POČÍTAČOVÉ SÍTĚ

1 Úvod

1.1 *Definice*

Pojmem počítačová síť se rozumí seskupení alespoň dvou počítačů, vzájemně sdílejících své zdroje, ke kterým patří jak hardware tak software. Předpokládá se sdílení *inteligentní*. Počítač, který poskytuje sdílení ostatním počítačům má možnost řízení přístupu ke sdíleným prostředkům. Z hlediska velikosti není síť nijak omezena. Pod pojem počítačová síť jsou zahrnuty i ostatní technické prostředky, které realizují spojení a komunikaci mezi počítači. Umožňují uživatelům komunikaci podle určitých pravidel, za účelem sdílení a využívání společných zdrojů nebo výměnu zpráv.

1.2 *Rozdělení sítí*

1. *podle rozlohy*
   a) LAN – (Local Area Network) lokální počítačová síť, je vytvořena na omezeném prostoru, pro jednu firmu, budovu lokalitu.
   b) WAN – (Wide Area Network) rozlehlá počítačová síť, více propojených vzdálených lokálních sítí. Nerozlehlejší je Internet.
   c) MAN – (Metropol Area Network) městská počítačová síť, menší než MAN, větší než LAN
   d) HAN – (Home Area Network) domácí počítačová síť, nový pojem zaváděný v souvislosti vznikajících domácích sítí
   e) PAN – (Personal Area Network) osobní počítačová síť, sítě vznikající propojováním PC nebo notebooku s telefonem nebo PDA. Tyto sítě jsou většinou bezdrátové infra nebo bluetooth.

Protože mezistupeň – městské sítě MAN – není charakteristický žádným výrazným specifickým rysem, mnozí autoři jej vůbec neuvádějí a zahrnují jej převážně pod sítě WAN. Připustíme-li přičlenění MAN do WAN jako podskupinu, zbývají výrazněji odlišné kategorie. Jejich odlišnosti shrnuje následující tabulka.

	LAN	WAN
kvůli čemu se zřizují	spíše pro potřeby sdileni	spíše pro potřeby komunikace
přenosová rychlost	vyšší (např. 10 až 100 Mbps)	nižší (např. 64 kbps)
topologie sítě	systematická (pravidelná)	nesystematická (nepravidelná)
vlastnictví přenosové infrastruktury	vlastni provozovatel	provozovatel si pronajímá
charakter uzlů	„menší“, převažují pracovni stanice	„větší“, převažují servery
dostupnost uzlů	„občas“ (podle potřeb uživatelů)	trvale
přenosové zpoždění	malé	velké
spolehlivost přenosových cest	vyšší	nižší

Hranice mezi LAN a WAN není ostrá a rozdíly mají tendenci se stále zmenšovat, což se projevuje např. v tom, že sítě LAN se zvětšují a sítě WAN se zrychlují. Je zřetelný trend neustálého zmenšování rozdílu mezi oběma kategoriemi sítí. V blízké budoucnosti bude zřejmě uživateli jedno, zda pracuje v síti LAN či WAN, všude bude mít stejné služby a bude používat stejný styl práce a tím si nebude muset uvědomovat rozdíl mezi LAN a WAN.

2. *podle topologie*
   a) sběrnicová – počítače jsou propojeny jedním kabelem
   b) hvězdicová – počítače jsou propojeny přes rozbočovací prvek paprskovitě
   c) kruhová – počítače jsou propojeny zpravidla jedním vedením do kruhu (fyzický nebo logický kruh)
   d) stromová – vícenásobná hvězdicová síť
3. *podle přenosové rychlosti*
   a) 10 Mbps sítě
   b) 100 Mbps sítě (Fast Ethernet)
   c) 1000 Mbps sítě (Gigabitový Ethernet)
4. *podle využití*
   a) PSIS – počítačové sítě v informačních systémech
   b) PSPA – počítačové sítě v průmyslových aplikacích
5. *podle standardu*
   a) Ethernet
   b) ARCnet
   c) Token Ring
   d) FDDI a další
6. *podle metody přístupu*
   a) náhodný přístup (stochastický), tzv. metoda kolize
   b) řízený přístup (deterministický), pomocí tzv. tokenu
7. *podle použití serveru (postavení uzlu v síti)*
   a) síť peer - to – peer, všechny počítače (uzly) si jsou rovny(symetrické postavení), nabízí si služby mezi sebou
   b) síť klient – server, server je zabezpečený počítač nabízející celou řadu služeb klientským počítačům. Servery mají speciální síťový operační systém a zabezpečení, klientům jsou definována práva.

	Síť serverového typu	Síť peer-to-peer
postavení uzlů sítě	asymetrické	symerické
umístění sdílených zdrojů	na jednom místě (na centrálním serveru)	na více místech (u vlastníků)
optimalizováno na	rychlost a výkon	jednoduchost
předpokládá se správce sítě	ano	ne
cena odvozena od počtu	uživatelů	uzlů

8. *podle komunikace*
   a) sítě spojové – před zahájením výměny dat je mezi oběma koncovými stanicemi navázáno spojení (telefonní sítě).
   b) sítě nespojové – spojení se nenavazuje, data jsou vysílána do sítě a jsou filtrována a směrována k cíli.
9. *podle způsobu propojení*
   a) metalické (drátové) – propojení je pomocí koaxiálního kabelu nebo kroucenou dvojlinkou
   b) optické – propojení je pomocí optických kabelů
   c) bezdrátové (wireless)

1.3 *Důvody vytváření počítačových sítí*

1. sdílení technických prostředků
- diskového prostoru
- tiskáren
- skenerů
- plotrů

2. sdílení programových prostředků
- databáze
- vzdálené zavádění OS
- instalační programy
- přenos dat

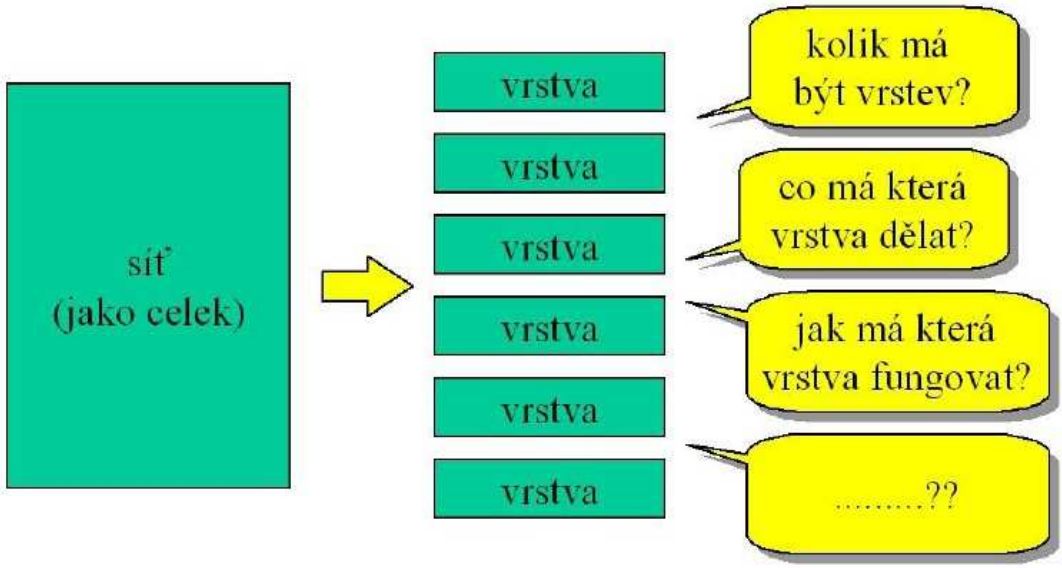
3. komunikace

4. ochrana dat
- 1. úroveň – uživatelské jméno a heslo
- 2. úroveň – seznam přístupových práv
- 3. úroveň – sledování provozu sítě

2 Modely a architektury počítačových sítí

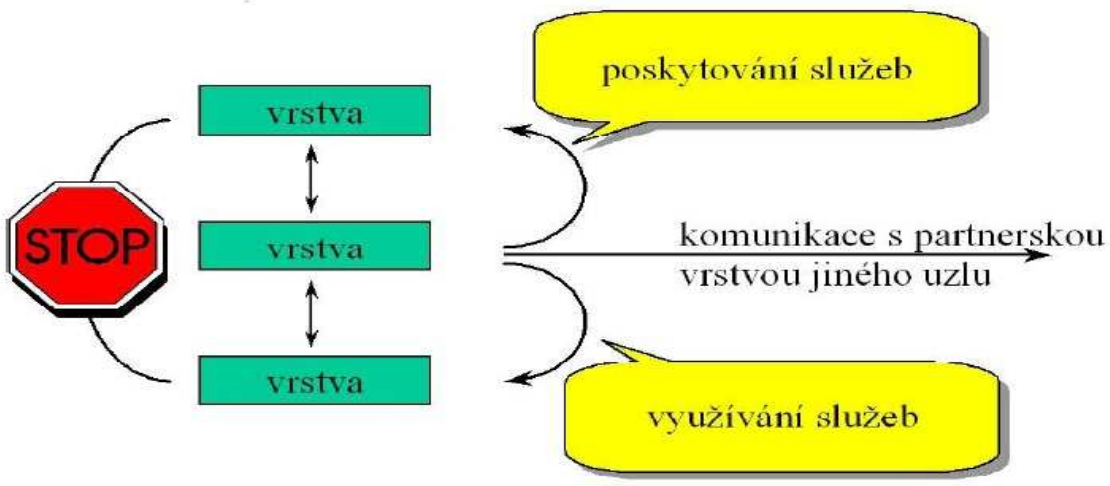
2.1 Úvod

Vytvořit jeden funkční celek počítačové sítě, který by fungoval od aplikace (např. internetový prohlížeč) až po elektrické signály generované síťovou kartou do přenosového média, by bylo velmi složité. K řešení celého problému se přistupuje procesem dekompozice. Jeden velký problém rozdělíme na více dílčích problémů, které se řeší postupně. Tím vznikly v modelech počítačových sítí hierarchicky uspořádané vrstvy, které mají své specifické úkoly (viz obr.1).



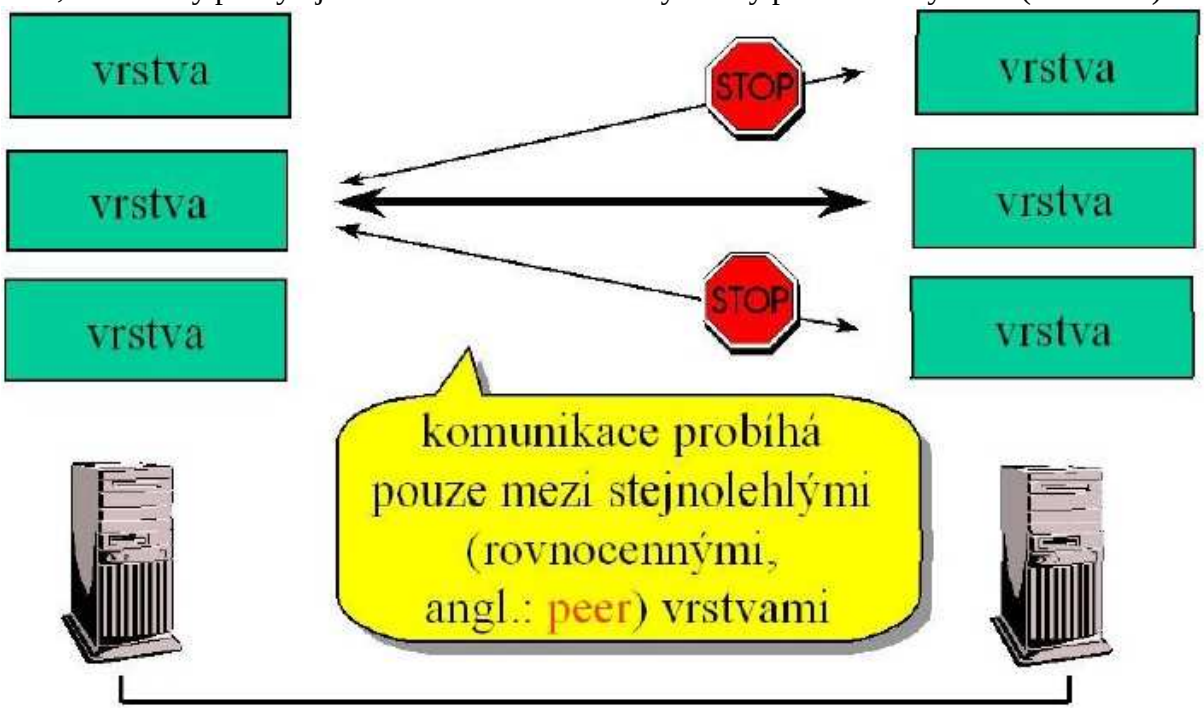
Obrázek 1 Dekompozice sítě na vrstvy

V rámci dekompozice problému do vrstev je nutné definovat pro jednotlivé vrstvy pravidla. Pravidla se týkají komunikace stejnolehlých vrstev u různých uzlů sítě (uzel sítě je uživatelský počítač – user, počítač, který služby poskytuje – server, nebo router – směrovač), komunikace mezi vrstvami nad sebou, úkoly jednotlivým vrstvám. Několik takových pravidel vysvětlí následující obrázky.



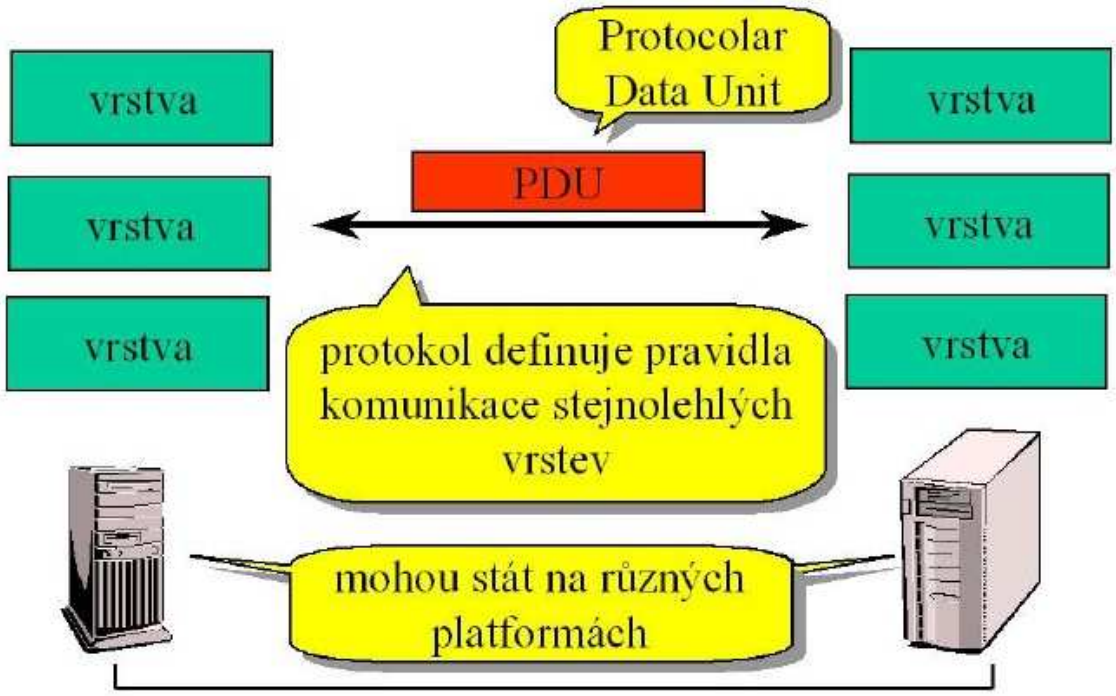
Obrázek 2 Komunikace mezi vrstvami

Konkrétní vrstva může komunikovat prostřednictvím protokolu se stejnolehlou vrstvou jiného uzlu, své služby poskytuje vrstvě nad sebou a služby vrstvy pod sebou využívá (obr. 2 a 3).



Obrázek 3 Komunikace mezi stejnolehlými vrstvami

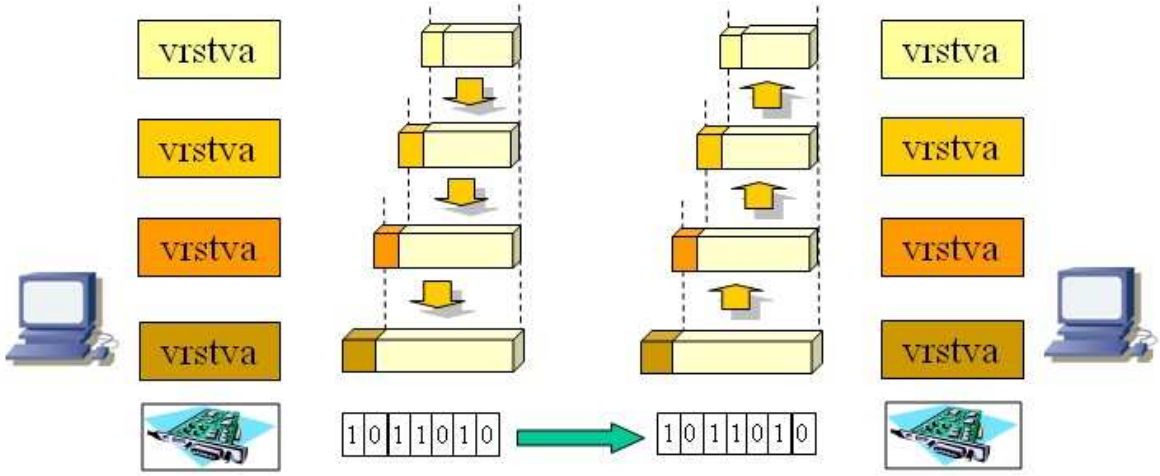
Vrstvy mezi sebou komunikují prostřednictvím protokolu (Protocolar Data Unit). Protokol definuje pravidla komunikace stejnolehlých vrstev, aniž by řešil detaily implementace. Z toho vyplývá, že komunikující uzly mohou pracovat na různých platformách (obr. 4).



Obrázek 4 Protokol

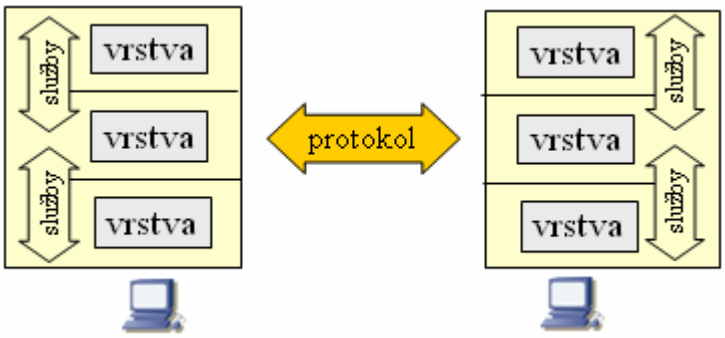
Komunikující uzly v počítačové síti si navzájem předávají data (PDU – rámce, pakety, segmenty). PDU se při odesílání z uzlu postupně předávají nižší vrstvě až nejnižší (fyzická)

vrstva odešle data. PDU je v každé vrstvě doplněn řídícími informacemi v hlavičce. Tyto informace využívá stejnolehlá vrstva uzlu, který data přijímá (obr. 5.).



Obrázek 5 PDU

Z uvedených obrázků můžeme vidět, že vrstvy mezi sebou komunikují vertikálně nebo horizontálně (obr.6).
Vertikální komunikace probíhá mezi vrstvami jednoho uzlu. Tuto komunikaci nazýváme služby (angl. services). Služby jsou poskytovány prostřednictvím rozhraní mezi vrstvami (např. porty TCP/IP).Služby ani rozhraní nejsou „vidět“ vně uzlu.Způsob realizace služeb, ani rozhraní nemusí být standardizováno.
Horizontální komunikaci nazýváme protokoly (angl. protocols). Probíhá mezi stejnolehlými vrstvami různých uzlů. Protokoly jsou „vidět“ z vně daného uzlu. Musí být standardizovány.



Obrázek 6 Služby a protokoly

2.2 Síťový model a architektura

Síťový model je ucelená představa o tom, jak mají být sítě řešeny. Zahrnuje představu o počtu vrstev a o tom, co má mít která vrstva na starosti. Nezahrnuje konkrétní představu o tom, jak má své úkoly plnit. Příkladem je referenční model ISO/OSI. Síťová architektura zahrnuje navíc konkrétní představu o fungování jednotlivých vrstev tj. obsahuje konkrétní protokoly. Příkladem síťové architektury je TCP/IP.

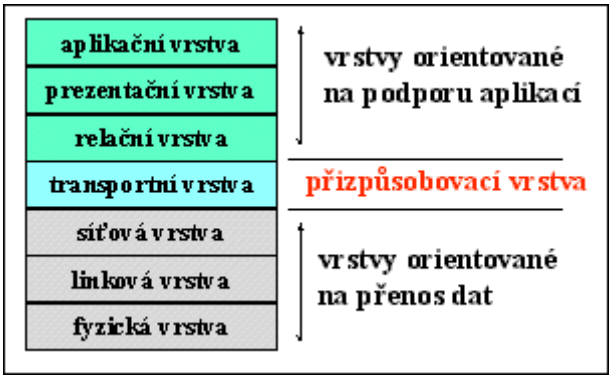
2.3 Síťový model ISO/OSI

První počítačové sítě v dnešním slova smyslu, pro rutinní provozování na komerčním principu a nikoli pro experimentální účely, se začínají budovat někdy v polovině 70. let, kdy se také na trhu objevují první produkty určené pro tyto sítě. Problém byl ale v tom, že byly ryze proprietární (tj. specifické pro konkrétního výrobce) a neumožňovaly vzájemnou interoperabilitu (schopnost systému vzájemně si poskytovat služby a efektivně

spolupracovat). Jednalo se o řešení, uvedená na trh velkými firmami (tehdy hlavně IBM a DEC) . To, co velmi brzy začalo chybět, byla taková síťová architektura, která by byla dostatečně otevřená, tedy nezávislá na konkrétním výrobci, široce dostupná ve svých specifikacích, umožňující požadovanou kompatibilitu a vzájemnou interoperabilitu řešení od různých výrobců a otevírající prostor konkurenci.
Úkolu vypracovat takovouto nezávislou architekturu se nakonec dobrovolně ujala mezinárodní standardizační organizace ISO (International Standards Organization, správně: International Organization for Standardization), sdružující národní standardizační organizace většiny vyspělých zemí světa. Zpočátku byl její záměr takový, že vypracuje jednotný standard pro fungování otevřených systémů - tedy vlastně pro fungování všech počítačů jako takových, aniž by se nutně muselo jednat o uzly zapojené do nějaké sítě. Mělo se to jmenovat "Open Systems Architecture" (doslova: architektura otevřených systémů), ale samozřejmě se brzy ukázalo, že něco takového je nad tehdejší možnosti (a určitě i dnešní, nehledě již na účelnost). Proto lidé z organizace ISO poněkud slevili, zejména v tom ohledu, že se nebudou zabývat fungováním počítačů jako takových, ale pouze tím, co se týká jejich vzájemné komunikace. Z honosného projektu "Open Systems Architecture" se tak stalo realističtější "Open Systems Interconnection Architecture" (doslova: architektura vzájemného propojování sítí). Nakonec však bylo nutné něco slevit i z této omezené představy - důvodem totiž byl zejména styl práce lidí z organizace ISO, kteří nepovažovali za možné přejímat jinde vyvinutá a jinde standardizovaná řešení, ale připouštěli pouze to, co sami schválí a vydají jako vlastní standard (takže vlastně nedůvěřovali v kompetentnost kohokoli jiného). Díky tomu, i díky dalším faktorům, se postup prací natolik zpomalil, že se záhy ukázalo jako nezbytné opět něco slevit: nevydávat vše jako skutečnou síťovou architekturu, tedy včetně všech protokolů, ale pouze jako určitý prázdný rámec - jako představu o tom, kolik má být hierarchických vrstev a co mají dělat, ale bez konkrétních protokolů, které by do těchto vrstev "zapadaly" (s tím, že tyto protokoly budou dopracovávány postupně podle toho, jak budou pokračovat práce na jejich vývoji). Konkrétním výsledkem pak musela být i další změna názvu. Z přechodného "Open Systems Interconnection Architecture" se posléze stal "Reference Model for Open Systems Interconnection" (doslova "referenční model pro propojování otevřených systémů"). Přitom slovní spojení "referenční model" je zde použito právě pro zdůraznění toho, že jde o obecnou koncepci, vzor, rámec resp. model (a nikoli o konkrétní a striktně definovaný předpis), který bude teprve postupem času naplňován konkrétními návody (protokoly) podle toho, jak tyto budou dostupné.

Sedm vrstev ISO/OSI

Autoři referenčního modelu ISO/IOSI dospěli k závěru, že hierarchických vrstev, které zajistí fungování sítě, by mělo být sedm. Rozdělili je přitom do dvou velkých bloků po třech vrstvách, mezi kterými je jedna"přizpůsobovací" vrstva. Blok tří spodních vrstev je přitom zaměřen na přenos dat v síti, zatímco blok tří vyšších vrstev je naopak zaměřen na potřeby jednotlivých aplikací a snaží se jim poskytovat potřebnou podporu. Přizpůsobovací vrstva mezi oběma bloky pak má vyrovnávat rozdíly mezi možnostmi bloku nižších vrstev, a potřebami bloku vyšších vrstev. Tento cíl asi nejlépe dokresluje představa, kterou autoři celého referenčního modelu zastávali: předpokládali, že tři nejnižší vrstvy budou v praxi realizovány tzv. veřejnými datovými sítěmi (tj. sítěmi, které někdo provozuje proto, aby mohl pro své zákazníky přenášet jejich data - podobně jako to veřejná telefonní síť dělá s telefonickými hovory). Přitom uživateli takovýchto veřejných datových sítí měly být úplně jiné subjekty, které si nemohly diktovat své podmínky ohledně způsobu fungování datové sítě (proto byla zařazena příslušná přizpůsobovací vrstva).



Obrázek 7 Vrstvy ISO/OSI modelu

Proberme si nyní funkci jednotlivých vrstev referenčního modelu ISO/OSI postupně směrem od nejnižší vrstvy k té nejvyšší. Přitom nebudeme zapomínat na základní pravidlo komunikace mezi hierarchicky uspořádanými vrstvami, které říká, že každá vrstva sama využívá služeb své bezprostředně nižší vrstvy, sama plní určité úkoly (které si lze představit jako "přidanou hodnotu" ke službám nižší vrstvy) a výsledek pak nabízí své bezprostředně vyšší vrstvě jako služby k využití.

Fyzická vrstva (physical layer)

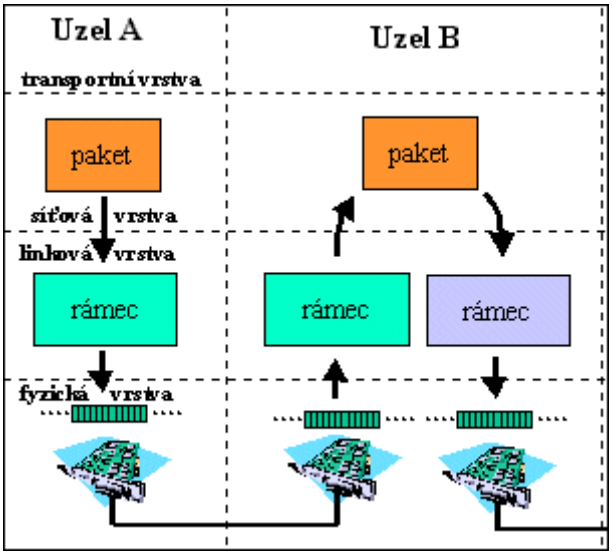
Úkolem fyzické vrstvy, která jako jediná nemá žádnou bezprostředně nižší vrstvu, je přenos jednotlivých bitů k přímým sousedům (sousedním uzlům, ke kterým vede přímé spojení). Fyzická vrstva se stará o to, aby každý bit byl přenesen korektním způsobem (aby jej příjemce správně rozpoznal a interpretoval), což mj. zahrnuje například otázky kódování, časování, modulace apod. Důležité přitom je, že fyzická vrstva nijak neinterpretuje přenášené bity, tj. nesnaží se jim přiřazovat nějaký význam (takže například nepozná, že nějaký bit je řídící a je třeba součástí něčí adresy, že je určitý bit součástí "čistých" dat apod.).

Linková vrstva (data link layer)

Linkové vrstva (někdy též "spojová vrstva") již může ke své činnosti využívat služeb bezprostředně nižší fyzické vrstvy, spočívající v přenosu jednotlivých bitů. Pomocí této služby pak linková vrstva realizuje přenos celých datových bloků, kterým se na této úrovni říká rámce (frames). Znamená to mj., že se tato vrstva musí postarat o správné rozpoznání začátku a konce každého rámce i jeho jednotlivých částí, včetně hlavičky a adres, které jsou v ní obsažené.
Důležité je, že podobně jako vrstva fyzická, dokáže vrstva linková přenášet své rámce jen k sousedním uzlům (neboli k uzlům, se kterými má přímé spojení). V prostředí lokálních sítí funguje na této úrovni například dobře známý ethernet.

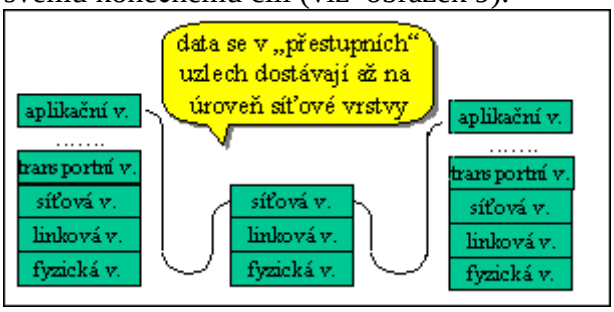
Síťová vrstva (network layer)

Hlavním úkolem síťové vrstvy je tzv. směrování, neboli nalezení vhodné cesty vedoucí od odesilatele dat až k jejich koncovému příjemci. V praxi totiž nemusí být každá dvojice odesilatel/příjemce vždy sousední v tom smyslu, že by mezi nimi existovalo přímé spojení (tj. v "dosahu" linkové vrstvy). Častější je spíše případ, kdy mezi odesilatelem a koncovým příjemce vede cesta pouze přes několik jiných uzlů (přestupních, mezilehlých uzlů), V takovém případě je ale nutné najít potřebnou cestou přes mezilehlé uzly (právě v tom spočívá směrování, anglicky "routing") a potřebný přenos přes mezilehlé uzly fakticky realizovat.



Obrázek 8 Vkládání paketů do rámců

Také síťová vrstva přenáší data po blocích, kterým se říká pakety (anglicky "packets"), zatímco na úrovni linkové vrstvy se jim říká rámce. Představa fungování je taková, že síťová vrstva v určitém uzlu rozhodne o dalším směru, kterým by měl být konkrétní paket přenesen k některému ze sousedních uzlů. Poté jej předá své linkové vrstvě, která paket vloží do svého rámce (obr. 8) a přenese k příslušnému sousednímu uzlu. Zde jej partnerská linková vrstva vybalí a předá datový paket své bezprostředně vyšší síťové vrstvě. Ta rozhodne, kterým směrem by měl být paket dále odeslán …a vše se opakuje, dokud datový paket nedorazí ke svému konečnému cíli (viz obrázek 9).



Obrázek 9 Směrování paketu síťovou vrstvou

Transportní vrstva (transport layer)

Úkolem transportní vrstvy je přizpůsobení možností tří nejnižších vrstev (síťové, linkové a fyzické) představám vyšších vrstev. Konkrétní představy a možnosti se přitom mohou dotýkat různých věcí, ale nejčastěji jde o rozdíly ve spolehlivosti přenosových služeb a v jejich spojovaném či nespojovaném charakteru. Například otázka spolehlivosti se týká toho, co se má stát při výskytu nějaké chyby při přenosu. Pokud ten, kdo chybu zjistí, je také povinen postarat se o nápravu, pak jde o službu tzv. spolehlivou. Naopak nespolehlivou službou je takový případ, kdy ten, kdo zjistí určitou chybu, nemá za povinnost ji napravovat (ale může poškozená data jednoduše zahodit a pokračovat dál). Logika nespolehlivých služeb je v tom, že mají menší režii a dokáží přenášet data rychleji a pravidelněji, přičemž o případnou nápravu se mohou efektivněji postarat vyšší vrstvy (pokud to vůbec chtějí).
Dalším významným úkolem transportní vrstvy (kromě již naznačeného přizpůsobení) je i rozlišování různých příjemců a odesilatelů v rámci jednotlivých uzlů. Až do síťové vrstvy včetně se totiž všechny přenosy týkají jednotlivých uzlů jako celků (a také příslušné adresy identifikují pouze uzly jako celky). Teprve transportní vrstva jde dále a rozlišuje jednotlivé příjemce v rámci těchto uzlů.

Relační vrstva (session layer)

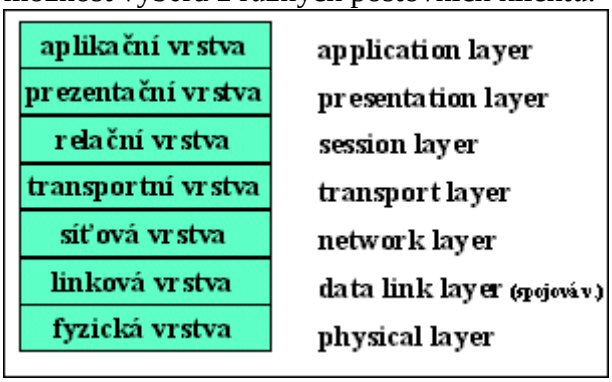
Relační vrstva je nejčastěji kritizovanou vrstvou referenčního modelu ISO/OSI, protože právě ona toho má co nejméně na práci v porovnání s ostatními vrstvami. Kromě toho je i docela nesnadné vysvětlit, co vlastně tato vrstva má dělat. Především má podporovat vedení relací. Ale co je to vlastně relace?
Lze ji přirovnat k dialogu, který může být veden například po telefonu (který zde odpovídá transportnímu spojení). Když se s někým po telefonu o něčem bavíte, náhle vám "spadne linka" a hovor je přerušen, vytočíte si volaného znovu a pokračujete v nedokončeném rozhovoru. Takže relace trvá nadále, ale může být realizována pomocí více transportních spojení. Může to být ale i naopak, pomocí jednoho transportního spojení může být realizováno více jednotlivých relací (například když dva telefonující pánové po svém rozhovoru předají sluchátka svým manželkám, které se baví o něčem úplně jiném).

Prezentační vrstva (presentation layer)

Až do úrovně prezentační vrstvy se všechny nižší vrstvy úzkostlivě snaží, aby přenesly data přesně v takové podobě, v jaké byly odeslány, tedy bit po bitu. Někdy ale jeden a tentýž řetězec bitů může mít pro různé uzly různý význam (například když každý z nich používá jiný způsob kódování znaků, je nutné provést potřebnou konverzi). A právě to je úkolem prezentační vrstvy. Obecně jde o to, aby přenesená data měla pro příjemce stejný význam, jaký měla pro odesilatele - a to nemusí obnášet zdaleka jen kódování textů. Týká se to například i znázornění čísel celých i čísel reálných a samozřejmě všech datových struktur atd.

Aplikační vrstva (application layer)

Původní představa o aplikační vrstvě byla taková, že v ní budou umístěny všechny aplikace používané v prostředí sítě. Později se ale od této představy poněkud ustoupilo, protože se to ukázalo jako prakticky neprůchodné. Důvodem je zejména skutečnost, že vše, co se nachází v určité vrstvě, musí být standardizováno (pokryto standardy), a tudíž i poměrně striktně "sešněrováno" co do způsobu fungování a dalších vlastností. Ovšem u konkrétních aplikací není žádoucí, aby jejich autoři byli příliš svazováni tam, kde to není nutné, tedy například při tvorbě uživatelských rozhraní či v tom, jak dalece vyjdou vstříc uživateli a jeho komfortu. Proto v aplikační vrstvě nakonec zůstaly pouze části aplikací - takové, které nutně musí být standardizovány - zatímco zbývající části aplikací byly vysunuty nad aplikační vrstvu (resp. zcela mimo rámec ISO/OSI). Asi nejlépe se tato představa ilustruje na příkladu elektronické pošty: v aplikační vrstvě zůstaly poštovní servery, které musí být standardizovány natolik, aby se mezi sebou dokázaly domluvit a předávat si zprávy takovým způsobem a v takovém formátu, kterému budou rozumět. Naproti tomu klientské programy el. pošty mohly být vysunuty nad aplikační vrstvu, což poskytlo potřebnou volnost jejich autorům a uživatelům možnost výběru z různých poštovních klientů.



Obrázek 10 Anglické názvy vrstev

Kritika ISO/OSI

Do vývoje referenčního modelu ISO/OSI bylo investováno opravdu mnoho prostředků a úsilí, bohužel s nepříliš velkým efektem. Celá koncepce ISO/OSI sice vznikala jako "ta jediná", "oficiální" či "ta správná" koncepce, podporovaly ji nejrůznějšími institucemi oficiálního charakteru, ale tržní síly nakonec rozhodly jinak. Prvotním důvodem byl zejména přístup autorů. Vše totiž vznikalo do značné míry od zeleného stolu, kdy se shromáždily určité požadavky na to, co by síť měla umět a po určité diskusi se tyto požadavky daly na papír a vydaly ve formě závazného standardu. Teprve poté se někdo začal zabývat tím, jestli je něco takového vůbec realizovatelné a pokud ano, jestli je to efektivní pro praktické použití a únosné z hlediska vývojových a výrobních nákladů. A zde obvykle nastal problém. Často se totiž zjistilo, že z původní představy je nutné značně slevit a vytvořit jen jakousi "rozumně implementovatelnou podmnožinu" příliš bohatého standardu. Hezkým příkladem jsou tzv. vládní profily OSI (GOSIP, Governmental OSI Profile). Když totiž státní instituce oficiálně propagovaly koncepci ISO/OSI jako jedinou správnou, musely ji vyžadovat i při všech nákupech síťového vybavení v okruhu své působnosti. K tomu ale musely specifikovat, co přesně mají na mysli (jako "podmnožinu"), aby výsledek byl alespoň vzájemně kompatibilní. Nabídka konkrétních produktů na platformě ISO/OSI však na trhu byla minimální, ne-li přímo nulová. A tak i autoři vládních profilů GOSIP časem připustili možnost použití produktů na bázi konkurenční koncepce TCP/IP. Celkově lze konstatovat, že koncepce ISO/OSI se prakticky vůbec neprosadila do praxe, která dala jednoznačně přednost koncepci TCP/IP (na které je mj. postaven i dnenší celosvětový Internet). Rozhodně to ale neznamená, že celé ISO/OSI patří na smetiště síťových dějin, to určitě ne. Kromě toho, že celá koncepce je velmi šikovná pro výuku problematiky síťování, je zde i mnoho dílčích řešení a myšlenek, které si přece jen našly svou cestou do praxe. Poměrně životaschopným se ukázal být například standard elektronické pošty X.400, který se dodnes používá a byly od něj odvozeny i některé komerčně velmi úspěšné systémy (například poštovní platforma MS Exchange firmy Microsoft). Podobně se ukázal být životaschopný i standard X.500 pro adresářové služby. Právě jeho zjednodušením a zmenšením vznikl protokol LDAP (Lightweight Directory Access Protocol) z rodiny TCP/IP, na kterém dnes funguje většina adresářových služeb v Internetu.

2.4 Síťová architektura TCP/IP

Úvod

V současných počítačových sítích dominuje rodina protokolů TCP/IP. Na této protokolové sadě funguje i největší počítačová síť Internet. Architektura TCP/IP pracuje na principu přepojování paketů alternativou je princip přepojování okruhů.

- **přepojováním okruhů** (*circuit switching*) – komunikace se odehrává po předem sestaveném okruhu (spojení) mezi zdrojovou a cílovou stanicí. Všechna data sledují jednu předem danou cestu sítí a jsou doručena ve správném pořadí. Komunikace v těchto sítích probíhá vždy spolehlivě, se spojením.
- **přepojováním paketů** (*packet switching*) – neexistuje sestavený okruh mezi zdrojovou a cílovou stanicí přes síť, místo toho se každý mezilehlý uzel (směrovač) na cestě rozhoduje, jakou cestou se paket pošle dál. Pakety se posílají individuálně, každý má ve svém záhlaví všechny potřebné informace pro přenos sítí (cílovou adresu, pořadí ve zprávě). Potenciálně tedy pakety nemusí sledovat stejnou cestu sítí a nemusí být doručeny k cíli v pořadí odeslání. Problematika skutečného doručení paketů, jejich duplicity a jejich pořadí je pak většinou záležitostí cílové stanice (málokdy se o tyto

funkce stará sama síť). Přepojování paketů lze realizovat se spojením (pak je cesta v rámci dané komunikace pro všechny pakety stejná) nebo bez spojení.

Historie TCP/IP

Počátky TCP/IP se datují do konce 60. let a jsou úzce spojeny s činností účelové agentury ARPA (Advanced Research Projects Agency) ministerstva obrany USA, která si nové protokoly nechala vyvinout pro svou počítačovou síť ARPANET. Na vývoji celé soustavy protokolů, financovaném prostřednictvím tzv. grantů ministerstva obrany (účelových dotací na výzkum) se pak podílela počítačově orientovaná pracoviště předních univerzit USA. Svou dnešní podobu získaly nové protokoly zhruba v letech 1977-79 a brzy poté na ně začala postupně přecházet i vlastní síť ARPANET, která se posléze stala zárodkem a páteří celého konglomerátu sítí, nazývaného dnes příznačně Internet. .
Agentura ARPA (mezitím přejmenovaná na DARPA) se pak snažila prosadit nově vytvořené protokoly (a vlastně i celou ucelenou síťovou architekturu) do praktického života i mimo síť ARPANET, především pak do akademického prostředí. Většina univerzitních počítačových pracovišť v USA v té době provozovala nějakou verzi tzv. BSD Unixu, pocházející ze střediska Berkeley Software Distribution (BSD) na University of California v Berkeley. Agentura DARPA si proto nechala u přední americké firmy Bolt, Beranek and man (BBN) na zakázku vyvinout implementaci TCP/IP protokolů pod operační systém Unix, a univerzitě v Berkeley přispěla výzkumnými granty na začlenění těchto protokolů do univerzitou distribuovaných produktů. Tím se protokoly TCP/IP prosadily do BSD Unixu, a posléze pak i do ostatních verzí Unixu buď přímo jako jejich standardní součást, nebo jako volitelný doplněk (option). Díky své popularitě se však záhy dostaly i na jiné platformy, a dnes jsou implementovány snad ve všech výpočetních prostředích, od osobních počítačů PC s operačním systémem MS DOS až např. po sálové počítače (mainframes) firmy IBM a operační systém VM. .
Pro svůj úzký vztah k síti Internet je soustava protokolů TCP/IP někdy označována také jako Internet protocol suite (doslova: soustava protokolů Internetu), nebo též Department of Defense (DoD) protocol suite, což naopak zdůrazňuje vztah k ministerstvu obrany USA.

Architektura TCP/IP

Architektura TCP/IP se zásadně liší od referenčního modelu ISO/OSI. Odlišnost je dána především okolnostmi při vzniku TCP/IP. Hlavní slovo měla akademická sféra nezatížená stereotypy telekomunikačních sítí. Tím byly dány hlavní zásady TCP/IP.

- budování „zdola nahoru“, důraz na praxi (nejprve se vytvoří funkční protokoly a ty se po ověření funkčnosti začlení do struktury architektury)
- snaha vytvářet jen ta řešení, která objektivně chybí (na rozdíl od ISO/OSI, který se snaží do svých standardů zahrnout všechna existující řešení a vytvořit tak komplexní sadu standardů);
- eliminování potřeby centrálního prvku sítě (síť by měla být schopna provozu i při výpadku kteréhokoli prvku);
- snaha přizpůsobit se předpokládaných výpadkům částí sítě a jejich nespolehlivosti.

Z těchto výchozích odlišností pak vyplývají odlišnosti v konkrétní stavbě architektury TCP/IP:

- nižší počet vrstev než ISO/OSI daný především tím, že většina aplikačně orientovaných funkcí byla v TCP/IP začleněna jako volitelná do aplikační

vrstvy, zatímco v referenčním modelu ISO/OSI je jejich část vyčleněna do relační a prezentační vrstvy;

- ponechání větší možnosti volby na všech vrstvách;
- přednost mají nespojovaná a nespolehlivá komunikace, při uplatnění principu „**best effort**“ (maximální snahy).

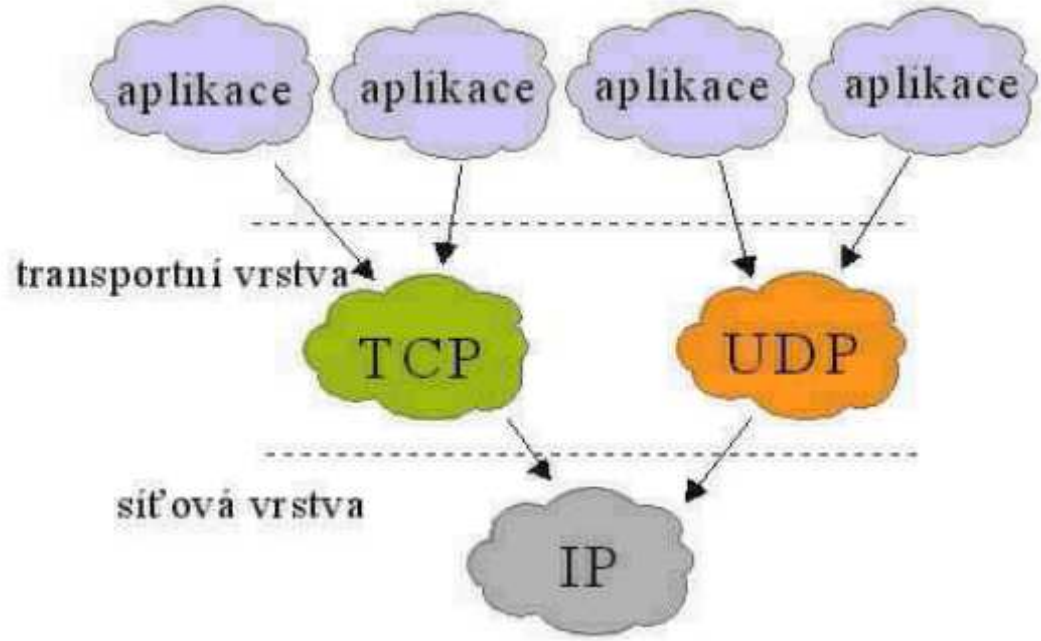
Z výše uvedených důvodů se architektura TCP/IP ustálila na 4 vrstvách, jak znázorňuje obrázek 11.

TCP/IP	ISO/OSI
aplikační vrstva	aplikační vrstva prezentační v. relační v.
transportní vrstva	transportní vrstva
síťová vrstva (IP vrstva)	síťová v.
vrstva síťového rozhraní	linková (spojová) v. fyzická v.

Obrázek 11 Vrstvy TCP/IP

Spolehlivá a nespolehlivá, spojovaná a nespojovaná komunikace.

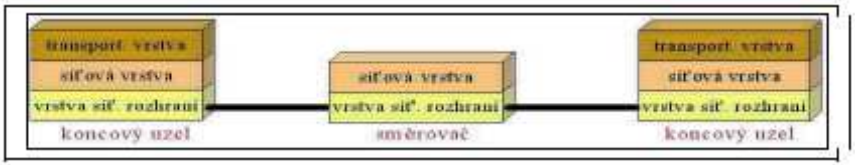
Architektura TCP/IP nabízí možnost spolehlivého či nespolehlivého, spojovaného či nespojovaného přenos dat. O tom, jaký typ přenosu se použije, rozhoduje aplikace volbou služby v transportní vrstvě. Spolehlivou spojovanou službu transportní vrstvy reprezentuje protokol TCP (Transmission Control Protocol), v opačném případě, tedy nespolehlivou nespojovanou službu protokol UDP (User Datagram Protocol)(viz obrázek 12).



Obrázek 12 Volba služby v transportní vrstvě aplikací

Je třeba připomenout, že nižší síťová vrstva s protokolem IP (Internet Protocol) již pracuje nespojově a nespolehlivě. Rozhodnutí tvůrců protokolové sady TCP/IP umožnit alternativní službu až na transportní vrstvě a ponechat služby síťové vrstvy pouze nespolehlivé a nespojované znamená, že spolehlivost se bude zajišťovat pouze na koncových uzlech. Na mezilehlých uzlech (nejčastěji směrovačích), které zahrnují pouze funkce vrstvy sítového

rozhraní a vrstvy síťové (viz obrázek 13), bude jedinou možnou službou nespolehlivý a nespojovaný přenos. Toto rozhodnutí je dosti zásadní pro celou koncepci budování TCP/IP sítí, protože to znamená, že síťová infrastruktura včetně mezilehlých uzlů (směrovačů) bude pracovat co nejjednodušeji a zároveň s maximálním omezením režie. Veškeré dodatečné služby (mezi něž zajištění spolehlivosti patří) budou implementovány pouze na koncových uzlech. Toto rozhodnutí je koncepčního charakteru zejména pro další rozvoj služeb TCP/IP sítí. Pokud totiž například nějaká budoucí verze protokolu TCP zdokonalí mechanismus zajištění spolehlivosti (či dokonce nahradí protokol TCP jiným), nebude nutné kvůli tomu provádět žádné změny na síťové infrastruktuře, postačí pouze změny v samotných koncových uzlech, kde se díky častější obměně hardware i operačních systémů provádějí snáze.



Obrázek 13 Rozdělení vrstev na mezilehlých a koncových uzlech

Vrstvy TCP/IP

Vrstva síťového rozhraní

Nejnižší vrstva, *Vrstva síťového rozhraní* (Network Interface Layer) má na starosti vše, co je spojeno s ovládáním konkrétní přenosové cesty 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 (koaxiální kabel, UTP, optická vlákna…Ethernet, Token ring….).

Síťová vrstva

Bezprostředně vyšší vrstva, která již není závislá na konkrétní přenosové technologii, je vrstva *Síťová*, v terminologii 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. Úkolem této vrstvy je dostat jednotlivé pakety od odesilatele 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.
Na této vrstvě pracují i další protokoly, např. ICMP, ARP, RARP.
Úkoly protokolů:
IP protokol je nespojovaný nespolehlivý protokol s částečnou detekcí chyb. Tato detekce se týká pouze kontrolního součtu hlavičky protokolu. IP protokol má tyto funkce:

- adresování stanic v internetové (síťové) vrstvě
- definice struktury IP datagramu
- směrování datagramů
- propojení internetové a transportní vrsty. Určitým protokolům jsou přiřazeny pevná čísla portů (TCP -6, UDP - 17)
- fragmentace a sestavení datagramů podle MTU - maximum Transfer Unit - maximální délka datagramu (Ethernet 1500B)

ICMP Internet Control Message Protokol přenáší zprávy o chybách a řídící zprávy (např. příkaz Ping). Je pevnou částí protokolu IP (využívá služeb IP) a proto je také nespolehlivý a nespojovaný protokol. Nejdůležitější zprávy jsou

1. Destination unreacheble - nedostupnost cílové stanice nebo služby
2. Source Quench - zpráva od příjemce nebo routeru pro zpomalení vysílání dat

3. Redirect požadavek brány nebo routeru na přímější cestu k cílové stanici - žádost o přesměrování
4. Echo request a echo replay - pro odezvu ping - určuje dostupnost stanice. - žádost o ozvěnu a odpověď s ozvěnou
5. Parametr problem - když je hlavička nečitelná (chybná) - chybný parametr

ARP (Address Resolution Protokol) zjišťuje fyzické adresy (MAC - Medium Access Control) podle logické IP adresy. Proto ARP vyšle paket s logickou IP adresou všem uzlům (broadcast) a ten, který ji u sebe najde předá zpět fyzickou adresu.

RAPR Reverse ARP - zjišťuje logickou adresu k fyzické (obdobně jako APR).

Transportní vrstva

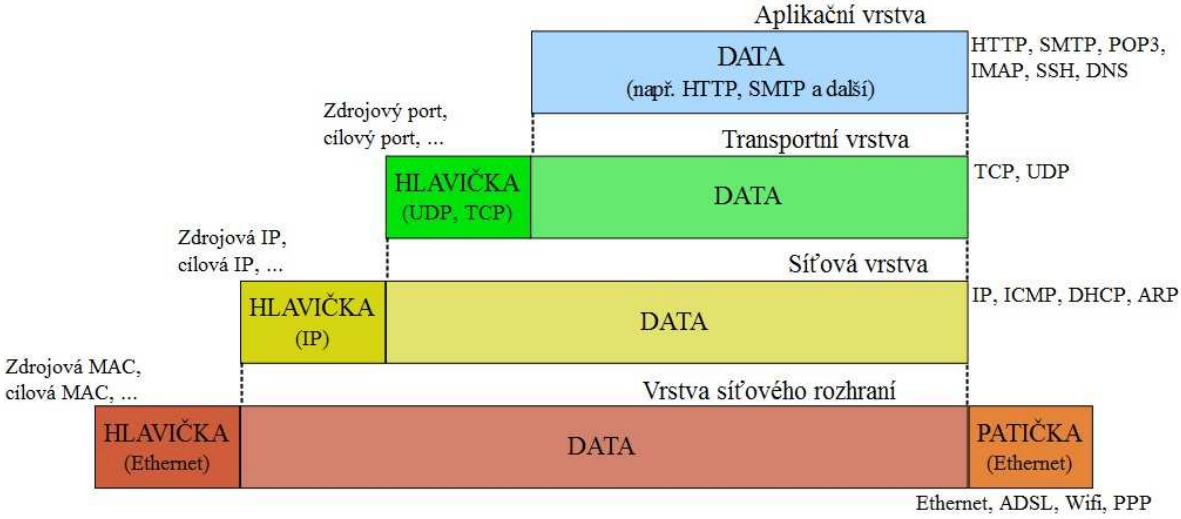
Třetí vrstva TCP/IP je označována jako *transportní vrstva* (Transport Layer), nebo též jako *TCP vrstva* (TCP Layer), neboť je nejčastěji realizována právě protokolem TCP (Transmission Control Protocol). Hlavním úkolem této vrstvy je zajistit přenos mezi dvěma koncovými účastníky, kterými jsou v případě 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.
Přestože je transportní vrstva TCP/IP nejčastěji zajišťována právě protokolem TCP, není to zdaleka jediná možnost. Dalším používaným protokolem na úrovni transportní vrstvy je protokol UDP (User Datagram Protocol), který na rozdíl od TCP nezajišťuje mj. spolehlivost přenosu - samozřejmě pro takové aplikace, které si to (na úrovni transportní vrstvy) nepřejí.

Aplikační vrstva

Nejvyšší vrstvou TCP/IP je pak vrstva *aplikační* (Application Layer). Jejími entitami jsou jednotlivé aplikační programy, které 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.

Encapsulace při odesílání dat

Při odesílání dat se provádí *encapsulace* (zapouzdřování - zabalování) od nejvyšší vrstvy dolů obr.14. Probíhá to tak, že aplikace vezme data (aplikační vrstva), která chce zaslat jiné stanici a doplní je o aplikační hlavičku. Tato data zašle nižší vrstvě (transportní), která odesílaná data rozdělí na segmenty, zabalí a přidá TCP (nebo UDP) hlavičku a vytvoří *TCP segment*. Další vrstva (síťová) doplní IP hlavičku a takto vznikne *IP paket* (někdy označovaný jako IP datagram). V poslední vrstvě (přístupové) se k paketu přidá ethernetová hlavička na začátek a trailer na konec, ten obsahuje *FCS* (Frame Check Sequence) - kontrolní součet (často se pro jeho výpočet používá CRC - cyclic redundancy check). Takto v posledním kroku vznikne *ethernetový rámec* (ethernet frame), který se vysílá na komunikační médium.
Pozn.: Výše uvedený popis se týkal protokolu IP, pokud se jedná o nějaký pomocný protokol (třeba ARP, ICMP), tak je situace obdobná.
Když cílové zařízení přijme data, provádí se obrácený postup *deencapsulace* (rozbalování) od nejnižší vrstvy nahoru a cílová aplikace dostane odesílaná data.



Obrázek 14 Zapouzdření

Paket vs. rámec

V souvislosti s daty a jejich přenosem po síti se používají dva důležité termíny, jsou to *paket* a *rámec*. Tyto termíny jsou hojně používány v literatuře, na internetu, i v praxi. Bohužel v literatuře existuje několik odlišných vysvětlení a také používání těchto výrazů je různé. My se budeme držet těchto definicí.

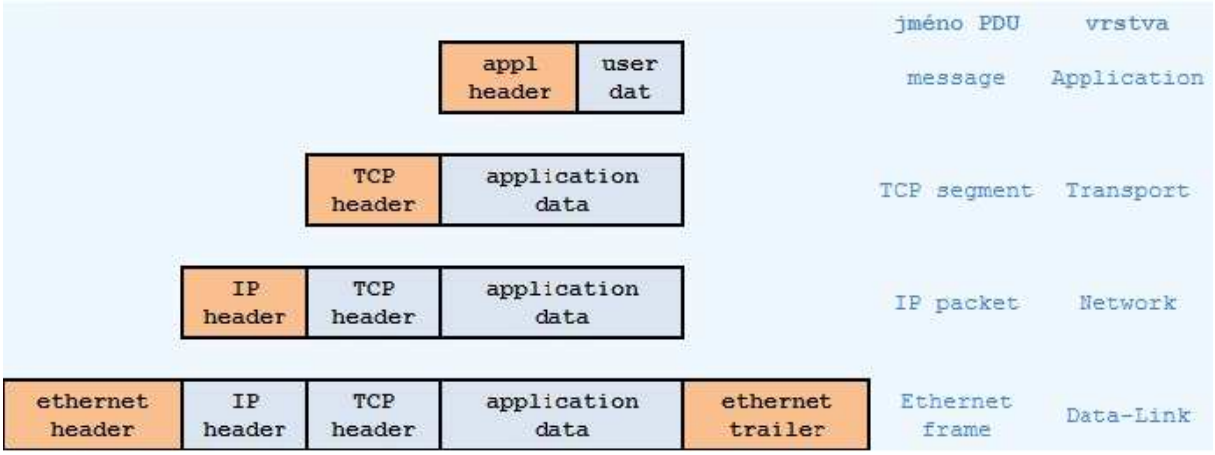
Paket (packet) v překladu znamená balíček a jedná se o formátovaný blok dat, který se přenáší v počítačové síti. O paketech se mluví v souvislosti se síťovou vrstvou. Paket obsahuje IP adresu, další atributy a data. Zabalí se do rámce a následně putuje sítí.

Rámec (frame) je to, co skutečně putuje v síti. Rámce vznikají až na fyzického vrstvě síťového rozhranní. Název naznačuje, že se spíše než o objekt jedná o časový úsek. Rámců existuje více typů, nejpoužívanější je *Ethernet II*, který umí přepravovat TCP/IP i IPX/SPX. Maximální velikost dat přenášených v rámci (tedy velikost paketu) je dána pomocí *MTU* (Maximum transmission unit) a váže se k linkové vrstvě. Standardní velikost MTU v ethernetu je 46 - 1500 bytů. Na začátku komunikace se zařízení pomocí ICMP domluví na velikosti MTU. Pokud vyžaduje druhá strana menší MTU, může se provést *fragmentace* - rozdělení rámce do více menších. Fragmentaci je možno zakázat příznakem v hlavičce paketu. Pokud je fragmentace zakázána a druhá strana akceptuje pouze menší MTU, tak odpoví chybou ICMP.

V obecné terminologii se používá označení *Protocol Data Unit* (PDU), což je datová jednotka na libovolné vrstvě (IP paket, rámec .). Když se PDU předá na nižší vrstvu, tak se označuje jako *Service Data Unit* (SDU), tam se doplní o *Protocol Control Information* (PCI), tedy hlavičku, a vznikne nové PDU.

Formát paketu - rámce

Základní tvar rámce je ***hlavička*** (header), ***data*** (payload) a ***zakončení*** (trailer). Data jsou složena ze zapouzdřených dat vyšších vrstev. Obrázek 15 zobrazuje čtyři vrstvy TCP/IP modelu spolu s hrubým formátem dat, jak jsou zapouzdřována odshora dolů. Uvedený příklad je pro protokol TCP.



Obrázek 15 Zapouzdření UDP

Ethernetová hlavička

Ethernetová hlavička obsahuje zdrojovou a cílovou MAC adresu (fyzickou adresu od hopu k hopu) a typ/délku. Typ v hlavičce určuje jaký protokol je použit na vyšší vrstvě (IP, ARP, atp.). Pro rozlišení jednotlivých rámců se na začátku vysílá speciální úvod (preamble) složený ze sekvence střídajících se jedniček a nul a SFD - oddělovač začátku rámce (obr.16).

úvod	SFD	cílová MAC adresa	zdrojová MAC adresa	typ / délka	data (payload)	CRC
7B	1B	6B	6B	2B	46-1500B	4B

Obrázek 16 Ethernetová hlavička

IP hlavička

IP hlavička obsahuje zdrojovou a cílovou IP adresu (logickou adresu komunikujících stran), dále určení protokolu pro další vrstvu (TCP, UDP, ICMP, apod.), kontrolní součet hlavičky a další hodnoty. Standardní velikost IP hlavičky je 20B, ale může ještě obsahovat volitelné vlastnosti. Tvar IP hlavičky záleží na použitém protokolu, následující příklad je pro IPv4 (obr.17).

bits	0-3	4-7	8-15	16-18	19-31
0	4	header length	Type of Service	total length (header + data)	
32	identification			flags	fragment offset
64	TTL		protocol	header checksum	
96	source IP				
128	destination IP				
160	options (if any)				
160/192+	DATA				

Obrázek 17 IP hlavička

TCP hlavička

TCP hlavička obsahuje zdrojový a cílový port, číslo sekvence a odpovědi (pro zajištění spolehlivosti), příznaky (kam patří SYN a ACK pro navázání spojení), velikost potvrzovacího okna a další. Standardní velikost je opět 20B (obr.18).

bits	0-3	4-7	8-15	16-31
0	Source Port			Destination Port
32	Sequence Number			
64	Acknowledgment Number			
96	Data Offset	Reserved	Flags	Window
128	Checksum			Urgent Pointer
160	Options (optional)			
160/192+	DATA			

Obrázek 18 TCP hlavička

Broadcast a Unicast

Když chceme poslat nějaká data v počítačové síti, je důležité správné adresování zprávy a s tím je svázána metoda vysílání. Záleží na tom, zda chceme data zaslat pouze jedné stanici, několika stanicím najednou nebo všem stanicím ve stejném subnetu.

Broadcast

Broadcast je jeden ze způsobů vysílání v TCP/IP síti (používá se nespojový protokol, např. UDP). Je to vysílání jednoho všem, tedy vysílaný paket je (teoreticky) zachycen všemi zařízeními v síti, lepé řečeno v dané broadcast doméně (subnetu). Toto vysílání se používá převážně v LAN sítích (ne WAN). Broadcasty jsou dnes používány pro řadu účelů (třeba DHCP, ARP) a využívá je velké množství aplikací. Tvoří velkou část provozu v LAN síti a zatěžují aktivní síťové prvky i stanice, proto je snaha o jejich minimalizaci. *Broadcast adresa* je adresa, na kterou se posílá komunikace v případě brodcastového vysílání. Jedná se o adresu, která má binárně samé jedničky. Na 3. vrstvě OSI modelu je to IP adresa `255.255.255.255` (občas se tak nepřesně označuje i broadcastová adresa subnetu, tedy poslední adresa v subnetu, viz dále). Na 2. vrstvě (fyzické) je broadcastová MAC adresa identicky adresa "se samými jedničkami" `FF:FF:FF:FF:FF:FF`.
Broadcast domain je logická část sítě, ve které mohou připojená zařízení přímo komunikovat. Mělo by se tedy jednat o jeden subnet a hranicí je router, který by broadcasty neměl přeposílat.
Pro rozdělení sítě na menší broadcast domény slouží routery nebo technologie VLAN.
Broadcast storm je kritický stav, když počet broadcastů v síti je tak velký, že není možno vytvářet nová spojení a stará spojení jsou rušena. Často vzniká z důvodu smyček v síti.

Unicast

Unicast je vysílání, kdy je paket zasílán jednomu cíli. Jedná se o běžnou komunikaci, kdy spolu komunikují dvě stanice.

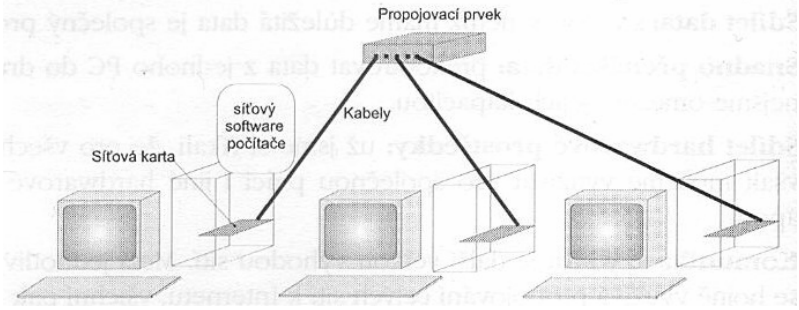
Multicast

Při této komunikaci se jedna informace doručuje skupině cílů. *Multicast* využívá efektivní metodu doručování, aby pakety v síti putovaly pouze jednou. Principem je, že se vytvoří mutlicastová adresa z rozsahu `224.0.0.0/4` (pro LAN je určeno 224.0.0.0/24) a klienti se k této adrese zaregistrují. Pro vytváření skupina a registrování se používá protokol *Internet Group Management Protocol* (IGMP).

3 Základní prvky (prostředky) počítačové sítě

Souhrn hardwarových a softwarových prvků, které zprostředkují vzájemnou spolupráci počítačů.

1. Síťové počítače
2. Síťové technické prostředky – pasivní a aktivní
3. Síťové programové prostředky – síťový operační systém, aplikace, utility

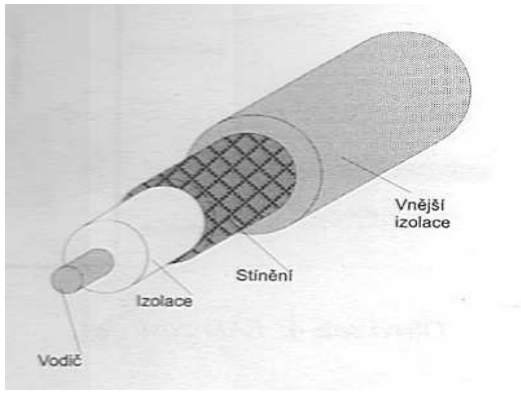


Mezi technické prvky sítě řadíme:
Pasivní prvky - data pouze přenášejí - kabely, konektory, ukončovací prvky (terminátory)
Aktivní prvky – přenášená data zesilují, filtrují, převádějí

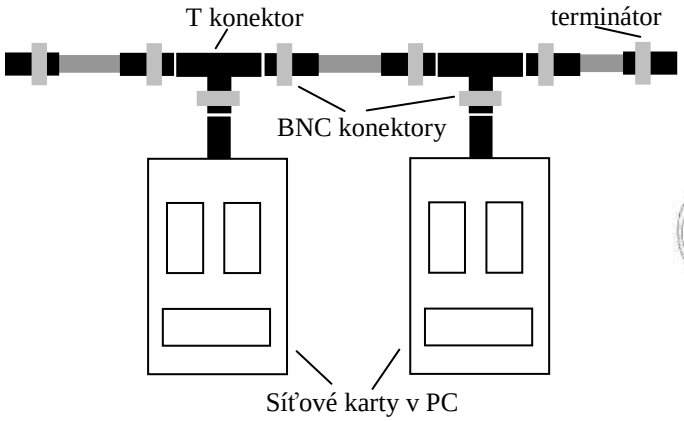
3.1 Pasivní prvky sítě - kabely

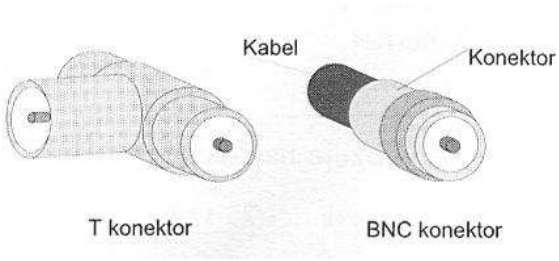
Dnes se nejčastěji používá stíněná nebo nestíněná kroucená dvoulinka (STP, UTP kabel), časté jsou optické kabely, koaxiální kabely se pro budování moderní počítačové sítě nepoužívají. Parametrem kabelů je max. *přenosová rychlost* v Mb/s (závisí především na rozsahu frekvencí, které je tento kabel schopen přenést) a *útlum* (zeslabení) přenášeného signálu na jednotku délky v dB/m, popřípadě dB/km.

Koaxiální kabel



Tvoří jej vnitřní vodič (měděný nebo postříbřený), kolem kterého je nanesena izolující vrstva dielektrika. Na této vrstvě je pak naneseno vodivé opletení (stínění), které je překryto další izolující vrstvou (vnějším pláštěm).
Vodivé opletení představuje „rozprostřený“ vodič, jehož podélná osa je shodná s osou vnitřního vodiče - proto označení „koaxiální“ (tj. souosý) kabel. Hlavní efekt vodivého opletení spočívá především v odstínění vnitřního vodiče od vlivu vnějšího rušení.

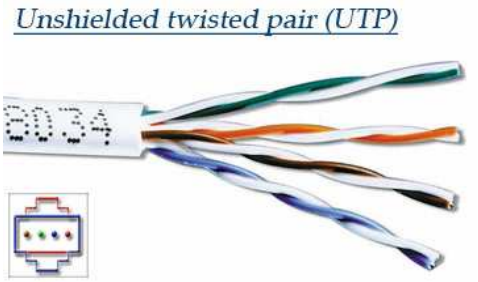




Koaxiální kabel je zakončen BNC konektorem, který se zasunuje do T konektoru a do síťové karty. Připojení nového počítače do sítě vyžaduje přerušení kabelu a vložení T konektoru. Používají se pro sběrnicovou topologii sítě, rychlost přenášených dat je max. 10 Mb/s.Vlnová Impedance kabelu je 50 Ω. Koaxiální kabel se používá pro sběrnicovou topologie, konec vodiče musí být ukončen terminátorem.

Kroucená dvoulinka (twisted pair cable - TP cable)

Kroucená dvoulinka je druh kabelu, který je používán v telekomunikacích a počítačových sítích. Je tvořena páry vodičů, které jsou po své délce pravidelným způsobem zkrouceny (anglicky: twisted pair, neboli kroucené páry). Důvodem kroucení vodičů je zlepšení elektrických vlastností kabelu. Minimalizují se rušení mezi jednotlivými páry vodičů a snižuje se interakce mezi dvoulinkou a jejím okolím, tj. je omezeno vyzařování elektromagnetického záření do okolí i jeho příjem z okolí.



Vychází se z principu *elektromagnetické indukce*. Dva souběžně vedoucí vodiče se chovají jako anténa - pokud jimi protéká střídavý proud, vyzařují do svého okolí elektromagnetické pole. Jsou-li vodiče vzájemně zkrouceny, vyzařované elektromagnetické pole se navzájem vyruší.

Druhy TP kabelů:

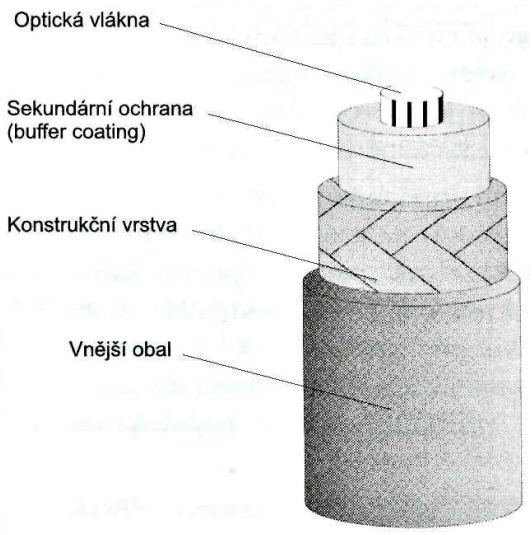
Nestíněná kroucená dvoulinka UTP (Unshielded Twisted Pair) - jednotlivé páry jsou vloženy pouze do vnější plastové izolace.

Stíněná kroucená dvoulinka FTP, STP - má navíc doplňkové stínění: - FTP (Foiled TP): společné stínění všech párů (kovová fólie)

- STP (Shielded TP): stínění jednotlivých párů

TP kabel pro počítačové sítě obsahují nejčastěji 4 páry. Dělí se do několika kategorií dle maximální frekvence přenášeného elektrického signálu (určuje max. přenosovou rychlost). Kabel je zakončen konektorem RJ 45. Slouží k přímému propojení 2 počítačů, k propojení více počítačů je potřeba aktivní síťový prvek (switch).

Optický kabel

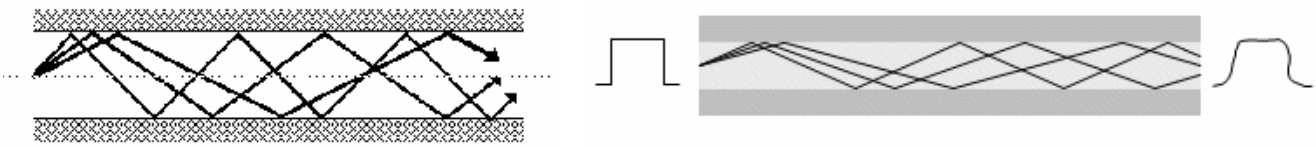


Optický kabel (fiber optic cable) je založen na odlišném principu než předešlé kabely. Data nejsou přenášená jako elektrické impulsy v kovových vodičích, ale světelnými impulsy v optických vláknech (křemičité sklo, plast).
Viditelné světlo je elektromagnetické záření přibližně o vlnové délce 400 až 750 nm (frekvence 3.9×10^{14} Hz až 7.9×10^{14} Hz). Optické kabely dosahují mnohonásobně vyšších přenosových rychlostí než kabely s metalickým jádrem (koaxiální kabel, kroucená dvoulinka).
Optická vlákna jsou velmi tenká (v řádu jednotek až desítek μm) a jsou uložena v ochranném obalu. Jsou velmi citlivá na mechanické namáhání a ohyby. Jejich ochranu proto musí zabezpečovat svým konstrukčním řešením optický kabel, který kromě jednoho či více optických vláken obvykle obsahuje i vhodnou výplň, zajišťující potřebnou mechanickou odolnost.
Existují dva druhy optických kabelů, které se liší způsobem vedení paprsku ve vlákně:

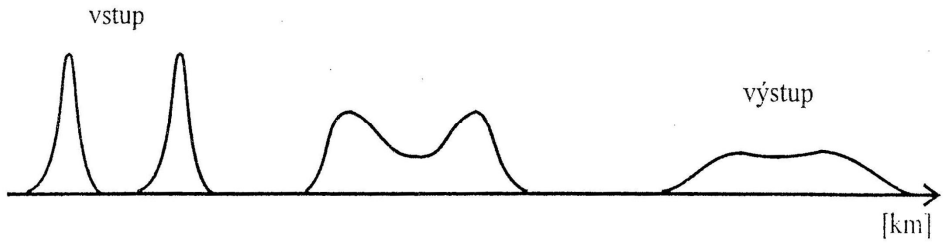
Mnohovidová vlákna (Multi-mode)

Způsob, jakým optické vlákno paprsek vede, záleží také na tom, jak se mění optické vlastnosti (konkrétně tzv. index lomu) na přechodu mezi jádrem vlákna a jeho pláštěm.
Fyzikální podstata vedení světelného paprsku vláknem:

Dopadá-li světelný paprsek na rozhraní dvou prostředí s různými optickými vlastnostmi (např. na rozhraní mezi jádrem a pláštěm), v obecném případě se část tohoto paprsku odráží zpět do původního prostředí, a část prostupuje do druhého prostředí. Záleží však na úhlu, pod jakým paprsek dopadá na rozhraní (dáno též optickými vlastnostmi obou prostředí). Je-li tento úhel větší než určitý mezní úhel, dochází k úplnému odrazu paprsku zpět do původního prostředí.

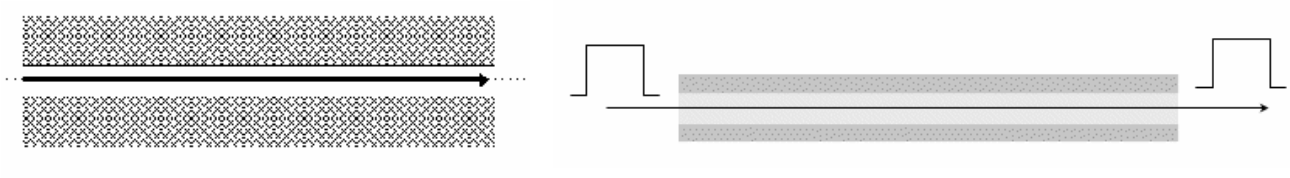


Mění-li se index lomu a je-li průměr jádra dostatečně velký (20-100 μm), jedná se o vlákno, schopné vést různé vlny světelných paprsků, tzv. vidy (modes).
Výhodou mnohovidových vláken je relativně nízká cena, snazší spojování a možnost použit jako zdroje světla (optoelektrický vysílač) LED diodu. Nevýhodou je, že se jednotlivé složky světelného signálu (vidy) odrážejí pod jiným úhlem (dorazí na konec vlákna v různém čase) – zkreslení paprsku při jeho přenosu. Zkreslení je navíc způsobeno pohlcením části světla materiálem vlákna, čí mechanickým ohybem vlákna.



Jednovidová vlákna (Single-mode)

Nejvyšších přenosových rychlostí lze dosáhnout na tzv. jednovidových vláknech, které přenáší jen jediný vid (jeden světelný paprsek).



Schopnosti vést jediný vid bez odrazů i ohybů se dosahuje buďto velmi malým průměrem jádra (řádově jednotky μm), nebo velmi malým poměrným rozdílem indexů lomu jádra a jeho pláště. Jednovidová vlákna jsou cenově o něco dražší než mnohovidová, lze je použít pro přenosy na delší vzdálenosti (až 100 km bez opakovače). Pro své buzení však vyžadují polovodičový laser (laserové diody).

Optické kabely mají především tyto výhody:

- přenos dat na velké vzdálenosti (km)
- vysoká rychlost přenosu dat Gb/s, Tb/s zvýšená použitím WDM technologie. WDM, neboli vlnový multiplex, je technologie, kdy v jednom optickém vlákně se šíří více světelných signálů o různých vlnových délkách současně – každý paprsek pak představuje jeden „přenosový kanál (nosič informace)“.
- odolnost proti všem elektromagnetickým rušením
- vysoká bezpečnost přenášených dat (optický signál se nedá odposlouchávat).
- nehrozí riziko zkratu

Nevýhodou je :

- velká cena optické kabeláže
- složité a drahé spojování optických kabelů.

Optické kabely se používají především pro budování páteřních sítí propojujících jednotlivé sítě, k propojení mezi budovami atd.

Optický kabel přenáší světelné paprsky, ale ze síťové karty vystupují elektrické impulsy. Proto je na konci každého kabelu nutný *převodník (konvertor).* Jeho úkolem je převést elektrický impuls na světelný paprsek a naopak. Umožňuje tedy napojit optický kabel na kroucenou dvoulinku.

3.2 Aktivní prvky sítě

Síťové karty (NIC – network interface cards)

Jedná se o rozhraní zajišťující přenos dat z počítače na spojovací vedení sítě a naopak podle pravidel daných síťovým standardem (přístupová metoda, síťový protokol).

Vybrané parametry síťových karet:

- typ kabeláže:
  - koaxiální kabel + BNC konektor

- kroucená dvoulinka (UTP, STP) + konektor RJ-45
- bezdrátové rozhraní + anténa pro kmitočet 2.4 GHz, resp. 5 GHz
- optický kabel
- některé starší karty (Combo) byly osazeny konektory RJ-45, BNC a Canon (AUI rozhraní)

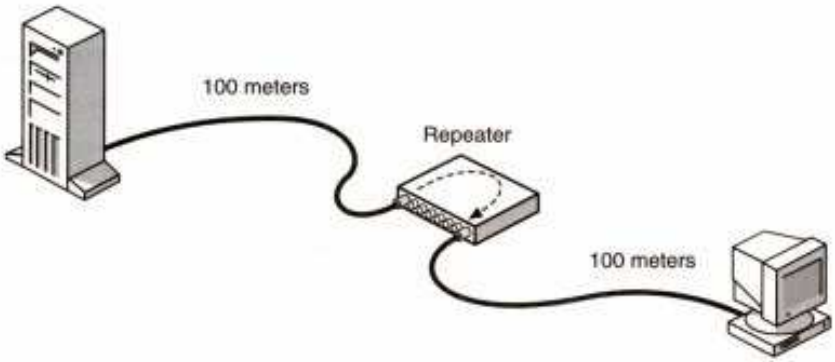
- typ sběrnice:
  - stolní počítače: ISA, PCI, PCI Express x1
  - notebooky: PC Card, Express Card
  - integrována na základní desce (dnes nejrozšířenější řešení), USB rozhraní

PCI PC Card (Cardbus) Express Card USB

- Wake-On: vzdálené spouštění počítače, počítač je možné spustit vzdáleně z jiného počítače v sítí. Všechny současné síťové karty tuto funkci podporují, nutná je podpora základní desky (formát ATX) a příslušný software.
- Ovladače pro daný operační systém - umožňují operačnímu systému ovládat síťovou kartu Podporují technologii PnP.
- Standard síťových prostředků (normy IEEE): Ethernet, FastEthernet, 802.11 (bezdrátové sítě), Token Ring, atd. Vychází z něj mimo jiné rychlost komunikace, typ kabelů a konektorů, metoda přístupu k přenosovému kanálu, max. délka sítě, topologie, atd.).
- Duplexní provoz (Full Duplex): schopnost současného přenosu mezi vysílající a přijímající stanicí v obou směrech (v současnosti všechny síťové karty standardu Ethernet)
- Vzdálené bootování: používalo se u stanic (počítačů), které neměly pevný disk. Síťová karta měla patici pro elektronický obvod (paměť) zvaný BootROM. S programem v této paměti se počítač připojil k serveru a načetl operační systém do operační paměti. Dnes se tento systém nevyužívá

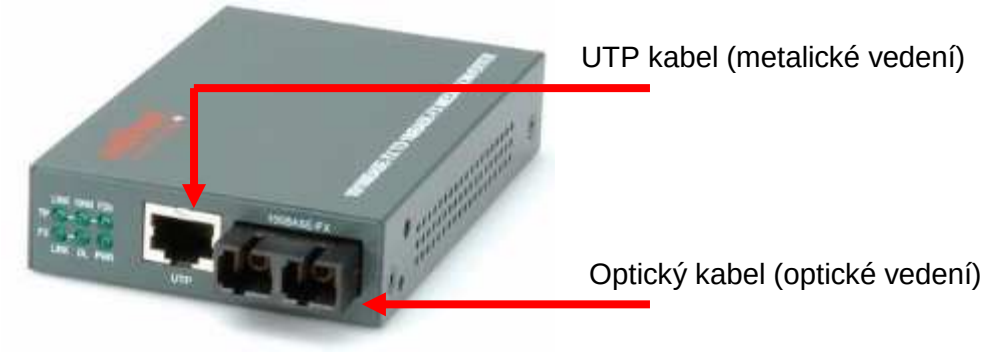
Opakovač (repeater)

Je nejjednodušším aktivním síťovým prvkem. Jeho úkolem je přijímat zkreslený, zarušený nebo jinak poškozený signál a opravený, zesílený a správně časovaný jej vyslat dále. Umožňuje tedy zvýšit dosah přenosového kanálu (např. propojení metalickým nebo optickým kabelem, bezdrátově) bez ztráty kvality a obsahu signálu.
Opakovač nedokáže filtrovat data (pakety), proto je rozesílá všem počítačovým stanicím v dané síti.



Převodník (konvertor)

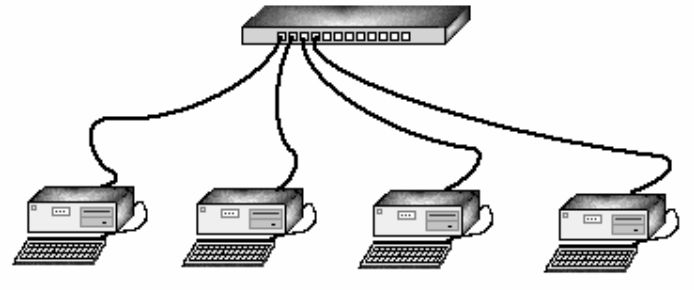
Provádí zesílení signálu a převádí jej z jednoho typu kabelu (např. optický kabel) na druhý (např. metalické vedení).



Rozbočovač (Hub, Koncentrátor)

Nezbytný prvek pro vytvoření hvězdicové topologie (struktury) sítě. Jeho základní funkcí je rozbočování signálu, neboli větvení sítě. Propojení mezi rozbočovačem a počítačem (resp. tiskárnou, IP telefonem, atd.) se provede kabelem UTP, který je zakončen konektorem RJ-45. Propojovacímu kabelu se říká patch kabel.

Rozbočovač funguje na principu opakovače, což znamená že veškerá data přicházející od jednoho koncového uzlu (jedné z přípojek) okamžitě rozesílá (opakuje) všem ostatním zařízením (posílá je současně do všech ostatních přípojek). Díky tomu pak všechna zařízení v síti přijímají „všechno“ i přesto, že jim data nejsou určena. Nemá tedy schopen filtrovat data. U větších sítí může docházet ke zbytečnému přetěžování těch zařízení, kterým data ve skutečnosti nejsou určena. V současnosti je již plně nahrazen přepínačem (switch).



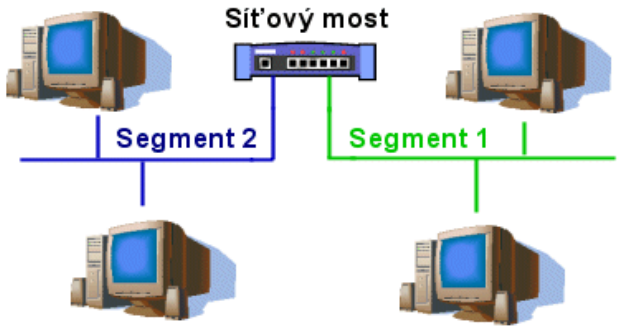
Jeho parametry jsou:

- počet a typ portů – počet počítačů, které je možné vzájemně propojit. Minimálně 4 porty. Vždy volíme počet portů s rezervou, rozšíření počtu portů lze provést připojením dalšího rozbočovače. Kromě počítačů lze do sítě připojit tiskárnu se síťovým rozhraním (RJ-45), IP telefon, atd. Současné rozbočovače jsou vybavený porty pro připojení UTP kabelu s konektorem RJ-45. Starší rozbočovače jsou doplněny BNC konektorem (koaxiální kabel).

- rychlost komunikace - 10 Mb/s, 100 Mb/s, 10/100 Mb/s a nejrychlejší 1 Gb/s. Je nutno si dát pozor na spolupráci síťové karty a rozbočovače z hlediska rychlostí.

Přepínač (Switch)

Switch je velmi podobný rozbočovači (HUBu) s tím zásadním rozdílem, že se chová jako „inteligentní“ prvek sítě. Analyzuje pakety a posílá je do té větve sítě, kde se nachází cílová adresa (filtrace paketů). Tím dochází k daleko menšímu zatížení daného segmentu sítě než v případě použití rozbočovačů.



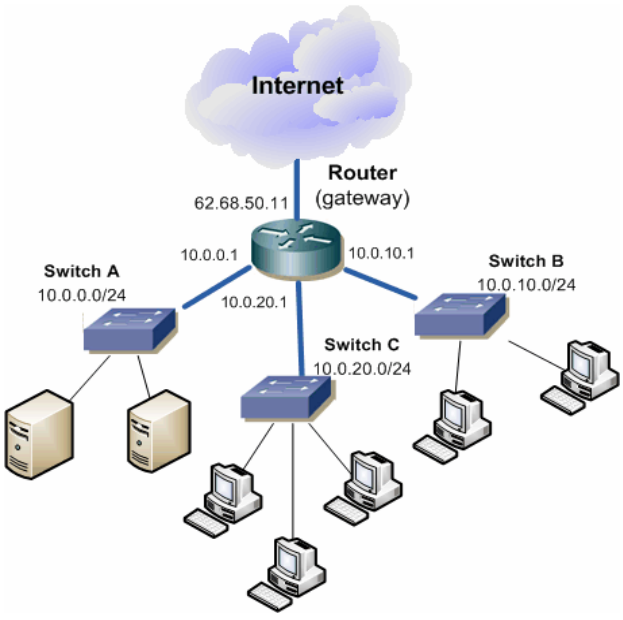
Switch má zároveň funkci tzv. *mostu* (bridge). Dokáže fyzicky propojit několik částí (segmentů) lokální (místní) sítě a řídit komunikaci mezi nimi.

Switch si pro každý port zaznamenává MAC adresy připojených počítačů. Podle těchto záznamů provádí filtrování či přesměrování paketů do jednotlivých částí lokální sítě. Tyto záznamy si průběžně aktualizuje. Pracuje však pouze v rámci jedné lokální sítě.

Směrovač (Router)

Pojmem *směrování* (routing, routování) je označováno hledání cest v počítačových sítích. Úkolem je dopravit datový paket určenému příjemci, pokud možno co nejoptimálnější cestou. Síťová infrastruktura mezi odesílatelem a příjemcem paketu však může být velmi složitá. Směrování se proto zpravidla nezabývá celou cestou paketu, ale řeší vždy jen jeden krok – komu data předat jako dalšímu. Ten pak rozhoduje, co s paketem udělat dál.

Směrovač je zařízení, které provádí směrování paketu v rozlehlé síti (např. při připojení k internetu). Jeho úkolem je tedy propojit počítače lokální sítě s počítači, které se nacházejí v jiných sítích. Každý počítač musí mít přidělenou IP adresu[1]. Narozdíl od mostu (switche), který dokáže paket směrovat pouze v rámci lokální (místní) sítě, obsahuje směrovač tzv. směrovací (routovací) tabulku, ve které jsou zaznamenány informace o dalších směrovačích, které patří jiným sítím.



Pro každý příchozí paket najde ve směrovací tabulce podle IP adresy cílové sítě (obsaženo v paketu) informaci o tom, kterému sousednímu směrovači paket zaslat. Je-li cílová síť připojená ke směrovači přímo, zašle paket rovnou cílovému zařízení.

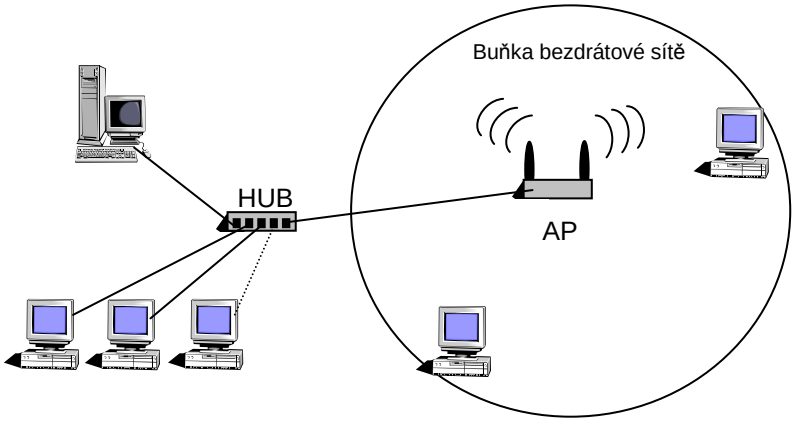
[1] IP adresa je 32 bitové číslo identifikující konkrétní zařízení v prostředí Internetu (např. 192.168.0.1).

Brána (Gateway)

Gateway (brána) je v počítačových sítích zařízení, které dokáže propojit dvě sítě s odlišnými protokoly. Brána například přijme zprávu z webové stránky (TCP/IP protokol), kterou odešle do mobilní GSM sítě v podobě SMS zprávy.

Přístupový bod (Access point - AP)

Přístupový bod komunikuje s bezdrátovými zařízeními ve svém dosahu a stará se o směrování (routování) paketů mezi bezdrátovými zařízeními a zpravidla také mezi pevnou kabelovou sítí. Přístup k AP může být zabezpečen pomocí přístupového klíče, filtrací MAC adres síťových zařízení snažících se o připojení, snížením výstupního výkonu AP, atd.



Současné přístupové body mohou sdružovat funkci výše uvedených zařízení, tedy opakovače, switche, mostu a směrovače.