

POČÍTAČOVÉ SÍTĚ

ÚVOD DO POČÍTAČOVÝCH SÍTÍ LAN

Počítačové sítě LAN jsou podmnožinou obecných počítačových sítí. Lze je tedy definovat jako výpočetní systémy, které se skládají z jistého počtu vzájemně propojených a spolupracujících počítačů, které mají určité charakteristické vlastnosti.

LAN – Local Area Networks - lokální počítačové sítě

Lokální síť se rozkládá na omezeném teritoriu, obvykle budova nebo komplex blízkých budov. Není třeba používat prostředků pro dálkový přenos. Další charakteristickou vlastností sítí LAN je jejich homogennost – to znamená, že jsou v nich zařazeny jen počítače jednoho druhu (obvykle PC).

WAN – Wide Area Networks - rozlehlé počítačové sítě

Jsou protikladem sítí LAN. V nich naopak je nutno používat prostředků pro dálkový přenos dat.

Základní součásti sítí LAN

- stanice sítě
- síťový hardware
- síťový software
- organizační zabezpečení

Stanice sítě

Označují se tak počítače, vzájemně propojené sítí, a to včetně jejich vybavení (např. tiskárny, plotry...)

Podle role, kterou v síti zastávají, dělí se na:

1. Servery

Tyto stanice poskytují některé své prostředky do sítě, ty pak mohou ostatní uživatelé sítě používat (kromě svých vlastních lokálních prostředků). Takto lze docílit mnohonásobně výhodného sdílení hardwarových i softwarových prostředků i datových souborů. Dále servery zajišťují chod sítě a realizují jednotlivé síťové funkce. Vzhledem k činnostem, které provádějí, bývají na ně kladeny vysoké požadavky, co se týká spolehlivosti a rychlosti. V síti může pracovat jeden nebo více serverů.

2. Pracovní stanice

Slouží uživatelům k provádění jejich prací. Tyto stanice do sítě nic nenabízejí, ale naopak umožňují přístup ke sdíleným síťovým prostředkům.

Síťový hardware.

Jsou to všechny technické prostředky, které slouží ke vzájemnému propojení jednotlivých stanic sítě. Jsou to především síťové desky, propojovací kabely a různé zesilovací a rozbočovací prvky. V současné době existuje několik standardů síťového hardware, např. Ethernet, Token Ring a další. Použitím určitého standardu je určeno, jakým způsobem mohou být stanice vzájemně propojeny, z jakých konkrétních prvků může být síť sestavena a také jakou rychlostí bude probíhat komunikace (podrobněji o síťových standardech viz dále).

Síťový software

Souhrn programových prostředků, které ve spolupráci se síťovým hardwarem zajišťují činnost sítě. Softwarové prostředky, používané v sítích LAN pracují buď jako rezidentní programy v prostředí vlastního operačního systému stanice (např. DOS, Windows) nebo jsou vytvořeny jako samostatný operační systém.

Síťový software určuje vlastnosti sítě – např. rozsah nabízených služeb, zabezpečení sítě, způsob práce v síti a koncepce uložení dat v síti. Podle toho, jakým způsobem je řešena koncepce uložení dat v síti (tj. v závislosti na vlastnostech síťového software), můžeme síť LAN rozdělit na dva typy:

a) síť PEER TO PEER

Podporují uchovávání dat na větším počtu stanic. Zde se programové vybavení pro servery a pracovní stanice příliš neliší. Obvykle se jedná o nevelké rezidentní programy, které se instalují a spouštějí na všech stanicích sítě. Cena takového software je stejná jak pro pracovní stanici, tak pro server. Počet serverů se zde nemusí nijak omezovat, serverem může být každá stanice, která disponuje něčím, co je vhodné nabídnout do sítě. Příklad této koncepce: v malé organizaci několik původně samostatných počítačů je propojeno do sítě. Jejich uživatelé si však data i nadále uchovávají na svých lokálních discích a pouze na několika stanicích se některé adresáře zpřístupní ostatním uživatelům s cílem umožnit jejich sdílení. Tyto stanice pak pracují jako **nevyhrazené (nondedicated) servery**, tzn. chovají se současně jako server i pracovní stanice. Typické pro síť **peer-to-peer** je tedy rozložení sdílených dat na mnoho stanic v síti.

V současné době k významným představitelům sítí tohoto typu patří:

- Personal NetWare (Novell) - nebo jeho předchůdce: NetWare Lite
- LANtastic (Artisoft)
- Windows for Workgroups (Microsoft)

b) sítě CLIENT TO SERVER

Představují mnohem vyšší úroveň sítí LAN. Zde je podporováno uložení dat na jednom či jen malém počtu serverů, to znamená centralizovaně.

V těchto sítích se software pro servery a software pro pracovní stanice podstatně liší. Zatímco na pracovních stanicích jsou i nadále používány nevelké rezidentní programy, na serverech sídlí samostatný vysoce výkonný operační systém, specializovaný na síťové činnosti. Cena tohoto op. systému bývá mnohonásobně vyšší, takže se nevyplácí instalovat v síti více serverů, než je nezbytně nutné. Na serverech se tedy vyskytuje naprostá většina sdílených dat, odehrává se zde většina síťových činností.

Z toho plyne možnost snadnějšího zabezpečení, archivace a zpracování **síťových dat**. Servery pracují téměř výhradně jako **vyhrazené (dedicated) servery**, tj. nelze je už využívat jako pracovní stanice. Na pracovních stanicích je jich pak uloženo jen nezbytné minimum a v případě bezdiskových stanic vůbec nic.

Hlavními představiteli sítí typu **Client to server** jsou: NetWare 3.x a 4.x od firmy Novell
Windows NT Advanced Server - Microsoft
Vines od firmy Banyan Systems

Organizační zabezpečení

Hlavním úkolem této základní čísta sítí LAN je dosáhnout takového stavu, aby byla zajištěna korektní činnost sítě. Sestává ze dvou složek:

- **personální zajištění** - uživatelé musí být náležitě poučeni o práci v síti, aby byla dostatečně zajištěna správa sítě. Také je určena jedna nebo několik vhodných osob do funkce správce sítě.
- **provozní pravidla** - souhrn pravidel a nařízení, která upravují způsob práce v síti. Jedná se např. o určení doby provozu sítě, způsob přihlašování do sítě, přidělování přístupových práv, používání hesel apod.

Výhody poskytované sítí LAN

Oproti práci na **samostatných počítačích** přinášejí **sítě LAN** řadu výhod. K těm nejvýznamnějším patří:

- sdílení dat
- sdílení prostředků
- vyšší spolehlivost výpočetního systému
- dokonalejší ochrana dat
- komunikace mezi uživateli

Sdílení dat

Tím se myslí skutečnost, že více uživatelů může pracovat s určitými daty současně. To je považováno za největší výhodu. Tato možnost je vyžadována řadou aplikací, které by bez toho nešlo vůbec provozovat.

Sdílení v sítích LAN se jednoduše praktikuje tak, že data, která je třeba sdílet se umístí na server a tam k nim pak mají všichni uživatelé sítě přístup.

Pomocí standardních prostředků sítě lze pro každého uživatele určit, jaké činnosti s daty mohou provádět.

Sdílení prostředků

Běžné uživatele zajímá nejvíce. Tímto způsobem lze totiž výrazně snížit pořizovací náklady na výpočetní systém. Pro představu: V organizaci například pracuje 20 pracovníků na PC. Ve variantě bez sítě hrozí nutnost zakoupit také 20 tiskáren. Jsou-li počítače propojeny do sítě, stačí pořídit tiskáren výrazně menší počet (třeba 3) a kvalitní, a nainstalovat je v síti tak, aby k nim měl přístup každý uživatel. Ten může pracovat tak, jako by měl svou vlastní tiskárnu u svého počítače.

Uvedené sdílení prostředků se ještě častěji týká disků. Servery jsou vybaveny velkokapacitními a spolehlivými disky a uživatelé na nich mají uložena všechna data nebo jejich naprostou většinu. Tím lze také ušetřit značné finanční částky. Mimo tiskáren a disků lze sdílet i další periferní zařízení, například disky CD-ROM, plottry, skenery, modemy apod.

Mimo hardwarových zařízení bývá výhodné sdílet i samotné programy. Ty jsou instalovány na serveru, odkud si je každý uživatel spouští.

Vyšší spolehlivost výpočetního prostředí

Bezprostředně souvisí se zmíněným sdílením prostředků. Díky tomu se totiž dá v síti snadno realizovat zálohování jednotlivých prostředků. **Například:** při poruše některé ze sdílených tiskáren lze bez problémů pokračovat v práci na jiné tiskárně. Nebo jsou-li data soustředěna na serveru, pak při poruše vlastní pracovní stanice stačí si přesehnout k jiné a může se pokračovat v práci.

Dokonalejší ochrana dat

Ochrana dat je třeba v procesu zpracování dat věnovat zcela mimořádnou pozornost. Datům totiž hrozí mnohá nebezpečí, např. ztráta dat při poruchách PC, při jejich neodborném zpracování nebo když k nim získají přístup nepovolané osoby. U samostatných počítačů si každý vlastník PC zajišťuje ochranu svých dat vlastními silami, což bývá často velmi nedostatečné.

U sítí je principiální výhodou to, že data jsou soustředěna na jednom nebo několika serverech. Pokud se věnuje dostatečná pozornost výběru co nejspolehlivějšího serveru, dbá se na fyzické zabezpečení serverů před nepovolanými osobami, pokud se využívá důsledně hesel a přístupových práv pro jednotlivé uživatele a pokud se provádí důsledně archivace dat, pak lze ochranu dat zajistit na poměrně vysoké úrovni.

Komunikace mezi uživateli

Počítačová síť umožňuje svým uživatelům mezi sebou komunikovat, t.j. předávat si mezi sebou zprávy a výsledky své práce. Komunikace v sítích bývá realizována různými způsoby. Nejjednodušší je prosté zasílání **zpráv**, obvykle jednořádkových.

Vyšší formou komunikace je **dialog (chat)**. Uživatel má při tom na obrazovce 2 okna, v jednom se zobrazuje text, který odesílá svému protějšku a ve druhém naopak přijímané zprávy od něj.

Velmi užitečnou formou je **síťová pošta**, která umožňuje předávat zprávy i těm uživatelům, kteří právě nejsou přihlášení. Zprávy se totiž udržují v prostředí sítě až do doby, než si je adresát převezme.

Zajímavá je i možnost **hlasové komunikace**. Z technického hlediska totiž není problém přenášet po síťovém vedení hlasovou zprávu v digitalizované podobě, či ji dokonce uchovávat v poštovní schránce.

TOPOLOGIE POČÍTAČOVÝCH SÍTÍ LAN

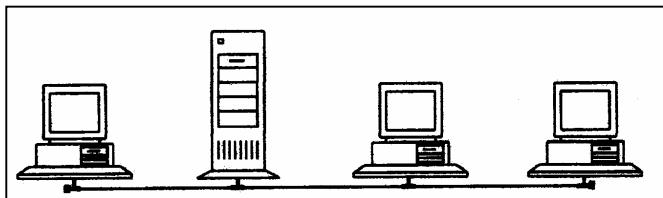
Topologie – způsob, jakým jsou jednotlivé stanice v síti vzájemně propojeny. Na rozdíl od sítí WAN, kde je používána volná forma propojení, vedoucí ke stavu, že mezi počítači běžně existuje více propojovacích cest, v prostředí LAN je tomu jinak. V rámci jedné sítě LAN existuje mezi každými dvěma stanicemi jen jediná spojovací cesta. V současné době se používají 3 základní typy topologií: **sběrníková**, **hvězdicová**, **kruhová**.

Sběrníková topologie

K propojení stanic je použito průběžné vedení, k němuž jsou jednotlivé stanice připojeny pomocí odbočovacího prvku (T – konektoru). Výhodou je jejich jednoduchost (propojení od stanice ke stanici) a menší spotřeba propojovacího kabelu.

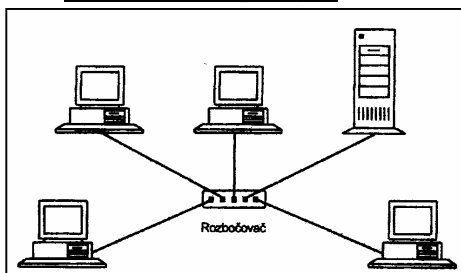
Nevýhodou je to, že v případě poruchy (nejčastěji u T konektoru) se ocitne mimo provoz celá síť. Dále u

koncových stanic musí být připojen ukončovací odpor (např. 50 ohmů), aby se zabránilo odrazům na volném konci vedení. Sběrníková topologie je často užívána tam, kde je použit pro spojení počítačů koaxiální kabel.



Obr. Příklad sítě se sběrníkovou topologií

Hvězdicová topologie.



Síť má podobu hvězdy. V jejím středu je zařízení nazvané **rozbočovač (HUB)** a k němu jsou připojeny jednotlivé stanice. Propojení připomíná stromovou strukturu. Ta se může jednoduše rozšiřovat tak, že na místě libovolné stanice se může zapojit další rozbočovač.

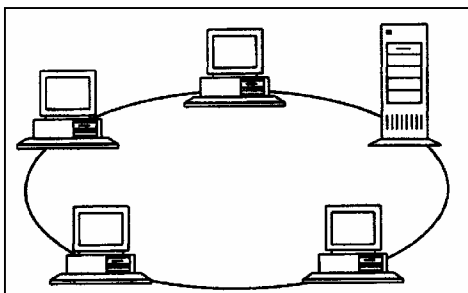
Výhodou je menší náchylnost k poruchám, poněvadž při poruše vedení či konektoru zůstane mimo provoz jen jedna stanice či jeden segment sítě. Nevýhodou je velká spotřeba kabeláže.

Obr. Příklad sítě s hvězdicovou topologií

Díky tomu se poruchy také mnohem snadněji vyhledávají. Tato technologie nejčastěji používá **kroucené dvojlinky**. Společným rysem sběrníkové i hvězdicové topologie je skutečnost, že zpráva vyslaná jednou stanicí se šíří ke všem stanicím, přijímá ji ovšem jen ta již je určena. U všech tří topologií pak je lhostejné, v kterém místě sítě je umístěn server. (obdobou hvězdicové topologie je **topologie stromová**).

Kruhová topologie

Stanice jsou propojeny tak, že vytvářejí souvislý kruh. Provoz je jednosměrný, tzn. že zprávy jsou předávány od stanice ke stanici stále jedním směrem.



Koncepce předávání zpráv je jednoduchá a snadno lze ověřovat neporušenost zprávy při oběhu celým okruhem.

Jsou zde však i jisté nevýhody. Při poruše sítě v kterémkoli místě je tato zcela vyřazena. Dále nutnost přemostování vypnutých či odpojených stanic pomocí speciálních zařízení (jednotky MAU)

Obr. Příklad sítě s kruhovou topologií

METODY PŘÍSTUPU NA SPOJOVACÍ VEDENÍ

Metodou přístupu máme na mysli způsob určování, která ze stanic pracujících v síti a hodlajících ve stejném okamžiku vysílat zprávu, může tuto zprávu skutečně odeslat. Jde tedy o pravidlo, kterým se rozhoduje mezi stanicemi soutěžícími o přístup na vedení. Použití určitého pravidla souvisí s topologií sítě a s použitým standardem síťového hardware.

V současnosti jsou používány tyto metody přístupu:

CSMA/CD

Mnohonásobný přístup s detekcí nosné a s detekcí kolize (*carrier sense multiple acces with collision detection*) Někdy se tato metoda nazývá metoda náhodného přístupu, což vyplývá z dalšího popisu.

Tento způsob rozhodování o tom, která ze stanic bude mít právo vysílat zprávu je velmi jednoduchý. Stanice, která chce vysílat zkontroluje, zda právě někdo jiný vysílá (detekce nosné). Když zjistí, že je na přenosovém kanálu (médiu) klid, zahájí vysílání své zprávy. Přitom ale kontroluje, zda v tomtéž okamžiku nezačala vysílat i jiná stanice a zda tedy nedochází ke kolizi zpráv. Pokud by tomu tak bylo (což zjistí obě vysílající stanice), přeruší obě odesílání zpráv a po chvíli (náhodně generovaný časový úsek) se o to budou pokoušet znovu. Stanice, která první detekuje kolizi, vyšle speciální krátký *signál oznamující kolizi* o 32 bitech.

Pokud na kanálu není klid, musí čekat až se uvolní.

Základním principem CSMA/CD je tedy *neustálé naslouchání nosné* pro zjištění obsazenosti média a pro detekování kolizí. Dalším podstatným principem je *náhodnost zpoždění* s jakým stanice při zjištění klidového stavu na médiu začne vysílat.

Výhodou této metody je její jednoduchost, což přináší vyšší rychlost práce v takové síti. To však platí jen při nižších a středních zatíženích sítě. Se vzrůstajícím zatížením sítě, tj. s přibývajícím množstvím paketů, které jsou přenášeny však dochází stále častěji ke kolizím zpráv a to dále znamená, že vznikají časové ztráty. Tím možnost rychlého přenosu dat klesá a v mezních situacích může dojít až k zahlcení celé sítě. De facto vlastně nikdy nelze zaručit, že zpráva bude do určité doby doručena. Říkáme, že metoda nemá *deterministický charakter*, tj. nemožnost určit, dokdy bude daná zpráva přenesena (*determinace = určení, vymezení*). To je nepříjemné zvláště u systémů řízení v reálném čase. Uvedená metoda se často používá u standardů Ethernet.

TOKEN RING – IEEE 802.5

Tato metoda je založena na zásadě, že právo vysílat zprávu má v každém okamžiku vždy pouze jediná stanice v síti. Toto právo – token – si pak stanice mezi sebou postupně předávají (*token* – v překladu „pešek“ – zvláštní rámeček, který obsahuje cílovou adresu. Stanice s touto adresou má po obdržení tokenu právo po určitou dobu spravovat přenosový prostředek. Může vyslat data, může vyzývat ostatní stanice a také přijímat odpovědi.).

Uvedená metoda se používá především v sítích s kruhovou topologií a v nich je postup předávání práva jednoduše určen fyzickým propojením stanic v kruhu. Postupuje se tak, že stanice, jakmile dostane zprávu vysílat, odešle tuto zprávu (má-li nějakou) a s ní i toto právo další stanici následující v kruhu. Výhodou této metody je její odolnost proti zahlcení i při vysokém zatížení sítě a její deterministický charakter (t.j. můžeme určit, dokdy bude daná zpráva k adresátovi přenesena). Mírnou nevýhodou oproti CSMA/CD je její větší složitost a z toho plynoucí o něco menší rychlost přenosu dat. Ta se ovšem uplatňuje hlavně při menších zátěžích, tj. v situacích kdy to není až tak podstatné.

TOKEN BUS - IEEE 802.4

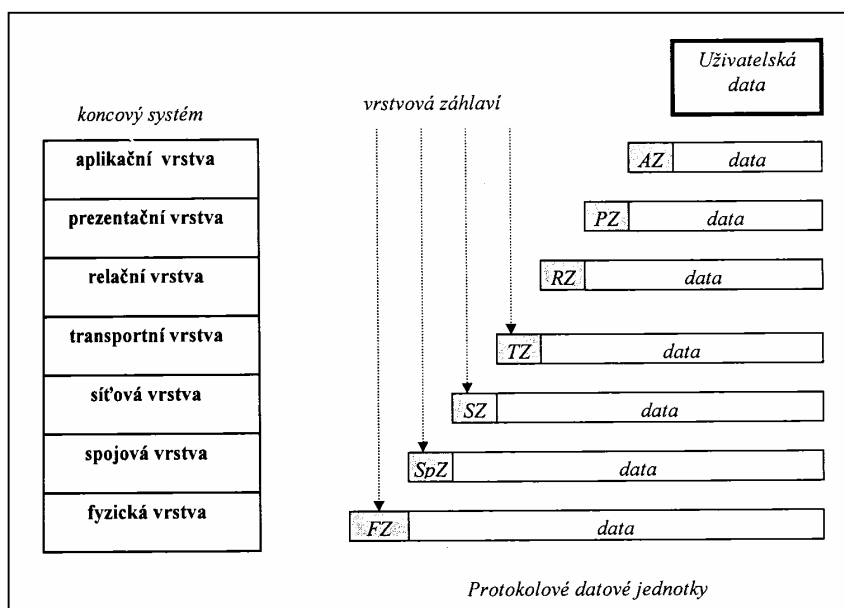
Obdobu předchozí metody, schopná pracovat i v sítích se sběrníkovou nebo hvězdicovou topologií. Postup předávání zpráv zde však není odvozen od fyzického propojení stanic do kruhu, ale je zde vytvořen tzv. logický kruh, do kterého si tato metoda sama seřadí stanice. Algoritmus této metody je však o něco složitější díky nutnosti udržovat stanice v logickém kruhu i přes jejich zapínání a vypínání.

Bývá používán např. u počítačových sítí standardu Arcnet.

Sít'ová architektura -model ISO / OSI

Sít'ová architektura je popsána **systémem vrstev, služeb, funkcí a protokolů**. Představuje strukturu řízení komunikace v systémech, tj. souhrn řídicích činností umožňujících výměnu dat mezi komunikujícími systémy a splňujících určité výkonnostní požadavky v požadovaných mezích. Komunikace a jejich řízení je příliš složitý problém sestávající z celé řady dílčích problémů a úkolů. Proto se přistoupilo k rozdělení tohoto problému do několika skupin, tzv. **vrstev**. Každá vrstva sít'ové architektury je definována **službou**, kterou je schopna poskytovat sousední vyšší vrstvě a funkcemi, které vykonává v rámci protokolu. Podmnožinou řídicích činností jsou **funkce**, které se vykonávají v jednotlivých vrstvách a které jsou charakterizované společným cílem, účelem a účinkem, např. řízení zabezpečení dat, řízení toku dat, směrování, vytvoření či zrušení spoje, adresování atd. Protokoly představují formální stránku řízení komunikace, protože poskytují formální nástroj na uskutečňování věcné náplně řízení komunikace a pomáhají tak realizovat příslušné komunikační funkce. Protokoly tvoří souhrn pravidel, formátů a procedur, určujících výměnu údajů mezi dvěma komunikačními prvky. Protokol specifikuje výměnu řídicích údajů mezi komunikujícími stanicemi tj. **protokolových datových jednotek – PDU (protocol data unit)**. Protokolové datové jednotky obsahují záhlaví s **protokolovou řídicí informací – PCI (protocol control information)**.

Pro definování způsobů komunikace mezi počítači již byla vytvořena řada standardů. K nejvýznamnějším, které se týkají i sítí LAN patří model definovaný organizací **ISO (International Standards Organization)**, která zavádí a rozšiřuje celosvětové standardy v mnoha oblastech. Model má název **Open Systems Interconnections** - odtud zkratka **OSI**. Důraz je kladen na **otevřenost**, tj. požadavek, aby všechna koncová zařízení, vyhovující mezinárodním normám byla volně připojitelná na síť s jednotnou sít'ovou architekturou. Zpráva, soubor nebo jakákoliv data, která budou odesílána do sítě, musí projít několika vrstvami, které všechny slouží k tomu, aby data sítí prošla přesně a neporušená. Nejvyšší vrstvou je vrstva aplikační, a to je jediná část procesu, kterou uživatel vidí (strana uživatele). Nejnižší je fyzická vrstva.



Referenční model OSI je sedmivrstvý. Každá ze sedmi vrstev architektury vykonává skupinu jasně definovaných funkcí potřebných ke komunikaci s jiným systémem. Pro svoji činnost **využívá služeb své sousední v hierarchii nižší vrstvy** (pokud existuje). Svoje **služby pak poskytuje sousední vyšší vrstvě** (pokud existuje). Uvedené vrstvy jsou v převážné míře realizovány sít'ovým softwarem (vrstvovými komunikačními protokoly). Požadavek na přenos zprávy, který např. vydá uživatel nebo jeho aplikační program, prochází na stanici odesílatele postupně jednotlivými vrstvami, počínaje vrstvou aplikační a konče vrstvou fyzickou. Při tom v každé z nich je podroben příslušnému zpracování. Po přenosu spojovacím vedením na stanici

adresáta pak opět prochází všemi vrstvami, nyní ovšem v obráceném pořadí, až dospěje k cílovému uživateli či k cílové aplikaci. Je třeba zdůraznit, že model **ISO / OSI** je navržen pro obecné sítě, tedy i pro síť **WAN**. U sítí **LAN**, které v některých směrech jsou jednodušší, nemusí být některé vrstvy vůbec nikdy využity, jiné jen částečně. Některé funkce a služby se opakují v několika vrstvách. Platí to zejména o řízení toku, formátování a zabezpečení, ale nejedná se o duplicitní, ale vzájemně se doplňující funkce svým rozsahem a určením.

Fragmentace a segmentace

Zprávy se podle svých délek dělí na **fragментy** a podle druhu sítě se z těchto fragmentů vytvářejí **bloky** (v transportní vrstvě), **pakety** (v síťové vrstvě), **rámce** (ve spojové vrstvě). Ve fyzické vrstvě se pracuje se sledem bitů (při sériovém přenosu) nebo skupin bitů, např. značek či oktetů (při paralelním přenosu). Každé zapouzdření vyvolává nadbytečnost přenášených zpráv, ale je nezbytné k funkci vrstevových a mezivrstevových protokolů. **Datové jednotky** v různých vrstvách někdy nemusí být slučitelné z hlediska svých délek. Může nastat potřeba zobrazit **datovou jednotku vyšší vrstvy (SDU)** do několika PDU. Vždy je pak nutné zajistit přesné označení všech částí příslušejících dané datové jednotce, aby bylo možné ji u příjemce opět složit. **Segmentace** může vyžadovat, aby do protokolové řídicí informace, tvořící záhlaví PDU, byly zavedené příslušné údaje (identifikace zprávy, pořadí ve zprávě apod.). V případě segmentace se zobrazuje SDU do několika PDU a ke každé z nich se přidává PCI. **Segmentace** (někdy označovaná jako fragmentace) může být výhodná z těchto

důvodů: chybové řízení je jednodušší v případech menších jednotek, menší jednotky vyžadují menší vyrovnávací paměť na přijímající straně.

Vrstvy modelu ISO / OSI

Aplikační vrstva (Application Layer)

Tato nejvyšší vrstva představuje rozhraní mezi prostředím sítě na jedné straně a uživateli nebo jejich aplikacemi na druhé straně. Účelem aplikační vrstvy je poskytnout aplikačním procesům přístup ke komunikačnímu systému a tím umožnit jejich vzájemnou spolupráci. Mezi služby poskytované aplikační vrstvou patří přenos zpráv, identifikace komunikačních parametrů, zjištění stupně okamžité připravenosti komunikujícího partnera, dohoda o mechanismech ochrany zpráv, výběr způsobu dialogu včetně postup jeho zahájení a ukončení atd.

Mezi nejznámější síťové aplikace patří např. elektronická pošta (např. aplikační program SMTP v architektuře TCP/IP) nebo přenos souborů (např. protokoly FTP nebo TFTP v architektuře TCP/IP)

Prezentační vrstva (Presentation Layer)

Zajišťuje jednak potřebnou konverzi přenášených dat, jednak jejich případnou komprimaci (pakování) a šifrování. Zmíněná konverze se uplatňuje v případě, že odesílatelova a cílová stanice používají rozdílnou vnitřní prezentaci dat (např. EBCDIC a ASCII). Použitím komprese se často dosáhne rychlejšího přenosu a zašifrování dat snižuje nebezpečí jejich zneužití. Prezentační vrstva zajišťuje transparentní přenos zpráv mezi koncovými uživateli a zabývá se tedy jen strukturou zpráv a nikoliv jejich významem, který je znám jen aplikační vrstvě.

Prezentační vrstvu podporuje celá řada norem, jako kódování textu (ASCII), kódování grafických informací (PICT, TIFF, JPEG, GIF), přenos obrazových, zvukových nebo multimediálních informací (MIDI, MPEG, HTML).

Relační vrstva (Session Layer)

zahajuje komunikaci. Na úrovni této vrstvy se řeší navazování, udržování a ukončování „logického“ spoje mezi oběma koncovými uživateli. Uvedený logický spoj, který se často nazývá relace (session), umožňuje zpravidla rychlejší přenos dat, než přenos dat ve formě datagramů - zde totiž nejsou datové pakety přenášeny připravenou a udržovanou trasou, vytvořenou touto relační vrstvou, ale každý z těchto paketů si sám hledá v síti svou cestu k cíli.

Transportní vrstva (Transport Layer)

chrání přenášená data. V této vrstvě nás již nezajímá způsob propojení mezi stanicemi, na této úrovni se řeší vlastní komunikace mezi koncovými uživateli, tedy mezi odesílatelem a adresátem. Základní činností této vrstvy je rozkládání odesílaných dat (např. velkého souboru) do segmentů a provedení kontrolních součtů a při příjmu jejich zpětné „skládání“ v cílové stanici. Také vytváří záložní kopie dat.

Síťová vrstva (Network Layer)

řídí přenos dat mezi dvěma stanicemi, mezi nimiž neexistuje přímé spojení. Mezi další služby patří síťové adresování, zahajování, vytváření a závěr síťových spojení, identifikace koncových bodů síťových spojení, obyčejný a spěšný přenos, oznamování vzniklých chyb (toto nemusí nutně vést ke zrušení příslušného síťového spojení, řízení datového toku, uvedení síťového spojení do výchozího stavu a příjem potvrzení. V této vrstvě musí být známý aktuální způsob propojení stanic v dané obecné síti. Na základě těchto informací pak tato vrstva zajišťuje volbu vhodné trasy pro přenos dat mezi dvěma uzly přes uzly mezilehlé. Na této úrovni jsou data přenášena ve větších blocích označovaných pakety a činnost této vrstvy se často nazývá routing (směrování). Při vysílání tato vrstva vytváří ze segmentů dat pakety pro odvysílání do sítě, spočítá je a přidá hlavičku, která obsahuje pořadí paketů a adresu počítače, který zprávu přijme.

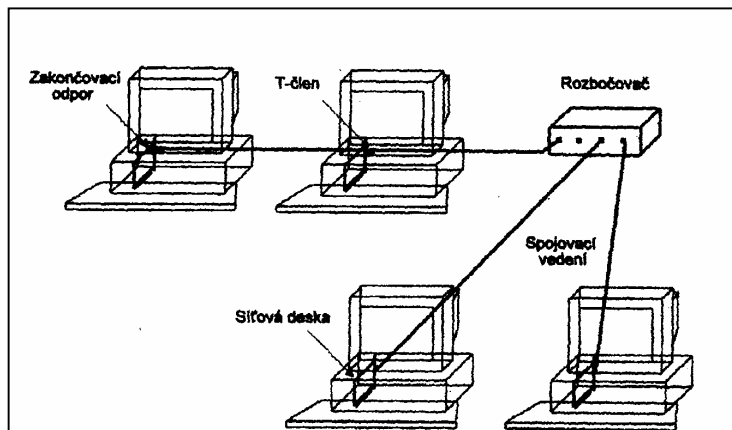
Spojová vrstva (Data link Layer)

Spojová vrstva musí umožnit zahajování, udržování a závěr vytvořených spojení, rozvětvení datových 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. Má za úkol zajistit s využitím vrstvy fyzické bezchybný přenos celých bloků dat mezi dvěma stanicemi, mezi nimiž existuje přímé spojení. Bloky dat zde nazýváme rámce (frames). Spojová vrstva mimo jiné ověřuje správnost přenosu dat (kontrolní součty) a v případě, že je zjištěna chyba, tak realizuje jejich opakované zaslání (uchovává pakety do té doby, než obdrží z následujícího bodu trasy potvrzení, že paket dorazil nepoškozený).

Fyzická vrstva (Physical Layer)

Tato vrstva je ze všech vrstev nejnižší, to znamená, že je nejbližší spojovacímu vedení. Úkolem této vrstvy je zajišťovat přenos zprávy na úrovni jednotlivých bitů. Určuje tedy převážně parametry technického typu, jako např. úroveň logické nuly a jedničky, časové průběhy signálů, jejich posloupnosti, typ použitých konektorů a rozložení signálů na jejich kontaktech apod. Při vysílání dat zakóduje data do média, které je bude přenášet. Jestliže bude např. zpráva přenášena telefonní linkou, bude to analogový signál. Pak se pakety pomocí tohoto média odešlou. Fyzické spojení může dovolit přenos bitových posloupností v plném nebo polovičním duplexu.

HARDWARE SÍTÍ LAN



Jsou to veškeré technické prostředky, které slouží k propojování stanic v síti.

Každou stanicí, která má být připojena do sítě, je třeba vybavit síťovou deskou. Každá síťová deska má konektor, ke kterému se pak připojuje síťové vedení (koaxiál. kabel, kroucená dvojlinka apod.) V malých sítích (několik blízko sebe umístěných stanic) již představují uvedené dvě komponenty dostačující výbavu k výstavbě hardwarové části sítě. U sítí složitějších je však třeba k zajištění potřebné úrovně signálů a ke větvení kabeláže používat různé zesilovače a rozbočovače.

Sít'ové desky

Nezbytná součást všech počítačů připojovaných do sítí LAN. Spolu s příslušným driverem a dalším síťovým softwarem totiž zajišťují přenos dat z počítače na spojovací vedení a naopak. Na jejich rychlosti a spolehlivosti do značné míry závisí výkonnost celé sítě.

V převážné většině mají podobu standardní přídavné desky, zasouvané do některého ze slotů na základní desce. Výjimečně mohou mít i jinou podobu, např. PCMCIA pro připojení notebooků (velikost kreditní karty), nebo mohou být integrovány přímo do základní desky.

V klasické podobě má každá síťová deska na zadní straně jeden nebo několik konektorů pro připojení síťového vedení. Dále na ní můžeme nalézt i několik polí propojek či mikropřepínačů, které slouží k jejímu konfigurování. Obvykle také patice pro vložení IO, který umožňuje vzdálené zavádění operačního systému i bezdiskových stanic. V současné době je na trhu obrovské množství rozmanitých typů síťových desek od různých výrobců.

Parametry síťových desek.

Sít'ové desky se mezi sebou liší v řadě parametrů, nejdůležitější z nich jsou tyto:

- **Standard síťového hardware, pro který je určena:** v současnosti jsou aktuální standardy Arcnet, Ethernet, Token Ring a FDDI. Každý segment sítě totiž musí odpovídat některému z existujících standardů. To znamená, že ve všech stanicích, které jsou daným standardem propojeny, musí být použity pouze síťové desky příslušné vybranému standardu.
- **Typ sběrnice základní desky:** dříve se používaly sběrnice ISA, EISA, MCA, současně používané jsou rychlé sběrnice PCI či VL-bus. V praxi je pravidlem, že nejrychlejší síťové desky se dávají na stanice s nejčilejší komunikací, tzn. hlavně servery, stanice zpracovávající databáze apod.
- **Typ spojovacího vedení:** v úvahu připadají koaxiální kabel, stíněná či nestíněná kroucená dvojlinka a optický kabel. Tím je také dán potřebný typ připojovacího konektoru na síťové desce.
- **Topologie sítě:** v prostředí některých síťových standardů je také významné, pro jakou topologii je síťová deska určena. Např. v síti Arcnet je třeba rozlišovat desky určené pro topologii sběrnice a hvězdicovou. Jsou i desky, které umožňují požadovanou vlastnost zvolit pomocí přepínače.

Instalace síťové desky

Jak plyne z předchozího výkladu, je třeba zvolit takovou síťovou desku, která svými parametry plně vyhovuje požadavkům, které se na ni v dané konkrétní situaci kladou.

Dále je třeba při instalaci desky nastavit ji tak, aby se chovala žádoucím způsobem, aby její požadavky na prostředky stanice nekolidovaly s požadavky jiných komponent stanice. Tato činnost se nazývá konfigurování síťové desky a provádí ji většinou správce sítě. Jedná se především o nastavení následujících parametrů:

- **Číslo přerušení** - souvisí s přerušovacím systémem daného PC. Tento systém umožňuje, aby se procesor dovídal o požadavcích, přicházejících od jednotlivých komponent PC (tedy i síťové desky), přerušil svoji práci, obsloužil tyto požadavky a pak se zase vracel ke své původní činnosti.
Na PC bývá k dispozici 16 přerušovacích kanálů, po kterých tyto požadavky mohou přicházet a pro síťovou desku je tedy jeden volný potřeba určit.
- **Adresa V/V portu.** Tímto parametrem se zadává adresa několika málo bytů v paměti RAM, přes které probíhá komunikace s deskou. I zde platí, že každá z komponent stanice musí mít nastavenou adresu V/V portu tak, aby nekolidovala s dalšími.
- **Identifikační číslo desky** - každá ze stanic, připojených k témuž segmentu sítě musí mít na desce nastaveno jedinečné, neopakující se identifikační číslo. Od něj je totiž odvozována adresa stanice v síti a ta musí být

jednoznačná. (pozn.: u desek standardu Ethernet je toto číslo nastaveno pevně už při výrobě, při čemž výrobci zaručují, že nebudou vyrobeny dvě desky se stejným číslem).

Vlastní konfigurování se provádí dvojím způsobem:

- u starších desek jsou pro tento účel propojky a mikropřepínače. Ke každé desce se pak dodává návod, jak při konfiguraci postupovat.
- u moderních desek se jejich konfigurování provádí softwarově. To znamená, že ke každé desce je dodávána disketa s programem, který konfiguraci snadno umožní. Některé programy dokonce umí konfiguraci desky provést úplně automaticky. Navíc tyto programy obsahují i prostředky pro otestování dané desky.

U moderních desek je také samozřejmostí, že disketa obsahuje také její vlastní driver. U starších desek to pravidlem nebylo a bylo potřeba sehnat vhodný standardní driver (např. NE2000)

Spojovací vedení a konektory

Slouží k přenášení dat mezi stanicemi. Základní vlastnosti vedení jsou určeny typem síťového standardu, který je v síti použit. Například u sítě Ethernet je možno např. použít koaxiálního kabelu (existují dva druhy), kabel musí mít impedanci 50 ohmů, topologie sběrnice a max. délka segmentu sítě do 200m.

Spojovací vedení představuje ve větších sítích poměrně významnou položku v pořizovacích nákladech, přičemž drahá je především cena práce při jejich instalaci. Proto už při návrhu sítě je třeba pečlivě zvážit typ spojovacího vedení, které se použije. Obecně se doporučuje volit perspektivní typy, které budou schopny vyhovět rostoucím nárokům po delší dobu.

V současné době připadají v úvahu tyto typy spojovacího vedení:

- a) **koaxiální kabel** - dvou vodičové asymetrické uspořádání, tvořené středovým (živým) měděným vodičem a stínící vrstvou z měděných drátků (jako izolace se používá polyetylen). V Ethernetu (IEEE 802.3) se používají dva typy koaxiálních kabelů, které se liší provedením, tloušťkou, impedancí, používanými konektory:

- **silný** (*thick*) - vodič jádra (který přenáší data) je obklopen čtyřmi vrstvami izolačního a stínícího materiálu. původní standardní médium, průměr kabelu asi 10mm, impedance 50 Ω . Bývá označován symbolem RG-6. Má velmi dobré elektrické vlastnosti, ale pro vysoké pořizovací náklady a nesnadnou montáž se speciálními konektory TCR se již příliš nepoužívá. Používá se především v instalacích pro Ethernet v páteřní síti (je náročnější na instalaci – ohyb)

tenký (*thin*) - vodič jádra je obklopen pouze jednou vrstvou stínění, oddělenou izolačním materiálem. Má průměr asi 5 mm, impedanci 50 ohmů, barvu černou nebo šedou. Označuje se RG-58. Ve srovnání se silným koaxiálem má poněkud horší elektrické vlastnosti.

Výhodou koax. kabelů jsou nízké pořizovací náklady a solidní odolnost proti elektromagnet. rušení.

Přesněji: elektromagnet. rušení má dvě složky, elektrickou a magnetickou. U koaxiálu stínění poskytuje dobrou ochranu proti složce elektrické, avšak jelikož stínění není z magnet. materiálu, tak proti rušení magnetickému neposkytuje ochranu žádnou. V tomto je lepší kroucená dvojlinka.

Hlavní nevýhodou je nižší přenosová rychlost oproti jiným spojovacím vedením, takže rozsah jeho použití v současné době už klesá i když stále je velmi rozšířen.

- b) **Symetrický kabel - kroucená dvojlinka** - tvořená dvěma rovnocennými vodiči, které jsou vzájemně zkrouceny (*twisted pair*). Vyskytuje se ve dvou formách: **stíněná** (označení: STP) – skládá se z měděných vodičů, kde každý z nich je obklopen izolačním materiálem (PVC) a dráty jsou kolem sebe obtočeny tak, aby vytvořily dvojice. V párech jsou sdruženy vždy dva dráty pro vysílání a dva pro příjem. Každý pár je obklopen stíněním (ve formě kovové folie) po celé délce vodičů. Dále se používá forma **nestíněná** (označení: UTP). Parametry symetrického kabelu: **přenosové** (útlum, impedance, zpoždění přenosu signálu) a **vazební** (ztráty přeslechem, ztráty rušením, šum).

Kroucená dvojlinka se používá u všech síťových standardů.

Čtyřpárový nestíněný kabel UTP je nejčastěji používaný z hlediska náročnosti odstraňování problémů v kabeláži. Kategorie, do nichž se dělí typy nestíněných symetrických kabelů mají tyto charakteristiky:

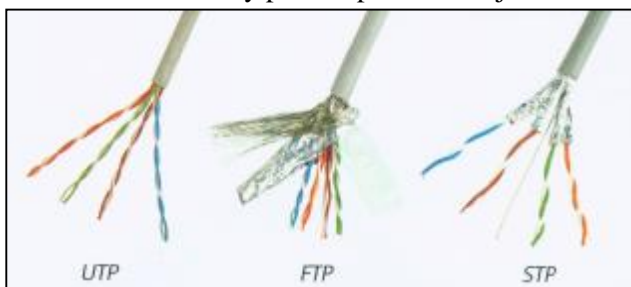
- **kategorie 1** = žádná výkonnostní kategorie
- **kategorie 2** = do 1 MHz (telefonní dráty)
- **kategorie 3** = do 16 MHz s přenosovou rychlostí až 10 Mb/s (např. Ethernet 10BASE-T, 100BASE-T4), označuje se jako úroveň pro přenos hlasových informací
- **kategorie 4** = do 20 MHz s přenosovou rychlostí až 16 Mb/s (např. Token-Ring, 10BASE-T, 100BASE-T4), označuje se jako úroveň pro přenos dat
- **kategorie 5** = do 100 MHz s přenosovou rychlostí až 100 Mb/s (100BASE-TX, 10BASE-T, popř. 1000BASE-T), označuje se jako úroveň pro přenos dat

Výhodnost kroucené dvojlinky spočívá:

- jednak v její lepší odolnosti proti rušení – zkroucení jejích vodičů způsobí, že rušení, které by se

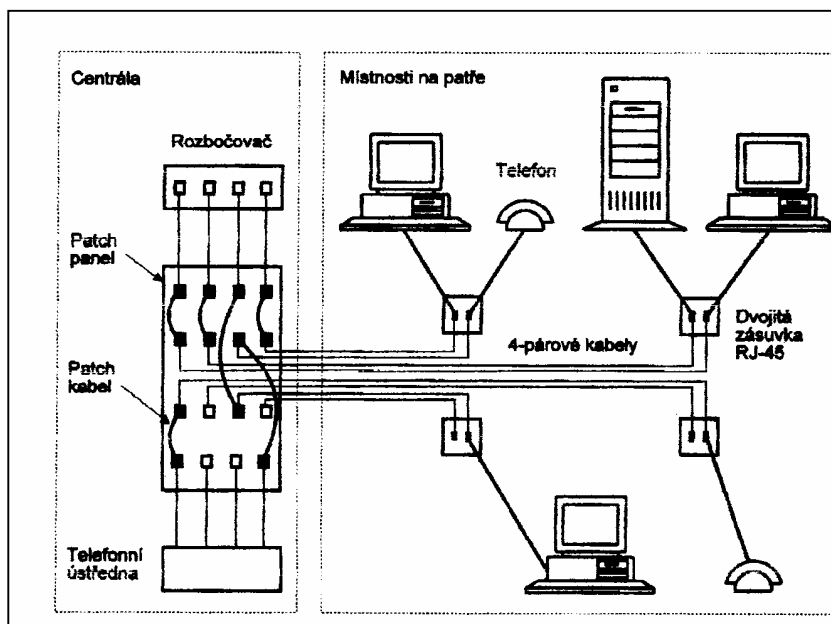
uplatnilo v daném místě jednoho vodiče se eliminuje rušivým napětím, které v tomtéž místě je na druhém vodiči (rušivá napětí jsou v protifázi). To se týká obou složek elektromagnetického rušení.

- jednak v její vyšší přenosové rychlosti - v prostředí Arcnet, Ethernet, Token Ring se používá dvojlinka kategorie 3 nebo 4 (u níž přenosová rychlost nepřesahuje 16 Mb/s). Existuje však jen o málo dražší kategorie 5 s přenosovou rychlostí 100 Mb/s, která vyhovuje modernímu vysoce výkonnému standardu FDDI. Je zřejmé, že při realizaci nové sítě je na místě použít toto vedení a tím si do budoucna připravit snadný přechod do oblasti sto megabitových rychlostí.
- možnost jejího využití v rámci *strukturované kabeláže*. Ta si klade za cíl přenášet jedním druhem kabelů veškeré potřebné informace. V rámci jedné budovy je tak možné vybudovat rozvody, které vycházejí z jednoho centra, např. telefonní ústředny a které končí v zásuvkách v jednotlivých místnostech. Těmito rozvody pak lze přenášet nejen telefonní hovory, ale i počítačová data, signály protipožárních čidel,



údaje měřicích zařízení atd. Za zmínku stojí, že všechny zmíněné signály jsou přenášeny současně. Ve strukturované kabeláži se totiž běžně používá kabel se 4 páry kroucené dvojlinky (dva páry jsou použity pro data, jeden pro telefon a zbývající pár pro cokoli jiného). Výhodná je i značná operativnost v uspořádání koncových zařízení v místnostech.

Obr.: schéma jednoduché strukturované kabeláže



c) **optický kabel** (fiber-optic cable).

Podstatou optického přenosu je přeměna elektrického informačního signálu na optický. Optický kabel je v sítích LAN perspektivním typem spojovacího vedení. Zde data nejsou přenášena kovovými vodiči, ale procházejí ve formě světelných impulzů průsvitnými vlákny. Vlákna jsou skleněná nebo plastová, jsou velmi tenká (tenčí než lidský hlas) a jsou uložena v obalu, který je chrání. Plastová vlákna mají vyšší trvanlivost, jejich přenosové parametry jsou ale horší než u skla.

Data uložená v počítači ve formě el. signálů jsou převáděna pomocí laseru nebo LED diody, umístěných na příslušné síťové desce do podoby světelných signálů. Tyto signály jsou vedeny optickým kabelem k přijímací části cílové stanice nebo rozbočovače, či jiného optického zařízení sítě. Protože je třeba, aby data proudila oběma směry, je každý optický spoj tvořen dvěma vlákny.

Používají se dva typy optických kabelů:

- **jednovidové (singlemode)**: velmi tenké vlákno s vysokou přenosovou kapacitou. Používá laser pro generování světelného paprsku, který dosahuje značných vzdáleností. Koherentní světlo z laseru má konstantní vlnovou délku a proto je při příjmu dosaženo lepší kvality než u mnohovidového vlákna (používá se pro vzdálenosti větší než 1 km)
- **mnohovidové (multimode)**: optický kabel využívající místo laseru světelné diody pro generování světla, které sestává z několika světelných délek. Protože dioda vysílá všemi směry, generovaný paprsek vniká do jádra

optického vlákna tak, že úhel dopadu paprsku s osou jádra je nenulový a dochází tak při jeho cestě optickým vláknem k odrazům od okrajů optického vlákna, proto je celková vzdálenost dosahu světelného paprsku omezena (vzdálenost: pouze stovky metrů).

Optický kabel má mnoho výhod:

- **vysoká přenosová rychlost** – snadno zvládne rychlosti 100Mb/s. Díky tomu jsou optické kabely nasazovány tam, kde je třeba přenášet velké objemy dat. Také útlum světla v kabelu je velmi nízký, takže kabelem lze propojovat i značně vzdálená místa (řádově kilometry).
 - **absolutní odolnost proti elektromag. rušení** - umožňuje to instalovat rozvody LAN i do silně narušených prostředí (např. výrobní haly). Také naprostá netečnost vůči bleskům a podobným jevům.
 - **zvýšené zabezpečení přenášených dat** – není možno instalovat nějaké „odposlouchávací“ zařízení, do něhož by se indukovala přenášená informace.
 - **jsou lehčí a tenčí než klasické kabely a realizují naprosté galvanické oddělení** obou propojovaných míst
- K nevýhodám patří zatím vysoké pořizovací náklady. Cena samotného kabelu je překvapivě nízká, ale drahé jsou související komponenty, zejména síťové desky, rozbočovače, převodníky, rozvaděče apod. Náročné a proto drahé je i samotné konektování optických kabelů.

Díky uvedeným výhodám i nevýhodám se optické kabely používají především na exponovaných místech, např. páteřní vedení pro spojení jednotlivých segmentů rozlehlých sítí. V běžných prostředích se díky nízkým nákladům stále používá koaxiální kabel nebo kroucená dvojlinka.

d) Bezdrátový spoj

Nejmodernější z možných spojovacích prostředků. Bezdrátový přenos v počítačových sítích se v současné době realizuje prostřednictvím radiového, popřípadě úzce směřovaného infračerveného nebo laserového paprsku (dosah v případě infračerveného bývá asi 300 m, v případě laserového až 2 km).

K propojení dvou míst sítě LAN je nutno v obou spojovaných místech instalovat vysílač / přijímač vybavený parabolickou anténou. Při tom mezi oběma místy musí být přímá viditelnost. Každé z těchto zařízení se připojuje na navazující rozvody LAN např. pomocí komunikačního mostu (bridge) nebo směrovače (router).

Hlavní výhodou je možnost propojovat místa, mezi kterými je obtížné realizovat kabelový spoj (široká řeka, hustá městská zástavba apod.) Nevýhodou jsou vysoké pořizovací náklady a značná choulostivost, která spočívá ve snadné narušitelnosti paprsku (např. hustý déšť nebo hustá mlha).

Propojování sítí - aktivní prostředky sítí

K propojení nevelkého počtu blízkých stanic stačí obvykle síťové desky, kabely a konektory, dalších prostředků netřeba, (např. u Ethernetu s koaxiálním kabelem se uvádí max. 25 stanic a 185 m).

Ve složitějších případech je třeba použít **aktivních prostředků**. Ty podle svého typu signál zesilují, rozbočují či jiným způsobem zpracovávají. Zpravidla nejde o levná zařízení, takže jejich cena má znatelný vliv na pořizovací náklad sítě. Prostředky propojování sítí se liší podle vrstvy architektury, na níž se komunikace mezi dvěma síťovými segmenty provádí. V zásadě lze propojovat na:

- fyzické vrstvě – **opakovače** (označované někdy jako rozbočovače, koncentrátoři nebo distributory)
- spojové vrstvě – **mosty a přepínače**
- síťové vrstvě – **směrovače**
- aplikační vrstvě – **brány**

Popis aktivních prostředků sítí:

Zesilovač nebo taky opakovač (repeater)

Pouze zesiluje procházející signál, takže slouží ke zvětšení rozsahu sítí. Na jeho vstupu i výstupu lze připojit kabel stejného typu. Není zde prováděna kontrola chyb, není použita vyrovnávací paměť. Pracují pouze v prostředí lokálních sítí (stejněho charakteru). Typickým příkladem použití opakovače je síť Ethernet, IEEE 10BASE-T, která je budována s centrálním rozbočovačem. V sítích Token-ring každá stanice provádí jako jednu z funkcí regeneraci signálu v kruhu, proto se žádné samostatné opakovače nepoužívají.

Převodník

Na rozdíl od zesilovače signál nejen zesiluje, ale také převádí na jiný typ kabelu (v prostředí sítě **Ethernet** např. převodník mezi optickým a koaxiálním kabelem).

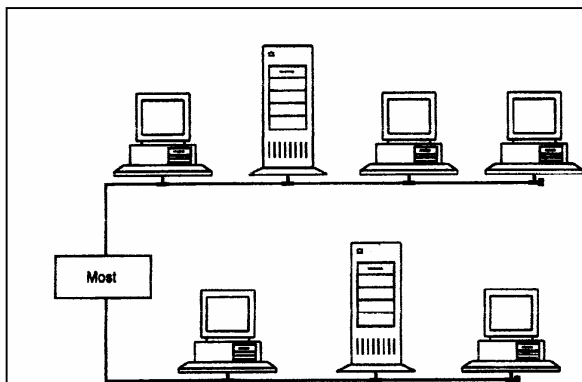
Rozbočovač (HUB)

Může nabývat velmi rozmanitých podob. Jeho základní funkcí je rozbočování signálu, čili větvení sítě. Je nezbytným prvkem v sítích s hvězdicovou topologií.

Tyto tři dosud uvedené prostředky signál pouze zesilují, rozbočují, či převádějí na jiné médium. Procházející informací se nijak nezabývají. Je to dáno tím, že pracují pouze na úrovni nejnižší vrstvy modelu **ISO/OSI**, tedy na úrovni **fyzické vrstvy**. Další prostředky už mají zabudovány jistou inteligenci a reagují na přenášené informace.

Most (bridge) a přepínač

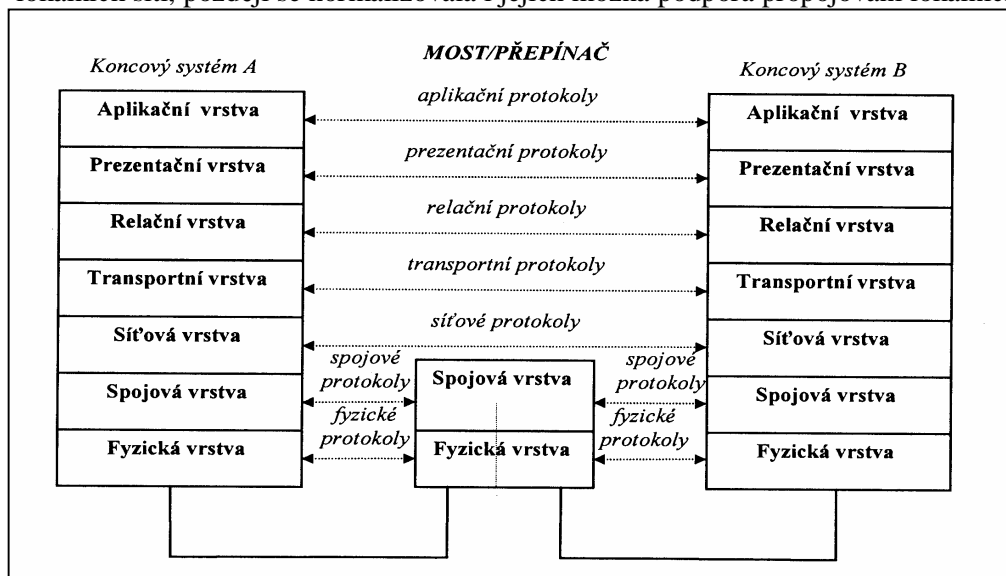
Toto zařízení slouží ke vzájemnému spojení dvou nebo více kabelových segmentů sítě a k přenosu rámců dat mezi nimi. Most pracuje na úrovni *spojoyvé vrstvy* modelu ISO/OSI a to přináší dvě důležité výhody. První výhoda spočívá v tom, že spojované segmenty sítě se mohou lišit na úrovni fyzické vrstvy. Což znamená, že pomocí mostu



je např. možné spojit segment sítě *Arcnet* se segmentem *Ethernet* apod. Druhá výhoda plyne z toho, že most je schopen rozeznávat jistou část adresy procházejících rámců. Díky tomu může provádět velmi důležitou činnost, označovanou jako *filtrace rámců*. Filtrace funguje takto: datový rámec, který vyšle stanice pracující v jednom ze segmentů, se tímto segmentem šíří a pochopitelně dospěje i k připojenému mostu. Ten dokáže rozpoznat, zda rámec je určen pro stanici v daném segmentu nebo jestli je jeho cíl jinde. V prvním případě most rámec dál nepustí (odfiltruje jej), ve druhém případě přenesení rámec do dalších připojených segmentů. Filtrace rámců způsobí, že rámec nepřechází zbytečně do segmentů, které nejsou jeho cílem a nezatěžuje tedy jejich provoz. Je to tedy významný prostředek použitelný pro snižování zatížení sítí.

Obr.: příklad využití mostu

Mosty byly prvními zařízeními propojujícími sítě a podsítě. I když se zpočátku orientovaly na přímé propojování lokálních sítí, později se normalizovala i jejich možná podpora propojování lokálních sítí na dálku,



prostřednictvím přenosového média jiného typu (např. páteřní síť FDDI). Režim práce mostům umožňuje kontrolovat rámce z hlediska chyb (na základě kontrolního součtu). Most, na rozdíl od opakováče, nepropustí chybné rámce (např. nepřipustně krátké nebo dlouhé).

Obr.: architektura mostu / přepínače

Později se vyvinuly *přepínače* pro lokální sítě, které sdílejí s mosty celou řadu společných vlastností, ale jejich účel a použití s mosty není shodné. Ve skutečnosti se nejedná o propojovací zařízení, ale o vylepšené řešení jednotlivých lokálních sítí: místo tradičního sdíleného přenosového pásma pro všechny připojené sítě se vyhrazuje celé pásmo malé skupině stanic (nebo dokonce stanici jediné). Přepínače v lokálních sítích lze výstižně definovat jako mosty s více porty. Přepínače pro Ethernet se skládají z procesorů, pracujících jako malé vnitřní mosty se dvěma porty. Procesory filtrují rámce, které se na portu objeví a dále je zpracovávají podle tabulky adres.

Směrovač (router)

Pracuje na úrovni síťové vrstvy modelu *ISO/OSI*, má však vyšší inteligenci než most. Most poslal rámec, který neodfiltroval dál do všech připojených segmentů. Směrovač dokáže zpracovávat adresy procházejících paketů dokonaleji. Díky tomu, že shromažďuje informace o všech spojených sítích, o způsobu jejich propojení a o všech pracujících serverech a směrovačích, dokáže každému procházejícímu paketu jeho konkrétní a nejkratší cestu k cíli. Jeho činnost se nazývá směrování paketů (packet routing) a obsahuje v sobě i filtraci paketů.

Brána (gateway)

Toto zařízení pracuje na úrovni nejvyšší vrstvy modelu ISO/OSI, to znamená na úrovni aplikační vrstvy. Slouží k připojování sítí LAN k cizímu prostředí, např. k sálovým počítačům IBM, k síti Unix, apod.

Aktivní prostředky pro síť LAN vyrábí mnoho výrobců a to ve velmi široké paletě typů a variant. Často u nich dochází ke slučování zmíněných funkcí, k jejich částečnému překrývání a k případným modifikacím.

Standardy síťového hardware

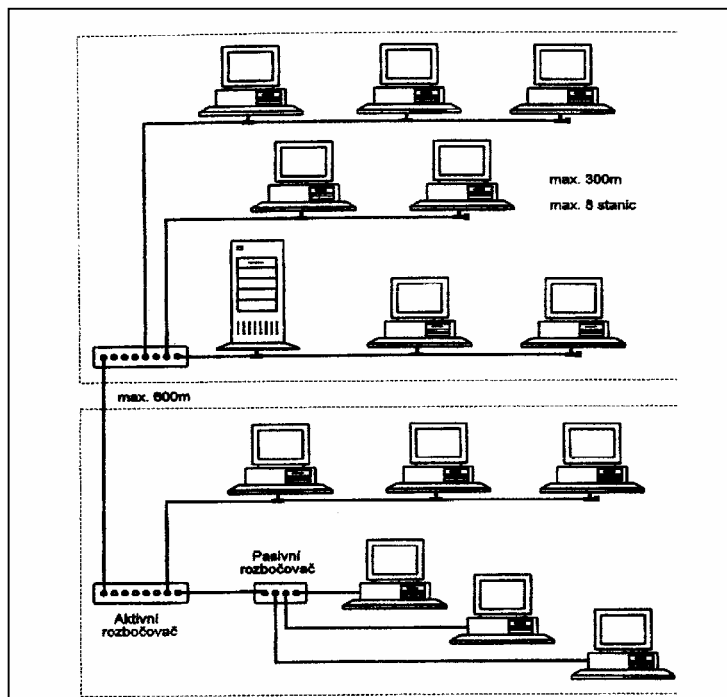
Každý z dále uvedených standardů definuje řadu parametrů sítě, které při její realizaci musí být dodrženy.

Především se jedná o parametry na úrovni fyzické, částečně i spojové vrstvy modelu **ISO/OSI**.

Volbou určitého standardu je určena např. rychlost přenosu dat v síti, metoda přístupu na spojovací vedení, topologie sítě, použitelné typy spojovacích kabelů, jejich maximální délky, pravidla propojování stanic apod.

V současné době se nejčastěji pracuje s těmito standardy: **Arcnet**, **Ethernet**, **IBM Token Ring**, **FDDI** a případně další standardy pro rychlost 100 Mb/s. Při návrhu sítě je třeba s uvažovanými standardy důkladně a podrobně seznámit. Zde uvedeme jen typické zobecněné vlastnosti.

Arcnet



Byl vyvinut společností Datapoint. Sítě s tímto standardem se vyznačují jednoduchostí realizace i případného dalšího rozšiřování a nízkou pořizovací cenou. To zřejmě byly hlavní důvody, proč se jim u nás v počátcích sítí **LAN** dávala přednost.

Jednoduchost je dána tím, že se používá jen velmi málo aktivních prvků, že lze libovolně kombinovat sběrníkovou a hvězdicovou topologii, že lze používat kabelových segmentů značných délek, takže i poměrně rozsáhlé sítě se dají realizovat bez problémů.

Jako metoda přístupu na spojovací vedení se používá **Token Bus**.

Hlavní nevýhodou **Arcnetu** v dnešní době je jeho nízká přenosová rychlost, která činí jen 2,5 Mb/s, tj. ze všech standardů nejnižší. Objevila se i nová varianta **Arcnet Plus**, nabízející přenosovou rychlost 20Mb/s, avšak i tento vylepšený typ má těžkou konkurenci v moderních standardech, disponujících přenosovou rychlostí 100Mb/s, jako např. **FDDI**.

Stavební prvky Arcnetu

Síťové desky jsou na našem trhu běžně k dispozici pro základní typy sběrnic PC a pro základní typy kabelů. Jistou zvláštností těchto desek je nutnost nastavovat na nich identifikační číslo, které je pak převzato do síťové adresy stanice. Rozsah adresy je 8 bitů, v rámci jednoho segmentu lze tedy používat maximálně 255 stanic, což u rozsáhlých sítí může být nevýhoda. U desek je také třeba rozlišovat, pro jakou topologii sítě jsou určeny.

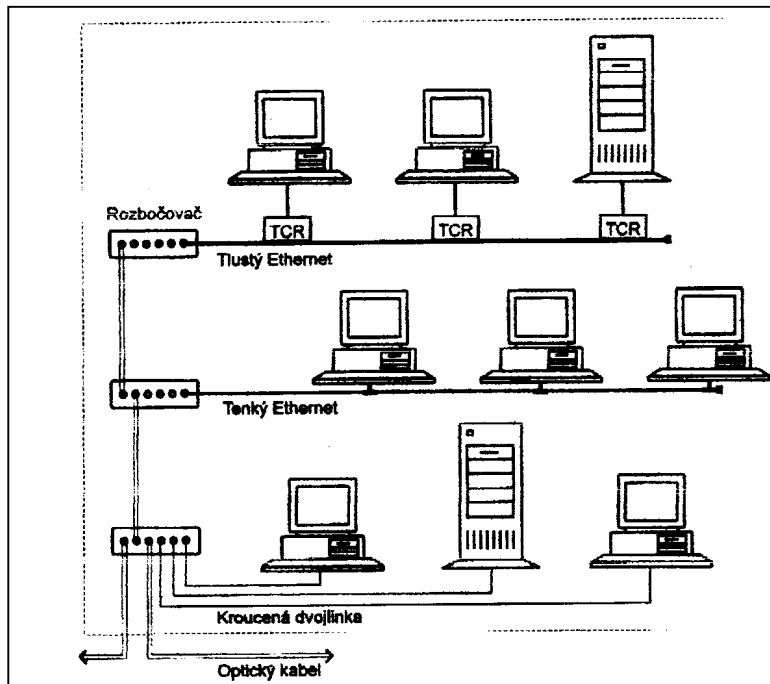
Kabely a konektory: nejčastěji se používá kroucené dvojlinky a koaxiálního kabelu. Koaxiál je odlišný od koaxiálu pro **Ethernet**, zejména vyšší impedancí (93 Ω). Z ostatních prvků se nejvíce uplatňují rozbočovače a to jak ve formě pasivní, tak i aktivní, které obsahují i zesilovač.

Ethernet - IEEE 802.3

Poznámka: **IEEE** (Institute of Electrical and Electronics Engineers) - mezinárodně uznávaná organizace sdružující odborníky z oblasti elektroniky. Členství v **IEEE** je individuální, otevřené všem dobrovolníkům. Kromě vzdělávací a publikační činnosti vytváří **IEEE** důležité technické normy. Jejím hmatatelným výsledkem je velké množství schválených norem a další se vyvíjí. Asi nejznámější normy **IEEE** se týkají oblasti komunikačních sítí. Výbor **IEEE 802** normalizoval prakticky všechny lokální a metropolitní sítě (**LAN** a **MAN**), jako 802.3 (normalizovaný **Ethernet**), 802.4 (normalizovaný **Token Bus**), 802.5 (normalizovaný **Token Ring**) atd.

Pochází od firmy Xerox. V současnosti je to u nás nejrozšířenější standard. Byl určen pro sběrníkovou topologii, ale používá se i pro hvězdicovou. Pro sítě, které s ním pracují je charakteristický solidní výkon a příznivá cena. Přenosová rychlost je 10Mb/s a rychlost při nižších a středních zatíženích sítě je příznivě ovlivňována použitou metodou přístupu na spojovací vedení - **CSMA/CD**. Významnou skutečností je i to, že umožňuje připojení adaptérů PCMCIA (připojení notebooků), spolupracuje se systémy bezdrátových spojů a představuje standardní prostředek pro vytváření sítí v prostředí operačních systémů Unix. Naopak nepříjemná je poměrná choulostivost na rušivé vlivy a nekorektní stavy. Odpojení zakončovacího odporu, případně přerušení či zkrat v kterékoliv části sítě má určité za následek výpadek celého segmentu sítě. Pro aplikace provádějící řízení rychlých procesů v reálném čase může být zase nepříjemný nedeterministický charakter použité metody **CSMA/CD**. Lze říci že **Ethernet** představuje výhodnou volbu. Zajímat se o jiný standard má smysl zřejmě pouze v případě vysokých či speciálních požadavků.

Sít'ové desky – pro Ethernet zde má uživatel k dispozici vše, na co si jen může vzpomenout. V běžné nabídce jsou desky pro různé systémové sběrnice a to v provedeních pro oba druhy koaxiálního kabelu (tlustý a tenký Ethernet), pro nestíněnou kroucenou dvojlinku a řada výrobců vyrábí i desky určené pro optický kabel. Některé desky jsou univerzální, obsahují více druhů konektorů. U desek pro Ethernet není třeba nastavovat identifikační číslo, to je na



vzdálenosti. Přímé připojení stanic je poměrně neobvyklé. Převážná většina výrobců působících v této oblasti nabízí pro Ethernet ucelené řady aktivních zařízení, která slouží k zesilování a rozbočování signálu a ke vzájemnému propojování sítí.

Označení podle IEEE 802.3:

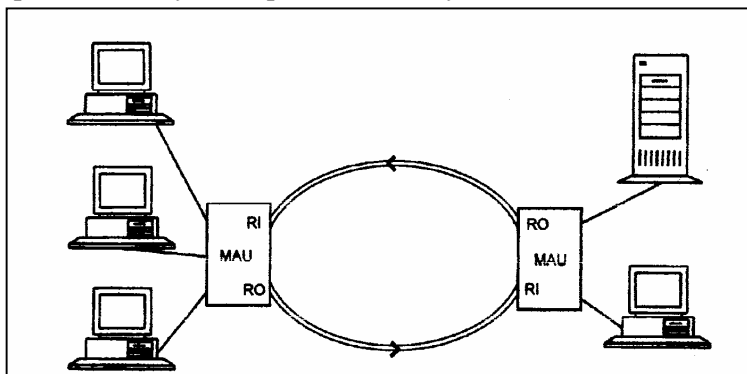
- **10** – přenosová rychlost v Mb/s
- **BASE / BROAD** – přenos v základním pásmu / širokopásmový
- **F / T / x** – přenosový prostředek nebo maxim. délka jednoho segmentu: optika / symetrický kabel / 2 nebo 5 jako délka segmentů ve stovkách metrů. Sítě **100BASE-T** patří mezi nejpopulárnější typy IEEE 802.3

IBM Token Ring - IEEE 802.5

Token, který pro stanici znamená právo vysílat, je zvláštní rámec, který obsahuje cílovou adresu.

Tyto sítě svého času patřily k nejvýkonnějším typům klasických LAN. To je dáno hodnotou přenosové rychlosti (16 Mb/s) a dále metodou přístupu na vedení Token Ring. Problémy zde vznikají z nutnosti přemostovat vypnuté a odpojené stanice. Proto v kruhu jsou zapojovány pouze speciální jednotky MAU (*Multistations Access Units*) a na tyto jednotky se pak jako ke středu hvězdy připojují jednotlivé stanice. Tyto jednotky pak v případě potřeby automaticky zajišťují jejich přemostění. Navíc vedení bývá kvůli spolehlivosti budováno jako dvojité.

Tato koncepce pochopitelně zvyšuje složitost a následně i cenu těchto sítí. Vyšší cena je důvodem, proč se v našich podmínkách tyto sítě příliš nerozšířily.



Obr.: příklad sítě IBM Token Ring

každé desce již pevně nastaveno.

Kabely a konektory – lze používat těchto typů spojovacích kabelů:

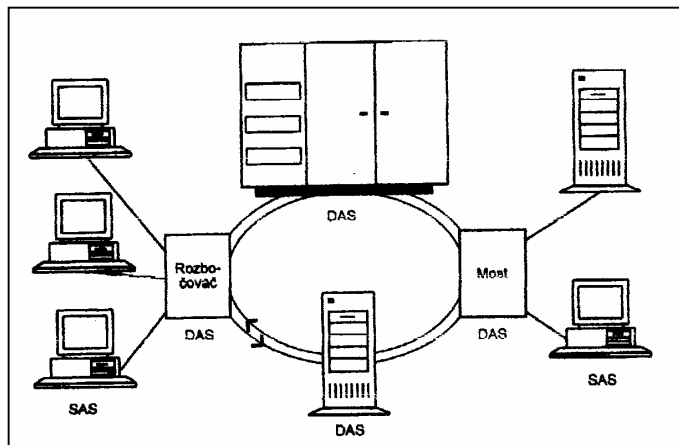
- tlustý Ethernet (thick Ethernet) -500 metrů, max. 100 stanic v síťovém segmentu
- tenký Ethernet (thin Ethernet) -185 metrů, max. 30 stanic v síťovém segmentu
- kroucená dvojlinka v nestíněném provedení vhodná pro hvězdicové topologie. Má impedanci 100 ohmů, je opatřován telef. konektorem RJ-45. Jde v podstatě o standardní telefonní kabel
- optický kabel . Používá se kabelů s průměrem vlákna 50 až 100 mikronů a s konektory ST. Možnost propojení až na vzdálenost 2 km. V sítích Ethernet se používá především k vzájemnému propojování rozbočovačů, mostů a směrovačů a to především tam, kde hrozí rušení nebo kde je potřeba překonat větší

Sít'ové desky: běžně jsou v provedení pro sběrnice ISA, EISA, MCA. Vzhledem k výkonnosti těchto sítí se u nich setkáváme s řadou pokročilých funkcí.

Kabely, konektory: v rámci tohoto standartu lze používat stíněnou nebo nestíněnou kroucenou dvojlinku nebo optické kabely. Optický kabel se používá především k realizaci základního kruhu, tj. k propojení jednotek MAU (RI – Ring In, RO – Ring Out). Ty jsou v podstatě rozbočovači a k nim se pak dvojlinkou připojují jednotlivé stanice.

FDDI - (*Fiber distributed data interface - optické rozhraní pro distribuovaná data*)

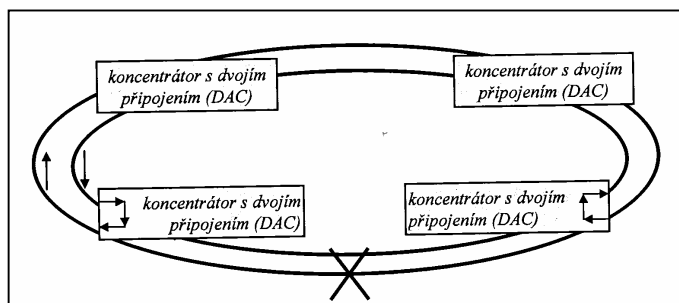
Moderní a perspektivní síťový standard. Jeho základním rysem je podobnost s metodou Token ring a přenosová rychlost 100 Mb/s, což oproti ostatním standardům představuje obrovský kvalitativní skok (např. proti Ethernetu 10x větší přenos.rychlost). Díky tomu je to v současnosti velmi výhodný prostředek pro řešení vysoce zatížených sítí. Síťové stanice a další zařízení (mosty a pod.) se připojují dvojím způsobem:



Obr.: příklad sítě FDDI

- buď přímo - označení **DAS** (*Dual Attached Stations*) – dvojitě připojené stanice
- nebo prostřednictvím příslušného rozbočovače - **SAS** – jednoduše připojená stanice

Standard **FDDI** je vhodný pro nejvyšší nároky, především pro připojování vysoce výkonných zařízení, pro sítě přenášející velké objemy dat (CAD/CAM , multimediální aplikace) a pro značně zatížené segmenty sítě, např. páteřní vedení.



Obr.: odolnost sítě FDDI proti poruchám

Proto lze doporučit při instalaci nových kabelových rozvodů takové typy kabelů, které tomuto standardu vyhovují. (např. kroucená dvojlinka kategorie 5).

FDDI používá kruhovou topologii. Pro zvýšení spolehlivosti je síť realizována ve formě dvou protisměrných okruhů. Běžně je používán pouze okruh primární , avšak vyskytne-li se v něm závada, automaticky se začne využívat okruh sekundární.

Další standardy pro rychlost 100 Mb/s

Fast Ethernet a 100VG-Anylan

Oba vznikly ze snahy zrychlit původní, dobře zavedený **Ethernet**. O jejich použití platí totéž co o **FDDI**.

Fast Ethernet kromě 100Mb rychlosti se vyznačuje stejným přístupem na vedení jako původní Ethernet, totiž metodou **CSMA/CD**. V jeho prostředí však nelze používat koaxiální kabel. Rozdělení do několika skupin:

- **100BASE-TX** : rozdílná vůči technologii **10BASE-T** je v nutnosti použít hardware podporující rychlost 100Mb/s.
- **100BASE-FX** : připojení pomocí mnohabodových optických kabelů (délka mezi uzly maximálně 2 km).

Gigabitový Ethernet

Touto technologií lze dosáhnout přenosové rychlosti až 1000 Mb/s. Dělí se do několika skupin:

- **1000BASE-SX** : komunikace probíhá prostřednictvím mnohabodových optických kabelů. Maximální délka segmentu se liší podle typů optického vlákna (275 – 550 m).
- **1000BASE-LX** : Kromě mnohabodových lze použít i jednovidová optická vlákna (délka u jednovidových vláken až 5 km).
- **1000BASE-CX** : pro komunikaci je použito stíněných kabelů (maximální délka segmentu je 25 m).
- **1000BASE-T** : čtyři páry strukturované kabeláže UTP kategorie 5 pro větší vzdálenosti (100 m).

Bezdrátové sítě standardu Wi-Fi - IEEE 802.11

Zkratka **Wi-Fi** je odvozena od termínu **Wireless Fidelity**, který by se dal volně přeložit jako bezdrátová přesnost či věrnost (jako zkratka **Hi-Fi** označuje zařízení s velmi přesnou reprodukcí zvuku, tak **Wi-Fi** označuje zařízení, která pomocí vysokých radiových frekvencí zaručují kvalitní datové propojení počítačů). V praxi jde o název druhu bezdrátové sítě, která funguje v bezlicenčním pásmu o frekvenci 2,4 GHz. Technicky se jedná o standard **IEEE 802.11b** pro vysokorychlostní bezdrátové přenosy.

Tato bezdrátová síť umožňuje uživatelům bezstarostné připojení k jejím prvkům, ať je to osobní počítač, notebook, PDA nebo třeba jiná Wi-Fi síť. To vše v maximální - ale spíše teoretické - rychlosti 11 Mb/s. Rychlost připojení závisí na vzdálenosti vysílače a přijímače a kvalitě signálu. Ta je závislá na co nejlepší přímé viditelnosti; ovlivňují ji tedy stromy, zástavba nebo jiná zařízení s elektromagnetickým zářením.

Rychlost bezdrátové sítě

Standard 802.11 se dělí na několik podskupin:

- **802.11b** je standard Wi-Fi pro bezdrátové LAN operující v 2,4GHz spektru s šířkou pásma 11 Mb/s,
- **802.11a** je odlišný standard pro bezdrátové LAN operující na frekvenci 5 GHz s maximálním datovým průtokem 54 Mb/s.
- **802.11g** je určen pro WLAN (Wireless LAN) operující s frekvencí 2,4GHz, ale s maximálním průtokem dat 54 Mb/s.

Existuje mnoho různých Wi-Fi zařízení, jejichž funkční rádius se různí v závislosti na použité technologii a anténě. Na volném prostranství tak lze připojit dvě zařízení na vzdálenost 350-1000 m za předpokladu, že se použije kvalitní externí antény. V budovách se maximální dosah prudce snižuje, a to na pouhých 30 až 100 m v závislosti na použitém stavebním materiálu. Největší překážkou všeobecně jsou kovy a kámen. Pod širým nebem jsou největším nepřítelem propojení stromy nebo keře s listím. Při přímé viditelnosti vadí špatné počasí Wi-Fi přenosu minimálně, ani sebesilnější dešť kvalitu signálu ztlačí neovlivní. To je výhoda Wi-Fi oproti optickým systémům přenosu dat, které jsou na nepříznivé povětrnostní podmínky, ať už mlhu či dešť, všeobecně mnohem náchylnější. Nepříjemným odpůrcem propojení Wi-Fi je však kombinace vody a listů. Mokré listy vytvářejí kompaktní vodní stěnu, která je, na rozdíl od deště tvořeného samostatnými kapkami, pro vlny v pásmu 2,4 GHz neprostupná. Tato vrstva mění elektromagnetické záření na tepelnou energii.

Reálně dosažované přenosové rychlosti

Právě vinou rušení signálu ať už přirozenými nebo umělými překážkami (zástavbou, stromy či jiným rušením) se rapidně snižuje nejen dosah, ale také kvalita a následně i rychlost signálu. Rychlost signálu totiž neklesá plynule, ale skokově po několika krocích. Za ideálních podmínek je modulační rychlost 11 Mb/s. Potom se snižuje na 5,5 Mb/s a dále na 2 Mb/s a 1 Mb/s. Rychlost přenosu klesne automaticky při zhoršené kvalitě signálu, protože nižší rychlostí se Wi-Fi zařízení snaží zvýšit kvalitu přenosu. Jakmile se podaří dosáhnout vyšší kvality přenosu, karty se opět snaží dosáhnout přenosu na vyšší rychlosti. Tento automatický mechanismus se nazývá **ARS** (Automatic Rate Selection).

Výše uvedené hodnoty se však týkají „modulační rychlosti“ - tedy ideální teoretické rychlosti bez jakýchkoli kolizí a rušení. Skutečná datová propustnost se pohybuje v závislosti na aktuálních podmínkách a dosahuje přibližně hodnot mezi 30 až 75 % modulační rychlosti. Pokud s jedním zařízením komunikuje současně více stanic, dělí se spolu o přenosový kanál a maximální rychlost přenosu se pak rozděluje mezi ně. Opět tak dochází k dalšímu zpomalení.

Komunitní sítě

V poslední době se po celém světě lavinovitě šíří i domácí nebo také „komunitní sítě“. V tomto případě jde vždy o skupinu lidí, kteří bydlí ve stejné lokalitě a chtějí sdílet například připojení k Internetu, data nebo si třeba chtějí jen občas zahrát po síti nějakou tu hru.

Problematika síťového software

Všechny síťové architektury jsou založeny na vrstevných modelech, kde se síťové funkce potřebné ke komunikaci mezi koncovými systémy logicky sdružují do vrstev tak, že funkce každé vrstvy využívá služeb nejbližší nižší vrstvy a poskytuje své služby nejbližší vyšší vrstvě. Spolupráce mezi objekty stejné vrstvy dvou otevřených systémů je řízena **komunikačním protokolem** prostřednictvím protokolových datových jednotek (PDU) za použití spojení vytvořeného sousední nižší vrstvou.

Síť Internet umožňuje propojení heterogenních sítí za použití souboru protokolů TCP/IP (Transmission Control Protocol / Internet Protocol).

Klíčový protokol IP provádí vysílání **datagramů** (TCP/IP používá místo pojmu paket pro síťovou datovou jednotku pojem datagram) na základě síťových adres obsažených v jejich záhlavích

IP adresa (IP – Internet Protocol)

Jestliže chceme v rámci sítě navázat spojení s jiným počítačem, musíme znát jeho IP adresu.

IP adresu musí mít každý počítač jinou. Protože jinak by nebylo možné rozlišit s jakým počítačem chceme komunikovat. Jeden počítač může mít i víc IP adres. To pokud má víc síťových adaptérů. IP adresy si nemůžeme jen tak libovolně vymyslet. Přiděluje je mezinárodní autorita pověřená správou IP adres. V současné době je 32 bitová verze IPv4. Protože dovoluje adresování pouze 4 miliard počítačů, je připravena nová verze IPv6. IPv6 už bude 128 bitová a k její implementaci by mělo dojít okolo roku 2005 – 2015.

IPv4 adresa má velikost 4 byte = 32 bitů. Nejčastěji se zapisuje v desítkové soustavě, kdy jednotlivé byte jsou odděleny tečkou. Každý byte může logicky nabývat hodnot od 0 - 255. Například: **192.44.118.192**

Adresa IP se skládá ze dvou částí **net - ID** (adresa sítě) a **host - ID** (adresa počítače). Podle toho jak jsou jednotlivé sítě rozlehle (kolik mají hostů) rozlišujeme tři hlavní třídy IP adres.

Popis tří hlavních tříd IP adres: A, B, C

Třída A



IP adresu třídy A v České republice nikdo nemá. Mají ji hlavně nadnárodní společnosti, vládní organizace USA atd. Dovoluje adresování jen 126 sítí, ale v každé z nich může být až 16 miliónů počítačů. Rozsah hodnot IP adres je: 0.0.0.0 až 127.255.255.255.

Třída B



Třída B umožňuje adresovat už 16 tisíc sítí a 65 tisíc počítačů v každé síti. První dva byte je adresa sítě a další dva adresa počítače. V Čechách ji mají významné organizace. Rozsah hodnot ve třídě B je: 128.0.0.0 až do 191.255.255.255.

Třída C



IP adresou třídy C dokážeme adresovat až 2 milióny sítí. V každé síti může být 254 počítačů. IP adresa třídy C je v Čechách nejpoužívanější. První tři byte jsou adresou sítě a jeden byte adresou počítače. Rozsah je: 192.0.0.0 až 223.255.255.255

Speciální IP adresy

Některé IP adresy jsou vyhrazeny pro speciální účely.

Rozsah od **224.0.0.0** do **239.255.255.255** je zařazen do třídy D. Tato třída je využívána pro multicasting. To znamená pro hromadné vysílání videa nebo audia.

Rozsah od **240.0.0.0** do **247.255.255.255** patří do třídy E. Tyto hodnoty jsou rezervovány pro další použití a pro experimentální účely.

127.0.0.0 nebo **127.0.0.1** jsou určeny k testovacím účelům. Nazývají se **loopback adresy**. Tyto adresy používá síťový software. Pošleme-li data na tuto adresu, nebudou vysílána přes žádný ze síťových adaptérů počítače do sítě. Pouze zjistíme zda je funkční software, nezávisle na tom, funguje-li síťový hardware.

Síťové adresy, tj. adresy, jejichž host část obsahuje samé nuly. Tyto adresy jsou využívány IP protokolem ke správnému směrování paketů mezi sítěmi.

Broadcast adresa: **255.255.255.255** je určena všem hostům v dané síti. Používají se k hromadnému rozesílání paketů.

Intranet, pokud je síť izolovaná, bez připojení k Internetu, lze použít libovolné IP adresy. Při připojení vnitřní sítě k Internetu by ale mohla nastat situace že budou existovat dvě stejné IP adresy. Této skutečnosti zabráňuje PROXY brána. Proxy brána může sloužit pro libovolnou službu protokolu **TCP/IP**.

Proxy je ve skutečnosti počítač, který je připojen libovolným způsobem k Internetu. Musí mít skutečnou IP adresu aby viděl "ven" a z "venku" byl vidět.

Při napsání nějaké www adresy na počítači ve vnitřní síti, prohlížeč odešle tento dotaz na proxy bránu. Ta se dotáže svým jménem na Internetu a poté předá požadavek zpátky počítači. A na okolních počítačích se nastaví adresa vyhrazená pro vnitřní síť. Rezervované IP pro vnitřní síť:

Třída A : 10.0.0.0 až 10.255.255.255

Třída B : 172.16.0.0 až 172.31.0.0

Třída C : 192.168.0.0 až 192.168.255.0

Metody potvrzování

Potvrzování je postup používaný pro zajištění spolehlivého doručení zprávy.

Schopnost potvrzování je součástí protokolů.

Rozeznáváme:

ACK - (acknowledgement) - pozitivní potvrzování

Jde o kontrolní kód - ASCII znak 6 (hexadecimálně 06H), vyslaný k vysílací stanici nebo počítači příjemci

jednotkou za účelem potvrzení připravenosti příjemce obdržet danou informaci, nebo bezchybného přenosu informace. Tato schopnost, vysílat a přijímat potvrzovací signály je vestavěna do softwaru. Samotné signály jsou pro uživatele neviditelné. Pracuje na tom principu, že vysílací stanice vyšle paket a přijímací stanice pošle potvrzení, zda paket došel v pořádku. Jestliže se vysílací stanice nedočká po určenou dobu (time-out) potvrzení tak paket vysílá znovu.



Pakety se musí číslovat, aby bylo jasné kolikrát se který poslal.

Vysílací stanice vyšle první paket. Ten přes přenosové médium v pořádku dorazí k přijímací stanici. Ta odešle potvrzení zpět že paket číslo jedna úspěšně dorazil. Vysílací stanice obdrží potvrzení a pošle paket číslo dva. Ten ale k přijímací stanici nedorazí. Vysílací stanice čeká po určenou dobu na potvrzení, po time-outu vysílá znovu paket č. dva. Ten dorazí k přijímací stanici která vyšle potvrzení, které ale nedorazí. Vysílací stanice po time-outu opět vyšle paket číslo dva. Přijímací stanice přijme paket číslo dva a vyšle potvrzení že došel v pořádku. Přijímací stanice přijme potvrzení a posílá paket číslo tři atd.

NAK - (negative acknowledgment) - negativní potvrzování

Jde o řídicí kód, symbol 21 v ASCII (hexadecimálně 15H) vyslaný nazpět do vysílací stanice nebo počítače jednotkou, která je adresátem, jako znamení, že vysílaná informace dorazila v nesprávném tvaru. Schopnost přijímat a vysílat potvrzení (acknowledgment signals) je zabudována do softwaru, uživatelé takového softwaru se nemusejí o vysílání a přijímání takových zpráv starat. Toto potvrzování je rychlejší než ACK, ale musí se vlastně s ním kombinovat. Je zde určená doba (time-out) po kterou počítač čeká jestli nepřijde negativní potvrzení o nějakém paketu - potom vysílá dále.

Skupinové potvrzování – okénkové potvrzování

Jedná se vlastně o takové potvrzování, kdy se například po každých 20 paketech vyšle potvrzení. Když je pozitivní tak se pokračuje dále, jestliže je negativní, tak se oznámí číslo porušeného paketu a vysílací stanice začne vysílat znovu od porušeného paketu dále. Tento systém se opakuje dokud neskončí přenos. Schopnost takového potvrzování obstarává opět software. Uživatel o ničem neví. Pokud je spojení mezi počítači kvalitní může se nastavit velké okno (1000 paketů), pokud je linka nekvalitní nastaví se malé okno, aby se nemuselo moc opakovat.

Nesamostatné potvrzování

Je to typ potvrzování, při kterém je k odeslanému paketu přiložen určitý typ zprávy, která obsahuje číslo poslaného paketu. Přijímací stanice toto číslo odešle zpátky jako potvrzení. Používá se to vždy po více paketech. Když je vše v pořádku, vysílací stanice pokračuje. Jestliže to nedojde v pořádku, odešlou se pakety znovu. Protože je potvrzení posíláno společně s daty ušetří se přenosová rychlost.

Protokol TCP/IP

Řekne-li se dnes **TCP/IP**, je to obvykle chápáno jen jako označení dvou přenosových protokolů, používaných v počítačových sítích s počítači na bázi Unixu, konkrétně protokolů TCP (Transmission Control Protocol) resp. IP (Internet Protocol). Ve skutečnosti ale zkratka TCP/IP označuje celou soustavu protokolů, ne nutně vázanou na operační systém Unix, přičemž TCP a IP jsou sice nejznámější protokoly této soustavy, ale zdaleka ne protokoly jediné. Správnější je ale považovat TCP/IP za ucelenou soustavu názorů o tom, jak by se počítačové sítě měly budovat a jak by měly fungovat.

Čtyři vrstvy TCP/IP

Zatímco referenční model ISO/OSI vymezuje sedm vrstev síťového programového vybavení, **TCP/IP** počítá jen se čtyřmi vrstvami. Nejnižší vrstva, vrstva síťového rozhraní (**Network Interface Layer**) (někdy též: linková vrstva resp. Link Layer) má na starosti vše, co je spojeno s ovládáním konkrétní přenosové cesty resp. sítě, a s přímým vysláním a přijímáním datových paketů. V rámci soustavy TCP/IP není tato vrstva blíže specifikována, neboť je závislá na použité přenosové technologii.

Vrstvu síťového rozhraní může tvořit relativně jednoduchý ovladač (device driver), je-li daný uzel přímo připojen například k lokální síti či ke dvoubodovému spoji nebo může tato vrstva představovat naopak velmi složitý

subsystém s vlastním linkovým přenosovým protokolem (např. HDLC apod.). Vzhledem k velmi častému připojování jednotlivých uzlů na lokální síť typu Ethernet je vrstva síťového rozhraní v rámci TCP/IP často označována také jako Ethernetová vrstva (**Ethernet Layer**).

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. Úkol této vrstvy je v prvním přiblížení stejný, jako úkol síťové vrstvy v referenčním modelu ISO/OSI - stará se o to, aby se jednotlivé pakety dostaly od 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.

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 například 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.

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