Jihočeská univerzita v Českých Budějovicích

Pedagogická fakulta

Katedra fyziky

Fyzická a linková úroveň přenosu v počítačových sítích

Zdeněk Tájek

Vedoucí bakalářské práce
Ing. Michal Šerý

České Budějovice 2006

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně a že jsem uvedl veškerou použitou literaturu.

Na tomto místě bych chtěl zanechat můj dík panu Ing. Michalu Šerému za cenné rady, podněty a připomínky, které mi pomohly vypracovat tuto práci.

OBSAH

1. Úvod - historie a struktura počítačových sítí

V sedmdesátých letech došlo ke vzniku potřeb vzájemného propojení jednotlivých počítačů, za účelem jejich vzájemné spolupráce. V začátku byly budovány tzv. terminálové sítě, které umožňovaly současnou práci několika uživatelů na jednom počítači. V této době se jednalo o počítač sálový. Zásadní nevýhodou této koncepce byla naprostá závislost terminálů na ústředním počítači.

Potřeba řešení jednotlivých úloh bez uvedené závislosti vedla ke vzniku počítačových sítí, které umožňují jednotlivým uživatelům současnou práci nejen v síti, ale i mimo ni. Rozvoj této novinky umožnilo především masové nasazování počítačů standardu IBM PC XT/AT v komerční sféře, které se projevilo dynamickým rozvojem sítí typu LAN (Local Area Network) ve všech možných oblastech jako jsou firmy, úřady a školy.

1.1 Struktura v počítačových sítí

Počítačová síť je systém vzniklý vzájemným propojením počítačů. Používá se pro řešení složitých úkolů pomocí většího počtu počítačů umístěných daleko od sebe. Tyto počítače mohou sice jednotlivé části zadání zpracovávat nezávisle, ale obvykle je vhodnější propojit je tzv. počítačovou sítí, která zajistí všem počítačům přístup k nejaktuálnějším informacím potřebným pro řešení úlohy.

Takže počítačovou síť můžeme definovat jako spojení dvou a více počítačů tak aby mohli navzájem sdílet své prostředky. Přitom je jedno zda se jedná o prostředky hardwarové nebo softwarové. [1]

1.2 Typy stanic v síti

V počítačové síti se mohou vyskytovat uzly dvou druhů. Jedny bývají označovány jako servery, druhé jako pracovní stanice. [1]

1.2.1 Pracovní stanice

Pro pracovní stanice je typické, že na nich uživatel provádí zpracování dat, a to způsobem podobným jako na samostatném počítači. Rozdíl je pouze v tom, že může navíc použít služby poskytované sítí. Pracovní stanice se neúčastní chodu sítě jinak, než že využívá služeb sítě. [1]

1.2.2 Server

Server je naproti tomu charakteristický tím, že zajišťuje chod sítě. Realizuje funkce sítě a poskytuje ostatním uživatelům některé svoje prostředky, jako například paměťovou kapacitu na discích, připojené tiskárny apod. Na servery jsou v síti zpravidla kladeny vyšší požadavky než na pracovní stanice, a proto bývají realizovány na nejvýkonnějších počítačích sítě. To se projevuje také na ceně, ta je většinou až stokrát vyšší než u pracovních stanic.

V síti může být libovolný počet serverů a pracovních stanic. Je-li serverů několik, mohou se v poskytování služeb a prostředků navzájem doplňovat, tak, že každý z nich bude mít jinou specifickou funkci.

Podle funkce serveru se rozlišují diskové servery, souborové servery, databázové servery, tiskové servery a některé další druhy serverů. Dnes jsou v našich podmínkách nejčastěji kombinovány souborové a tiskové servery.

Diskový server umožňuje uživatelům sdílet rozsáhlý disk, rozdělený na několik tzv. virtuálních disků, s nimiž pracují uživatelé shodně jako s disky svých pracovních stanic na fyzické úrovni. Diskový server lze snadno implementovat a je velmi efektivní, ovšem používán je mnohem méně než server souborový.

Souborový server rovněž umožňuje sdílet uživatelům vysokokapacitní disk, avšak nikoli na fyzické úrovni, nýbrž na úrovni logické. Tento server může na rozdíl od předchozího implementovat různé způsoby ochrany souborů či dat proti současnému přístupu více uživatelů. Ochrana dat před neoprávněným použitím je obvykle realizována pomocí hesel, popřípadě pomocí přístupových práv jednotlivých uživatelů. Realizace souborového serveru je sice složitější než u serveru diskového, přesto je tento typ serveru používán mnohem častěji.

Databázový server umožňuje uživatelům sdílet data ve společné databázi a poskytuje jim možnost přístupu k ní. Dále zabezpečuje udržení integrity sdílené databáze. Přístup k databázi pomocí databázového serveru na rozdíl od souborového výrazně snižuje tok dat sítí, čímž přispívá ke zvýšení jejího výkonu. Databázové servery jsou proto velice perspektivní a už nyní se začínají rozšiřovat.

Tiskový server umožňuje uživatelům počítačové sítě provádět tisky sestav na tiskárnách k tomuto serveru připojených. Server obvykle pracuje s frontou požadavků na tisk, přičemž uživatel může většinou svému požadavku specifikovat typ výstupního formuláře, počet potřebných kopií atd. Velice často bývá funkce tiskového serveru sdružována s funkcí serveru souborového.

Vzniká ovšem dilema, zda v síti provozovat jeden nebo více serverů. Použití jediného serveru vede v případě poruchy k ukončení provozu sítě, naopak při provozování více serverů v síti lze při poruše některého z nich provozovat alespoň ty úlohy, které tento server nevyžadují. Použití více serverů v síti také vede ke zvýšení její výkonnosti, neboť výpočetní kapacita jediného, byť sebevýkonnějšího serveru není nekonečná. Naopak více serverů zvyšuje cenu sítě. Jako server se v počítačových sítích obvykle používá velmi výkonný počítač s rozsáhlou pamětí RAM a obrovským diskovým systémem. Naproti tomu jako pracovní stanice stačí standardní počítače nebo tzv. bezdiskové pracovní stanice. [1]

1.3 Hlavní důvody zavádění počítačových sítí

Důvody vedoucí k propojení jednotlivých počítačů do počítačové sítě mohou být čtyři:

- **Zvýšení spolehlivosti výpočetního systému** - toho lze dosáhnout především zálohováním jednotlivých prostředků výpočetního systému. Například informace nemusí být ukládány v jediném počítači, ale mohou být v počítačové síti zálohovány v jiném počítači. V takovém případě výpadek jednoho počítače neohrozí zpracování celé úlohy, protože informace je možno získat z jejich záložní kopie a výpočetní kapacitu nepracujícího počítače dokážou nahradit počítače zbývající.
- **Sdílení prostředků výpočetního systému** - tato možnost vede ke snížení nákladů, neboť mnohá, poměrně drahá zařízení nemusí být v konfiguraci každého počítače, ale postačí, aby byla prostřednictvím počítačové sítě každému jednotlivému počítači dostupná.

- **Sdílení společných informací** - informace mohou být uloženy v počítačové síti pouze jedenkrát, pokud nepočítáme jejich záložní kopie a pro ostatní počítače je postačující, mohou-li sdílená data požadovaným způsobem využívat. Realizace přístupu k datům je závislá na charakteristice a množství dat.
- **Komunikační prostředí** - posledním důvodem je vytvoření velice výkonného komunikačního prostředí pro jednotlivé uživatele počítačové sítě. Pokud je příjemce připojen k síti a není-li zablokován příjem zpráv, jakákoli komunikace může probíhat prakticky okamžitě. [1]

1.4 Klasifikace sítí dle rozlohy

1.4.1 LAN – lokální síť

Lokální počítačová síť se nejčastěji rozkládá v rámci jedné nebo několika místností či několika sousedních budov. Většina moderních sítí LAN podporuje širokou škálu počítačů a jiných zařízení. Každé zařízení musí používat vlastní fyzické protokoly a datového spojení pro konkrétní síť a všechna zařízení, která chtějí komunikovat se všemi ostatními v síti, musí používat stejný komunikační protokol. [1]

1.4.2 MAN – metropolitní síť

Metropolitní počítačová síť je veřejná síť pracující vysokou rychlostí a schopná přenášet data na vzdálenost desítky kilometrů. Většinou podporuje data i hlas. Tato síť je menší než WAN ale větší než LAN. Pro klasifikaci pro ní platí přibližně to samé co v síti LAN. [1]

1.4.3 WAN – globální počítačová síť

Další typ sítě, která se rozprostírá na větším území, jehož vzdálenost je prakticky neomezená, se nazývá globální počítačová síť. Zde se pro připojení používá přenosových prostředků veřejné telekomunikační sítě, nejčastěji telefonních kanálů.

Interprocessor distance	Processors located in same	Example
1 m	Square meter	Personal area network
10 m	Room	Local area network
100 m	Building	
1 km	Campus	
10 km	City	Metropolitan area network
100 km	Country	Wide area network
1000 km	Continent	
10,000 km	Planet	The Internet

Tabulka 1 – rozdělení sítí podle rozlehlosti

Zásadním rozdílem WAN oproti LAN je skutečnost, že spojení mezi jednotlivými uzly sítě nebývá trvalé, ale naváže se pouze v případě potřeby komunikace mezi jednotlivými uzly. Po ukončení komunikace se spojení opět zruší. Někdy tvoří výjimku trvalé propojení mezi řídícími uzly sítě, ani to však není pravidlem. Jako servery ve WAN zpravidla nevystupují osobní počítače, ale počítače střediskové, popř. superpočítače. Jako uzly WAN mohou vystupovat nejen jednotlivé počítače, ale i celé počítačové sítě. Přínosem WAN je skutečnost, že nabízejí prakticky okamžitě informace z libovolného místa světa.

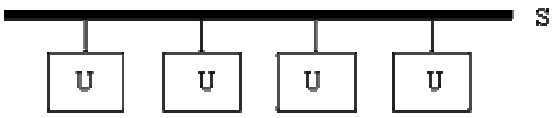
Existuje také několik WAN s celosvětovou působností, které mají i několik desítek uzlů v České republice. Patří sem zejména síť Internet. Jde o nadsíť, která sdružuje desetitisíce podsítí celého světa. Po telefonní síti jde o druhou největší komunikační síť na světě. Internet umožňuje nejen přenášet informace, ale také využívat výpočetní kapacity superpočítačů, které jsou součástí sítě. [1]

1.5 Topologie sítí

Topologie sítě charakterizuje způsob, jakým jsou mezi sebou propojeny jednotlivé stanice. Je to vlastnost sítě, ke které se přihlíží hlavně ve fázi zavádění sítě, kdy se propojení stanic realizuje, ve vlastním provozu se již příliš neuplatňuje. Topologie sítě je plně určena použitým síťovým hardwarem. V oblasti sítí jsou v současnosti běžné následující typy:

1.5.1 Sběrnicová topologie

Základem počítačové sítě je společná sběrnice, na níž jsou připojeny jednotlivé uzly sítě.



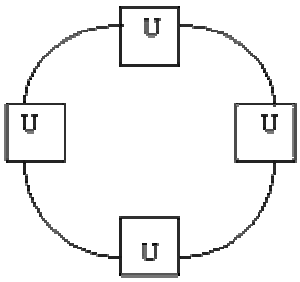
Obrázek 1 – schéma počítačové sítě se strukturou sběrnice
(U – uzel, S – sběrnice)

Jakákoli informace vysílaná některým uzlem je předána na sběrnici, kde postupuje směrem ke všem uzlům až k zakončovacímu prvku sběrnice, tzv. terminátoru.

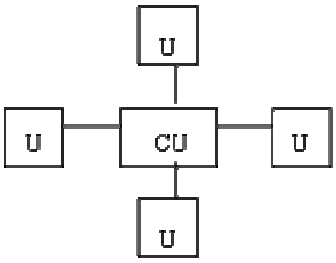
Každý uzel sítě přijímá všechny informace vyslané na sběrnici, avšak zpracovává je jen v případě, že je uveden jako adresát předávané informace. [1]

1.5.2 Kruhová topologie

Informace jsou v sítích s touto strukturou přenášeny od zdroje ve zvoleném směru přes jednotlivé uzly sítě až k adresátovi. Oproti struktuře typu sběrnice je však možné, aby bylo v jednom okamžiku přenášeno v síti více informací za předpokladu odlišných tras jejich přenosu. [1]



Obrázek 2 – schéma kruhové struktury



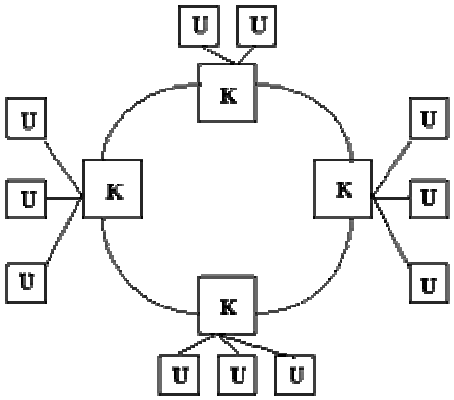
Obrázek 3 – schéma struktury typu hvězda (CU – centrální uzel)

1.5.3 Hvězdicová topologie

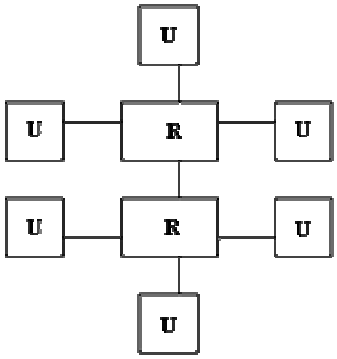
Při použití struktury, která je na obrázku 3, je každý uzel připojen vlastním spojem k uzlu centrálnímu a komunikuje jen s ním. Centrální uzel buď informace směruje k adresátovi, nebo je předává všem dalším uzlům. [1]

1.5.4 Kombinované topologie

Kombinací struktury typu hvězda a kruh vznikne hvězdicový kruh. Jednotlivé uzly sítě jsou hvězdicově připojeny k uzlům vyššího řádu tzv. koncentrátory, ty uzavírají kruh.



Obrázek 4 – struktura hvězdicový kruh
(K - koncentrátor)



Obrázek 5 – schéma stromovité struktury
(R – rozbočovač)

Další modifikací struktury typu hvězda je tzv. stromová struktura, která vlastně odpovídá několika hvězdám, jejichž centrální uzly tzv. rozbočovače jsou propojeny. [1]

2. Referenční model ISO/OSI

V dobách vzniku vzájemného propojování jednotlivých počítačů za účelem jejich vzájemné spolupráce vznikaly sítě budované podle vlastních koncepcí předních výrobců počítačů jako jsou sítě firmy IBM, SNS či DNA. Možnost zapojení do ostatních sítí byla vázána na vlastnictví produktů příslušného výrobce, který si v rámci vlastní síťové architektury vytvářel své specifické konvence a protokoly.

Postupem času vyvstala naléhavá potřeba jednotného standardu pro vzájemné propojování počítačových systémů různých typů a koncepcí, pocházejících od různých výrobců. Potřebu vytvoření takovéhoto standardu si uvědomila mezinárodní organizace ISO (International Standards Organization), která se rozhodla specifikovat závazný standard, který nalezl jako model sítě široké rozšíření.

Pod názvem Open System Interconnection, nebo zkráceně OSI byl definován model ISO, který určuje hierarchické uspořádání struktury komunikačních sítí, a který byl uznán celosvětově všemi výrobci jako závazná reference.

Referenční model OSI stanovuje určitá pravidla, která jsou nutná, aby spolu mohly komunikovat počítače různých hardwarových platforem a provozních systémů. Toto jsou některé cíle, jejichž naplnění ISO se svým referenčním modelem sleduje:

- **Interakce mezi sítěmi s různými protokoly** - jestliže se mají kontaktovat sítě s různými protokoly, musí být vytvořeny přechody a model OSI definuje komunikační pravidla, která jsou nadřazena protokolům.

- **Přenos na fyzické úrovni** - je definován přenos datových bitů přes fyzikální cesty.
- **Kontrola dat** - důležitou úlohou referenčního modelu je zajistit zabezpečený kontrolní mechanismus přenosu dat, aby byla možná transparentní korekce chybných datových bitů.
- **Určení vysílače a přijímače dat** - referenční model popisuje rovněž způsob, jak a kdy vysílají a přijímají síťová zařízení data a jak se realizuje pružný přechod mezi vysílačem a přijímačem.
- **Realizace fyzického přechodu ve vrstvách různých medií** - referenční model stanovuje závazné normy pro přípojky, kabely, adaptéry a zásuvky.
- **Přiřazení síťových komponentů jednotlivým vrstvám** - směrovače, mosty, multiplexory a vysílače tvoří soubor síťových komponentů, které jsou začleněny do referenčního modelu OSI a proto výrobci hardware mají přesné definice toho, co jednotlivé komponenty mohou provádět, aby síť pracovala bez problémů. [2]

Referenční model OSI je základem každé sítě jako teoretické schéma, a tím platí i pro každou síť IP, která teoreticky může být považována za rovnocennou s každou jinou sítí. Referenční model nemá nic společného s reálnými poměry. Je to spíše čistě myšlenkový model, podle kterého musí probíhat realizační procesy pro funkční síť.

2.1 Vrstvový model

Při stanovení jednotlivých úloh sítě, které tvoří základ pro bezporuchovou a normalizovanou komunikaci, popisuje OSI sedm

vrstev. Každá vrstva komunikuje přesně definovaným způsobem s hierarchicky nadřazenou a podřízenou vrstvou. Komunikační protokoly mezi vrstvami jsou rovněž definovány.

Každá vrstva uvnitř vrstvového modelu přebírá definovanou úlohu, které se v celku doplňují pro funkční komunikační infrastrukturu. Každá úloha může mít další podúlohy, aby bylo možno splnit úlohy komunikační vrstvy.

Protokoly slouží pro komunikaci mezi podúlohami. Mohou být sdruženy do skupin protokolů které pak tvoří protokolový sklad. Protokoly takového skladu jsou přísně hierarchicky členěny a jejich úlohy jsou v rámci komunikačního systému přesně definovány. Uvnitř skladu přijímá protokolová vrstva dat hierarchicky nižší vrstvy a vysílá data do odpovídající vyšší hierarchické vrstvy.

Jedním z hlavních cílů modelu s přesnou definicí spojení, je hardwarová komunikace nezávislá na provozním systému. Dva počítačové systémy mohou vždy být spolu v kontaktu, jestliže pracují se stejnými protokolovými sklady. Každá vrstva, která má přenášet určité úkoly, si vyměňuje data s jinými počítači jen na stejné protokolové úrovni. Jestliže jedna vrstva nemůže správně splnit úlohu, která je jí určena deleguje se tato úloha na jinou vrstvu.

Počítače si mohou na podkladě tohoto modelu také vyměňovat data mezi sebou, i když mají zcela rozdílnou architekturu. Počítač s Windows, který pracuje s určitým protokolovým skladem, může být v kontaktu s počítačem Unix nebo Macintosh, jen pokud tento pracuje se stejným skladem protokolu. Metoda kategorizace stejných stupňů na vrstvách nezávislých protokolů se označuje jako Peer- Layer Communication (PLC).

Tabulka 2 Přehled vrstev a označení paketů		
Číslo vrstvy	**Označení vrstvy**	**Označeni dat. paketu**
7	Aplikační	zprávy
6	prezentační	pakety H1
5	Relační	pakety H2
4	transportní	segmenty
3	Síťová	datagramy
2	linková	rámce
1	Fyzická	bity

Jestliže má být informace přenesena od jednoho počítače ke druhému, probíhá nejprve protokolovým skladem vysílajícího počítače. Každá vrstva vysílajícího počítače přidává administrativní a pro přenos potřebné informace, které se zaznamenávají jako záhlaví na začátku binárních informací. Přijímající počítač přečte došlé záhlaví, interpretuje je a zavádí tyto informace do požadované vrstvy. Záhlaví se pak podle vrstev opět obnovují, až je dosaženo cílové vrstvy.

Záhlaví a vlastní přenášená informace tvoří dohromady paket. Podle vrstvy, v níž se data aktuálně nalézají ke zpracování, jsou datové pakety různě označeny. V tabulce 2 je uveden přehled užívaných označení paketů a vrstev. [2]

2.1.1 Sedm vrstev modelu ISO/OSI

Fyzická vrstva - účelem této nejnižší vrstvy je aktivace, udržování v aktivním stavu a dezaktivace fyzických spojení určených pro přenos bitů nebo značek. Fyzické spojení může být vytvořené ve formě propojení datových okruhů s využitím zprostředkovacích funkcí ve fyzické vrstvě. Datový okruh představuje komunikační cesta ve

fyzických médiích mezi dvěma fyzickými vrstvami a prostředky potřebné pro uskutečnění přenosu bitů přes tuto komunikační cestu.

Linková vrstva - tato vrstva, zvaná též jako spojová musí umožnit zahajování, udržování a závěr vytvořených spojení, formátování rámců, identifikaci koncových bodů spojení, seřazování přenášených rámců, oznamování neopravitelných chyb síťové vrstvě, detekci a opravu chyb, řízení toku, identifikaci a výměnu parametrů a dodržování hodnot výkonnosti spojových služeb.

Síťová vrstva - účelem této vrstvy je poskytovat síťové spojení otevřeným systémům, které spolu chtějí komunikovat. Poskytuje transportní vrstvě nezávislost na směrování a zprostředkování souvisejícími s vytvářením příslušných síťových spojení. Zprostředkovací funkce a protokoly zahrnující rozšířenou službu pro přenos po úsecích, které se využívají v rámci síťové služby uplatněné mezi koncovými otevřenými systémy, kde se realizují pod transportní vrstvou.

Transportní vrstva - tato vrstva poskytuje transparentní, spolehlivý a cenově přístupný přenos s požadovanou kvalitou a optimalizuje nejrůznější síťové služby. Je postavená mezi uživatele a síť a její služby poskytované vyšším vrstvám nezávisejí na vlastní síťové implementaci. Transportní vrstva poskytuje relační vrstvě zahájení, udržování a závěr transportních spojení a přenos bloků. Nestará se o směrování, ani o zprostředkování, s výjimkou některých propojení sítí.

Relační vrstva - smyslem této vrstvy je organizovat a synchronizovat dialog mezi spolupracujícími prezentačními vrstvami a řídit výměnu dat mezi nimi. Tato vrstva poskytuje vytváření a závěr relačního spojení, normální a spěšný přenos zpráv, pozdržený přenos

zpráv (část zpráv přenesená relačním spojením se uvolňuje pro adresáta až na pokyn odesílatele), synchronizaci relačního spojení a oznamování výjimečných stavů prezentační vrstvě.

Prezentační vrstva - úkolem této vrstvy je poskytovat takovou reprezentaci informace, kterou aplikační vrstva používá při komunikaci či se na ni odvolává. Cílem je, aby přenášené zprávy byly pro aplikaci prezentovány jednotným způsobem bez ohledu na svou různorodost, vlastnosti svých zdrojů a spotřebičů.

Aplikační vrstva - účelem této vrstvy je poskytnout aplikačním procesům přístup ke komunikačnímu systému a tím umožnit jejich vzájemnou spolupráci. Mezi služby poskytované aplikační vrstvou patří přenos zpráv, identifikace komunikujících parametrů, zjištění stupně okamžité připravenosti komunikujícího partnera, stanovení pověření pro komunikaci, synchronizace spolupracujících aplikací. [2]

3. Síťový model TCP/IP

TCP/IP je zkratka slov Transmission Control Protocol / Internet Protocol. Tento protokol se používá po celé síti Internet a nejenom na ni. Přestože se stal standardním souborem protokolů teprve v poslední době, je starý již více jak dvacet let. V počátku byl použit pro spojení vládních počítačů, nyní je jeho největší využití v síti Internetu, jenž se stala největší celosvětovou sítí. Jako TCP/IP standard se tento síťový protokol začal prosazovat v době, kdy byl implementován do systému Unix a jemu podobných, zhruba někdy kolem roku 1980. Díky této podpoře a zároveň díky jeho vyplývající historické kompatibilitě vůči velkému množství hardwarových a softwarových systémů se dnes těší velkému rozšíření.

3.1 Historie protokolu TCP/IP

Úplné počátky vzniku používání síťového protokolu TCP/IP se nacházejí v době, kdy žádostí ministerstva obrany v USA byl vznesen požadavek, na vytvoření komunikační sítě, jenž by zabezpečovala spojení i v případě jaderné války. Tato síť tedy měla poskytovat jednoduchou a bezproblémovou komunikaci v případě jaderného ohrožení a dokonce i po jaderné válce.

V roce 1964 společnost Rand Corporation publikovala řešení, kde uvedla, že je jasné, že každý centrální úřad, jakékoliv centrální síťové centrum by bylo zřejmým a nevyhnutelným terčem nepřátelského útoku. Proto to měla být síť založená na decentralizované koncepci, žádné systémové centrum, žádná centrální správa. Z čehož vyplynulo logické vyústění, že i kdyby došlo k jaderné

válce a hlavní komunikační centra by byla zničena, tak by stále tato síť měla být schopna provozu.

Rand řešil tento problém za hlubokého vojenského utajení a od začátku koncipoval danou síť tak, aby právě fungovala i v nekonzistentním stavu. To znamená, že některé uzly a spojovací linky budou nutně chybět. Principy byly jednoduché.

Síť vlastně nikdy nebude pokládána za 100% spolehlivou, a proto bude navržena takovým způsobem, aby alespoň byla zachována nějaká možná komunikační cesta. Všechny uzly sítě budou z hlediska svého stavu rovnocenné a každý uzel bude mít svou vlastní autoritu pro vytváření, předávání a přijímání zpráv. Samotné zprávy budou rozděleny do paketů, každý paket bude nezávisle adresován. Paket bude vycházet z některého konkrétního uzlu sítě a končit na jiném, cílovém uzlu, přitom se bude pohybovat v síti samostatně. Konkrétní cesta, po které bude sítí procházet, nebude důležitá, podstatný bude pouze výsledek. V zásadě si uzly budou paket přehazovat více či méně směrem k jeho cílového určení tak dlouho, dokud neskončí na správném místě. I když budou velké celky sítě vyřazeny z činnosti, nevadí, pakety budou pořád kolovat a předávány těmi uzly, které nebyly zničeny. Takovýto poněkud nahodilý doručovací systém může být neefektivní z hlediska obvyklého chápání, rychlých a přesně definovaných komunikačních cest, je však zato extrémně robustní.

Tak později vznikla síť Arpanet. Tato síť se nazývala podle pentagonské agentury ARPA (Advanced Research Projects Agency). Roku 1969 byly instalovány první uzly této sítě a o několik let později již tato síť obsahovala na 37 uzlů. Ze sítě ARPANET se později stala dnešní páteřní síť Internetu. Původně sloužil ke sdílení prostředků výpočetní techniky, kdy byl strojový čas počítačů dosti drahý. Později se

z této sítě stal „federálně dotovaný elektronický poštovní úřad“, jenž se začal využívat v daleko větší míře než sdílení strojového času.

Během 70-tých let se síť ARPANET stále více rozrůstala; její decentralizovaná struktura tuto expanzi jen usnadňovala. Na rozdíl od standardních firemních počítačových sítí mohl ARPANET připojovat mnoho různých typů počítačů, stačilo, aby tyto počítače rozuměly paketově-orientovanému protokolu nové "anarchistické" sítě, vše ostatní bylo nepodstatné. [3]

3.2 Protokoly v ARPANETU, předchůdce TCP/IP

Původním ARPA-protokolem pro komunikaci byl NCP (Network Control Protocol), ale s postupem času a vznikem pokročilejších technologií začal být NCP nahrazován mnohem propracovanějším standardem vyšší úrovně označovaným TCP/IP. TCP/IP vznikl jako výsledek projektu agentury DARPA, který měl za cíl zkoumat techniky a technologie pro propojování paketových sítí různých typů. Systém sítí, nebo "síť sítí" navržený v rámci tohoto projektu vešel ve známost pod označením Internet. Sada protokolů TCP/IP (v současnosti se jedná zhruba o několik desítek protokolů a další vznikají) má dvě skupiny:

- **TCP (Transmission Control Protocol)** - Je protokol transportní vrstvy. Hlavním účelem protokolu TCP je získávat elektronické zprávy libovolné délky a převádět je do sekvence paketů, zpravidla o velikosti 64kb, na zdrojovém uzlu a pak je znovu sestavuje do původních zpráv na cílovém uzlu sítě. Díky tomu může software řídící síťovou komunikaci zasílat zprávy po částech a kontrolovat každou z těchto částí samostatně. V případě, že se nepodaří daný paket přenést, tak se přenos opakuje. Efektivita přenosu je právě dána paketovým přenosem.

Při chybě v přenosu se nemusí posílat celý balík dat, ale jen chybný paket.

- **IP (Internet Protocol)** – Je to protokol síťové vrstvy a u každého paketu ověřuje jeho korektnost a obhospodařuje adresování, a to tak, aby pakety mohly být směrovány nejen přes řadu uzlů, ale dokonce i přes řadu sítí pracujících s různými komunikačními protokoly, nejen s původním Arpanetovským NCP standardem, ale i s jinými protokoly. Dále zajišťuje, aby byly pakety posílány ve správném pořadí a co možná nejvhodněji, co se týče cesty přenosu.

Od roku 1977 začal být TCP/IP používán jinými sítěmi pro připojování k Arpanetu. Samotný Arpanet zůstával pod pevným řízením přinejmenším do roku 1983, kdy se jeho vojenský segment oddělil a vytvořil samostatnou vojenskou síť Milnet. Protokol TCP/IP všechny tyto nově příchozí sítě propojoval dohromady a Arpanet se stával stále menší a menší částí oné ohromně rostoucí sítě jiných připojených počítačů. [4]

3.3 Síťový model TCP/IP

Síťový model TCP/IP je modelem vrstveným. Vychází z podstaty dělení vrstev od návrhářů síťového referenčního modelu OSI. Ovšem při konstrukci tohoto protokolu se vycházelo úplně z jiných předpokladů. Dělí se na čtyři vrstvy.

Vrstva síťového rozhraní - síťovým modelem TCP/IP není nikterak omezeno použití jakékoliv přenosové technologie která bude použita na úrovni vrstvy síťového rozhraní. Je to jakýsi univerzální mezičlánek, právě mezi aplikační vrstvou a vrstvou síťového rozhraní. Tento protokol, je navržen tak, že je mu jedno, jestli se budou data

přenášet po relativně spolehlivých cestách, kde dochází k častým chybám při přenosu, nebo po zcela spolehlivých cestách, kde je chybovost přenosu žádná nebo velice minimální. Neví také nic o tom jakou rychlostí se data budou přenášet, jaké bude zpoždění při přenosu či jaká bude velikost přenášených bloků.

Síťová vrstva - tato vrstva je navržena pro co možná maximální přenosovou rychlost na úkor spolehlivosti. Se spolehlivostí se autoři vypořádali tak, že při navrhování přenechali tyto starosti vyšším vrstvám tohoto modelu. Ovšem není pravdou, že by se tato vrstva vůbec nestarala o bezchybný přenos, pouze nepovažuje za svou povinnost starat se o jakoukoliv nápravu, když se některá data při přenosu poškodí. Samotná data posílá po blocích nespojitě. V podstatě nepočítá s tím, že při začátku přenosu naváže spojení s adresátem. Data vyšle v bloku, který obsahuje cílovou adresu. Tímto způsobem je zabezpečena dosti velká robustnost při přenosu, nebo dojde-li někde na již zvolené přenosové cestě k přerušení přenosové cesty k adresátovi, tak si bloky zvolí jinou cestu.

Transportní vrstva - hlavním úkolem této vrstvy je zajistit přenos mezi dvěma koncovými účastníky, kterými jsou v případě TCP/IP přímo aplikační programy. Podle jejich nároků a požadavků může transportní vrstva regulovat tok dat oběma směry, zajišťovat spolehlivost přenosu, a také měnit nespojovaný charakter přenosu na spojovaný v síťové vrstvě.

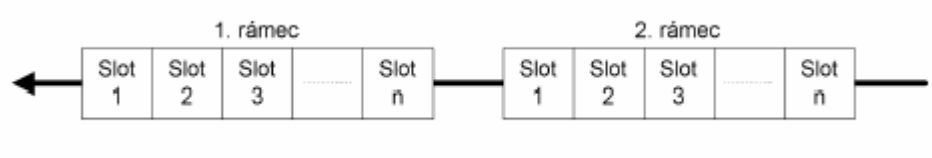
Aplikační vrstva - poslední vrstva na rozdíl od RM OSI neobsahuje různé podpůrné prostředky pro konverzi dat, komprimaci, šifrování, synchronizaci přenosu atd. Toto všechno musí být již naprogramováno v aplikaci. Tato vrstva slouží pouze k napojení pro uživatelského rozhraní dané aplikace, ze které probíhá další ovládání. [5]

4. Základní formy přenosů

Základní funkcí každé počítačové sítě je přenos datových signálů od jednoho počítače ke druhému. V počítačových sítích se můžeme setkat s nejrůznějšími formami přenosu signálů, které mohou být navíc různým způsobem modulovány a kódovány. Rozeznáváme přenos synchronní, paketový a asynchronní. [6]

4.1 Synchronní přenos

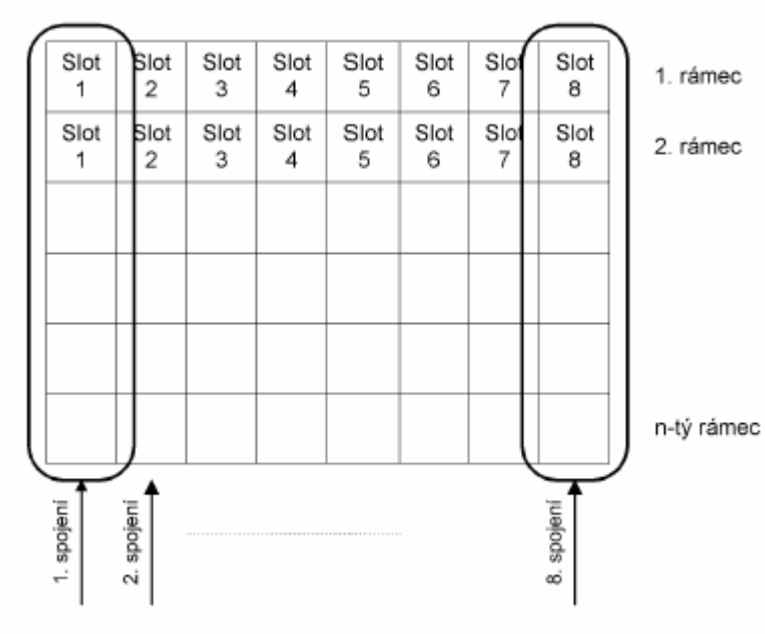
Synchronní přenos je vyžadován např. pro zvuk a video, tj. v případě, kdy je třeba stejnoměrně po dobu přenosu zajistit požadovanou šíři pásma. Stane-li se, že odesílatel nevyužije zajištěné pásmo, pak pásmo zůstává nevyužito.



Obrázek 6 - Rozdělení rámců na sloty u synchronního přenosu

Garance šíře přenosového pásma se u synchronního přenosu provádí rozdělením přenášených rámců na sloty. Pro dané spojení se pak v každém přenášeném rámci vyhradí jeden či více slotů, viz obr.6. Jestliže v každém rámci je např. slot číslo 1 vyhrazen pro naše spojení, pak jelikož rámce stejnoměrně plynou sítí za sebou, tak naše aplikace má garantovánu šíři pásma, která je dána tím, kolik slotů číslo jedna přenese síť za vteřinu. Podstata věci se dá pochopit, když se několik rámců nakreslí pod sebe do super rámce, viz obr. 7. Sloty pod sebou patří témuž spojení.

Se synchronním přenosem se můžeme setkat u připojení podnikové telefonní ústředny k ústředně Telecomu. Ta bývá připojena např. linkou E1, která obsahuje 32 slotů, každý o šířce pásma 64 kb/s. Slot lze využít pro telefonní hovor. Současně je tak teoreticky garantováno 32 hovorů, některé sloty se však používají jako služební. Internet nepoužívá synchronní přenos, tj. negarantuje šíři přenášeného pásma. Kvalitní přenos zvuku či videa se v Internetu zpravidla dociluje předimenzováním přenosových linek. [6]



Obrázek 7 – Super rámec

4.2 Paketový přenos

Paketový přenos je výhodný zejména pro přenos dat. Pakety nesou data obecně různé délky. Paket nese data vždy jedné aplikace, jednoho spojení. Jelikož jsou pakety různé délky, nelze garantovat šíři pásma. Výhodou je efektivní využití pásma, protože v případě, že

aplikace nepotřebuje přenášet data, pak pásmo mohou využít jiné aplikace. [6]

Obrázek 8 – Paketový přenos dat

4.3 Asynchronní přenos

Asynchronní přenos používá protokol ATM. Tento typ přenosu kombinuje paketový přenos se synchronním přenosem.

Obrázek 9 – Asynchronní přenos dat

Podobně jako u paketového přenosu jsou u asynchronního přenosu data přenášena v malých paketech, které se však nazývají buňky. V jedné buňce se přenáší data jedné aplikace, jednoho spojení. Avšak buňky mají stejnou délku, takže garantuje-li se, že každá x-tá buňka bude k dispozici konkrétní aplikaci, konkrétnímu spojení, pak se tím garantuje i šířka pásma. Navíc, pokud aplikace buňku neodešle, může být odeslána buňka jiné aplikace. [6]

4.4 Parita

Při sériovém i paralelním přenosu dat může docházet k chybám, jejichž důsledkem je přijetí opačné hodnoty jednoho či několika bitů, než jaké byly původně vyslány. Nejjednodušším, ale současně také nejméně účinným způsobem zabezpečení znaku ,kterým je umožněno následně rozpoznat výskyt chyby je doplnění datových bitů jedním dalším bitem tak, aby celkový počet jedniček ve znaku byl lichý, nebo sudý podle toho zda se jedná o lichou paritu nebo sudou paritu. Příjemce musí vědět, zda mu odesilatel posílá znaky se sudou, nebo lichou paritou.

Pokud počet jedničkových bitů nesouhlasí s očekávanou paritou, může si příjemce dovodit, že došlo k chybě při přenosu jednoho nebo obecně lichého počtu bitů. Má-li přijatý znak očekávanou paritu, není to ještě záruka jeho bezchybnosti. Pomocí jediného paritního bitu nelze rozpoznat chyby v sudém počtu bitů. Zabezpečení pomocí jednoho paritního bitu je tedy vhodné používat jen tam, kde je pravděpodobnost výskytu chyb v jednotlivých bitech malá a pravděpodobnost výskytu chyb ve více bitech současně zanedbatelná.

Lze se setkat také s tím, že se paritní bit nastavuje vždy na 0 respektive na 1. Smysl je ten, že odesílatel může vysílat sedmibitové znaky doplněné tímto konstantním paritním bitem, které příjemce přijme jako osmibitové znaky bez parity, čímž se ale ztrácí možnost detekovat přenosové chyby. [6]

5. Přenosové techniky

Z historického hlediska vznikly dvě hlavní skupiny přenosových technik. Jsou to přenosové techniky fungující na principu přepojování okruhů, schopné garantovat trvale dostupnou přenosovou kapacitu a vyhovující multimediálním přenosů, a pak přenosové techniky založené na principu přepojování paketů, vyhovující zase nárazovosti počítačových služeb typu přenosu souborů.

Přenosové techniky jsou záležitostí, která se může týkat různých vrstev vrstevnatých modelů. Techniky na bázi přepojování paketů vznikly na úrovni síťové vrstvy a v průběhu dalšího vývoje zčásti pronikly i do vrstvy nižší. Techniky multiplexování, týkající se rozdělení jedné přenosové cesty na více relativně samostatných přenosových kanálů, resp. jejich využití pro potřeby přenosu dat od různých příjemců k různým odesilatelům pak obvykle patří do nejnižší, fyzické přenosové vrstvy. [7]

5.1 Simplex, duplex, poloduplex

Podle toho, v jakém směru probíhá přenos dat mezi dvěma účastníky A a B, rozlišujeme následující způsoby přenosu:

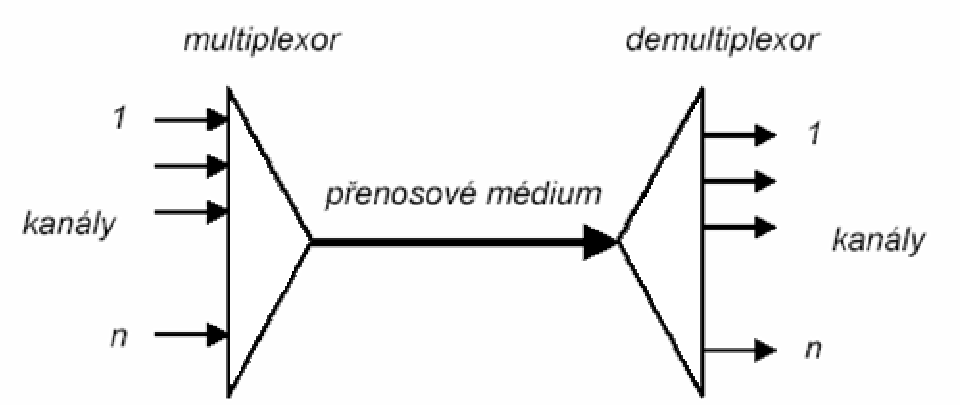
- **Simplexní přenos, simplex** - u simplexního přenosu probíhá komunikace mezi uživateli pouze v jednom směru a nikoli ve směru druhém. Využívá se zde pouze jediný kanál. Používá se u většiny optických přenosů, které svou fyzikální podstatou nic jiného neumožňují.
- **Poloduplexní přenos, poloduplex** – poloduplexní přenos může probíhat v jednom nebo druhém směru, ale nikdy ne současně, protože pro příjem i odesílání dat je využíván jediný kanál.

- **Plněduplexní přenos, duplex** - umožňuje přenos současně v obou směrech a lze jej vytvořit několika způsoby:

    1. **Jako čtyř drátové vedení** - každý směr přenosu probíhá po svém páru vodičů.
    2. **Vytvořením dvou frekvenčně oddělených kanálů** na jednom dvoudrátovém spoji.
    3. **Využitím potlačení ozvěn** – kdy modem současně vysílá i přijímá na jednom dvoudrátovém spoji. K oddělení signálů používá techniku potlačení zpětné vlny tj. odečtením vlastního signálu od přijímané směsi dokáže modem rozpoznat přijímaná data. [8]

5.2 Multiplex

Aby byla přenosová kapacita přenosového média lépe využita, přenáší se často jedním médiem současně nebo zdánlivě současně více datových toků. Zařízení, která umožňují sdružit několik kanálů na jedno přenosové médium, se nazývají multiplexory. K zpětnému oddělení kanálů na opačné straně přenosové cesty se potom používají demultiplexory. [9]



Obrázek 10 – Multiplexor a demultiplexor

5.2.1 Obvodový multiplex

V minulosti byl hojně využíván, ale dnes se používá jen výjimečně. Jeho možnosti byly omezeny pouze na přenos nízkofrekvenčních přenosových prostředků, tedy pro telefonní rozvody. Využití spočívalo ve sdružení okruhů po metalickém vedení. Za pomoci transformátorů bylo možné po dvojici dvoupárových vedení přenášet tři telefonní signály.

Dva okruhy přímo využívají dvě kmenové vedení. Pomocí vyvedených středů transformátorů se připojí sdružený okruh. Proud z každého vodiče sdruženého okruhu se rovnoměrně rozdělí do obou vodičů páru kmenového vedení a neovlivní signál kmenového vedení. Podmínkou je přesná symetrie obou polovin vinutí transformátorů s vyvedeným středem. Využitím středů transformátorů fantomních okruhů lze obdobně vytvořit ještě superfantomní okruh. Po čtyřech párech vedení se tak mohlo přenášet sedm nezávislých nízkofrekvenčních signálů. [10]

5.2.2 Frekvenční multiplex

Frekvenční dělení přenosové cesty využívá skutečnosti, že je obvykle k dispozici širší pásmo kmitočtů než obsadíme přenášeným signálem. Přesuneme-li přenášené signály daného kmitočtového pásma do vyšší kmitočtové polohy a vedle nich umístíme další takové signály posunuté o jiný kmitočet, dokážeme přenosovou cestu několikanásobně využít.

Kanály v základním pásmu se posunou o hodnotu kmitočtu do nové frekvenční polohy. Rozestupy kmitočtů musí zaručit, aby se sousední kanály nepřekrývaly. Navíc je nutné ponechat určitou rezervu. Každý posunutý kanál má tzv. nosný kmitočet na který je základní

signál namodulován. K přenosu se využívá několik druhů modulace. Mezi nejčastěji využívané při frekvenčním multiplexu řadíme amplitudovou a frekvenční.

Signál namodulovaný na nosný kmitočet amplitudovou modulací má amplitudu proměnnou dle svého základního průběhu. Signál modulovaný frekvenční modulací přičítá nebo odečítá kmitočet svého základního průběhu k nosnému kmitočtu. Nosný kmitočet musí být minimálně desetkrát větší než největší obsažený kmitočet modulovaného signálu, který chceme přenášet. [10]

5.2.3 Časový multiplex

Jednotlivým kanálům, tvořeným základními signály se přiřazuje na společné přenosové cestě vymezený časový úsek a ostatní časové úseky využívají další kanály. Časové dělení je realizováno přepínači pracujícími synchronně v obou koncových zařízeních. Časové sdružování provádí multiplexor a po přenosu signál opět rozděluje do jednotlivých kanálů demultiplexor**.**

Aby se využil časový multiplex bez neúnosného zkreslení přenášeného signálu je nutné přenášet digitální signál. Digitální systémy využívají pulzní kódovou modulaci k digitalizaci analogového signálu a kombinují ji s principem časového dělení ke sdružování signálů pro efektivní využití přenosových cest. [10]

5.2.4 Vlnový multiplex

Vlnový multiplex je možné využít pouze při přenosu signálů po optickém vedení. Je založen na vysílání optického záření na několika různých vlnových délkách po témže optickém vlákně. Každá vlnová

délka nese namodulovaný jiný elektrický signál. Signál z optických vysílačů v zařízení A pracujících na různých vlnových délkách je navázán do vlákna, přenesen k zařízení B, kde se pomocí optických filtrů rozdělí opět na několik dílčích optických signálů a ty se opětovně převedou na signál elektrický.

Obsazení vlnových délek v okolí 1550nm pro 8 elektrických signálů se nazývá hustý vlnový muldex. Při vývoji se uvažovalo i o řídkém vlnovém muldexu s rozestupy řádově desítek nanometrů. Ten by však obsadil relativně široké pásmo, a proto není využíván. [10]

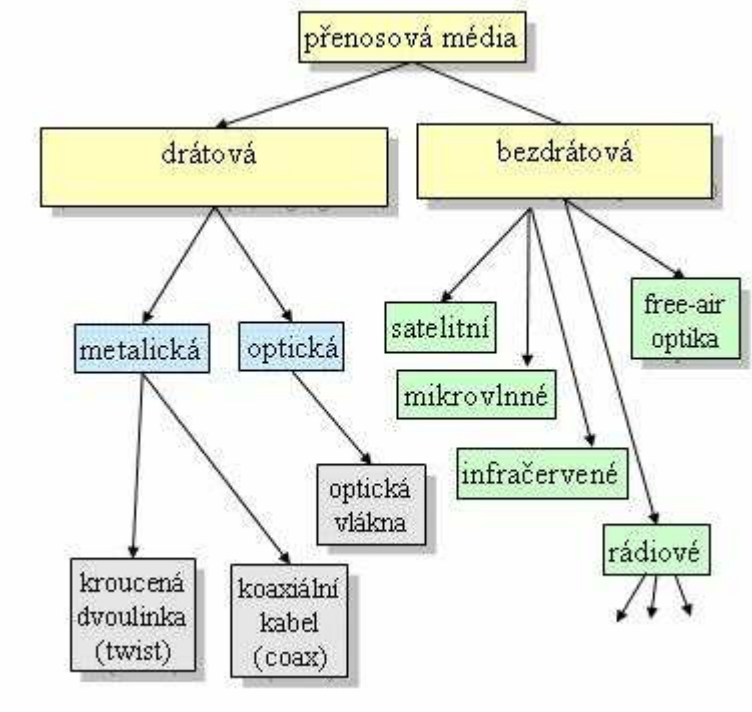
5.2.5 Prostorový multiplex

Jedná se o nejjednodušší, ale o ekonomicky nejnáročnější multiplex. Jde o metalický kabel s potřebným množstvím párů vedení, kde počet párů se rovná počtu přenášených signálů, případně jde o optický kabel, kde počet vláken se rovná počtu přenášených signálů.

Je nutné ho využít tam, kde charakter současně přenášených signálů je takový, že jej není možné bezchybně přenést po daném vedení. Prostorový multiplex je možné využít rovněž tam, kde je k dispozici potřebná kapacita přenosového vedení, případně, kdy nejsme při návrhu přenosové cesty nijak limitováni. [10]

6. Přenosová média

Základem pro fungování počítačových sítí jsou přenosová média, protože právě ona a pouze ona fakticky přenáší nějaká data. Rozdělují se do dvou základních skupin a to na drátová (vodičová) a bezdrátová média.



Obrázek 11 – Klasifikace přenosových médií

Drátová média se vyznačují tím, že přenášený signál prochází pouze skrze ně a až na nežádoucí vyzařování, které se co nejvíce omezuje, je signál neopouští. U bezdrátová médií se šíří signál ve formě elektromagnetických vln otevřeným prostorem, ať již ve všech směrech či jen v určitém konkrétním směru. [11]

6.1 Drátová přenosová média

Drátová média se dále rozdělují na metalická a optická. Optická média se vyrábějí jako optická vlákna přenášející světelné paprsky, která jsou nejčastěji skleněná, ale existují i optická vlákna vyrobená z plastů. Metalická drátová média se nejčastěji vyskytují buď v podobě kroucené dvoulinky, nebo v provedení koaxiálních kabelů. Existují však i různé hybridy mezi oběma variantami.

6.1.1 Metalická drátová média

Nejčastěji se používá kroucená dvoulinka, kde se jede na doraz, co se týká kapacitních možností a koaxiální kabely, u kterých existují jisté rezervy.

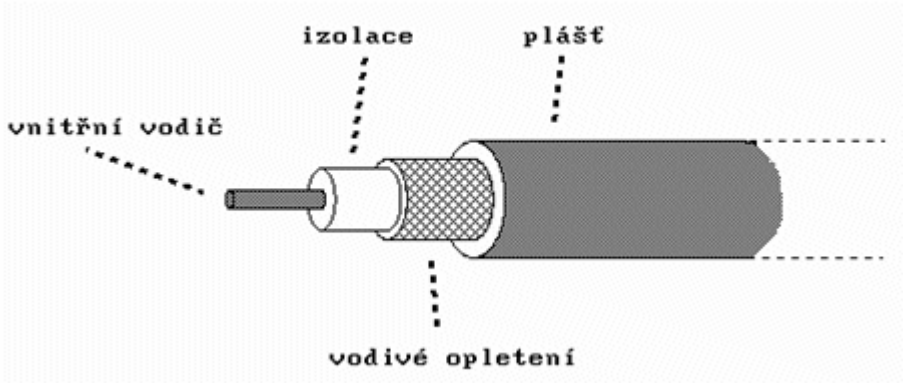
Kroucená dvoulinka je tvořena dvěma izolovanými měděnými vodiči navzájem spirálovitě zkroucenými. Tento pár vodičů představuje jeden komunikační spoj. Určitý počet párů vodičů je svázán do kabelu chráněného pevným vnějším obalem. Vzájemné zkroucení jednotlivých párů vodičů minimalizuje jejich vzájemné elektromagnetické interference.Vyrábí se ve dvou variantách jako stíněná a nestíněná.

Nestíněná kroucená dvoulinka UTP je levnější než stíněná a proto byla běžně používána v infrastruktuře lokálních počítačových sítí. V roce 1991 byl publikován standard, který specifikuje tři kategorie UTP kabelů:

- Kategorie 3 kabelů UTP pro přenosy o rychlosti až 16 Mhz
- Kategorie 4 kabelů UTP pro přenosy o rychlosti až 20 Mhz
- Kategorie 5 kabelů UTP pro přenosy o rychlosti až 100 Mhz

U stíněné kroucené dvoulinky STP je každý pár navzájem zkroucených vodičů obalen kovovou síťkou zabraňující interferenci mezi páry vodičů. Protože je tento typ kabelu dražší než kabely UTP a také práce s nimi je náročnější, tak pokud to bylo možné používala se kabeláž STP mnohem méně než kabeláž UTP.

Koaxiální kabel je tvořen dvěma vodiči. Uvnitř koaxiálního kabelu se nachází vnitřní vodič, kolem kterého je vrstva izolace a kolem ní pak ve formě vodivého opletení druhý vodič. Jeho střed se přitom shoduje se středem vnitřního vodiče. Podstatné ale je, že druhý vodič ve formě vodivého opletení funguje jako účinné stínění po celé délce koaxiálního kabelu, a tím výrazně zmenšuje vyzařování směrem ven.



Obrázek 12 – Schéma koaxiálního kabelu

6.1.2 Optická média

Optický vodič je 2 až 125 μm tenké pružné médium schopné vést optický paprsek. Optický kabel je cylindrický a je složen ze tří soustředných částí. Vnitřní část je jádro, které je obaleno světelně isolační vrstvou a vnějším obalem je plášť chránící funkční část kabelu před mechanickým poškozením, navlhnutím, námrazám apod.

Optická vlákna se rozdělují na mnohovidová optická vlákna s průměrem jádra 50; 62,5 nebo 100 mikrometrů a jednovidová optická vlákna s průměrem jádra 4 až 10 mikrometrů.

Mnohovidová optická vlákna přenáší signál ve formě impulzů. Tyto světelné impulsy se přitom šíří vláknem po částech, označované jako vidy. Každý z nich přitom vstupuje do optického vlákna pod trochu jiným úhlem, a proto se přenáší po trochu jiné dráze což způsobuje zkreslení původního signálu.

Jednovidová optická vlákna jsou výkonnější variantou optických vláken, která vedou světlo jen v podobě jediného vidu. Zde pak nedochází ke zkreslení, a tudíž dosah souvislého segmentu optického vlákna může být větší, typicky až desítky kilometrů. Ovšem tento druh vlákna je dražší než vlákno mnohovidové, a vyžaduje také dokonalejší konektory, světelné zdroje a přijímače.

Mezi výhody optických kabelů v porovnání s vodiči metalickými patří zejména:

- vyšší přenosová kapacita
- menší rozměry a hmotnost
- menší přenosový útlum
- odolnost proti elektromagnetickému rušení
- schopnost přenášet signál na extrémně dlouhé vzdálenosti bez nutnosti obnovy signálu

6.2 Bezdrátová přenosová média

Bezdrátové technologie představují nejrůznější systémy, zařízení a prostředky, které eliminují kabelové vedení, a současně zachovávají stejné služby. Takže nemusí být zařízení fyzicky připojena kabelem, ale využívají se nejrůznější bezdrátové přenosové cesty založené na elektromagnetickém vlnění. Podle frekvence elektromagnetického vlnění se dají bezdrátová média rozdělit do několika skupin.

6.2.1 Rádiové přenosy

Pro přenosy dat se využívá šíření elektromagnetických vln v rádiové části spektra. Vlastnosti rádiových vln se mění v závislosti na použité frekvenci. Při nižších frekvencích tyto vlny sice dokáží obejít všelijaké terénní překážky, ale jejich síla rychle klesá se vzdáleností od vysílajícího zdroje. Vlny vyšších frekvencí zase mají tendenci šířit se více přímočaře, a lze je tudíž mnohem lépe směrovat, resp. přesněji zacílit na určitý konkrétní cíl. Ovšem nevýhoda je že s rostoucí frekvencí jsou rádiové přenosy citlivější na atmosférické podmínky.

6.2.2 Mikrovlnné přenosy

Takto se označují přenosy na frekvencích nad 300 Mhz. Při těchto frekvencích již je možné soustředit energii vln do poměrně úzkého svazku a ten cíleně nasměrovat pomocí vhodné parabolické antény na konkrétní cíl. Ten ale musí být v dosahu přímé viditelnosti, protože takovýto svazek těžko dokáže obcházet nebo procházet terénní ani jiné překážky. Jelikož se takovýto svazek šíří po ideální přímce, vadí mu i zaoblení zemského povrchu. Proto se v praxi umisťují vysílače i přijímače na vhodně vyvýšená místa. Kvůli zakřivení zemského povrchu

a terénním překážkám se pak musí budovat mikrovlnné přenosové trasy na větší vzdálenosti jako řetězce přijímačů a vysílačů, které fungují jako retranslační stanice.

6.2.3 Infračervené přenosy

Přenosy pomocí vln v infračervené části spektra jsou dnes oblíbeným řešením na velmi krátkou vzdálenost, například pro komunikaci mezi notebooky nebo mobilními telefony. Infračervené vlny neprostupují skrz překážky, a tudíž přenosy v jedné místnosti nemohou ohrozit eventuelní souběžný přenos v jiné místnosti a ze stejného důvodu jsou i relativně odolné vůči vnějšímu odposlechu. Na otevřeném prostranství však infračervené přenosy nejsou použitelné, protože naše slunce svítí v infračervené části spektra stejně intenzivně, jako v jeho viditelné části.

6.2.4 Mobilní přenos

Takto se označuje přenos, při kterém se alespoň jeden z účastníků bezdrátového přenosu pohybuje. Základním problémem takovýchto komunikací je kromě dosahu a kvality přenosu také problém s použitím frekvencí tak, aby každá komunikující dvojice mohla používat samostatnou frekvenci, a jednotlivé přenosy se neovlivňovaly navzájem. Pokud se totiž počet vzájemně komunikujících dvojic může dynamicky měnit, není možné jim potřebné frekvence přidělit staticky. Tento problém s přidělováním frekvencí u mobilních bezdrátových komunikací se nejčastěji řeší rozdělením celkového teritoria pohybu na dílčí oblasti neboli buňky, do kterých jsou umístěny základnové stanice. V rámci každé buňky pak pohybující se stanice komunikuje se základnovou stanicí buňky na některé z frekvencí, které jsou pro danou

buňku vyhrazeny. Přitom všechny okolní buňky používají odlišné frekvence, tak aby nedocházelo k interferenci. Při přechodu pohybující se stanice z jedné buňky do jiné dochází k předání spojení ze základnové stanice opouštěné buňky na základnovou stanici nové buňky.

6.2.5 Světelné přenosy

Přenos se provádí tak, že pomocí vhodného laseru se nasměruje úzký paprsek světla ve viditelné části spektra a nechá se šířit vzduchem. Takovéto laserové přenosové systémy jsou již ze své podstaty jednosměrné, a v praxi se proto používají dvojice protisměrných paprsků. Nevýhodou je relativně velká závislost na atmosférických podmínkách, které mohou změnit cílené nasměrování úzkého laserového paprsku tak, že mine svůj cíl.

6.2.6 Satelitní přenos

Satelitní komunikace využívá k šíření signálu buď stacionární satelity, nebo soustavu satelitů pohybujících se vůči povrchu Země. Nejefektivnější jsou přenosy směrem k uživateli, které mohou mít všesměrový charakter, tj. směřovat k více příjemcům současně. Jakmile má být realizován i přenos opačným směrem, musí být použita nějaká forma řízení přístupu k přenosovým kanálům, které satelity vytváří. Dobře zavedenou satelitní technologií, určenou primárně pro přenos dat, je technologie VSAT. Novějším řešením jsou asymetrická řešení, jako např. řešení DirecPC společnosti Hughes, které využívá satelitní spojení pro přenos dat směrem k uživateli, zatímco pro opačný směr jsou využívány pozemní přenosové trasy, zejména telefonní síť. Toto řešení však již připadá v úvahu spíše pro větší uživatele.

6.2.7 Bezdrátové přenosy

Bezdrátové přenosy jsou takové přenosy, které využívají některou z technik přenosu bez použití drátových přenosových cest, a při které vysílač i přijímač jsou pevné a nepohybují se. Podle provedení bezdrátového přenosu se používají termíny lokální smyčka a bezšňůrový přenos.

Lokální smyčka je bezdrátová náhrada metalického vedení mezi telefonní ústřednou a účastnickým přístrojem v domácnosti. Obecněji se takto označuje bezdrátový spoj, který zakončuje určité vedení tím, že vytváří jeho poslední část vedoucí až ke koncovému uživateli.

Bezšňůrový přenos je takové provedení různých domácích spotřebičů, které nahrazuje klasickou šňůru pomocí bezdrátových přenosů. Jde například o bezšňůrové telefony, jejichž sluchátka komunikují se svou základnovou stanicí bezdrátovým způsobem. Mobilita je zde možná, ale jen ve velmi malém dosahu.

7. Zabezpečení dat při přenosech

Při přenosech dat může docházet k chybám, a v jejich důsledku může příjemce přijmout jiné znaky, než jaké mu odesílatel původně vyslal. Jedním možným prostředkem pro následnou detekci vzniklých chyb je přidání paritního bitu ke každému přenášenému znaku. To je však jen nejjednodušší a také nejméně účinný případ použití bezpečnostních kódů.

Základní myšlenka použití bezpečnostních kódů je velmi jednoduchá v tom že původní znaky se podle přesně definovaných pravidel transformují na znaky jiného typu. Např. osmibitové znaky se přidáním jednoho paritního bitu převedou na devítibitové. Teprve ty se pak skutečně přenesou a příjemce si je převede zpět do jejich původního tvaru. Některé znaky jiného typu však nemohou z původních znaků řádným způsobem nikdy vzniknout, např. při používání liché parity by nemělo nikdy dojít k získání znaku se sudou paritou. Pokud pak příjemce přijme takový znak, který při daných pravidlech transformace nemá žádný vzor, může jej oprávněně považovat za chybně přenesený znak.

Bezpečnostní kódy jsou v zásadě dvojího typu, a to:

- **Detekční kódy -** umožňují pouze rozpoznat, že přijatý znak je chybný.
- **Samoopravné kódy -** umožňují kromě detekce chyb i opravu chybně přeneseného znaku, takže jej není nutné přenášet znovu což u detekčního kódu obecně nutné je.

Použití bezpečnostních kódů vždy znamená, že se v rámci každého znaku ve skutečnosti přenáší více bitů, než kolik by bylo k vyjádření vlastního znaku nezbytně nutné. Zabezpečení proti chybám

není navíc nikdy stoprocentní, jeho účinnost však roste s počtem bitů navíc. Nejjednodušší detekční kód přidává k datovým bitům jeden další bit a dokáže detekovat chybu v jednom bitu. Samoopravný kód, který umožňuje následnou opravu chyby v jediném bitu tzv. rozšířený Hammingův kód, přidává ke každému 8-bitovému bytu navíc pět bitů, resp. 6 bitů ke každému 16-bitovému slovu.

V praxi je výhodnější nezabezpečovat proti chybám jednotlivé znaky, ale celé posloupnosti znaků resp. celé přenášené bloky dat. Dodatečné bity, používané k detekci chyb se pak nepřidávají znovu ke každému znaku, ale jen jednou k celému bloku dat a přenesou se spolu s ním. Je-li pak chyba detekována, nelze ji v rámci bloku lokalizovat až na jednotlivé znaky. Místo toho musí být celý blok prohlášen za chybný a přenesen znovu. To ovšem nemusí být vůbec na závadu, protože přenosy dat téměř vždy probíhají po celých blocích, a nejmenší jednotkou dat, jejíž opakované vyslání si může příjemce vyžádat, je právě celý blok a nikoli jednotlivé znaky. [12]

7.1 Podélná parita

Podélná parita je jedním možným způsobem zabezpečení celého bloku dat, chápaného jako posloupnost jednotlivých znaků. Zde se nekontroluje sudý resp. lichý počet jedničkových bitů v jednotlivých znacích, ale sudý resp. lichý počet jedničkových bitů ve stejnolehlých bitových pozicích všech znaků v bloku. Je-li tedy blok dat tvořen např. osmibitovými znaky, přidá se k celému bloku osm paritních bitů a každý z nich se nastaví tak, aby byla dodržena sudá resp. lichá parita.

Použití podélné parity se někdy kombinuje i se zabezpečením jednotlivých znaků pomocí sudé resp. liché parity, která se pak pro odlišení od podélné parity označuje jako příčná či znaková parita. [12]

7.2 Kontrolní součet

Další možností zabezpečení celého bloku dat je součet jednotlivých znaků v bloku, které jsou pro tento účel chápány jako celá dvojková čísla bez znaménka. Kontrolní součet se typicky provádí jako součet modulo 2^8 nebo 2^{16}, tj., že výsledkem je kontrolní součet o délce jednoho nebo dvou bytů.

Kontrolní součet i podélnou paritu lze vyhodnocovat průběžně při přijímání jednotlivých znaků bloku. V případě kontrolního součtu se každý nově přijatý znak přičítá ke stávajícímu mezisoučtu, zatímco v případě podélné parity se provádí operace XOR jednotlivých bitů nového znaku se stávajícím mezivýsledkem. [12]

7.3 Cyklické kódy

Nejúčinnější formu zabezpečení bloku dat představuje použití cyklických kódů CRC. Také zde se podobně jako u výpočtu podélné parity či kontrolního součtu průběžně na základě jednotlivých znaků bloku průběžně vypočítává zabezpečovací údaj. Ten se na konci celého bloku porovná se zabezpečovacím údajem, který podle stejných pravidel vypočítal odesílatel a připojil k odesílanému bloku dat. Pokud se oba údaje shodují, lze přenesený blok s vysokou pravděpodobností považovat za správný. Zabezpečení pomocí šestnáctibitového cyklického kódu totiž dokáže spolehlivě odhalit všechny chyby až v šestnácti po sobě jdoucích bitech, a chyby ve větším počtu bitů s přesností 99,9984 %.

Vynikající účinnosti zabezpečení pomocí cyklického kódu vyžaduje dosti pokročilý matematický aparát, vlastní způsob výpočtu zabezpečovacího údaje je však velmi jednoduchý . Stačí k němu jednoduchý posuvný registr, umožňující provést operaci XOR s pevně

danou maskou. Hodnota této masky je jednoznačně určena generujícím polynomem, na kterém musí být příjemce i odesílatel předem dohodnuti. Použitelných tvarů těchto polynomů je více. V oblasti komunikací se nejčastěji používá polynom $x^{16} + x^{12} + x^5 + 1$, doporučený organizací CCITT. [12]

8. Řízení toku dat

Základní charakteristikou všech mechanismů a technik řízení toku je skutečnost, že průběh přenosu by se měl řídit možnostmi příjemce, a nikoli schopnostmi odesílatele. Rozhodující slovo by tedy měl mít příjemce, který by měl mít možnost diktovat tempo vzájemné komunikace. Konkrétně by měl mít právo přimět odesílatele, aby dočasně pozastavil odesílání dalších dat, a následně jej zase mohl informovat, že ve vysílání může pokračovat.

V praxi je konkrétní řízení toku často kombinováno s mechanismy potvrzování. Když už příjemce vysílá zpět k odesílateli informaci o tom, zda a jak co přijal, je vhodné s ní spojit i informaci o tom, co dalšího je či není schopen přijmout, tedy informace potřebné pro řízení toku. [13]

8.1 Jednotlivé potvrzování

Důležité je, že potvrzení může být kladné, potvrzující bezchybný přenos, nebo naopak záporné, signalizující chybně přenesený blok. Podstatné je také to, jak odesílatel s potvrzením nakládá. Jedna základní možnost je taková, že když odesílatel odešle nějaký blok dat, nejprve čeká na odezvu druhé strany. Pokud dostane kladné potvrzení, pokračuje odesláním dalšího bloku a znovu čeká na potvrzení. Pokud dostane záporné potvrzení, odešle stejný blok znovu.

Kromě toho ale musí počítat ještě se dvěma dalšími možnostmi. Mohl by se ztratit celý přenášený blok, takže příjemce ani neví, že by měl něco potvrzovat, anebo že se ztratilo samotné potvrzení, které příjemce vygeneroval. V obou případech odesílatel musí určitou dobu čekat po určitý časový limit. Když do uplynutí této doby nedostane

žádné potvrzení, interpretuje to stejně jako potvrzení záporné a přenos bloku opakuje. Velikost časového limitu musí být volena velmi pečlivě. Pokud by byla příliš krátká, odesílatel by mohl opakovat přenos dříve, než mu potvrzení přijde. Naopak pokud by byl časový limit příliš velký, odesílatel by čekal zbytečně dlouho a přenos by se zbytečně zpomaloval. [14]

8.2 Kontinuální potvrzování

Jednotlivé potvrzování je vhodné pouze pro takové sítě, ve kterých cesta tam a zpět od odesílatele k příjemci netrvá dlouho. Tedy tam, kde je malé přenosové zpoždění. Týká se to hlavně lokálních sítí LAN. V rozlehlých sítích WAN je přenosové zpoždění relativně velké, a kvůli tomu neúměrně narůstají prodlevy, způsobené čekáním na potvrzení každého jednotlivého bloku.

V prostředí rozlehlých sítí je proto výhodnější kontinuální potvrzování. Od jednotlivého potvrzování se liší v tom, že když odesílatel odešle nějaký blok, nečeká na jeho potvrzení, ale pokračuje odesláním dalšího bloku. Posílá tedy jednotlivé datové bloky jeden za druhým a teprve zpětně přijímá potvrzení o tom, jak byly tyto bloky doručeny. Pokud ale odesílateli přijde záporné potvrzení, nebo se ani po uplynutí časového limitu nedočká žádného potvrzení, a musí vše interpretovat jako záporné potvrzení, tak existují dvě možné varianty, jak odesílatel zareaguje. [14]

8.2.1 Selektivní opakování

Selektivní opakování spočívá v tom, že odesílatel znovu odešle právě ten blok, který se poškodil či ztratil a dále pokračuje, jako kdyby se nic nestalo. Nevýhodou selektivního opakování je vyšší náročnost na

příjemce. Pokud totiž přijme nějaký poškozený blok nebo jej nepřijme vůbec, ještě nějakou dobu poté musí přijímat následující bloky, které ale nemůže zpracovávat. Místo toho je musí někam ukládat a čekat, až dostane původně poškozený či ztracený blok znovu. Teprve pak může začít zpracovávat i následující, již přijaté bloky. [14]

8.2.2 Opakování s návratem

Opakování s návratem spočívá v tom, že když odesílatel dostane záporné potvrzení, nebo mu vyprší časový limit, znovu odešle příslušný blok a poté pokračuje těmi bloky, které po něm následují bez ohledu na to, že některé z nich mohly být odeslány v mezidobí. Jde sice o šetrnější variantu vůči příjemci, ale na druhé straně může zbytečně plýtvat přenosovou kapacitou. Může totiž znovu přenášet bloky, které se již jednou přenesly úspěšně bez chyb. [14]

8.3 Samostatné a nesamostatné potvrzování

Na závěr bych se zastavil u toho, jakou konkrétní podobu mohou mít potvrzení, zasílaná od příjemce směrem k odesílateli. Jednou možností je, že potvrzení jsou zcela samostatná, neboli jde o principiálně stejné bloky, v jakých se přenáší i samotná data. Mají tedy svou vlastní hlavičku, která určitým způsobem zvyšuje režii na přenos.

Snaha eliminovat tuto režii vedla ke vzniku nesamostatného potvrzování. To spočívá v tom, že příjemce původních dat čeká s jejich potvrzením, dokud v protisměru necestuje nějaký jiný datový blok z nějakého jiného přenosu a do něj jen přidá své potvrzení. Využívá tedy toho, že zmíněný blok v protisměru patřící nějakému jinému přenosu, již tak jako tak má svou hlavičku a další náležitosti a tudíž je přírůstek režie na zajištění potvrzení minimální. I nesamostatné potvrzování má

však své nevýhody. Zejména to, že příjemce nemůže čekat příliš dlouho na to, až bude v protisměru přenášen nějaký jiný datový blok, do něhož by své potvrzení vložil. Odesílatel o tom totiž neví a mohl by mu vypršet časový limit. V praxi se příjemce snaží o nesamostatné potvrzení jen chvíli, pokud se mu nepodaří, přechází k samostatnému potvrzení. [14]

9. Závěr

Cílem mé práce bylo stručně a co možná nejjednodušeji popsat fyzickou a linkovou úroveň přenosu v počítačových sítích, tak, aby jednotlivé body byly srozumitelné pro laika, a zároveň aby tato práce byla takovým malým průvodcem pro někoho, kdo by se chtěl touto problematikou zabývat.

10. Použitá literatura

1. http://www.volny.cz/krivka/struktura_pc_siti.htm
2. http://www.earchiv.cz/a92/a212c110.php3
3. http://www.manualy.sk/archiv/a629k150.htm
4. http://www.earchiv.cz/a95/a504c502.php3
5. http://www.earchiv.cz/a92/a231c110.php3
6. http://www.manualy.sk/archiv/a140c110.htm
7. http://www.manualy.sk/archiv/a649k150.htm
8. http://www.earchiv.cz/b05/b1000001.php3
9. http://www.fme.vutbr.cz/opory/pdf/p_site.pdf
10. http://www.elektrika.cz/data/clanky/pvvpt
11. http://www.earchiv.cz/b05/b0900001.php3
12. http://www.earchiv.cz/a91/a141c110.php3
13. http://www.manualy.sk/archiv/a527k130.htm
14. www.pcworld.cz/pcw.nsf/6cac9c2b3bf47bb3c12570f9003d6854/e21a1e4e82e52531c12570f9003d240e?OpenDocument