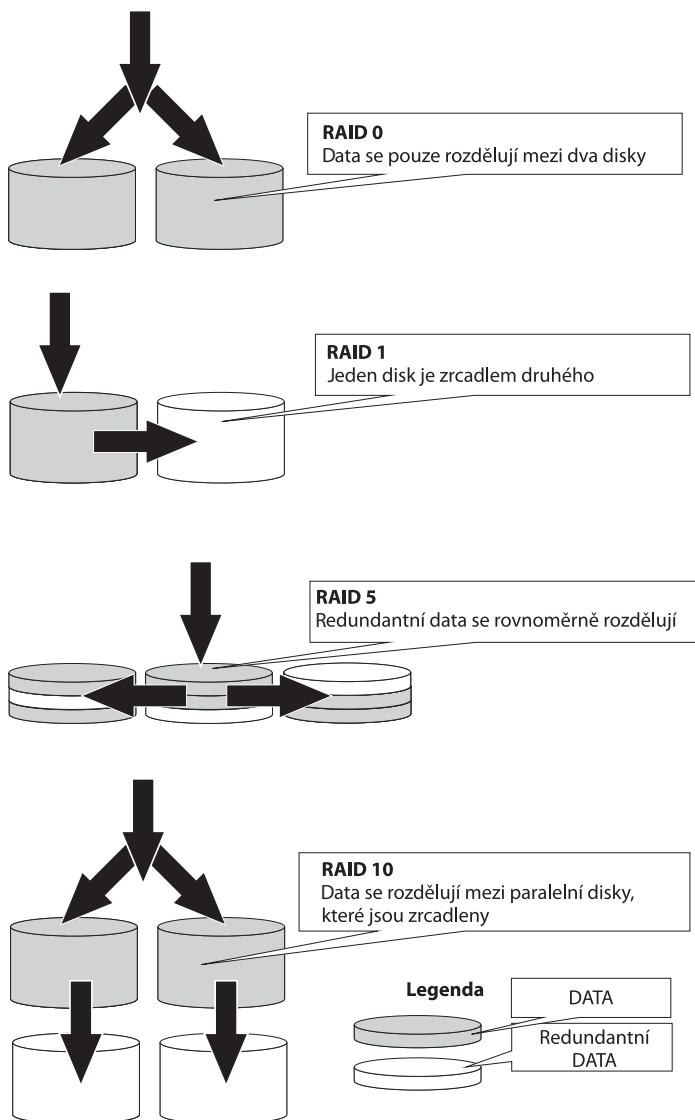
Typ	Princip	Výhody	Nevýhody
RAID 0, striping	Data se rozdělují mezi několik disků.	Zvýšení kapacity, snížení přístupové doby při čtecích i zapisovacích operacích.	Nezvyšuje bezpečnost, pokud jeden disk zhavaruje, ztratíme všechna data.
RAID 1, mirroring	Data se současně zapisují na více disků (většinou dva). Jeden disk je úplnou kopií druhého.	Data jsou 100% redundantní. Vysoká bezpečnost, při poruše primárního disku přebírá jeho funkci sekundární disk. Dochází ke zvýšení čtecích operací díky současnému čtení ze dvou disků.	Kapacita jednoho disku je zrcadlena na disk další. K uložení dat je tak potřebná dvojnásobná kapacita (2 disky).
RAID 5, striping s redundancí	Data jsou rozdělována mezi více disků. „Nadbytečná“ paritní data jsou rozprostřena na všechny disky. Zhavarovaný disk je možné vyměnit. Jeho data jsou pak zrekonstruována pomocí paritních redundantních údajů.	Zvýšení výkonu při čtecích operacích. Redundantní data zaberou jen část kapacity disků (není třeba zdvojnásobovat kapacitu disků). Havarovaný disk je možné vyměnit a pole dopočítá a zrekonstruuje chybějící data.	Potřeba minimálně tří disků.
RAID 10 striping s mirroringem (RAID 0 + RAID 1)	Data jsou rozdělována mezi několik disků (RAID 0). Dosáhne se tak vysoké rychlosti. Každý z disků RAID 0 je ještě zrcadlen.	Vysoká rychlost kombinovaná s bezpečností.	Na striping potřebujeme 2 disky a na zrcadlení další 2 – potřeba minimálně 4 disků.

- ♦ **RAID 0:** Zvýší pouze rychlost sekvenčního čtení a sekvenčního zápisu. Najde proto využití pouze v případech, kdy je třeba rychlého zápisu či čtení velkých bloků dat – například při editaci filmů, fotografií, audionahrávek atd. Pro servery je jeho použití nevhodné.
- ♦ **RAID 1:** Je již v serverech (především těch levnějších) používán. Administrace RAID 1 je jednoduchá, kdykoliv můžete jeden z disků odebrat, kdykoliv můžete synchronizovat data mezi disky.
- ♦ **RAID 5:** Je pro servery typický. Pro jeho sestavení jsou potřeba minimálně 3 disky.
- ♦ **RAID 10:** Nevýhodou je větší počet disků potřebných k vytvoření pole. Nevýhoda je však kompenzována velkou rychlostí pole.

Vytvoření RAID

Rozhraní RAID může být realizováno dvěma způsoby:

- ♦ Softwarově, kdy je RAID vytvářen operačním systémem. Metodu RAID umějí výhradně síťové operační systémy.
- ♦ Hardwarově, kdy je RAID vytvářen řadičem pevných disků.



Obrázek 2.1: Princip RAID

DVD-ROM

Tou musí být vybaven každý server, protože síťové operační systémy se dodávají na několika CD discích a mnoho příslušenství se instaluje z disků DVD. Někdy může být výhodná také zapisovací mechanika, především zapisovací mechaniky DVD mají slušné kapacity a mohou se použít pro zálohování dat. Ve srovnání s páskovými jednotkami jsou však jejich velikosti stále malé a je potřeba zvážit, zda pro případné zálohování budou mít dostatečnou kapacitu.

Pásková jednotka

Jak již bylo řečeno – nejdražší jsou data. Pásková jednotka se používá pro jejich zálohování. Přestože jsou data chráněna (před havárií serveru) nějakým systémem RAID, je dobré zapsat je ještě na pásku. Páska se pak ukládá odděleně od serveru. Data jsou tak chráněna proti krádeži, požáru serveru nebo celé budovy. Navíc je možné z páskové zálohy data obnovovat – vrátit se k jejich starší verzi.

Síťové operační systémy umějí zapisovat na pásku vybraná data v určitém čase (např. v noci) – tím se eliminuje nízká rychlost pásky. Při pořizování pásky nesmíme zapomenout na její kapacitu – ta musí odpovídat předpokládané velikosti zálohovaných dat.

Ostatní hardwarové prvky

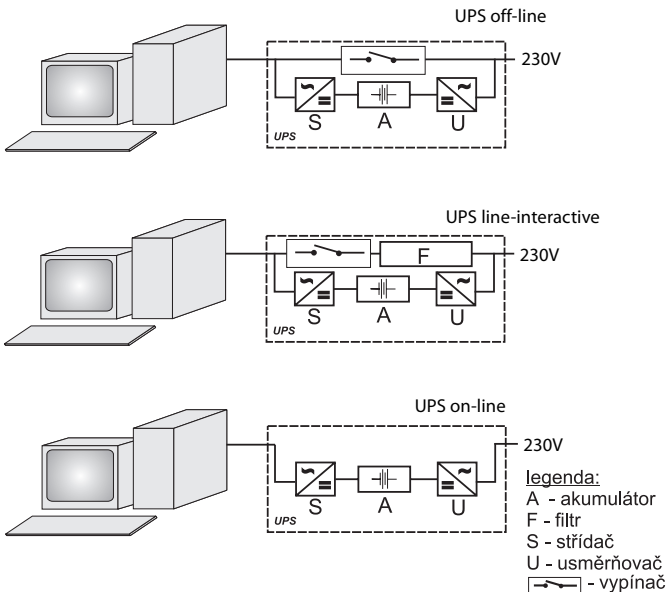
Z předešlého výkladu je jasné, že pro server musíme použít speciální základní desku, která dovolí multiprocessing a bude mít dostatečnou kapacitu pro operační paměť.

Dnes se do nových serverů standardně vkládají síťové karty o rychlosti 1 GB/s.

Dalším podstatným znakem serverů jsou velké skříně, do nichž se musí vejít několik disků a pásková jednotka. Důležité je také propracované chlazení (server se nevypíná). Často jsou prvky ve skříně v modulárním provedení dovolujícím výměnu jednotlivých modulů za chodu serveru. Je takto možné měnit disky, ventilátory atd.

Záložní zdroje UPS (Uninterruptible Power Supply)

Přerušení napájecího napětí serveru může způsobit velké problémy. Pro mnoho aplikačních programů i samotný síťový operační systém představuje náhlé ukončení práce (bez uložení dat) nedefinovaný stav, jehož následkem může být nutnost nové instalace systému nebo programu (nemluvě o ztrátě dat aplikačních programů).



Obrázek 2.2: Principy UPS

Problematika UPS je široká a přesahuje rámec knihy, přesto si alespoň základní informace o napájecích zdrojích řekneme. Nejdříve k tomu, co náhradní zdroj obsahuje. Základem je samozřejmě akumulátor, ten musí být hermetizovaný, aby z něho nevycházely jedovaté výpary (určitě nemůžeme použít autobaterii). Akumulátor musíme dobít, dalším obvodem je tedy usměrňovač, který mění střídavý proud z elektrorozvodné sítě na stejnosměrný. Výstupní napětí z UPS však musí být střídavé, mezi akumulátorem a výstupem z UPS je střídač (měnič stejnosměrný signál na střídavý). Právě kvalita střídače od sebe jednotlivé UPS odlišuje. Vyrobit ze stejnosměrného proudu dokonalou sinusoidu s frekvencí 50 Hz není tak jednoduché. Technicky to samozřejmě možné je, ale stojí to peníze, takže se se skutečně sinusovým výstupem při napájení z akumulátoru setkáte pouze u kvalitnějších UPS (line-interactive či online). Základní obvody UPS mohou být různě zapojeny, což je asi základním kritériem při hodnocení UPS:

- ◆ **UPS offline** jsou nejnižší a nejlevnější třídou záložních zdrojů. Mají jen jednoduchý nabíjecí obvod s usměrňovačem pro nabíjení akumulátorů a jednoduchý střídač s většinou nekvalitním lichoběžníkovým výstupem. Pokud je v elektrorozvodné síti dostatečně vysoké napětí, tak se počítač napájí přímo z ní, bez účasti jakýchkoliv filtrů či elektroniky v UPS. Jestliže hodnota napájecího napětí poklesne, přichází na řadu napájení z akumulátoru, které bohužel nemívá sinusový průběh (ale počítačům to zas tak nevadí).
- ◆ **UPS online** jsou naopak třídou nejvyšší, nejkvalitnější a nejdražší. Pracují tak, že výstup z UPS je vždy tvořen střídačem napájeným z akumulátorů a akumulátor je stále dobíjen z elektrorozvodné sítě. Počítač není vlastně nikdy připojen přímo k napájecí síti. Je tedy oddělen od všech poruch a nepravidelností v napájecí síti.
- ◆ **UPS line interactive** jsou jakýmsi mezičlánkem mezi oběma předešlými variantami. V základním režimu je spotřebič napájen přímo z elektrorozvodné sítě, ale napájecí napětí je v UPS upravováno. Jsou odfiltrovány šumy, někdy si elektronické obvody poradí bez účasti akumulátorů s mírným podpětím či přepětím.



Poznámka: Na obrázku 2.2 Principy UPS je přepínání mezi přímou napájecí větví a napájením přes baterie symbolizováno vypínačem.

K zálohování napájecího napětí počítačů jsou asi nevhodnější UPS line interactive. Máme-li přísné požadavky na kvalitu napájecího napětí (tvar, odrušení...), budeme muset sáhnout hlouběji do kapsy a pořídit si UPS online.

Při výběru UPS musíme také zohlednit jejich technické parametry:

- ◆ **Výkon UPS** se udává ve VA (voltampérech) a musí být o něco větší než výkon napájecího zdroje serveru. Výkon napájecího zdroje serveru se vyjadřuje ve W (watt). Vztah mezi zdánlivým výkonem (voltampéry) a činným výkonem (watty) je pro napájecí zdroje serveru 0,7. (Činný výkon záložního zdroje by měl být 0,7 krát větší než zdánlivý výkon napájecího zdroje serveru.)
- ◆ **Čas napájení z UPS** – jde o dobu, během níž je UPS schopná napájet server z baterií. UPS slouží k překlenutí krátkodobých výpadků napájení a ukončení systému, proto je horní hranice této doby zhruba dvacetiminutová. Platí přímá úměra mezi dobou zálohy a výkonem UPS. Při vyšším výkonu UPS (ve vztahu k výkonu zdroje serveru) se prodlužuje doba napájení z baterií. (Podívejme se na třetí řádek tabulky: kdybychom použili zálohovací zdroj 1 000 VA pro napájení serveru 450 W, vzroste doba napájení z baterií na cca 60 min.)

- ◆ **Softwarové vybavení** je především pro servery životně důležité. Ve výbavě UPS bývá program (ten nahrajeme k síťovému operačnímu systému), který plní několik funkcí: podává informace o stavu baterií, o tom kdy UPS napájela PC z baterií, posílá zprávy o výpadcích napájecího napětí na e-mailovou adresu... Hlavní funkcí softwaru UPS je však legální ukončení operačního systému po určité době (kdy již hrozí nebezpečí, že se vybijí akumulátory v UPS). Pro komunikaci mezi UPS a serverem se používá sériový port nebo USB.
- ◆ **Stav baterií** je také velmi důležitý. Z vybitých baterií není napájení možné. Většina UPS má na čelním panelu kontrolní diody, z nichž je možné stav baterií vyčíst. Informaci zjistíme většinou také softwarově. Životnost baterií bývá 3 až 4 roky.

Pro představu uvádím tabulku výkonové řady jednotek UPS určených pro servery. Doba napájení je ještě závislá na momentální zátěži serveru (a také stavu baterií), a tak v tabulce udávám její mezní hodnoty.

Tabulka 2.2: Typické parametry záložních zdrojů

Výkon UPS	Výkon zdroje serveru	Doba napájení
620 [VA]	390 [W]	6–14 [min.]
700 [VA]	450 [W]	5–17 [min.]
1 000 [VA]	650 [W]	6–18 [min.]
1 400 [VA]	950 [W]	7–18 [min.]
2 200 [VA]	1 600 [W]	8–24 [min.]
3 000 [VA]	2 250 [W]	5–15 [min.]

Dedikace (vyčlenění) serveru

Server může být dedikovaný (vyčleněný). V takovém případě na něm běží pouze síťový operační systém a k běžné práci jej vůbec nepoužíváme. Opakem je server nededikovaný, na němž můžeme provádět běžnou práci a ještě na něm běží síťový operační systém. Takovouto práci dovolují například síťové operační systémy Windows Server. Uvědomíme-li si však, že na server jsou koncentrována data sítě, je běžná práce na něm nevhodná (už fyzický přístup ke konzole serveru je nebezpečný) a především u větších sítí se používá jen zřídka.

Softwarové požadavky na server

Každý server nabízí *služby* (u Windows Serveru používá Microsoft termín *role*). Mezi základní patří:

Souborový server (file server)

Je prvotní funkcí každého síťového operačního systému, která zabezpečuje:

- ◆ víceuživatelský přístup k souborům: s jedním souborem může současně pracovat více uživatelů,
- ◆ vede evidenci uživatelů, kteří se mohou k serveru přihlásit, a má přehled o tom, co mohou a nemohou dělat na discích, adresářích (složkách) či s konkrétním souborem (např. někdo může soubory jen číst, jiný je vůbec nevidí, další má k souborům přidělena vyšší práva – zapisovat do nich, mazat je).

Tiskový server (print server)

Síťový operační systém zprostředkuje přístup k jedné tiskárně více uživatelům. Opět se definuje, co může uživatel s tiskárnou provádět (jen tisknout, konfigurovat, mazat tiskové úlohy atd.). Dnes tato služba (role) ustupuje do pozadí, snadnější je použít hardwarový tiskový server.

Aplikační server

Servery neslouží pouze jako sklady dat, ale často jsou na nich spuštěny programy (aplikace) společně všem uživatelům sítě. Aplikací je celá řada, jsou určeny pro různé obory: Jde o různé ekonomické informační systémy zajišťující účetnictví, skladovou evidenci, kontakty na zákazníky, ekonomické rozborů. Dále se používají např. výrobní programy, sledující a řídicí průběh výroby.

Mezi další, často používané role (služby) serveru patří:

- ◆ DHCP server, který automaticky přiděluje adresy IP počítačům v síti.
- ◆ DNS server, zajišťující překlad adres IP na názvy. (Oba produkty se týkají práce s protokolem TCP/IP a jsou vysvětleny v části Protokol TCP/IP.)
- ◆ Program pro připojení sítě k Internetu. Ten zprostředkuje přístup k Internetu více počítačům a připojovanou síť navíc chrání před neoprávněným vniknutím z vnějšku (tato funkce se nazývá Firewall).
- ◆ Program pro elektronickou poštu.
- ◆ Programy pro správu velkých databází.

Pro začátečníka bývá orientace ve spleti názvů jednotlivých aplikačních serverů velmi složitá. Výrobci síťových operačních systémů nabízejí také softwarové balíky. Jejich základem je operační systém, který je doplněn o jednotlivé aplikace. Tabulka ukazuje tyto programové balíky, jejich přehled je doplněn i o vysvětlení významu jednotlivých aplikací.

Tabulka 2.3: Programové balíky

produkt	Microsoft Small Business Server 2008	Linux
Operační systém	Windows Server 2008 Standard	Linux
Elektronická pošta	Microsoft Exchange Server 2007 Standard Edition	Sendmail, IMAP a LDAP servery
Připojení k Internetu		Proxy cache Squid
Sdílení a publikace dokumentů	Windows SharePoint Services 3.0	
Distribuce aktualizací:	Windows Server Update Services 3.0	
Správa databází	Microsoft SQL Server 2008 Standard	PostgreSQL, MySQL



Poznámka: Cílem tabulky je vysvětlení terminologie nejpoužívanějších aplikačních serverů, není tedy úplným popisem produktů (a zde integrovaných služeb) a nezabývá se licenční politikou.

Umístění serveru

Z předešlých řádků to nemusí být na první pohled zřejmé, ale síťový hardware (ani software) neklaďou žádné požadavky na umístění serveru. Ten tedy může být umístěn na libovolném místě sítě.

Praktické umístění serveru je dáno spíše požadavky organizačními. Umisťuje se tak, aby nerušil svým hlukem okolí a aby byl dobře zabezpečen před krádeží a neodbornou obsluhou.

Síťové protokoly

Další nedílnou součástí síťového softwaru jsou síťové protokoly. Protokol definuje komunikační pravidla, jimiž se řídí výměna dat v síti. Pro správnou funkci sítě je tedy nutné, aby všechny stanice v síti používaly stejný protokol.

V praxi se vždy setkáme se sadou protokolů, které navzájem spolupracují. U sítě LAN se fakticky používá pouze sada protokolů TCP/IP. Dříve používané protokoly NetBEUI a IPX/SPX jsou již minulostí.

Protokol TCP/IP

Tato skupina protokolů je dnes určitě nejrozšířenější. Původně byla navržena pro síť, z níž se vyvinul Internet. Dnes je rodina protokolů TCP/IP používána ve všech sítích LAN, kde se stala standardem a své předchůdce zcela vytlačila.

Z funkčního hlediska můžeme TCP/IP rozdělit na tři vrstvy (reprezentované samostatnými protokoly):

- ◆ **aplikační vrstvu** (spolupracující s konkrétními programy),
- ◆ **transportní vrstvu** (protokoly TCP a UDP),
- ◆ **síťovou vrstvu** (protokoly IP).

Spolupráce vrstev probíhá asi takto: Program (tj. aplikace) potřebuje navázat spojení se svým protějškem na jiném počítači. Použije k tomu aplikační vrstvu, od níž putuje požadavek na spojení do transportní vrstvy. Ta zorganizuje dopravu dat (data rozdělí na segmenty, naváže spojení, zkontroluje, zda byla data doručena). Vlastní přenos zajišťuje nižší – síťová vrstva. Segmenty, které obdržela od nadřazené vrstvy, „zabalí“ do datagramů a doručí vzdálenému počítači.

Aplikační vrstva

Je tvořena množinou protokolů spolupracujících s jednotlivými aplikačními programy. Jejich funkci se pokusím vysvětlit na jednoduchém příkladu:

Při prohlížení webových stránek používáme prohlížeč (nejčastěji asi Internet Explorer, ale existují i jiné programy, např. Firefox, Opera, Safari atd.). Prohlížeče spolupracují s internetovými servery, na nichž jsou webové stránky uloženy a uživatelům nabízeny (opět různými speciálními programy pro publikaci WWW, nakonec webové stránky můžeme nabízet i prostřednictvím Windows). Vidíme, že při brouzdání Internetem spolupracují různé programy různých výrobců. Jejich spolupráce je zajištěna aplikačním protokolem – vlastně soustavou norem, které musí tyto programy respektovat. (Při prohlížení WWW stránek jím je protokol *http*.)

Aplikačních protokolů je mnoho, některé z nich (ty nejnámější) ukazuje tabulka.

Tabulka 2.4: Neznámější aplikační protokoly

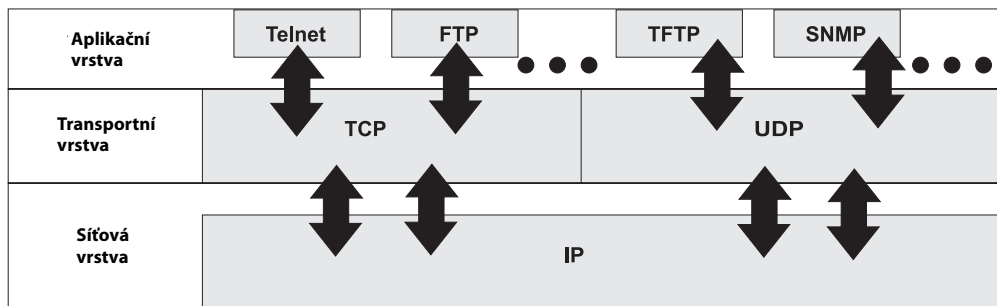
Služba	Funkce
FTP – File Transfer Protocol (datový kanál)	Používá se pro přenos souborů mezi vzdálenými PC
Telnet	Pro jednoduché terminálové relace (v podstatě ovládáme obrazovku vzdáleného PC)
Server DNS – Domain Name System	Organizuje názvy počítačů v Internetu a jejich vazby na IP adresy
WWW – protocol HTTP (Hypertext Transfer Protocol)	Protokol používaný k uspořádání WWW stránek a pohybu mezi nimi
SMTP – Simple Mail Transfer Protocol	Protokol zajišťující přenos zpráv mezi servery Internetu (používaný hlavně pro elektronickou poštu)
POP3 – Post Office Protocol	Jeho posláním je dopravit poštu z elektronické schránky na náš počítač

Transportní vrstva

Je jakýmsi jádrem celé soustavy TCP/IP, tvořeným pouze dvěma protokoly: TCP a UDP.

Protokol TCP (Transmission Control Protocol)

Od aplikační vrstvy (prostřednictvím některého protokolu) přebere data, která rozdělí na segmenty, očísluje a seřadí podle toho, jak mají být postupně odeslány. Před začátkem výměny dat zahájí relaci s transportní vrstvou protějščího počítače. Poté začne s vysíláním a potvrzováním jednotlivých datových segmentů.

**Obrázek 2.4:** Rodina protokolů TCP/IP

Vlastní odesílání je již věcí síťové vrstvy, což je popsáno dále. (Vše funguje také opačně: Od síťové vrstvy jsou přebrány datové segmenty, které TCP setřídí. Pokud některý chybí, tak si jej znovu vyžádá. Ze segmentů složí data a předá je prostřednictvím aplikačního protokolu některému z programů.)

Protokol UDP (User Datagram Protocol)

UDP má stejné poslání jako TCP: převezme data od aplikace, sestaví z nich segmenty a předá je k odeslání síťové vrstvě. Na rozdíl od TCP nepotřebuje vytvářet před přenosem dat relaci s protějškem a nekontroluje, zda byly datagramy protějškem přijaty.

Protokol UDP je jednodušší, ale méně spolehlivý. Některé programy jej využívají namísto protokolu TCP pro rychlý a nenáročný přenos dat (bez zajištění spolehlivosti).

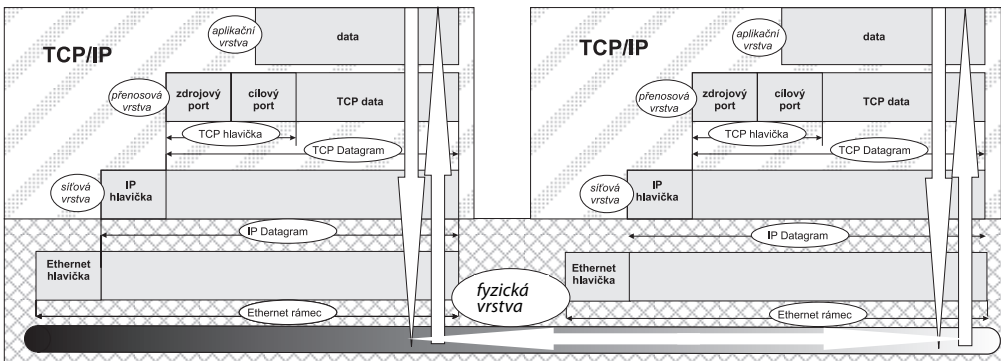
Protokol IP (Internet Protocol)

Pracuje v síťové vrstvě soustavy TCP/IP. Od nadřazených protokolů transportní vrstvy obdrží datové segmenty s požadavkem na odeslání. K segmentům připojí vlastní hlavičku a vytvoří datagram IP. V hlavičce IP je především IP adresa příjemce a odesílatele, což předznamenává hlavní poslání protokolu: doručení jednotlivých datagramů k příjemci – provádí tedy adresování a směrování datagramů mezi počítači.

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

Uspořádání protokolů TCP/IP ukazuje obrázek 2.4 *Rodina protokolů TCP/IP*. Komunikace mezi jednotlivými protokoly probíhá bránami, anglicky porty. Černé šipky na obrázku porty znázorňují. V soustavě TCP/IP odpovídá každému protokolu jedna brána.

Na druhém obrázku *Spolupráce v TCP/IP* je naznačena vzájemná výměna dat mezi jednotlivými vrstvami protokolů TCP/IP. Vlastní přenos provádí zařízení fyzické vrstvy – síťová karta, kabeláž a aktivní prvky kabeláže.



Obrázek 2.5: Spolupráce v TCP/IP

Adresace v sítích TCP/IP

Při zprovoznování sítě založené na protokolu TCP/IP je pro nás z praktického hlediska nejdůležitější práce s adresami.

Základní a nejobecnější pravidlo adresace je jednoduché – každá stanice musí mít originální číslo, navíc je potřebné, aby z čísla bylo zřejmé umístění stanice v síti či síťovém segmentu. Každá stanice

má tedy svou IP adresu reprezentovanou čtveřicí čísel oddělených tečkou. Obecně je ve výpočetní technice výchozím formátem čísel dvojková abeceda. Pokud vyjádříme IP adresu dvojkově, bude adresa tvořena čtyřmi osmibitovými čísly. (Osm bitů představuje jeden bajt. Je možné také říci, že IP adresa je tvořena čtyřmi bajty.) Celá adresa může například vypadat takto: 11000000.10101000.00000001.00001011. Vyjadřování ve dvojkové soustavě není každému srozumitelné, a proto se pro zápis čísel IP adresy mohou použít ještě jiné číselné soustavy: šestnáctková a nám nejpřirozenější desítková. Uvedme k nim velice stručně několik poznámek.

- ◆ **Dvojková (binární):** Má pouze dvě číslice 0 a 1, a jak již bylo řečeno, je soustavou, s níž pracují hardwarové prvky PC.
- ◆ **Šestnáctková (hexadecimální):** Jejím základem je šestnáct znaků: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, A, B, C, D, E, F. Občas se s ní v adresaci IP také setkáme. V šestnáctkovém vyjádření by výše uvedená dvojková adresa vypadala takto: C0.A8.01.11.
- ◆ **Desítková (dekadická):** Je tou soustavou, v níž jsme zvyklí pracovat, a proto ji budeme dále používat. Naše příkladová adresa vypadá v desítkové soustavě takto: 192.168.1.11.

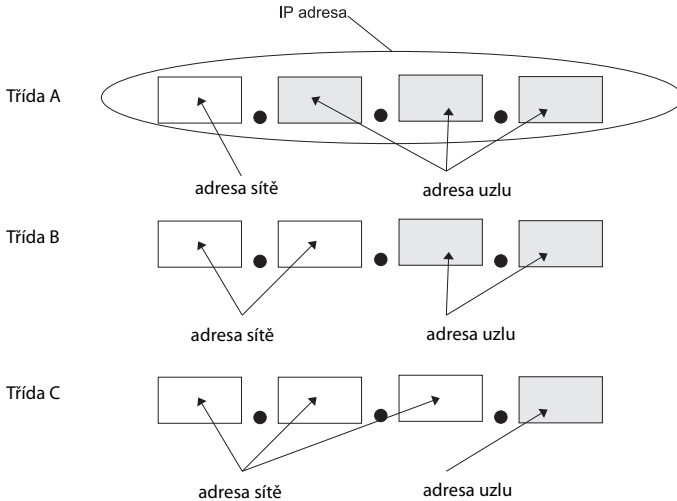


Tip: Pro převody mezi soustavami existují přesná pravidla, také význam a váha jednotlivých číslic soustav jsou přísně definovány. Popis obou skutečností přesahuje rámec knihy, přesto se zmíním alespoň o snadném způsobu převodu mezi soustavami, který je v praxi nejdůležitější. Můžeme využít program Kalkulačka, který najdeme v Příslušenství Windows. Přepneme-li její obrazovku do vědeckého rozhraní (v menu Zobrazit), můžeme jednoduše provádět převody. Zvolíme soustavu, z níž chceme převádět (tlačítko Hex je pro šestnáctkovou, Dec pro desítkovou, Bin pro binární soustavu), a pak přepneme kalkulačku do cílové číselné soustavy. Na displeji vidíme výsledek převodu.



Obrázek 2.6: Program Kalkulačka

V praxi mezi sebou spolupracují různé sítě, jednotlivé sítě mohou být navíc rozděleny na části – segmenty. V IP adrese počítačů spojených do sítě nestačí uvést pouze číslo konkrétního počítače, ale potřebujeme znát ještě číslo sítě (nebo jejího segmentu), v níž je počítač zařazen. Část IP adresy pak vyjadřuje číslo sítě a zbytek popisuje adresu počítače v této síti. Podle toho, jaká část adresy je věnována síti a jaká číslu PC, jsou IP adresy rozděleny do tříd. Třídy sítí vidíme v tabulce, která ukazuje kolik čísel ze čtveřice je vyhrazeno pro určitý typ adresy (čím více bajtů je věnováno adrese sítě, tím více sítí můžeme adresovat, ale tím méně číslic zbude na adresy počítačů v síti a naopak). Vše ještě přibližuje obrázek.



Obrázek 2.7: Třídy TCP/IP

IP adresy byly poprvé použity v Internetu a až později se začaly používat v lokálních sítích. Aby nedocházelo ke konfliktům adres (mezi IP adresami lokálních sítí a adresami internetovými), byly v každé třídě IP adres vymezeny pro lokální síť adresové rozsahy. Jsou to:

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

Tabulka 2.5: Třídy sítí IP

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

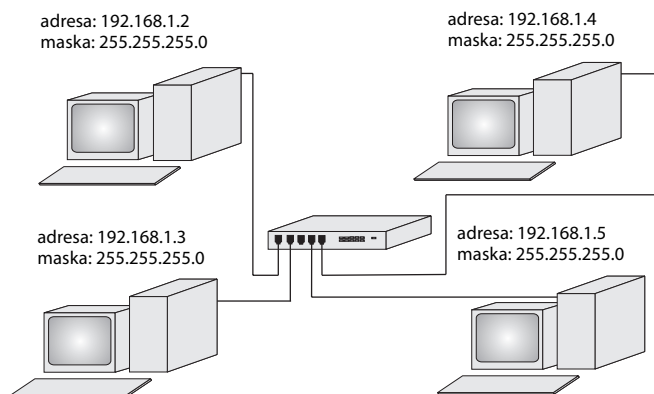
Jak vidíme v tabulce, je IP adresa navržena variabilně, adrese sítě je možné vyhradit 1 až tři číslice (neboli bajty). Abychom poznali, která část adresy je síťová, je nedílnou součástí IP adresy také **síťová maska**. Maska je opět čtyřbajtové číslo, vycházející přirozeně z dvojkové soustavy. V masce jsou na místě síťové adresy vždy zapsány jedničky (vyjadřujeme se dvojkově).

Pro IP adresy vyhrazené lokálním sítím se používají standardní síťové masky:

- ◆ pro **třídou A**, kde je adrese sítě určen první bajt (první číslo), je binární tvar masky 11111111.00000000.00000000.00000000, hexadecimální FF.00.00.00 a dekadický 255.0.0.0,

- ◆ pro **třídě B**, kde jsou adresy sítě určeny první dva bajty (první dvě čísla), je binární tvar masky 11111111.11111111.00000000.00000000, hexadecimální FF.FF.00.00 a dekadický 255.255.0.0,
- ◆ pro **třídě C**, kde jsou adresy sítě určeny první tři bajty (první tři čísla), je binární tvar masky 11111111.11111111.11111111.00000000, hexadecimální FF.FF.FF.00 a dekadický 255.255.255.0.

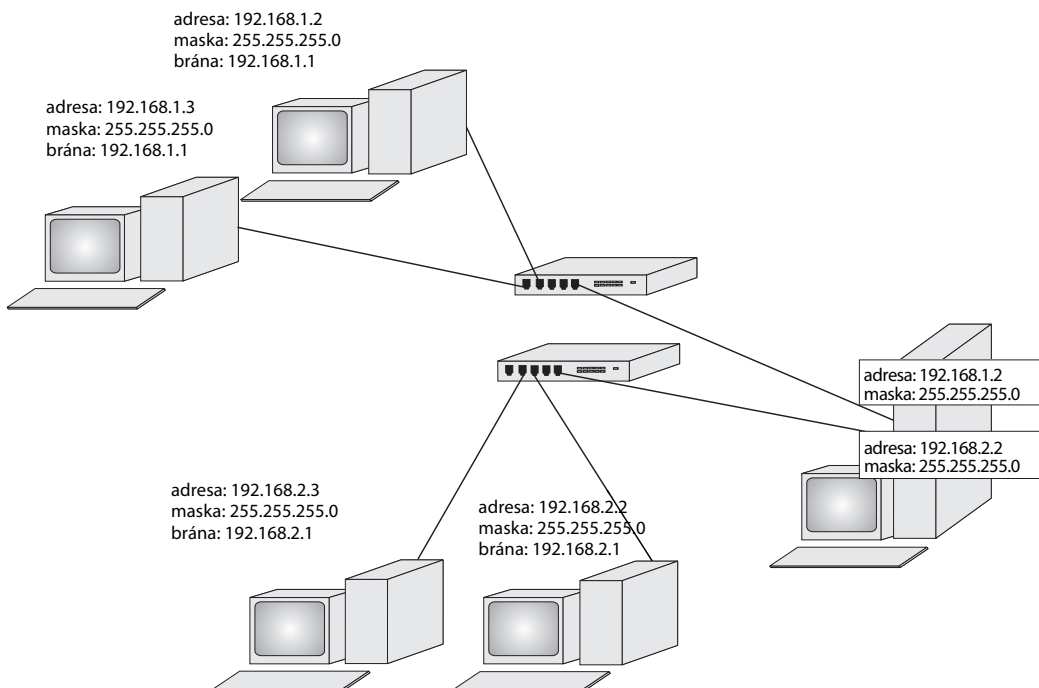
Na obrázku vidíte malou síť a její konfiguraci protokolem TCP/IP. Jde o jednu síť, se síťovou adresou 192.168.1 (třída C). V síti jsou čtyři uzly (počítače) s adresami 192.168.1.2, 192.168.1.3, 192.168.1.4 a 192.168.1.5. Každý počítač má tedy svou originální adresu a ke každé adrese patří síťová maska 255.255.255.0 odpovídající třídě C.



Obrázek 2.8: Adresace v síti TCP/IP

Propojování sítí TCP/IP

Již jsme se několikrát zmínili o tom, že počítače zapojené v síti nekomunikují pouze v rámci vlastní sítě, ale je také možná výměna dat s počítači umístěnými v jiné síti. Kvůli mezisítové komunikaci obsahuje IP adresa další údaj – **bránu (gateway)**. Brána je nepovinnou částí adresy, kterou potřebujeme pouze při výměně dat mezi dvěma sítěmi. Jde opět o číselný údaj stejného formátu jako IP adresa (můžeme ji vyjádřit dvojkově, šestnáctkově i desítkově). Brána je IP adresou, na niž budou směřovány pakety v případě, že jejich adresa bude mimo rozsah vlastní sítě – budou-li posílány na adresu jiné sítě než té, z níž jsou vysílány. Vše nejlépe pochopíme z obrázku 2.9. Jsou zde dvě sítě TCP/IP: první s rozsahem adres 192.168.1.x a druhá má rozsah 192.168.2.x. Součástí každé sítě je ještě jedna síťová karta počítače, kterým jsou obě sítě spojeny. Tento počítač pak plní funkci brány spojující obě sítě. Na síťových stanicích je zadána brána – číslo síťové karty, kam budou mířit datové pakety v případě, že jejich cílová adresa není obsažena v síti, z níž byly vyslány. Software počítače – brány pak zajistí převod mezi oběma kartami.



Obrázek 2.9: Propojování sítí TCP/IP

DHCP a DNS

Závěrem se ještě zmíním o dvou pojmech, které s adresací TCP/IP úzce souvisejí. Nepoužívají se však vždy a při konfiguraci malých sítí LAN se s nimi setkáme pouze okrajově:

- ◆ **DHCP (Dynamic Host Configuration Protocol).** Automaticky přiděluje IP adresy. Bývá nabízen jako služba síťového operačního systému – je to tedy program spuštěný na serveru (tzv. server DHCP). Po připojení stanice do sítě jí je serverem přidělena IP adresa.
- ◆ **DNS (Domain Name System).** Tato služba byla vyvinuta pro Internet, v němž má každý počítač svou IP adresu, ale počítačů je mnoho a bylo by nemožné zapamatovat si, pod jakým číslem jsou skryty hledané údaje. Proto existuje DNS, která převádí čísla na lépe zapamatovatelné názvy. DNS rozděluje počítače do zón nazývaných domény. (Například všechny počítače v ČR jsou zařazeny do domény .cz.) Domény se dále řadí do stromové struktury. DNS zadáváme tehdy, když počítač připojujeme k Internetu a musíme zadat IP adresu alespoň jednoho serveru, který DNS převod provede.

Informace o nastavení protokolu TCP/IP

Pro zjištění základních informací o nastavení TCP/IP je ve Windows XP Vista a Windows 7 k dispozici příkaz *IPCONFIG*.

- ◆ Ve Windows XP poklepnáním na tlačítko *Start* → *Spustit*, v okně *Spustit* zadáme příkaz *cmd*.
- ◆ Ve Windows Vista poklepnáním na tlačítko *Start*, v řádku *Zahájit hledání* zadáme příkaz *cmd*.

(Okno *Spustit*, respektive *Zahájit hledání*, vyvoláme také rychlou volbou – současným stiskem kláves *Windows* a *R*.) Po zadání *cmd* máme k dispozici okno příkazové řádky, kam napíšeme příkaz *ipconfig* a následně vidíme základní údaje o TCP/IP. Chceme-li získat informace detailní, přidáme ještě parametr *all*, příkaz bude mít tvar *ipconfig /all*.

```

E:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Verze 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

E:\Documents and Settings\Jarda>ipconfig

Konfigurace protokolu IP systému Windows

Adaptér sítě Ethernet Připojení k místní síti 3:

    Přípona DNS podle připojení . . . . . : lan
    Adresa IP . . . . . : 10.0.0.1
    Maska podsítě . . . . . : 255.255.255.0
    Účchozí brána . . . . . : 10.0.0.138

E:\Documents and Settings\Jarda>ipconfig /all

Konfigurace protokolu IP systému Windows

    Název hostitele . . . . . : jarduwxp
    Primární přípona DNS . . . . . : 
    Typ uzlu . . . . . : neznámý
    Povolení směrování IP . . . . . : Ne
    WINS Proxy povoleno . . . . . : Ne
    Prohledávací seznam přípon DNS . . . : lan

Adaptér sítě Ethernet Připojení k místní síti 3:

    Přípona DNS podle připojení . . . . . : lan
    Popis . . . . . : Realtek RTL8139 Family PCI Fast Ethernet NIC
    Fyzická adresa . . . . . : 00-13-D3-98-61-05
    Protokol DHCP povolen . . . . . : Ano
    Automatická konfigurace povolena : Ano
    Adresa IP . . . . . : 10.0.0.1
    Maska podsítě . . . . . : 255.255.255.0
    Účchozí brána . . . . . : 10.0.0.138
    Server DHCP . . . . . : 10.0.0.138
    Servery DNS . . . . . : 10.0.0.138
    Zapůjčeno . . . . . : 25. prosince 2005 23:40:24
    Zápůjčka vyprší . . . . . : 26. prosince 2005 1:40:24

E:\Documents and Settings\Jarda>

```

Obrázek 2.10: Příkaz ipconfig /all – Windows XP

```

C:\Windows\system32\cmd.exe
C:\Users\Jarda>ipconfig /all

Konfigurace protokolu IP systému Windows

    Název hostitele . . . . . : Jarda-PC
    Primární přípona DNS . . . . . : 
    Typ uzlu . . . . . : hybridní
    Povolení směrování IP . . . . . : Ne
    WINS Proxy povoleno . . . . . : Ne
    Prohledávací seznam přípon DNS . . . : lan

Adaptér sítě Ethernet Připojení k místní síti:

    Přípona DNS podle připojení . . . . . : lan
    Popis . . . . . : Intel 21140-Based PCI Fast Ethernet Adapter
    Fyzická adresa . . . . . : 00-03-FF-9F-61-05
    Protokol DHCP povolen . . . . . : Ano
    Automatická konfigurace povolena : Ano
    Spojení - místní adresa IPv6 . . . . . : fe80:98f7:16e1:301:e4f3:8<Přeferované>
    Adresa IPv4 . . . . . : 10.0.0.2<Přeferované>
    Maska podsítě . . . . . : 255.255.255.0
    Zapůjčeno . . . . . : 24. října 2007 21:03:23
    Zápůjčka vyprší . . . . . : 24. října 2007 23:03:23
    Účchozí brána . . . . . : 10.0.0.138
    Server DHCP . . . . . : 10.0.0.138
    IALD DHCPv6 . . . . . : 134218751
    Servery DNS . . . . . : 10.0.0.138
    Rozhraní NetBIOS nad protokolem TCP/IP . . . . . : Povoleno

Adaptér pro tunelové připojení Připojení k místní síti*:

    Přípona DNS podle připojení . . . . . : lan
    Popis . . . . . : Microsoft ISATAP Adapter
    Fyzická adresa . . . . . : 00-00-00-00-00-00-E0
    Protokol DHCP povolen . . . . . : Ne
    Automatická konfigurace povolena : Ano
    Spojení - místní adresa IPv6 . . . . . : fe80:5efe:10.0.0.2%12<Přeferované>
    Účchozí brána . . . . . : 
    Servery DNS . . . . . : 10.0.0.138
    NetBIOS nad TCP/IP . . . . . : zakázáno

C:\Users\Jarda>

```

Obrázek 2.11: Příkaz ipconfig /all - Windows Vista, velmi podobně vypadá také obrazovka Windows 7

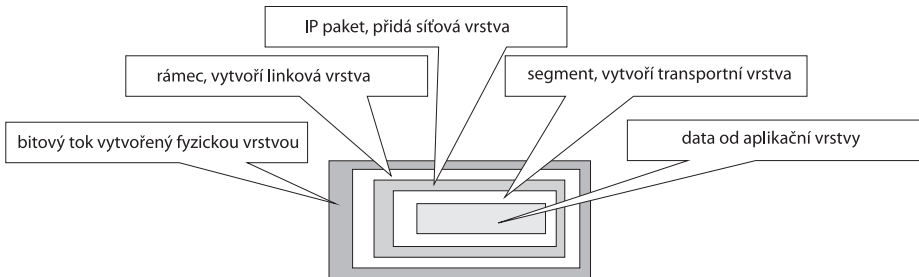
A co dál

Na obrázku vidíme, že protokoly TCP/IP vůbec neznají linkovou a fyzickou vrstvu, definovanou standardem ISO/OSI. Práci těchto dvou vrstev však musí někdo udělat. V soustavě TCP/IP to zůstává na hardwaru. Ten pracuje také podle určitých norem. Těmi jsou v sítích LAN téměř vždy standardy *ethernetu*, o němž již byla řeč (viz *Standardy síťového hardwaru*).

ISO / OSI	TCP / IP
aplikační	aplikační
prezentační	
relační	
transportní	transportní
síťová	síťová
linková	Ethernet
fyzická	

Obrázek 2.12: Souvislost mezi standardem ISO/OSI a sadou protokolů TCP/IP

Soustava protokolů TCP/IP (která je téměř vždy realizována softwarově) vytvoří pakety IP, které předá hardwaru (ten je v počítači představován síťovou kartou). Karta (její linková vrstva) paket přebere, přidá k němu svoje poznámky – vytvoří tak *ethernetový rámec*. Ethernetový rámec přebere fyzická vrstva a převede jej na elektrické (nebo optické) impulsy – tzv. *bitový tok*. Celému systému práce se říká zapouzdření a představu zapouzdřených dat vidíte na obrázku.



Obrázek 2.13: Zapouzdření

Fyzická adresa (MAC)

Paket IP používá logické IP adresy, ale linková vrstva a její rámec používají fyzické adresy – MAC adresy (Media Access Control address). Jde o unikátní adresu síťové karty, kterou u ethernetových karet zadává již ve výrobě. Adresa je šestibajtová, první tři bajty identifikují výrobce (každý výrobce má přiděleno svoje číslo) a druhé tři bajty přiděluje svým výrobkům sám výrobce. Je tak zabezpečeno to, že neexistují dvě stejné MAC adresy. Hodnotu MAC adresy vaší síťové karty zjistíte příkazem `ipconfig /all`, na obrázcích s výpisem příkazu `ipconfig` ji najdete v řádce Fyzická adresa.



Obrázek 2.14: Představa MAC adresy