Počítačové sítě

(dsi)

Pomocný studijní text pro předmět
vyučovaný ve druhém ročníku bakalářského studia
oboru 23-70-7 Aplikovaná informatika a řízení

Garant: Ing. Jan Roupec, Ph.D.

Brno, listopad 2002

OBSAH

1 ÚVOD 3

2 DATOVÁ KOMUNIKACE 5

2.1 DATOVÉ SPOJE, KANÁLY A OKRUHY 5
2.2 MULTIPLEXORY 6
2.3 PROPOJOVACÍ ZAŘÍZENÍ 7
2.4 PŘENOS DAT 8
2.4.1 Přenosová a modulační rychlost 8
2.5 ŘÍZENÍ DATOVÉHO SPOJE 9
2.5.1 POTVRZOVÁNÍ 10
2.6 KONCOVÁ A UKONČUJÍCÍ ZAŘÍZENÍ 10

3 ROZDĚLENÍ POČÍTAČOVÝCH SÍTÍ 11

3.1 METODY PŘÍSTUPU K MÉDIU 14

4 KABELY POUŽÍVANÉ V POČÍTAČOVÝCH SÍTÍCH 17

4.1 METALICKÉ KABELY 17
4.1.1 Nesymetrické kabely 17
4.1.2 Symetrické kabely 18
4.1.3 Parametry metalických kabelů 19
4.2 OPTICKÉ KABELY 20
4.2.1 Druhy optických vláken 22

5 PLATFORMY LAN 25

5.1 ETHERNET 26
5.1.1 Formát rámce 27
5.1.2 Ethernet s koaxiálním kabelem 28
5.1.3 Ethernet s kabelem UTP 30
5.1.4 Topologická omezení 32

6 NORMALIZACE POČÍTAČOVÝCH SÍTÍ 34

7 PROPOJOVÁNÍ POČÍTAČOVÝCH SÍTÍ 38

7.1 BRIDGE 39
7.2 ROUTER 41
7.2.1 Routovací algoritmy 43
7.2.2 Vnitřní směrovací protokoly 45

8 RODINA PROTOKOLŮ TCP/IP 49

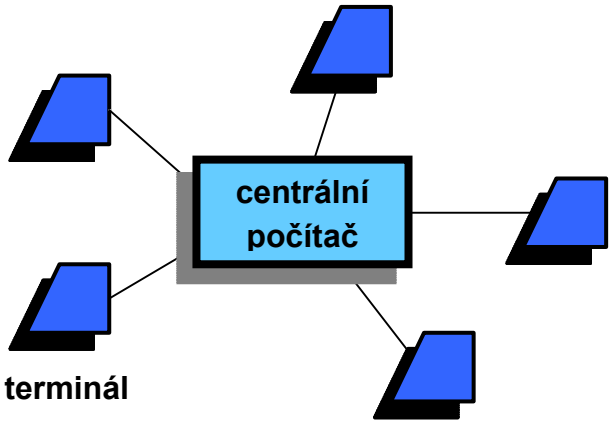
8.1 ADRESACE V PROTOKOLU TCP/IP 51
8.1.1 Podsíťování (subnetting) 53
8.1.2 Problém nedostatku IP adres 53

8.1.3 IP adresy třídy D *55*
8.1.4 IP verze 6 ..... *55*
8.2 DATOVÝ KOMUNIKAČNÍ MODEL 55
8.2.1 Síťová vrstva *57*
8.2.2 Internetová vrstva *57*
8.2.3 Transportní vrstva *58*
8.2.4 Aplikační vrstva *59*
8.3 SLUŽBA DNS 62
9 SLUŽBA WWW 66
9.1 JAZYK HTML 66
9.2 STATICKÉ A DYNAMICKÉ WWW STRÁNKY 67
9.2.1 WWW stránky dynamické na straně serveru *68*
9.2.2 WWW stránky dynamické na straně klienta *68*
10 VYSOKORYCHLOSTNÍ SÍTĚ 70
10.1 PŘEPÍNÁNÍ 70
10.1.1 Virtuální sítě *72*
10.2 FAST ETHERNET 73
10.3 GIGABIT ETHERNET 75
10.4 100VG-ANYLAN 75
10.5 FDDI 76
10.6 ATM 77
11 BEZDRÁTOVÉ SÍTĚ 79
11.1 ARCHITEKTURA TECHNOLOGIE IEEE 802.11 79

Autor děkuje za podporu z Projektu rozvoje bakalářských programů na Fakultě strojního inženýrství VUT v Brně a za možnost začlenit do textu některé poznatky získané při řešení výzkumného záměru CEZ: J22/98: 261100009 „Netradiční metody studia neurčitých a komplexních systémů“.

1 ÚVOD

Historicky nejstarším způsobem využívání počítačů je tzv. **dávkový režim**. Přímý přístup k počítači byl vyhrazen jeho technické obsluze, uživatelé (z tohoto pohledu byli hlavními uživateli programátoři) zadávali své požadavky obsluze, obvykle na papíře nebo ve formě sady děrných štítků příp. děrných pásek.



Obr. 1.1: *Centrální počítač s terminálovou sítí*

Se zvyšováním výkonu počítačů a vývojem nových periferních zařízení bylo možné postupně přejít k **interaktivnímu režimu** práce. Uživatel (v této fázi už nikoliv nutně programátor) mohl sám (bez zprostředkující role obsluhy) komunikovat s počítačem pomocí zařízení zvaného **terminál**. Terminál představoval zařízení umožňující textový vstup (pomocí klávesnice) a textový (později i grafický) výstup (na papír nebo na obrazovku). Jako první terminály se uplatňovaly např. dálnopisné přístroje. Počítače byly velmi drahé a v tomto interaktivním režimu se nutně projevovaly ztrátové časy, kdy počítač čekal, až si uživatel u terminálu rozmyslí svoji další činnost. Aby byly drahé počítače lépe využity, začal se používat multitaskový (víceúlohový) a víceuživatelský režim, kdy na počítači je zdánlivě současně vykonáváno několik programů a počítač zdánlivě současně obsluhuje více uživatelů (ve skutečnosti samozřejmě počítač uživatele i úlohy obsluhuje postupně a svoji pozornost rychle přepíná mezi úlohami a uživateli). Bylo běžné, že k počítači bylo připojeno mnoho terminálů (typicky desítky), začalo se hovořit o architektuře tzv. střediskového počítače s terminálovou sítí. K úspěšnému provozu bylo nutné, aby operační systémy poskytovaly ochranu uživatelů tak, aby bylo možné řídit práva přístupu konkrétních uživatelů ke konkrétním datům (datovým souborům, programům), uživatel se musel identifikovat jménem a heslem. Toto řešení se v sedmdesátých letech 20. století silně rozšířilo. Poskytovalo nebývalé možnosti práce – ať se uživatel přihlásil kdekoliv, vždy měl k dispozici svoje data a programy, bylo možné, aby skupiny uživatelů v případě potřeby používaly společná data (**sdílení dat**),

všichni oprávnění uživatelé mohli využívat drahé periferie, např. tehdy velmi drahé tiskárny (**sdílení periferií**). Kromě výhod lze hovořit i o některých nevýhodách. Zejména to byla velká finanční náročnost takového řešení – centrální počítače i terminály byly velmi drahé (takže přístup k počítači nemohl mít každý, používání počítačů se vyplácelo pouze v některých aplikačních oblastech). Další nevýhoda spočívá v tom, že o výkon centrálních počítačů se dělilo mnoho uživatelů, takže doba odezvy byla proměnlivá podle zatížení (terminál je pouze vstupní a zobrazovací jednotka, programy běží v centrálním počítači, nikoliv v terminálu). Uživatel byl také závislý na technické obsluze počítače (např. které disky byly momentálně založeny, jaký papír je v tiskárně apod.).

Po vynálezu mikroprocesoru (první mikroprocesor I4004 se začal vyrábět v roce 1971, populární I8080 potom v roce 1974) se objevila další možnost – **osobní mikropočítač**. Tyto počítače byly levné, takže každý mohl mít osobní mikropočítač trvale k dispozici. Je zřejmé, že u osobních mikropočítačů nebylo možné používat sdílení dat ani periferií; každý mikropočítač pracoval izolovaně a samostatně.

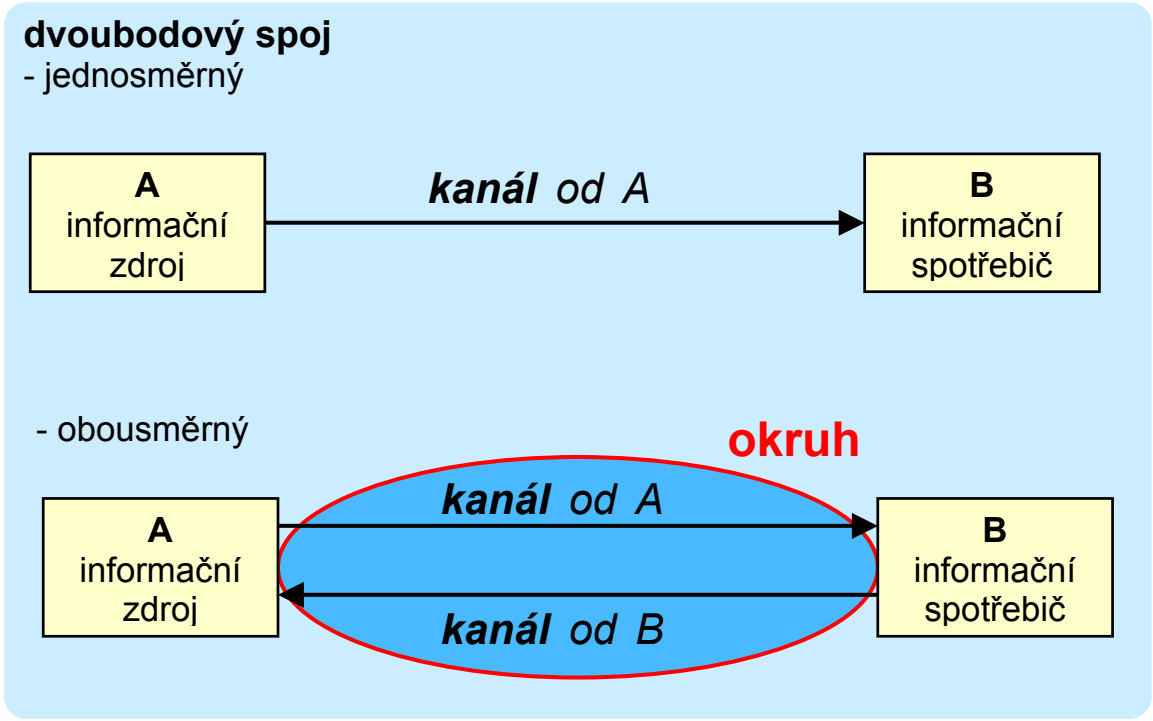
Počítačové sítě jsou logickým vyústěním snahy zachovat výhody střediskových počítačů s terminálovou sítí i osobních mikropočítačů a současně eliminovat nevýhody obou těchto řešení. Všechny technické prostředky sítě (střediskové počítače, mikropočítače, periferní zařízení) jsou vzájemně propojeny, uživatel se síti identifikuje jménem a heslem a může využívat z kteréhokoliv místa všechny prostředky, jejichž využití má povoleno.

Je třeba poznamenat, že i u střediskových počítačů byla snaha tyto propojovat, ať už z důvodu zálohování např. u řídících počítačů, propojování počítačů různých organizačních jednotek téže instituce (např. bankovní sítě) nebo zajišťování aplikací jinak neprovozovatelných (např. rezervace letenek). Vznikla tak řada firemních řešení (z nejznámějších např. DecNet), o počítačových sítích v pravém slova smyslu se ovšem začalo hovořit až později.

2 DATOVÁ KOMUNIKACE

2.1 Datové spoje, kanály a okruhy

Základní jednotkou datové komunikace je **spoj**, který umožňuje výměnu informací mezi informačním zdrojem a informačním spotřebičem. Spoje mohou být dvoubodové (pro komunikaci mezi dvěma účastníky) a vícebodové (komunikace více uživatelů). Dvoubodový spoj se skládá ze dvou **stanic** propojených **přenosovou cestou**. Cesta pro jednosměrný přenos informací se nazývá **kanál**, cesta pro obousměrný přenos informací se nazývá **okruh**. Situace je schematicky znázorněna na obr. 2.1.



Obr. 2.1: Dvoubodové spoje

Pokud mezi stanicemi existuje pouze kanál, hovoří se o **simplexním** přenosu (*simplex, SX*). Obousměrný provoz (vybavený okruhem) může být:

- **duplexní** (*full duplex, FDX*) – obousměrný současný provoz (informace mohou být současně přenášeny oběma směry)
- **poloduplexní** (*half duplex, HDX*) – obousměrný střídavý provoz (informace mohou být přenášeny oběma směry, v jednom okamžiku však pouze jedním směrem)

Datové okruhy lze podle jejich řešení a vlastností rozdělit několika způsoby, např. na:

- **pevné** datové okruhy (mezi stanicemi je přímé spojení, není mezi nimi použito žádné přepínací zařízení)
- **komutované** (**přepínané**) datové okruhy – mezi mnoha stanicemi je vytvořeno spojení umožňující jejich různá propojení, konkrétní spojení dvou (nebo více) stanic je realizováno za účasti přepínacího zařízení (např. telefonní síť s telefonními ústřednami)

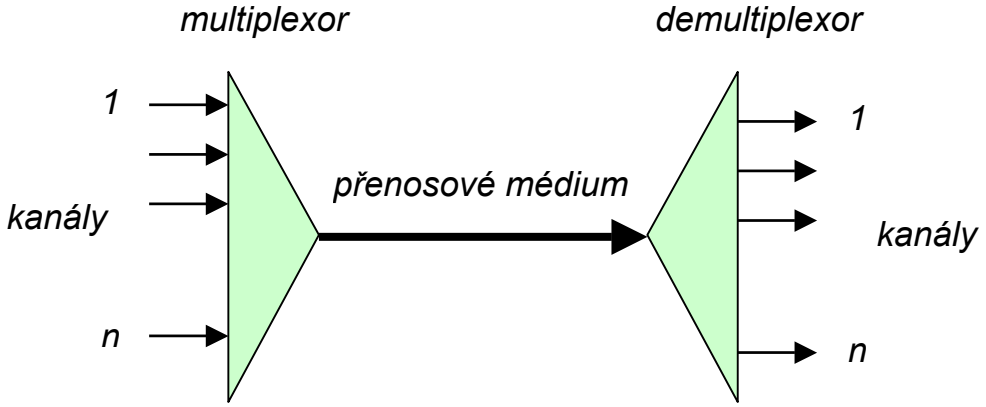
Podle charakteru přenášených signálů lze dělit okruhy na:

- **analogové** – signál se průběžně spojitě mění v čase a může dosahovat libovolné hodnoty z nějakého rozsahu,
- **digitální** – signál se mění pouze v určitých časových okamžicích a dosahuje vždy jedné ze dvou možných hodnot, reprezentujících dvojkovou hodnotu 0 a 1.

Podle své podstaty se okruhy dělí na

- **drátové** – používají metalické nebo optické vodiče,
- **bezdrátové** – k přenosu se používají elektromagnetické vlny rádiové nebo optické (obvykle IR).

Obvykle se setkáváme s **fyzickými** okruhy, kde přenosová cesta je podložena fyzickým přenosovým médiem nebo prostředím. Nastávají také případy, kdy data jsou po cestě zaznamenána a až následně odeslána adresátovi (střadačové spojování). Mezi koncovými stanicemi pak neexistuje fyzická cesta v pravém slova smyslu, ale pouze cesta pomyslná. Takové okruhy mají obdobné vlastnosti jako fyzické okruhy, a nazývají se **virtuální okruhy** (*virtual circuit, VC*). Podobně jako fyzické okruhy mohou tyto být pevné nebo komutované, hovoří se o **pevných virtuálních okruzích** (*permanent virtual circuit, PVC*) a **přepínaných virtuálních okruzích** (*switched virtual circuit, SVC*).



Obr. 2.2: Multiplexor a demultiplexor

2.2 Multiplexory

Aby byla přenosová kapacita přenosového média lépe využita, přenáší se často jedním médiem současně (nebo zdánlivě současně) více datových toků (kanálů). 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** (obr. 2.2).

Multiplexory pracují na dvou základních principech:

- **kmitočtové dělení** (frekvenční multiplex, *Frequency Division Multiplex*, *FDM*): kmitočtové pásmo se rozdělí na dílčí podpásma, každému kanálu je přiděleno jedno kmitočtové podpásmo, používá se zejména v telefonii, multiplexory jsou spolehlivé a levné,

- **časové dělení** (časový multiplex, *Time Division Multiplex*, *TDM*): přenosový čas je rozdělen na časové rámce a časové úseky, každému zařízení (kanálu) je přidělován jeden úsek v každém cyklu, tento princip je základem **časových** (synchronních) **multiplexorů**.

Velmi často se používají tzv. **statistické časové multiplexory** (*Statistical Time Division Multiplex*, *STDM*), nazývají se také asynchronní multiplexory. Na rozdíl od výše zmíněných multiplexorů synchronních přidělují časové rámce nikoliv v pevně daných časech, ale podle momentálních potřeb (v nejjednodušším případě na celou dobu trvání spojení). STDM obsahují vyrovnávací paměť pro přicházející data od připojených zařízení. Podporují inteligentní řízení toku dat a mohou plnit i další funkce (např. diagnostika).

2.3 Propojovací zařízení

V reálně existujících sítích obvykle nenastávají případy, kdy pro libovolnou dvojici komunikujících zařízení existuje samostatná přenosová cesta (viz topologie počítačových sítí, kap. 3). Vznikne-li potřeba komunikace dvou zařízení, je potřeba mezi nimi vytvořit spojení (kanál nebo okruh – fyzický nebo virtuální). Přepojování se dělí na:

- přepojování okruhů,
- přepojování paketů.

Přepojování okruhů je nejstarší způsob používaný v telegrafních a telefonních sítích (a také v sítích ISDN). Lze je dále rozdělit na **prostorové** a **časové**. Prostorové přepojování okruhů (spojování) znamená fyzické propojení (vystavění) přenosové cesty od zdroje ke spotřebiči, tato cesta je obvykle udržována (tzn. blokována) po celou dobu trvání spojení (např. klasické telefonní spojení). Časové přepojování vychází z podstaty časového dělení s tím, že ze společného časového rámce se vydělují časové úseky pro různé kanály (v uzlových bodech potom odesílané do různých směrů).

Přepojování paketů vzniklo z přepojování zpráv. Přepojování zpráv vychází z názoru, že je neúčelné udržovat spojení během celého trvání dialogu dvou zařízení, jako je tomu u přepojování okruhů. Každá zpráva je posílána separátně, obvykle tak, že ani pro poslání zprávy není vystavěna kompletní cesta, ale využívá se přenosu s mezilehlou pamětí v přepojovacích uzlech. Protože zpráva nemá definovaný žádný limit délky (shora ani zdola), nelze v komunikační síti s přepojováním zpráv ani odhadnout časové poměry přenosu. Z toho důvodu se zavádějí tzv. pakety, tj. datové shluky s omezenou minimální i maximální délkou (dlouhé zprávy se rozdělují do více paketů, příp. extrémně krátké zprávy se posílají v paketech jisté minimální délky – doplňují se na délku paketu). V klasické podobě používají přepojování paketů rozlehlé sítě X.25.

Kromě pojmu paket se používá také pojem **rámec** (*frame*). Tímto označením se rozumí paket doplněný o režijní údaje dané konkrétní počítačové sítě (adresace příjemce a odesílatele, zabezpečení přenosu proti chybám apod.). V počítačových sítích se tedy na fyzické úrovni zasílají rámce.

Pakety i rámce mají obecně proměnlivou (i když z obou stran limitovanou) délku. V případě extrémně vysokých nároků na přesnost dodržení časových poměrů datových přenosů (např. při obrazových nebo zvukových přenosech) se jeví jako výhodné pracovat s rámci konstantní (obvykle velmi malé) délky. Takové rámce se nazývají **buňky** (*cells*). Principu přepojování buněk používá síť ATM (viz kap. 10).

2.4 Přenos dat

Nejmenší jednotka informace, která slouží pro přenos, je jeden bit. Přenos dat se odehrává v jednom ze dvou režimů: paralelní a sériový.

U **paralelního přenosu** se přenáší několik (obvykle 8, 16, …) bitů současně (po separátních vodičích). Paralelní přenos je rychlý, používá se ale pouze na malé vzdálenosti (příp. zpoždění v přenosu jediného bitu znamená při příjmu nesrozumitelnost celého znaku).

Sériový přenos znamená přenos bit po bitu, přenášené znaky je třeba předem převést do posloupnosti bitů a po příjmu je opět složit. Charakteristickou hodnotou je doba na přenos jednoho bitu (*bit time*).

Důležitá je otázka **synchronizace** vysílače a přijímače, tedy určení okamžiků, kdy je stav signálu důležitý, kdy je hodnota dat platná. U paralelních přenosů se tato otázka obvykle řeší přídavnými řídícími signály (několik signálů navíc při paralelním přenosu mnoha bitů nepředstavuje významnou technickou komplikaci datového rozhraní). U sériových přenosů nebývá možné tyto řídící informace přenášet separátně. Podle způsobu synchronizace při přenosu se hovoří o přenosech asynchronních a synchronních.

Při **asynchronním přenosu** dat se posílá každý znak zvlášť a každý znak má svoji synchronizaci. Před posláním vlastního datového znaku se vyšlou rozběhové bity – tzv. *start bity* – (změna signálu s definovanou dobou trvání nebo definovaným průběhem), po této úvodní sekvenci jsou vysílány jednotlivé bity znaku (s definovanou dobou přenosu jednoho bitu), následovat může paritní bit a přenos je zakončen závěrnými bity (tzv. *stop bity*). Asynchronní přenos je relativně neefektivní, režie spojená se synchronizací každého znaku zvlášť je značná. Asynchronní přenos se používá zejména pro pomalejší přenosy nebo přenosy menších objemů dat.

Při **synchronním přenosu** se posílají celé bloky dat ve formě souvislého bloku bitů, každý blok je předcházen synchronizačními bity. V době, kdy se nepřenášejí žádná data, přenášejí se speciální klidové znaky. Synchronní přenos vyžaduje vyrovnávací paměť. Používá se především pro vysoké rychlosti přenosu.

2.4.1 Přenosová a modulační rychlost

Přenosová rychlost (datová rychlost, rychlost spoje) udává množství informací (v bitech) přenesených za jednotku času, používané jednotky jsou bit/sekunda (b/s) a odvozené násobky (kb/s, Mb/s, Gb/s).

Modulační rychlost (symbolová rychlost, baudová rychlost) vyjadřuje počet změn signálu za jednotku času (počet logických stavů signálu za sekundu). Jednotkou je 1 Bd

(baud, dle Ing. Baudota, fr.). Tato rychlost představuje frekvenci přenášeného signálu a je omezena šířkou pásma kanálu.
Pokud hodnota stavu signálu odpovídá právě jednomu bitu, je přenosová rychlost rovna modulační rychlosti. Je výhodné, aby přenosová rychlost byla vyšší než modulační. V tabulce 2.1 jsou hodnoty modulačních a přenosových rychlostí pro nejpoužívanější modemová doporučení.

Doporučení CCITT/ITU-T	Modulační rychlost [Bd]	Počet bitů na stav signálu	Přenosová rychlost [bit/s]
V.22bis	600	4	2400
V.32	2400	4	9600
V.32bis	2400	6	14400
V.34	2400–3200	9	28800

Tab. 2.1: Přenosové a modulační rychlosti modemových doporučení

2.5 Řízení datového spoje

Z hlediska řízení toku dat je při datových přenosech nutné provádět zejména následující činnosti:

- synchronizace na úrovni rámců – rozpoznání začátku a konce,
- organizace provozu na spoji dvou nebo více partnerů,
- řízení toku rámců zabraňující zahlcení přijímače,
- reakce na výskyt chyby (zjištěné),
- identifikace komunikujících partnerů.

Uživatelům komunikace (obvykle programy využívající komunikaci) v počítačové síti jsou poskytovány služby různých druhů:

- **nespojovaná nepotvrzovaná služba**
  - vysílá se bez ohledu na výsledek zpracování rámců při příjmu
  - pro úspěšné použití nutná nízká chybovost (např. LAN)
  - vhodné i pro řízení v reálném čase (je-li preferováno malé zpoždění před spolehlivostí)
- **nespojovaná potvrzovaná služba**
  - přijímací strana potvrzuje přijetí
  - pokud nedojde potvrzení do jisté doby, vysílač pokus o vysílání opakuje
- **spojovaná služba**
  - všechny vyslané rámce jsou přijaty právě jednou se zachováním pořadí
  - před přenosem dat je fáze navázání spojení
  - po ukončení přenosu dat je fáze zrušení spojení

2.5.1 Potvrzování

Problematika potvrzování poskytuje vysílajícímu možnost ověřit, že data byla v pořádku přijata, a přijímajícímu uzlu umožňuje požádat o zopakování dat, která byla přijata chybně např. v důsledku problémů na přenosové cestě. Existují některé základní přístupy:

- **Pozitivní potvrzování** – po přijetí každého datového rámce je od adresáta k odesílateli zaslán rámec s potvrzením správného příjmu. Pokud potvrzení nepřijde, odešle odesílatel data znovu (samozřejmě s omezeným počtem opakování). Tato varianta má některé záporné vlastnosti:
  - značná režie (provoz na síti se zdvojnásobuje),
  - nelze detekovat situaci, kdy data byla doručena v pořádku a "ztratil" se až rámec s potvrzením.
- **Negativní potvrzování** vychází z názoru, že správná funkce je normální a smysl má reagovat pouze na chyby. Na správně přijatý rámec příjemce nijak nereaguje a pouze v případě přijetí chybného rámce požádá o zopakování. Tato metoda nedokáže sama o sobě problematiku potvrzování řešit, neboť nedetekuje situace ztráty datových rámců nebo nedostupnosti adresáta.
- **Číslování paketů, skupinové potvrzování**: Vysílané datové jednotky jsou očíslovány souvislou vzestupnou číselnou řadou. Přijímač dokáže detekovat, zda dostal všechna data. Aby vysílající strana věděla, že přenos probíhá v pořádku, je každý *n*-tý rámec pozitivně potvrzován, pokud potvrzení nepřijde, je celá sekvence zopakována. Obvykle se tato metoda kombinuje s negativním potvrzováním – přijímající strana okamžitě upozorňuje odesílatele na chybně přijatá data příp. i na data chybějící.

2.6 Koncová a ukončující zařízení

V datové komunikaci se z hlediska funkčnosti rozeznávají dva základní typy zařízení:

- **koncové (datové) zařízení** (*data terminal equipment*, *DTE*) – využívá komunikačních služeb pro svoji vlastní činnost, která je jiného charakteru (počítače, terminály, tiskárny, bankomaty, v rozsáhlých sítích rovněž routery),
- **ukončující (datové) zařízení (okruhu)** (*data-circuit terminating equipment*, *DCE*, někdy nesprávně též *data communications equipment*) – poskytuje přístup ke komunikačním prostředkům nebo je přímo implementuje, poskytuje rozhraní mezi sítí a koncovým zařízením. Jedná se o modemy, ústředny, datové koncentrátory, rozbočovače, přepínače apod.

3 ROZDĚLENÍ POČÍTAČOVÝCH SÍTÍ

Počítačové sítě se rozdělují podle mnoha hledisek. Toto rozdělení není pouze formální, ale vydělují skupiny sítí, které mají obdobnou technickou realizaci, obdobnou oblast použití a obdobné vlastnosti. Nejobvyklejší je rozdělení podle **rozlehlosti**:

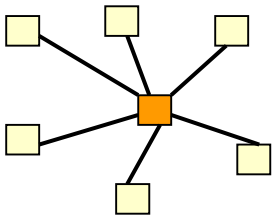
- **lokální počítačové sítě** (*Local Area Networks*, *LAN*)
  - sítě malého rozsahu, obvykle jedna firma, místnost, patro, menší budova
  - rozlehlost max. několik kilometrů (obvykle méně)
  - všechny prostředky (zejména přenosové cesty) ve vlastnictví provozovatele (tzn. nepoužívají se veřejné datové linky)
- **metropolitní počítačová síť** (*Metropolitan Area Networks*, *MAN*)
  - sítě v městské aglomeraci
  - rozlehlost typicky v desítkách kilometrů
- **rozsáhlé počítačové sítě** (*Wide Area Networks*, *WAN*)
  - sítě značného rozsahu, rozměry omezeny dosahem civilizace

LAN, MAN a WAN se vzájemně liší nejen rozměry, ale hlavně charakterem provozu a používanými technickými prostředky. Vzhledem k tomu, že jak druhy aplikací provozovaných v sítích, tak také technické prostředky se velmi rychle vyvíjejí a mění, stírají se a posouvají hranice mezi jednotlivými druhy sítí. Např. se ustupuje od používání pojmu MAN v původním smyslu (provoz i technické řešení sítí MAN a WAN nevykazuje v současné době výrazné rozdíly), pojem MAN se stává spíše názvem vyjadřujícím vlastnickou nebo organizační strukturu. Kromě uvedených tří kategorií se někdy používá kategorie čtvrtá – **kampusní sítě** (*Campus Area Networks*, zkratka CAN se neužívá). Tento pojem se vztahuje k sítím v určitém rozlehlejším areálu (univerzita, nemocnice, lázně, tovární areál, …). Motivací pro užívání tohoto pojmu je skutečnost, že tyto sítě se charakterem provozu blíží sítím lokálním, ovšem vzhledem k jejich rozměrům se často nevystačí s technickými prostředky typickými pro lokální sítě.

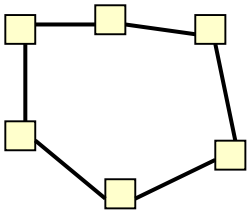
Charakteristickou vlastností počítačové sítě je její **topologie**. (Topologie je obor matematiky, zabývající se zkoumáním vlastností a vztahů geometrických útvarů, které se zachovávají při oboustranně spojitých, vzájemně jednoznačných zobrazeních. Topologií počítačové sítě se rozumí způsob geometrického uspořádání a propojení uzlů sítě.) V případě, že mezi libovolnými dvěma uzly sítě (počítači) existuje právě jedna cesta, hovoří se o sítích s **jednoznačnou** topologií. Používají se ’následující základní topologie:

- **hvězda** (*star topology*) – koncové uzly bývají počítače, ve středu hvězdy je umístěn propojovací prvek (obr. 3.1),
- **kruh** (*ring topology*, obr. 3.2),
- **sběrnice** (*bus topology*, obr. 3.3),
- **páteř** (*backbone topology*) – základem je sběrnice, na ni ale nejsou přímo připojeny počítače, ale další sítě s různou topologií – obvykle opět sběrnice (obr. 3.4),

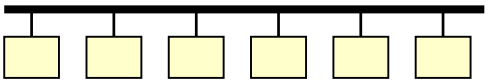
- **strom** (*tree topology*) – v počítačových sítích často splývá stromová a hvězdicová topologie, strom často vzniká propojením několika hvězd, samozřejmě při zachování jednoznačné topologie (obr. 3.5),
- **neomezená topologie** (*unlimited topology*) – obecná síť s nejednoznačnou topologií, extrémním případem je propojení tvořící úplný graf („každý s každým“), tato obecná topologie se používá spíše v rozlehlejších sítích (existence záložních cest pro případ poruchy).



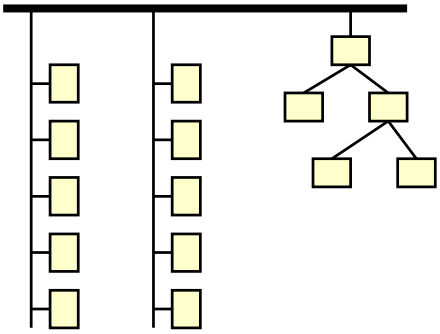
Obr. 3.1: Stromová topologie



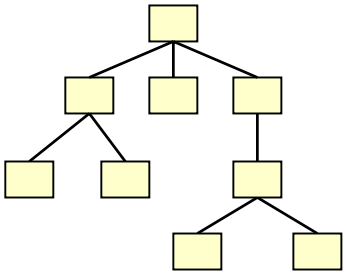
Obr. 3.2: Kruhová topologie



Obr. 3.3: Sběrnicová topologie



Obr. 3.4: Páteřová topologie



Obr. 3.5: Stromová topologie

Podle hierarchického uspořádání počítačů v síti se rozlišují sítě:

- **rovný s rovným** (*peer-to-peer*, *p2p*)
  - všechny počítače v síti jsou hierarchicky rovnocenné,
  - principiálně každý počítač může poskytovat svoje prostředky a služby všem ostatním počítačům (některé prostředky lze ze sdílení vyloučit konfigurací nebo sdílení vázat na oprávnění uživatele),
  - vhodné spíše pro sítě s menším počtem počítačů (malé LAN),
  - typický software pro tento typ sítí v minulosti představovaly systémy Lantastic, Netware Lite, MS Windows 3.11, později Windows 95, Windows 98, u Windows NT/2000/XP je podpora sítí p2p zachována,

- **klient/server** (*client/server*)
    - v síti se nacházejí dva druhy počítačů: poskytovatelé služeb (servery) a konzumenti služeb (klienti, stanice)
    - v některých případech lze na serverech současně pracovat jako na stanicích (tzv. nevyhrazené servery, *non-dedicated servers*), v jiných to není možné (vyhrazené servery, *dedicated servers*)
    - typický software je např. Novell Netware, MS Windows NT/XP/2000 (v konfiguraci server/workstation)
    - poměr serverů a stanic v síti bývá typicky 1:10 až 1:100
    - obecně mohou servery sloužit pro různé služby a účely, např.:
        - **diskový server** (*disc server*) – poskytuje kapacitu disku (na úrovni služeb BIOS, tzn. stopa/sektor)
        - **souborový server** (*file server*) – poskytuje kapacitu disku na úrovni souborového systému
        - **tiskový server** (*print server*) – pro připojení sdílené tiskárny (tiskáren), umožňuje řadit tiskové úlohy do front, s úlohami ve frontě manipulovat a tisknout
        - **server jmen** (*name server*) – viz kap. 8
        - komunikační, databázové a různé další specializované servery

Rozdíl mezi sítěmi typu klient/server a rovný s rovným je pouze záležitostí použitého softwaru, po stránce technické není v těchto sítích rozdíl (konkrétní síť se může podle použitého programového vybavení chovat jako síť klient/server nebo rovný s rovným).

Kromě uvedených sítí client/server a peer-to-peer se někdy hovoří také o sítích **host/terminal**. V tomto případě se nejedná o počítačovou síť v pravém slova smyslu, ale obdobu architektury centrálního počítače se sítí terminálů (viz kap. 1). Přesto je řazení tohoto pojmu do počítačových sítí oprávněné. V dnešní době se už obvykle nepoužívají terminály jako speciální technická zařízení, ale terminály emulované pomocí programů běžících na běžných počítačích. Propojení počítačů (jak toho, který hraje roli „centrálního počítače“, tak i počítačů, na kterých běží emulované terminály) je provedeno pomocí počítačové sítě. Pokud si to aplikace (tedy uživatelé) přejí, mohou využívat architekturu host/terminal (a terminál běží třeba jako úloha v jednom okně počítače jinak používaného jako stanice v síti klient/server). roli centrálního počítače v těchto případech obvykle hraje počítač s operačním systémem UNIX. Terminály bývají obvykle textové (alfanumerické), používají se ovšem i terminály grafické (např. s rozhraním *X-Windows*).

Někdy se uvádí dělení sítí na **sítě soustředěné** a **sítě rozsáhlé**. Přívlastkem soustředěná síť se označuje síť, ve které v celém jejím rozsahu (na všech datových linkách) se v jednom okamžiku nachází maximálně jedna datová zpráva, rozsáhlé jsou potom sítě, ve kterých (jako celku) může být přenášeno více datových zpráv současně. Je zřejmé, že toto dělení souvisí jednak s rozlehlostí sítě ve vztahu k rychlosti přenosu dat a maximální velikosti přenášené zprávy (rámce), jednak s organizací provozu v síti a s její topologií.

Používají se i další dělení než zde uvedená, např. na sítě **soukromé** a **veřejné** apod.

3.1 Metody přístupu k médiu

Z přehledu používaných topologií počítačových sítí plyne, že obvykle neexistuje mezi každou myslitelnou komunikující dvojicí počítačů speciální přenosová cesta, která by byla kdykoliv k dispozici. Požadavky jednotlivých počítačů nastávají spontánně (z pohledu ostatních účastníků komunikace v náhodných okamžicích). S výjimkou neomezené topologie typu „úplný graf" nutně nastávají okamžiky, kdy je nárokováno využití přenosové cesty dvěma nebo více počítači požadujícími vysílání. Situace je navíc komplikována tím, že většina LAN je principiálně koncipována jako síť soustředěná. Má-li síť zůstat funkční, je nutné zvolit nějakou strategii přidělování přenosové kapacity účastníkům komunikace, tyto strategie se označují jako metody řízení přístupu k médiu (přístupové metody, *Media Access Control*). V praxi používané metody lze podle jejich filozofie rozdělit do čtyř skupin.

- **Metody statického přidělování** – přenosové kapacity jsou pevně rozděleny pro jednotlivé účastníky. Používá se:
  - *frekvenční multiplex* (*FDMA*) – viz kap. 2.2
  - *časový multiplex* (*TDMA*) – viz kap 2.2, zejména v družicových sítích
- **Metody centrálního přidělování** – v tomto případě existuje zařízení, které je oprávněno přidělovat přenosovou kapacitu:
  - *na žádost* – počítač požadující vysílání požádá centrum o přidělení přenosové cesty, tato žádost probíhá obvykle na zvláštním služebním kanále. Do této kategorie patří metoda DPA používaná sítí 100VG-AnyLAN.
  - *na výzvu* (*pooling*) – přidělovací centrum se (periodicky) dotazuje počítačů, zda si nepřejí vysílat.
- **Metody náhodného přidělování** vycházejí z názoru, že při slabém provozu (vzhledem k přenosové kapacitě) a náhodných okamžicích vzniků požadavků na vysílání je výhodné začít vysílat pokud možno okamžitě a nezdržovat se režií spojenou s řízením přístupu. Může docházet ke **kolizím**, kdy v soustředěné síti současně vysílají dva nebo více účastníků. Použití pouze v sítích, ve kterých se vysílaný signál v zanedbatelně krátkém čase rozšíří ke všem účastníkům (tedy ne např. pro kruhové sítě).
  - *ALOHA* – vyvinuto v roce 1970 Havajskou universitou pro potřeby tamního rozhlasu. Když účastník komunikace potřebuje vysílat, neprodleně vysílá. Pracuje se s potvrzováním, pokud do stanovené doby nepřijde potvrzení od adresáta, předpokládá se, že se vyskytla kolize a přenos se opakuje. Tato strategie vede k neuspokojivým výsledkům v případě silnějšího provozu. Udává se využití přenosové kapacity na 18%, při zavedení časování (tzv. *řízená ALOHA*) se využití zvýší až na 36%. Navzdory zdánlivě neefektivní strategii ukázala se jako perspektivní a její zdokonalené verze (viz dále) se používají v dnešních nejrozšířenějších počítačových sítích.
  - *Rezervační ALOHA* – podobná jako ALOHA, stanice, která úspěšně odvysílala rámec, má prioritní právo pokračovat ve vysílání. Využití je v oblasti družicových sítí.

- *CSMA* (*Carrier Sense Multiple Access*) – metoda vícenásobného přístupu s příposlechem nosné. Před zahájením vysílání se vždy testuje, zda již nevysílá někdo jiný, pokud ano, vysílání se nezahájí. Vznik kolizí není vyloučen (rychlost šíření signálu je konečná, takže vysílaný signál se nerozšíří ke všem účastníkům komunikace okamžitě – v nulovém čase), ale podstatně omezen.
- *CSMA/CA* (*Carrier Sense Multiple Access/Collision Avoidance*) – po každém uskutečněném vysílání se rezervuje doba potřebná pro přenos potvrzovacího rámce. Vznik kolizí opět není úplně vyloučen. Použití v rádiových sítích. (avoidance = anglicky „vyvarování se“)
- *CSMA/CD* (*Carrier Sense Multiple Access/Collision Detection*) – metoda je podobná jako CSMA, vysílající počítač ale během vysílání stále sleduje, zda signál, který se v síti nachází odpovídá signálu, který on sám vysílá. Pokud tomu tak není, vyhodnotí situaci jako kolizi a všechny počítače v síti na kolizi upozorní speciálním signálem označovaným **jam** (má charakter šumu). Po kolizi každý uzel náhodnou dobu počká a pokus o vysílání opakuje. Náhodné zpoždění se generuje algoritmem binárního exponenciálního odpočítávání. Pokud se ani po šestnácti pokusech po první kolizi nepodaří data odvysílat, další pokusy se nekonají a je hlášena chyba spojení. Metoda CSMA/CD je používána v síti Ethernet.

- **Metody distribuovaného přidělování**
  - *Token Ring* (*kruh řízený příznakem oprávnění*) je metodou používanou v sítích s kruhovou topologií. Pokud žádný počítač nepožaduje vysílání, cirkuluje v kruhu příznak (token). Pokud si uzel přeje vyslat rámec, musí počkat na token a místo něj vyslat svoje data. Token je v kruhu pouze jeden, takže vysílat může v jednom okamžiku pouze jedna stanice. Jakmile bity vyslaného rámce prošly celým kruhem, vysílač je z kruhu odstraňuje. Po odvysílání celého rámce je opět vyslán token. Tato metoda elegantně řeší potvrzování – uzel, kterému byla data určena, může přímo v rámci nastavit příznak, že rámec byl v pořádku doručen. Popsaná metoda se používá v síti s názvem **Token Ring** (síť vyvinutá firmou IBM, podpora ostatních výrobců je nízká).
  - *Token Bus* (*logický kruh*) je metoda principiálně podobná metodě Token Ring, používá se u sítí s jinou než kruhovou topologií. Příznak opravňující k vysílání (token) zůstává a předává se mezi stanicemi. Stanice jsou očíslované (podle pořadí jejich zařazení do kruhu – pořadí, v jakém byly zapnuty), číslo určuje jejich pozici v logickém kruhu, ve kterém cirkuluje token i vysílané datové rámce. V jednom okamžiku může vysílat nanejvýš jedna stanice (existuje pouze jeden token). Realizace této metody je poměrně komplikovaná – je nutno řešit např. problémy spojené se zařazováním nové stanice do kruhu (byl zapnut další počítač) a s vypnutím počítače (je nutno jej vyřadit z logického kruhu). Metoda Token Bus byla implementována v síti Arcnet, která se dnes již nepoužívá

Zvolená metoda přístupu k médiu je pro konkrétní síť velmi důležitá, neboť jednak do značné míry předurčuje její vlastnosti, jednak má vliv na tzv. topologická omezení (zjednodušeně řečeno maximální a příp. i minimální rozlehlost sítě při dané topologii související s požadavky na maximální přípustné zpoždění rámce při průchodu sítí). Obecně platí, že při malém zatížení je výhodné použití sítě s náhodným přidělováním, taková síť bude subjektivně i objektivně vykazovat nejkratší odezvy. U sítí s distribuovaným přidělováním se projevuje vliv doby oběhu tokenu kruhem, takže odezva se bude zhoršovat se stoupajícím počtem zapojených stanic v síti bez ohledu na skutečný provoz (to platí zejména pro sítě s logickým kruhem, u sítě Token Ring se tento vliv uplatní méně vzhledem k rychlosti šíření signálu a maximálnímu přípustnému rozměru sítě). Při překročení jistého mezního zatížení ovšem u sítí s náhodným přidělováním dochází k tzv. zahlcení, kdy prudce narůstá počet kolizí (zejména mnohonásobně opakovaných) a doba odezvy se prudce zhorší, u sítí s jiným druhem řízení přístupu sice také dojde ke zhoršení odezvy, ale časové poměry odesílání dat zůstávají předvídatelné.

4 KABELY POUŽÍVANÉ V POČÍTAČOVÝCH SÍTÍCH

V případech drátových okruhů (viz 2.1) jsou dráty (elektrické vodiče, světlovodná vlákna) sdružovány v kabelech. Podle druhu nosné veličiny, podle uspořádání a vlastností se kabely dělí na:

- **metalické** – veličinou, která nese informaci, je elektrické napětí nebo proud,
- **optické** – nosnou veličinou je světelné záření.

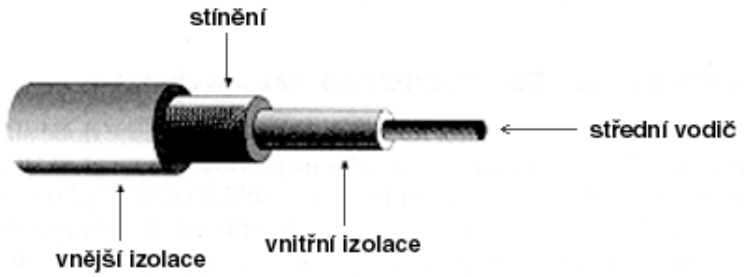
4.1 Metalické kabely

Podle druhu elektrického přenosu se používají dva základní druhy kabelů:

- **nesymetrický kabel** (koaxiální kabel),
- **symetrický kabely** (*twisted pair*, kroucená dvojlinka).

4.1.1 Nesymetrické kabely

Nesymetrický (koaxiální) kabel je tvořen dvěma vodiči v provedení, kdy vnitřní vodič nesoucí signál je obalen vnějším vodičem, který bývá uzemněn a tvoří stínění (obr. 4.1).

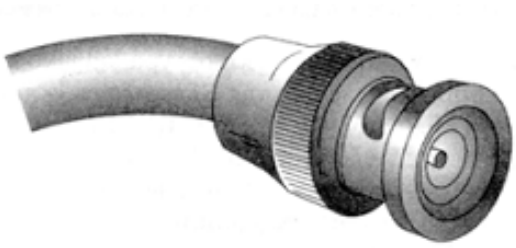


Obr. 4.1: Struktura koaxiálního kabelu

Vlastnosti koaxiálních kabelů lze shrnout do následujících bodů:

- dobrá odolnost proti elektromagnetickému rušení,
- horší odolnost proti magnetickému rušení,
- obvyklé použití pro frekvence do 50 MHz,
- vysoká vlastní kapacita, poměrně vysoký útlum při vysokých frekvencích,
- impedance obvykle 50 – 100 Ω,
- použití pro dvoubodové spoje a pro topologii sběrnice.

Pro připojování koaxiálního kabelu se používají koaxiální konektory, nejčastěji se jedná o tzv. konektory BNC (obr. 4.2).

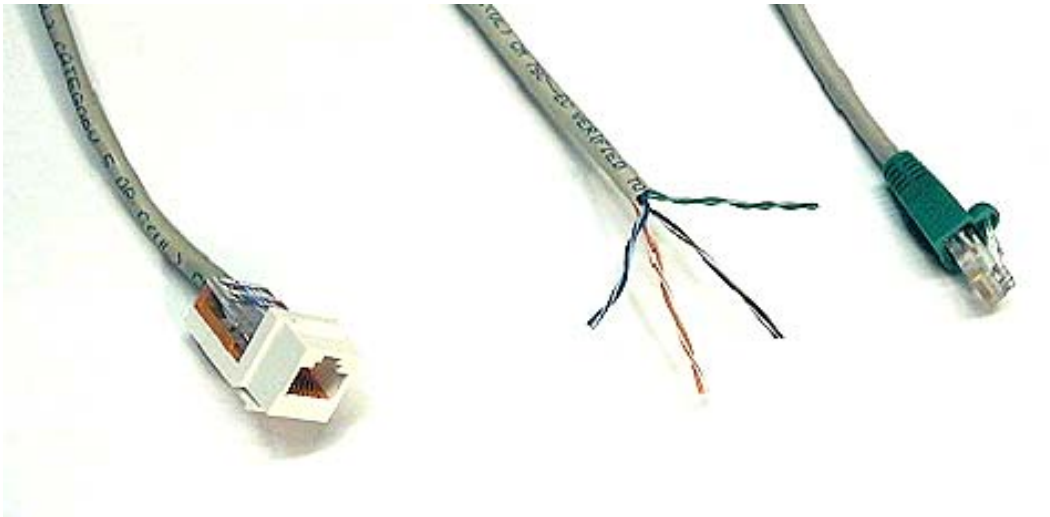


Obr. 4.2: Konektor BNC

4.1.2 Symetrické kabely

Symetrické kabely jsou složeny z párů vzájemně zkroucených vodičů. Jejich základní vlastnosti lze vyjádřit následujícími body:

- levnější než koaxiální kabel,
- obecně horší vlastnosti (ztráty při přenosu vyšších kmitočtů, malá odolnost proti rušení, velké přeslechy mezi páry téhož kabelu apod.),
- používají se jako stíněné (*shielded twisted pair*, *STP*) i nestíněné (*unshielded twisted pair*, *UTP*),
- použití pro dvoubodové spoje,
- impedance obvykle 100 Ω (UTP, STP pro Ethernet) a 150 Ω (STP pro Token Ring),
- v kabelu nejčastěji 4 páry (tzn. celkem 8 drátů).

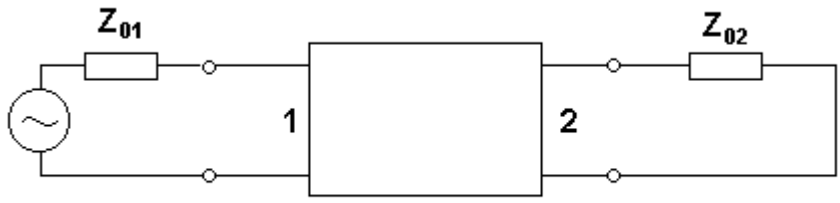


Obr. 4.3: UTP kabel, zásuvka a konektor RJ45

Podle EIA/TIA (EAI – *Electronics Industry Association*, TIA – *Telecommunications Industry Association*) se symetrické kabely na základě svých parametrů člení do několika kategorií, příslušnost kabelu ke kategorii vyjadřuje jeho vhodnost pro určitou oblast použití.

4.1.3 Parametry metalických kabelů

Datové přenosy v počítačových sítích obvykle vyžadují vysoké frekvence přenášených elektrických signálů. Při těchto frekvencích nelze zanedbat elektrické parametry kabelů (odpor, kapacita, indukčnost), takže kabel je třeba považovat za čtyřpól s obecnou impedancí. Při přenosech signálu je žádoucí, aby nedocházelo k odrazu signálu a tím k nežádoucím interferenčním jevům, které by způsobovaly problémy při příjmu. Proto musí být přenos realizován jako přenos impedančně přizpůsobeným čtyřpólem, na jehož svorkách nevzniká odraz vln napětí a proudu. Máme-li zdroj napětí s vnitřní impedancí Z_{01} a spotřebič s impedancí Z_{02} propojené vedením chápaným jako obecný čtyřpól s obrazovou impedancí Z_0 (obr. 4.4) a uvažujeme-li čtyřpól takových vlastností, kdy svorky 1 a 2 jsou vzájemně zaměnitelné (pro vedení splněno), pak k odrazům nebude docházet právě v případě, kdy $Z_{01} = Z_{02} = Z_0$. V tomto případě se hovoří o **impedančně přizpůsobeném vedení**. V praxi to znamená, že kabely musejí být na obou koncích opatřeny impedancí patřičné velikosti. U dvoubodových spojů bývá toto impedanční přizpůsobení součástí připojovaných zařízení, u sběrnic (realizovaných obvykle koaxiálními kabely) se na oba konce kabelu připojuje tzv. zakončovací člen (zakončovací odpor).



Obr. 4.4: Přenos obecným čtyřpólem

Poznámka: Z_0 je tzv. obrazová impedance vedení. Tato veličina se používá jako charakteristická hodnota čtyřpólu nebo vedení s rozloženými parametry. Lze ji chápat jako odpor, který vedení klade šířící se elektrické vlně. Obrazovou impedanci lze určit jako $Z_0 = \sqrt{Z_k \cdot Z_p}$, kde Z_k je impedance čtyřpólu nakrátko (impedance naměřená na vstupních svorkách při zkratovaných svorkách výstupních) a Z_p je impedance čtyřpólu naprázdno (impedance naměřená na vstupních svorkách při nezapojených výstupních svorkách). Pro vedení přibližně platí vztah $Z_0 = \sqrt{\frac{L}{C}}$, kde L je indukčnost a C kapacita vedení.

Kromě obrazové impedance se u metalických kabelů obvykle udávají další parametry:

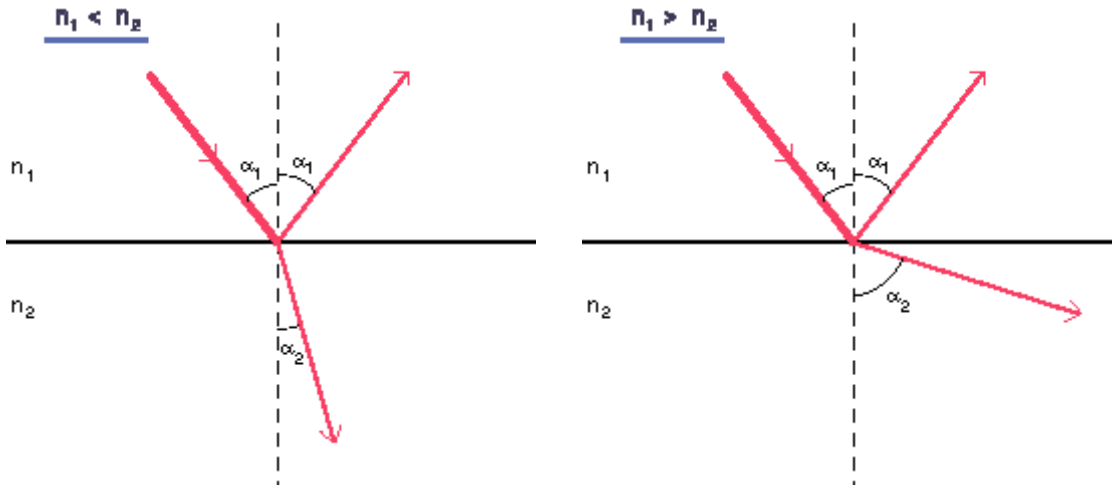
- **mezní frekvence**, pro kterou je kabel určen,
- **útlum** (*attenuation*) – udává se útlum na 100 m délky nebo na 1000 ft, v dB, důležitá je frekvence, pro kterou je udáván,
- **kapacita** (*capacitance*) – pF/ft

- **přeslech na blízkém konci** (*NEXT, Near End Crosstalk*) – poměr úrovní signálů indukovaných v ostatních párech k signálu vysílaného do jednoho z párů, měřeno na stejném konci, do kterého je vysíláno, udává se v dB, hodnota závislá na frekvenci,
- **přeslech na vzdáleném konci** (*FEXT, Far End Crosstalk*) – poměr úrovní signálů indukovaných v ostatních párech k signálu vysílaného do jednoho z párů, měřeno na opačném konci, do kterého je vysíláno, v dB, závislý na frekvenci

U kabelů se mohou vyskytovat i další parametry, které předurčují oblast jeho použití, např. zda vodiče jsou realizovány jako dráty nebo jako lanka, zda je kabel určen pro vnější nebo vnitřní použití (tzn. jak odolává povětrnostním vlivům), zda je kabel samonosný, zda izolace kabelu je nehořlavá apod.

4.2 Optické kabely

Na rozhraní dvou prostředí s různým indexem lomu (index lomu $n = \frac{c}{v}$, kde c je rychlost světla ve vakuu a v je rychlost světla v konkrétním prostředí) mění světelný paprsek rychlost a směr, část vstupuje do druhého prostředí a část je odražena zpět. Podle toho, zda index lomu výchozího prostředí je větší nebo menší než index lomu prostředí nového, dochází ke změně směru světelného paprsku od kolmice nebo ke kolmici (obr. 4.5).



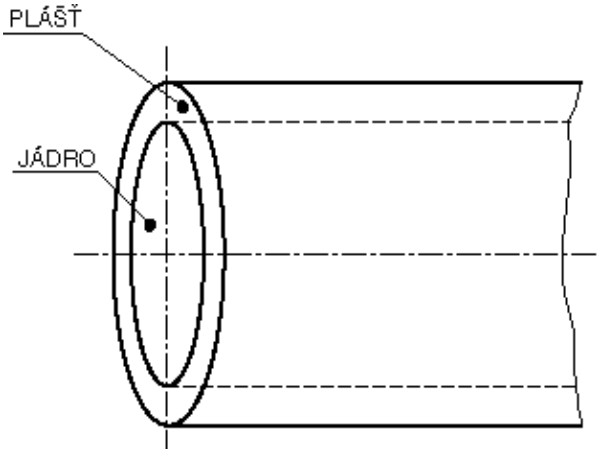
Obr. 4.5: Lom světla ke kolmici (vlevo) a od kolmice (vpravo)

Pro $n_1 > n_2$ je vždy $\alpha_2 > \alpha_1$. Zajímavá je situace, kdy $(\alpha_2 > 90°) \wedge (\alpha_1 < 90°)$. V tomto případě žádné záření nevstupuje do nového prostředí a nastává tzv. **totální odraz** (*total internal refraction*, *TIR*). Mezní hodnota α_1, pro který $\alpha_2 = 90°$, se nazývá kritický úhel α_C.

Platí $tg\,\alpha_C = \frac{n_1}{n_2}$. Na popsaném fyzikálním jevu je založeno vedení světla tzv. světlovodem.

Optické vlákno se obvykle skládá z jádra a pláště, každý z nich je vyroben ze skla s jiným indexem lomu (světelný paprsek se šíří uvnitř jádra, aby došlo k totálnímu odrazu, musí být index lomu jádra větší než index lomu pláště a vstupní úhel – α_A na obr. 4.7 – musí

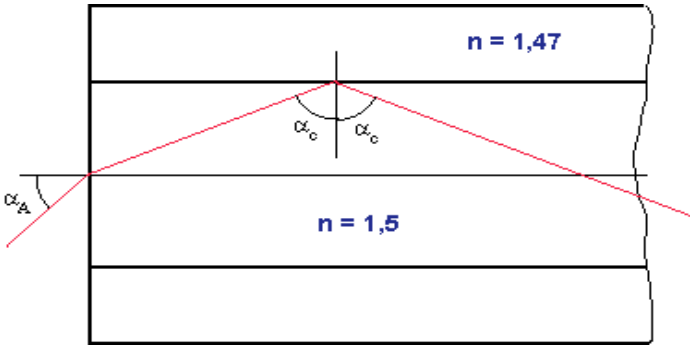
být takový, aby paprsek na rozhraní jádra a pláště dopadal pod větším než kritickým úhlem). Situace je znázorněna na obr. 4.6 a 4.7.



Obr. 4.6: Struktura optického vlákna.

Optická vlákna se označují zlomkem, kde čitatel znamená průměr jádra a jmenovatel průměr pláště, obě hodnotu jsou v mikrometrech (jeden z obvyklých rozměrů vlákna je 62,5/125).

Zájem o světelné přenosy nastal v šedesátých letech 20. století (v souvislosti s objevem laseru). Zpočátku se optická vlákna používala jen pro přenosy na krátké vzdálenosti, ale již v sedmdesátých letech byly vyvinuty technologie výroby velmi čistých skel, současně nastal pokrok v polovodičové technice (zdroje světla, detektory, signálové a číslicové obvody), které umožnily dosáhnout přenosů na vzdálenosti větší. V současné době optická vlákna umožňují běžně přenos signálu na vzdálenost desítek kilometrů bez potřeby opakovačů.



Obr. 4.7: Průchod paprsku optickým vláknem

Optická vlákna nacházejí uplatnění zejména v oblasti telekomunikací, počítačových sítí, kabelových televizí, v uzavřených televizních okruzích, u optických snímačů různých veličin apod. Ke všeobecným výhodám optických kabelů patří zejména:

- menší energetické ztráty při přenosu než u elektrických signálů,
- větší šířka pásma (a v důsledku možnost přenosu více kanálů současně),
- optická vlákna jsou lehčí a tenčí než elektrické vodiče,

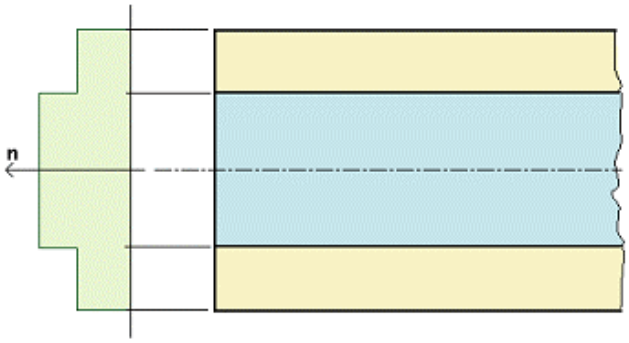
- prakticky absolutní odolnost proti rušení,
- dokonalé galvanické oddělení komunikujících zařízení,
- nemožnost odposlechu,
- možnost bezpečného použití v požárně nebo explozivně nebezpečném prostředí (nevznikají jiskry ani ztrátové teplo, po roztavení izolace nedojde ke zkratu).

Naproti tomu lze u optických vláken hovořit i o určitých nevýhodách (ve srovnání s metalickými kabely):

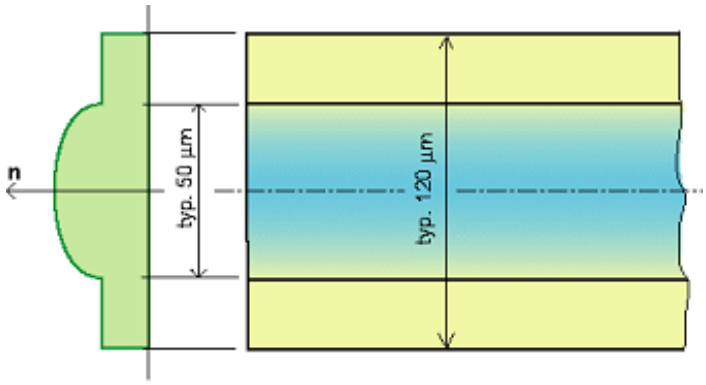
- vyšší cena (ovšem surovina je levná – písek),
- obtížnější montáž, zejména spojování (vyškolené osoby, speciální drahé zařízení a měřící přístroje),
- malá mechanická pevnost (nejsou samonosné, k dosažení samonosnosti je nutné kabely opatřovat speciálními výztuhami – obvykle laminátová nebo kevlarová vlákna).

4.2.1 Druhy optických vláken

Přechod mezi jádrem a pláštěm vlákna může být výrobně realizován různě. Pokud je mezi jádrem (sklo s vyšším indexem lomu) a pláštěm (sklo s nižším indexem lomu) náhlý přechod, hovoří se o vláknech se **skokovou změnou indexu lomu** (*step index fiber*) – obr. 4.8. Je-li přechod mezi dvěma materiály s různým indexem lomu pozvolný, jedná se tzv. **gradientní** vlákna (*graded index fiber*) – obr. 4.9.



Obr. 4.8: Vlákno se skokovou změnou indexu lomu



Obr. 4.9: Gradientní optické vlákno

Optickým vláknem se může šířit jeden nebo více *vidů*. (Vid je druh vlny ve vlnovodu nebo dutinovém rezonátoru, lišící se od jiných rozložením elektromagnetického pole.) Šíří-li se

vláknem pouze jeden vid, hovoří se o vláknech **jednovidových** (*single mode*, *SM*), v opačném případě jde o vlákna **mnohovidová** (*multi mode, MM*). Počet vidů šířících se vláknem

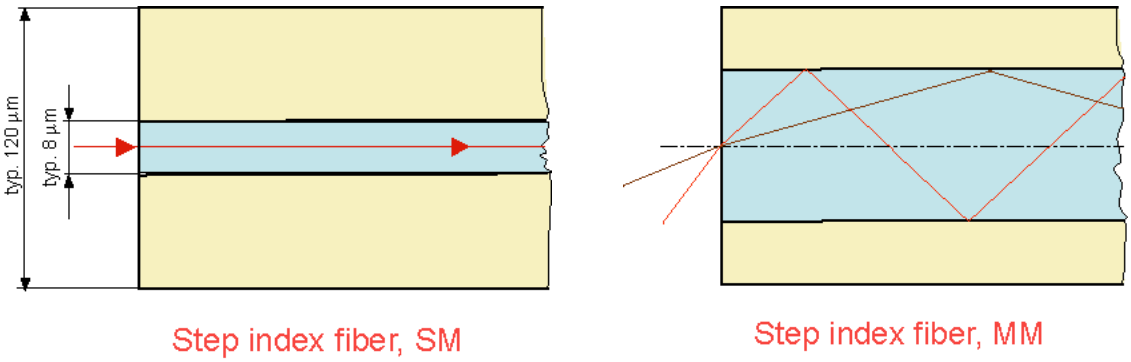
$$N = \begin{cases} \dfrac{V^2}{2} & V \geq 2.405 \\ 1 & V < 2.405 \end{cases}$$

kde V je tzv. *normovaná frekvence*:

$$V = \frac{\pi A d}{\lambda}$$

d je průměr jádra vlákna, λ je vlnová délka a $A = n\sin\alpha$ je numerická apertura. Z uvedených vztahů je zřejmé, že pro daný materiál vlákna a danou vlnovou délku světla bude počet vidů závislý na průměru jádra.

Vlákna se skokovou změnou indexu lomu se vyrábějí jako jednovidová (SM) i jako mnohovidová (MM) – obr. 4.10, vlákna gradientní se používají výhradně jako mnohovidová a zkratka MM se s nimi obvykle nespojuje.



Obr. 4.10: Jednovidová a mnohovidová optická vlákna

U mnohovidových vláken dochází k jevu nazývanému **vidová (modální) disperze**. Příčinou tohoto jevu je různá délka dráhy různých vidů při průchodu vláknem. Důsledkem tohoto jevu je „rozmazání“ obdélníkového pulsu při průchodu vláknem (energie pulsu je nesena všemi vidy, různé vidy ovšem dorazí na konec vlákna v různém okamžiku). Při přenosu několika úzkých izolovaných pulsů následujících za sebou v krátkých časových intervalech může modální disperze způsobit, že na konci vlákna tyto izolované pulsy splynou v jediný dlouhý puls. Vidová disperze se pochopitelně neuplatňuje u jednovidových vláken. Pokud je používáno jiné než monochromatické světlo, uplatňuje se ještě **barevná disperze**.

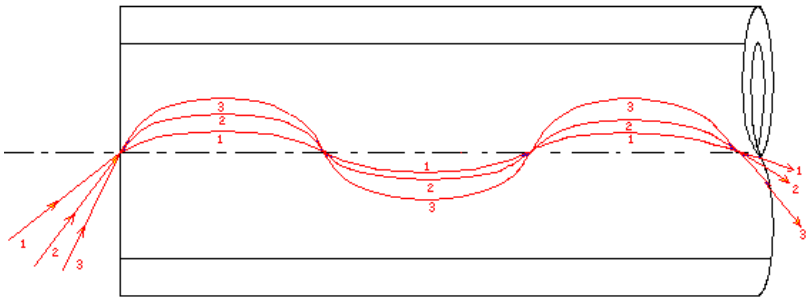
Zajímavou možnost, jak eliminovat negativní vliv vidové disperze, přinášejí gradientní vlákna. Protože index lomu se mezi jádrem a pláštěm mění spojitě, je změna směru jednotlivých vidů v kabelu rovněž spojitá, a dráha jednotlivých vidů tak připomíná sinusoidu (obr. 4.11). Index lomu se zvyšuje směrem k ose vlákna, takže vidy pohybující se blíže k ose mají nižší rychlost šíření, směrem k okraji vlákna naopak rychlost šíření roste. Různá délka dráhy různých vidů je tak do jisté míry kompenzována různou rychlostí šíření, takže vliv vidové disperze je nižší než u MM vláken se skokovou změnou indexu lomu.

V důsledku disperze vykazuje optický přenos jistá omezení, a to:

- omezená šířka pásma (bandwidth),
- omezená vzdálenost (délka optických vláken).

V praxi se používá parametr **B.D.P.** (**bandwidth distance product**), který je součinem maximální frekvence v MHz a délky vlákna v km (jednotkou je MHz km). Typické hodnoty B.D.P. jsou:

- 6 – 25 MHz km u MM vláken,
- 500 – 1500 MHz km u SM vláken,
- 100 – 1000 MHz km u gradientních vláken.



Obr. 4.11: Šíření vidů v gradientním vlákně

Vlastnosti jednotlivých druhů optických vláken lze stručně shrnou do následujících bodů:

- **MM vlákna:**
  - typické použití pro LAN (spíše kratší vzdálenosti),
  - přenos více vidů znamená přenos větší energie (lze připustit větší útlum a snížit nároky na zdroj světla),
  - jako zdroj světla se obvykle používají LED,
  - nižší požadavky na útlum znamenají nižší nároky na čistotu skla (nižší cena),
  - snadnější (tzn. levnější) spojování vláken než SM,
  - nejběžnější vyráběné rozměry 62,5/125 MM nebo 50/125 MM,
  - použití světla s vlnovou délkou obvykle 1300 až 1550 nm.
- **SM vlákna:**
  - typické použití v telekomunikacích (přenosy na velké vzdálenosti),
  - použití světla s vlnovou délkou obvykle 850 až 1300 nm,
  - nedochází k vidové disperzi,
  - jeden přenášený vid znamená nižší přenášenou energii (důsledek: vyšší požadavky na zdroj světla a na čistotu skla – malý útlum),
  - zdroj světla laser (dražší než obyčejná LED),
  - vyšší cena kabelů (vysoká čistota skla kvůli malému útlumu).
- **gradientní vlákna:**
  - do značné míry eliminována vidová disperze,
  - přenáší se více vidů (tzn. obdobné množství energie, jako u MM vláken),
  - levnější než SM vlákna,
  - zdroj světla obvykle laser (lze použít i LED).

5 PLATFORMY LAN

V průběhu vývoje se začala objevovat různá technická řešení pro lokální počítačové sítě. Některá řešení byla úzce spjata pouze s některým výrobcem (firemní řešení). Zpočátku neexistovala žádná standardizace, později se ale některá původně firemní řešení stala podkladem pro vznik standardu vydaného některou normalizační institucí (specifikace firemních řešení se obvykle týkala především kabelů, elektrických parametrů, adresace a formátu rámců, proto touto institucí byla často IEEE). Některá řešení se ukázala být málo perspektivními a jejich doba života byla velmi krátká, jiná v původní nebo mírně pozměněné formě přežívají do dnešních dnů. V tabulce 5.1 je přehled některých vybraných platforem používaných pro LAN.

Platforma	**Arcnet**	**Token Ring**	**Ethernet**	**Fast Ethernet**	**100VG AnyLAN**
Vznik	Datapoint, 1976	IBM, 1985	Xerox 70. léta, DEC, Intel, Xerox – 1980	14.7.1995	HP, AT&T, červen 1995
Norma	–	IEEE 802.5	IEEE 802.3	IEEE 802.3	IEEE 802.12
Přenosová rychlost	2,5 Mb/s	4 Mb/s (16 Mb/s)	10 Mb/s	100 Mb/s	100 Mb/s
Topologie	strom	kruh	sběrnice, páteř, hvězda, strom	hvězda (strom)	hvězda, strom
Přístupová metoda	Token Bus	Token Ring	CSMA/CD	CSMA/CD	DPA
Max. rozlehlost	6500 m	–	2800 m	412 m	4000 m
Max. počet stanic	255	260/kruh	1024		
HW adresa	8 bitů	48 bitů			
Kabely	koax. RG 62 (93 Ω)	IBM (STP 150 Ω)	koax. RG58 (50 Ω), UTP, STP (100 Ω)	UTP, STP (100 Ω)	

Tab. 5.1: Parametry vybraných platforem LAN

V tabulce 5.1 se maximální rozlehlostí myslí vzdálenost dvou nejvzdálenějších stanic v rámci jediné sítě (tzn. sítě, která se z hlediska použití přístupové metody jeví jako jedna síť). Totéž platí pro maximální počet stanic.

HW adresa (hardwarová adresa, MAC adresa) je číslo, kterým se identifikují stanice a které se používá jako adresa při příjmu a vysílání. Je obvyklé, že hodnota hw adresy je vložena přímo výrobcem do síťového adaptéru (karta do počítače umožňující připojit počítač k počítačové síti), a že tuto hodnotu nelze měnit konfigurací. Existují ale zařízení, u kterých změnu provést lze. Výjimkou je Arcnet, kde adresa byla nastavitelná na síťovém adaptéru pomocí přepínačů. Je nezbytně nutné, aby hw adresy všech propojených počítačů byly unikátní, tímto požadavkem je dána značná délka hw adresy u většiny sítí, dokonce je zaručena i unikátnost adres při kombinacích různých platforem (např. Ethernet a Token Ring).

Arcnet byla první běžně používanou platformou pro LAN a při jejím vzniku se s propojováním do rozsáhlejších sítí neuvažovalo. I malý počet bitů hw adresy byl jednou z příčin, proč byly sítě Arcnet postupně nahrazeny jinými platformami (většinou Ethernetem) a to dříve, než došlo k přijetí nějaké normy týkající se Arcnetu (používaná metoda řízení přístupu k médiu – Token Bus – ovšem standardizována je, a sice jako IEEE 802.4).

5.1 Ethernet

Počítačová síť Ethernet vychází z experimentální sítě, kterou vyvinula a již v roce 1975 použila firma Rank Xerox (označení Ethernet je ochranná známka firmy Xerox). Postupem času tato síť dosáhla značného rozšíření, k řešení se připojily další firmy (DEC a Intel) a dodnes se jedná o nejrozšířenější síťovou platformu pro sítě LAN. Zmíněné firemní řešení sítě posloužilo jako základ standardu IEEE 802.3. Původní Ethernet pracoval s přenosovou rychlostí 10 Mb/s, později byla pod názvem Fast Ethernet uvedena na trh varianta umožňující používat rychlost 100 Mb/s, v současné době je standardizován a běžně používán tzv. Gigabit Ethernet pracující s rychlostí 1000Mb/s je přijata i norma pro další rychlejší verzi. Obecně lze říci, že Ethernet představuje vcelku levné a spolehlivé řešení a je podporován celou řadou výrobců. Základní vlastnosti sítě Ethernet jsou do značné míry determinovány použitou metodou přístupu k médiu, kterou je CSMA/CD.

Ethernet ve své originální verzi používal typicky topologii sběrnice příp. páteř, dnes lze v závislosti na použitých kabelech a síťových aktivních prvcích uvažovat o všech topologiích s výjimkou kruhové (tato topologie není slučitelná s přístupovou metodou CSMA/CD).

V této části je popsána pouze nejpomalejší (10 Mb/s) varianta Ethernetu, rychlejší modifikace budou zmíněny v kapitole 10.

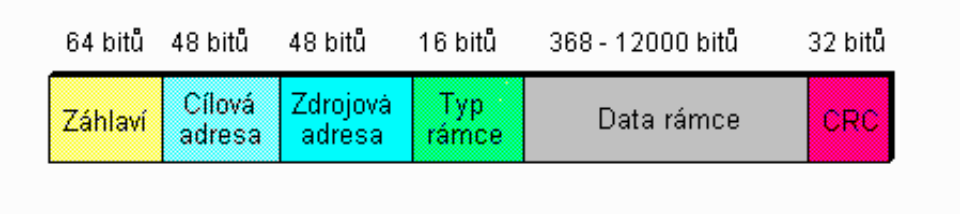
Označení	Typ kabelu	Impedance	Max.	Poznámka
10 BASE-2	koaxiální	50 Ω	185 m 300 m (extended segment)	tzv. tenký (thin) Ethernet, šedý kabel, RG58, topologie sběrnice
10 BASE-5	koaxiální	50 Ω	500 m	tzv. tlustý (thick) Ethernet, žlutý kabel, topologie sběrnice
10 BASE-T	UTP cat. 3,4,5	100 Ω	100 m	dvoubodové spoje, topologie hvězda, strom
10 BASE-F	optické vlákno	–	1000 m	
AUI		–	50 m	

Tab. 5.2: Kabely používané v sítích Ethernet 10 Mb/s

Původně byla síť Ethernet navržena pro použití koaxiálního kabelu. V souladu se standardem je možné používat i kabely UTP a samozřejmě optická vlákna. Kabely pro použití v síti Ethernet mají označení, ve kterých je obsažena přenosová rychlost, pro kterou jsou určeny, následuje slovo BASE (označuje přenos v základním pásmu) nebo BROAD (přenos v rozšířeném pásmu, téměř se nepoužívá) a za pomlčkou následuje specifikace typu kabelu.

5.1.1 Formát rámce

Rámec v síti Ethernet má proměnlivou délku, minimální délka je 64 bytů (512 bitů), maximální 1518 bytů (12144 bitů). Formát rámce je na obr. 5.1.



Obr. 5.1: Formát rámce Ethernet

Význam jednotlivých polí je následující:

- **Záhlaví** (*Preamble*)
  zahájení rámce, synchronizace: 62 bitů série 101010..., dva bity 11
- **Cílová adresa** (*Destination Ethernet Address*)
  adresa příjemce (8 bytů), všeobecná adresa – rámec určený všem: všechny bity 1
- **Zdrojová adresa** (*Source Ethernet Address*)
  adresa odesílatele (8 bytů)
- **Typ rámce** (*Length or Type*)
  pro rámce IEEE 802.3: délka datového pole v bytech
  pro rámce Ethernet II (používáno protokolem TCP/IP): typ paketu (>1500)
- **Data**
  data, minimálně 46 bytů, maximálně 1500 bytů (maximální délka přenášených dat se označuje jako MTU – Maximum Transmission Unit)
- **CRC** (*Cyclic Redundancy Check*)
  Kontrolní posloupnost rámce (Frame Check Sequence), 32 bit CRC vypočítaný dle polynomu 10000010011000001000111010110111 , tj.
  $x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^{8}+x^{7}+x^{5}+x^{4}+x^{2}+x+1$

Cyklická redundantní kontrola (CRC)

Ke *k*-bitovému rámci generuje vysílač *n*-bitovou posloupnost (kontrolní posloupnost rámce **FCS**) tak, aby celých *k*+*n* bitů (FCS se připojí za původní rámec a přenáší se *k*+*n* bitová posloupnost) bylo beze zbytku dělitelných stanoveným číslem (nenulový zbytek je indikace chyby). Generování FCS i kontrola na přijímací straně se obvykle provádí hardwarově.

Následující příklad je z matematického hlediska silně zjednodušený, pro pochopení způsobu výpočtu by ale měl postačovat. Pro snadnější zápis zavedeme označení:

M původní zpráva o délce *k* bitů
P určený dělitel o délce *n*+*1* bitů
R kontrolní posloupnost rámce (FCS), délka *n* bitů
T skutečně vysílaná zpráva (původní zpráva se zabezpečením přidaným na konec), délka *k*+*n* bitů

Na posloupnosti bitů se nahlíží jako na koeficienty polynomu proměnné *x*. Např. pro zprávu $M = 11001001$ bude odpovídající polynom $M(x) = x^7 + x^6 + x^3 + x^0$ a pro stanovený dělitel $P = 1101$ bude polynom $P(x) = x^3 + x^2 + x^0$. Ve všech operacích se používá aritmetika modulo 2 (sčítání i odčítání se provádí jako *xor*, přenos ani výpůjčka neexistuje).

Postup pro generování R je následující: M se vynásobí 2^n (posune se o n bitů doleva), výsledku odpovídá polynom $x^n M(x)$, ten se vydělí polynomem $P(x)$, výsledkem je polynom $Q(x)$ odpovídající bitové posloupnosti Q (podíl je pro další práci nezajímavý) a zbytek $R(x)$ odpovídající *n*-bitové posloupnosti R. Formálně lze operaci zapsat:

$$\frac{x^n M(x)}{P(x)} = Q(x) + \frac{R(x)}{P(x)} .$$

Pro výše uvedené konkrétní hodnoty:

(11001001 · 1000) : 1101 = 10010010, zbytek **010**.

R se použije jako FCS, vysílá se posloupnost $T = 2^n M + R$, pro shora uvedená zadaná data T = 11001001010.

Na přijímací straně se zkontroluje, zda polynom $T(x)$ je beze zbytku dělitelný $P(x)$, nulový zbytek je signálem, že přenos proběhl úspěšně. Platí:

$$\frac{T(x)}{P(x)} = \frac{x^n M(x) + R(x)}{P(x)} = Q(x) + \frac{R(x) + R(x)}{P(x)},$$

$R(x) + R(x) = 0$ (vzhledem k používané aritmetice modulo 2 musí platit $R + R = 0$).

Jak již bylo uvedeno, pro Ethernet je podle IEEE 802 předepsáno používání polynomu: 10000010011000001000111010110111 , tj.

$$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$$

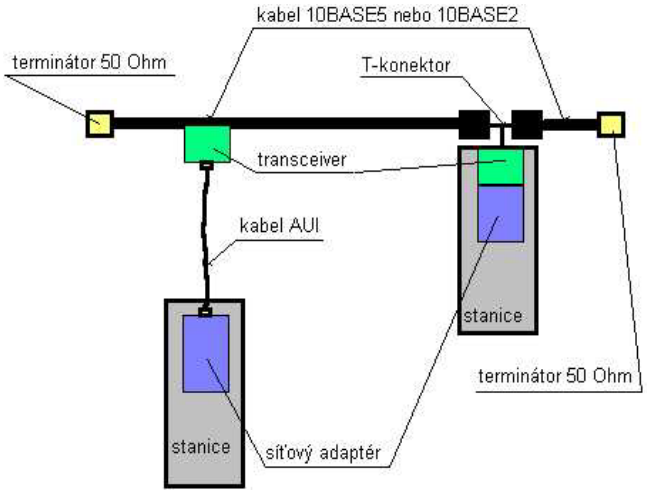
tento polynom generuje FCS o délce 32 bitů. (Pro diskety se dle CCITT používá 10001000000100001, pro magnetické pásky 10001000000000101.) Lze dokázat, že pomocí CRC se detekují:

- všechny jednobitové chyby,
- všechny dvoubitové chyby, pokud má P alespoň 3 členy,
- všechny liché počty chyb, pokud P obsahuje člen x + 1,
- všechny dávkové chyby kratší než délka FCS,
- většina delších dávkových chyb (např. CRC CCITT detekuje 99,997% 17-tibitových chyb a 99,998% 18-tibitových chyb).

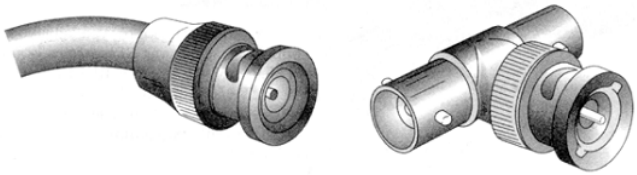
5.1.2 Ethernet s koaxiálním kabelem

Při použití koaxiálního kabelu je základní topologií sítě sběrnice, další možností je páteřová topologie. Pro připojení počítače k síti je nutné počítač opatřit síťovou kartou, která obsahuje síťový adaptér (obvody pro připojení ke sběrnici počítače, vyrovnávací paměť pro uložení přijatého rámce, obvody pro kontrolu CRC) a *transceiver* (slovo vzniklo zkrácením ze dvou slov – *transmitter* a *receiver* – vysílač a přijímač). Konkrétní realizace připojení počítače ke kabelu může mít dvě varianty: buď je transceiver součástí síťové karty (obr. 5.2 vpravo), nebo

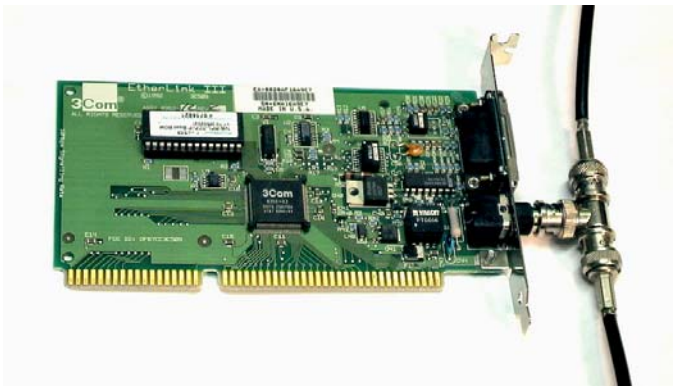
je použit externí transceiver (obr. 5.2 vlevo). V případě použití externího transceiveru je k propojení transceiveru a síťového adaptéru použit transceiverový kabel (tzv. kabel AUI). Řešení s externím transceiverem je obvykle používáno u kabelu 10BASE-5 (tlustý Ethernet), transceiver na síťové kartě se používá pouze pro kabel 10BASE-2 (tenký Ethernet). Připojení kabelu 10BASE-2 k síťové kartě je realizováno pomocí T-spojky BNC (obr. 5.3 vpravo), provedení připojení je patrné z obr. 5.4. Na obou koncích musí být segment koaxiálního kabelu opatřen zakončovacím členem o impedanci 50Ω. Na obr. 5.5 je jedno z možných provedení externího transceiveru a detail konektoru používaného pro koaxiální kabel 10BASE-5.



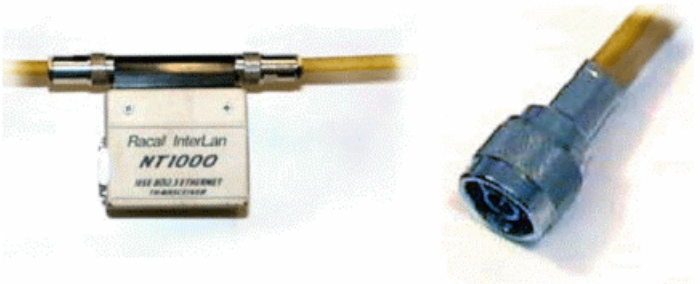
Obr. 5.2: Připojení stanice ke koaxiálnímu kabelu



Obr. 5.3: BNC konektor pro kabel 10BASE-2 a T-spojka (vpravo)

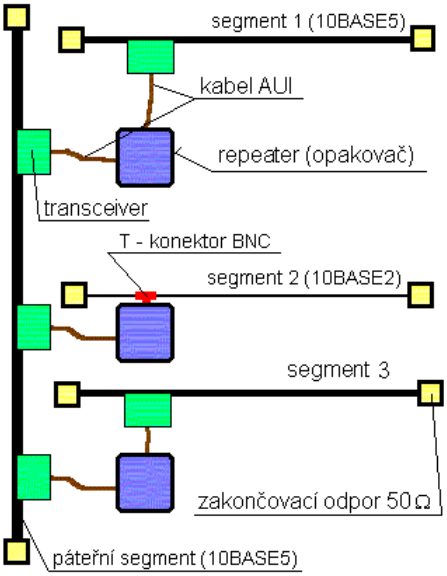


Obr. 5.4: Síťová karta připojená ke koaxiálnímu kabelu 10BASE-2



Obr. 5.5: Externí transceiver a konektor pro kabel 10BASE-5

Maximální délka segmentu koaxiálního kabelu (segmentem se rozumí úsek kabelu od jednoho terminátoru ke druhému) a počet připojených stanic jsou limitovány. Pokud je třeba budovat rozlehlejší síť nebo připojit více stanic, je možné propojit několik segmentů koaxiálního kabelu pomocí prvku zvaného **repeater** – *opakovač*. podobně jako počítače i opakovače se připojují buď přímo ke koaxiálnímu kabelu nebo s využitím externího transceiveru. Opakovač je neinteligentní zařízení, provádí pouze regeneraci (zesílení) signálu a nedokáže např. oddělit lokální provoz na jednotlivých segmentech. Opakovače se vyrábějí i v provedení tzv. víceportových opakovačů, které umožňují propojit více než dva segmenty koaxiálního kabelu. S využitím opakovačů často dochází ke změně topologie sítě na páteřovou (obr. 5.6).



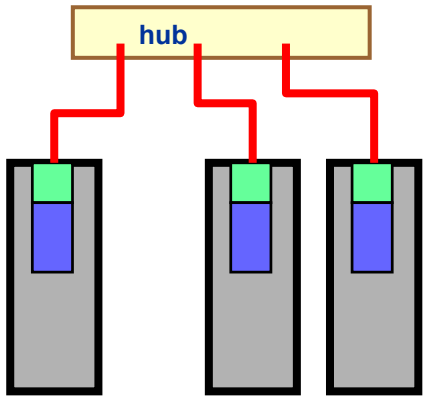
Obr. 5.6: Použití opakovačů

Jak již bylo uvedeno, délka segmentů i počet stanic jsou limitovány. Při použití opakovačů je limitován také počet opakovačů mezi nejvzdálenějšími počítači a tím i celková maximální rozlehlost sítě. Topologická omezení daná normou IEEE 802.3 jsou uvedena v tabulce 5.3.

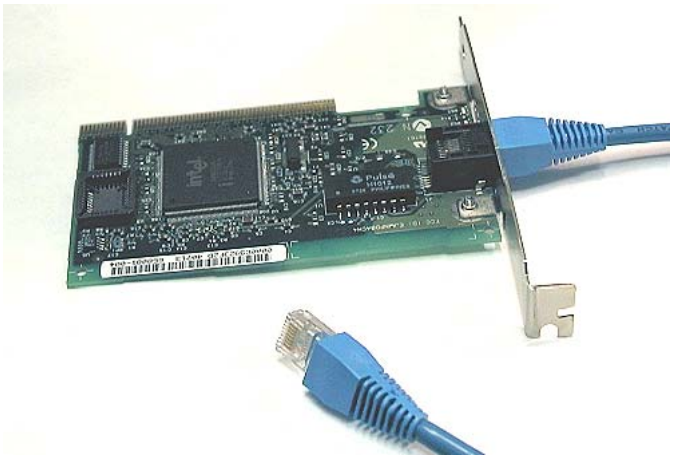
5.1.3 Ethernet s kabelem UTP

Při použití UTP kabelu je základní topologií sítě hvězda. Jako centrální prvek hvězdy je použit **rozbočovač** (nebo také koncentrátor, nejčastější označení je *hub*), který je možno chápat jako mnohoportový opakovač. Propojení počítačů do sítě s využitím hubu je na obr. 5.7.

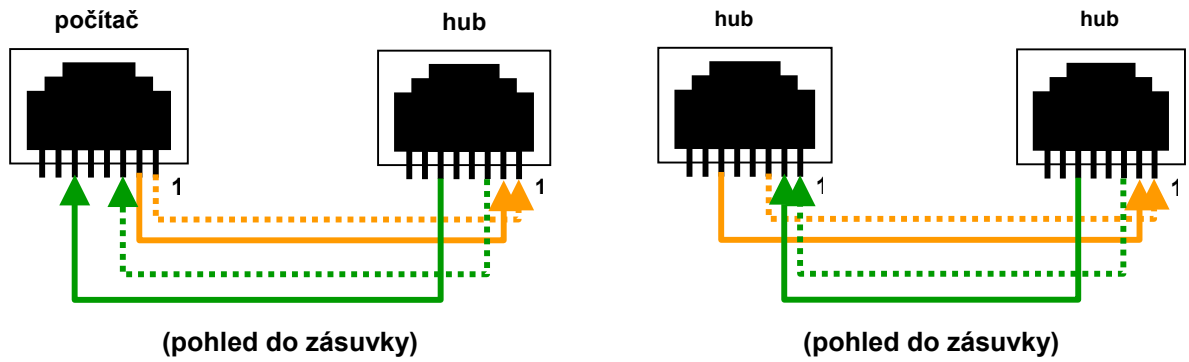
K připojení kabelu k síťové kartě (obr. 5.8) nebo k hubu se požívají konektory RJ-45, provedení kabelu, konektoru a zásuvky RJ-45 je na obr. 4.3 (v kapitole 4). Při použití kabelů UTP se nepoužívají externí transceivery. Protože u UTP kabelu se vždy jedná o dvoubodové spoje, nepoužívají se externí zakončovací odpory a impedanční přizpůsobení je provedeno přímo v propojovaných zařízeních (hub, síťová karta, …).



Obr. 5.7: Propojení počítačů UTP kabelem



Obr. 5.8: Síťová karta s připojeným UTP kabelem



Obr. 5.9: Zapojení přímého (vlevo) a kříženého (vpravo) kabelu

Na rozdíl od použití koaxiálního kabelu, kdy komunikace probíhá výhradně v režimu poloviční duplex, na UTP kabelu může probíhat přenos v režimu poloviční i plný duplex,

neboť pro každý směr přenosu dat je v kabelu k dispozici zvláštní pár vodičů. Pro nejběžnější propojení typu hub – počítač (tedy DCE – DTE) se používá tzv. přímý kabel. Pro propojení DCE – DCE (tedy např. propojení dvou hubů) nebo DTE – DTE (propojení dvou počítačů, používáno velmi zřídka, má-li síť být tvořena pouze dvěma počítači) se používá tzv. křížený kabel. Zapojení obou kabelů je na obr. 5.9.

Stejně jako u koaxiálního kabelu i pro UTP kabely platí topologická omezení, konkrétní hodnoty jsou uvedeny v tabulce 5.3.

5.1.4 Topologická omezení

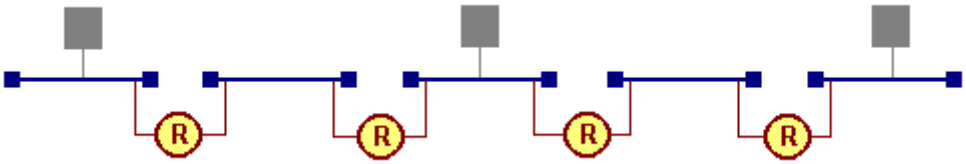
Topologická omezení sítě Ethernet vycházejí ze dvou limitujících faktorů. Prvním je ztráta kvality signálu (útlum, rušení, odrazy při nedostatečném impedančním přizpůsobení – reálné vedení má vlivem konektorů, zakřivení, apod. často impedanci odlišnou od jmenovité impedance kabelu) při jeho šíření reálným kabelem. Tento vliv vede na nutnost omezit maximální délku kabelu (segmentu) a také maximální počet přípojných míst (konektorů) na segmentu (pro koaxiální kabel). Druhým faktorem je doba, za jakou se signál rozšíří mezi nejvzdálenějšími uzly sítě. S ohledem na použitou metodu CSMA/CD je nutné, aby toto zpoždění bylo co nejmenší, aby bylo možné spolehlivě detekovat kolize i pro nejkratší možný rámec. Na zpoždění má vliv nejen konečná rychlost šíření signálu vedením, ale hlavně zpoždění v opakovačích. Proto je limitován maximální počet propojených segmentů. Konkrétní hodnoty omezení při použití jednotlivých typů kabelů je v tabulce 5.3, schématická zobrazení maximálně rozlehlých sítí pro jednotlivé kabely je na obr. 5.10 až 5.13.

Specifikace IEEE 802.3	Max. délka segmentu	Max. počet segmentů mezi uzly	Max. počet opakovačů mezi uzly	Max. rozlehlost sítě	Max. počet uzlů na jednom segmentu	Min. vzdálenost mezi uzly
10BASE-5	500m	5 (z toho 2 link segmenty)	4	2500 m	100	2,5 m
10BASE-2	185 m	5 (z toho 2 link segmenty)	4	925 m	30	0,5 m
10BASE-2 Ext.	300 m	3	2	900 m	100	0,5 m
10BASE-T	100 m	5	4	500 m	2	0,5 m

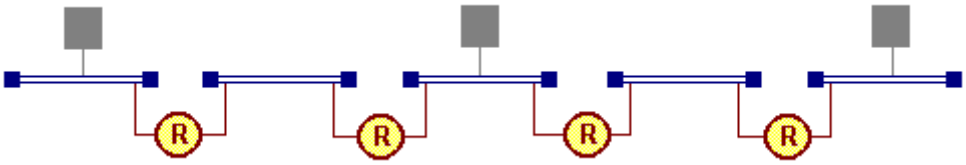
Tab. 5.3: Topologická omezení sítě Ethernet při použití metalických kabelů

Link segment uváděný v tab. 5.3 je segment, na který nesmějí být připojeny žádné uzly. *10BASE-2 ext.* značí použití tzv. rozšířeného (extended) segmentu. V použitém kabelu není rozdíl, ale je nutné, aby všechny prvky (síťové karty, opakovače) připojené na tento segment podporovaly specifikaci rozšířeného segmentu, v případě kombinace klasických a extended zařízení bude celý segment nefunkční (elektrické specifikace jsou odlišné). V tabulce uváděné maximální rozlehlosti nezahrnují délky AUI kabelů, takže při jejich použití a využití jejich

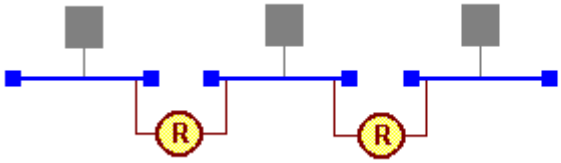
maximální povolené délky může být maximální rozlehlost větší až o 100 m (2 x 50 m) na každý opakovač.



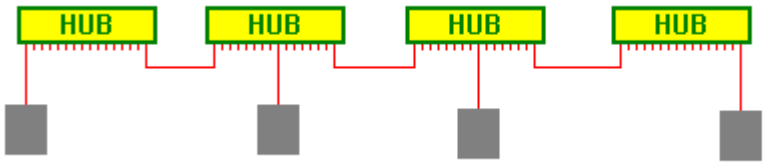
Obr. 5.10: Maximální topologie sítě pro kabel 10BASE-5



Obr. 5.11: Maximální topologie sítě pro kabel 10BASE-2

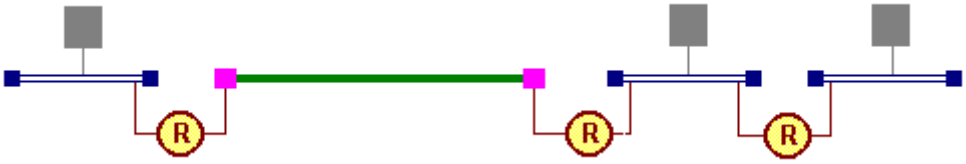


Obr. 5.12: Maximální topologie sítě pro kabel 10BASE-2 ext.



Obr. 5.13: Maximální topologie sítě pro kabel 10BASE-T

V literatuře bývá zvykem uvádět pro maximální rozlehlost sítě Ethernet hodnotu 2800 m. Tato hodnota vychází z konfigurace na obr. 5.14, použit je jeden segment 10BASE-F (o délce 1000 m), tři segmenty 10BASE-5 (každý o délce 500 m), tyto celkem čtyři segmenty jsou propojeny třemi repeatery, každý z nich používá externí transceivery připojené pomocí AUI kabelů maximální přípustné délky (50 m).



Obr. 5.14: Konfigurace sítě Ethernet pro maximální rozlehlost

6 NORMALIZACE POČÍTAČOVÝCH SÍTÍ

Zejména v počátečních dobách převládala v oblasti počítačových sítí firemní řešení. Protože bylo nutno zajistit, aby aplikační software nebyl závislý na konkrétní síti jednoho konkrétního výrobce a aby bylo možné do sítí propojovat různé počítače různých výrobců a používající různé operační systémy, bylo nutné podniknout kroky ke standardizaci sítí. Tato standardizace se samozřejmě musela týkat nejen technického vybavení (kabely, konektory, elektrické signály, kódování), ale také adresování počítačů, formátů předávaných zpráv a v neposlední řadě poskytovaných služeb. V roce 1977 organizace ISO založila samostatný výbor s názvem **OSI** (*Open Systems Interconnections*), jehož práce se zpočátku týkala vývoje modelu komunikační architektury a normalizovaných přenosových kódů. Za rok a půl byl vyvinut a schválen referenční model OSI (obvykle se označuje **ISO/OSI**). Tento referenční model se člení na sedm vrstev, jednotlivé vrstvy jsou číslovány vzestupně zdola nahoru. Každá z vrstev plní svou úlohu tak, že využívá služeb vrstvy nižší a poskytuje svoje služby vrstvě vyšší. Vysílání dat představuje v modelu postup směrem od vyšších vrstev k nižším, příjem naopak od nižších vrstev k vyšším. Struktura modelu a názvy vrstev jsou na obr. 6.1.

<table>
<tr><td>Application</td><td>7. Vrstva aplikační</td><td rowspan="3">uživatelský systém</td></tr>
<tr><td>Presentation</td><td>6. Vrstva prezentační</td></tr>
<tr><td>Session</td><td>5. Vrstva relační</td></tr>
<tr><td>Transport</td><td>4. Vrstva přenosová</td><td rowspan="4">transportní systém</td></tr>
<tr><td>Network</td><td>3. Vrstva síťová</td></tr>
<tr><td>Data Link</td><td>2. Vrstva linková</td></tr>
<tr><td>Physical</td><td>1. Vrstva fyzická</td></tr>
</table>

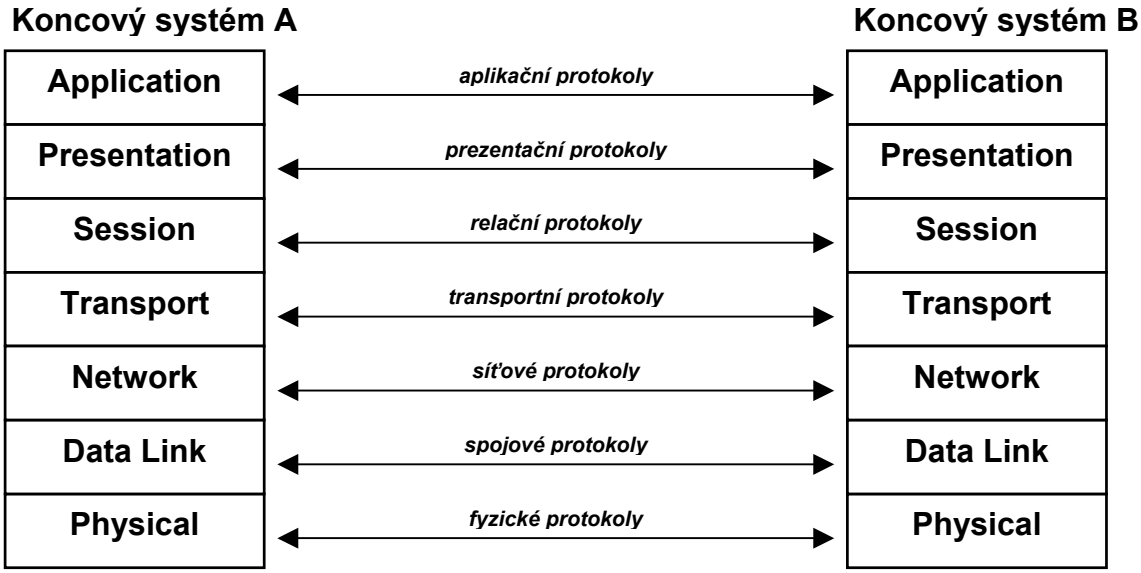
Obr. 6.1: Struktura referenčního modelu ISO/OSI

Komunikaci mezi dvěma procesy ve dvou různých systémech (počítačích připojených do sítě) si lze představit jako komunikaci odpovídajících vrstev modelu ISO/OSI (obr. 6.2). Spolupráci sousedních vrstev si lze představit podle obr. 6.3. Při vysíláni (pohyb shora dolů) vyšší vrstva ($n + 1$) předá vrstvě nižší (n) přes její přístupový bod data. Vrstva n opatří tato data řídící informací pro svůj protějšek v cílovém koncovém systému a takto doplněná data předá jednotce nižší. Tímto způsobem průchod dat pokračuje, až se data dostanou k fyzické vrstvě, která data odvysílá po daném médiu. Příjem probíhá analogicky, data postupují zdola nahoru.

Základní charakteristika jednotlivých vrstev je následující:

- **aplikační vrstva** (*application layer*)
  - Poskytuje aplikačním procesům přístup ke komunikačnímu systému.
  - Komunikace aplikačních procesů se svými protějšky ve stejné vrstvě v jiném systému.

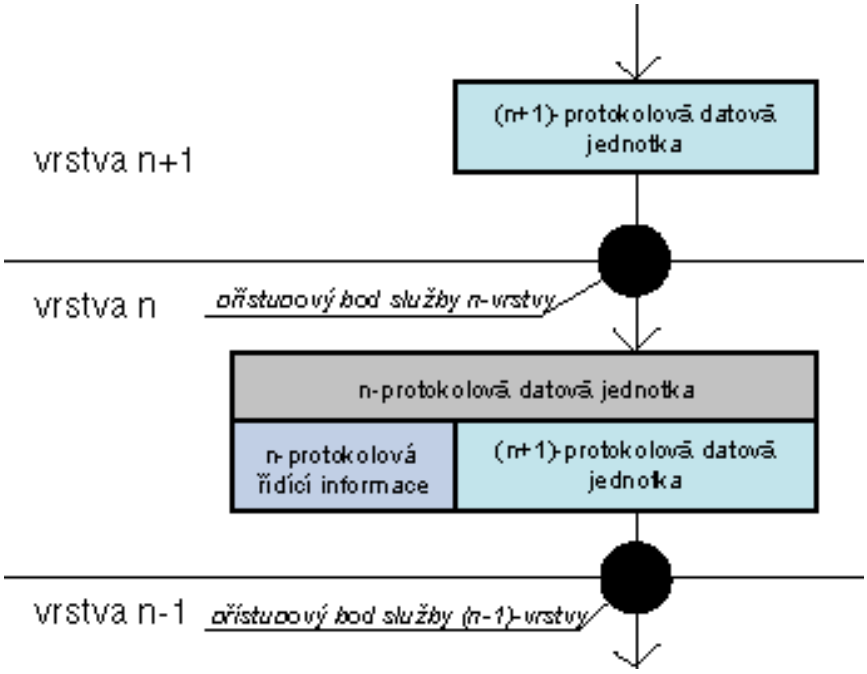
- Vrstva bývá často obcházena (aplikace její služby zajišťují samy), např. u databázových systémů.
- Služby:
  - přenos zpráv,
  - identifikace komunikujících parametrů (jména, adresy, podpisy),
  - zjištění připravenosti komunikujícího partnera,
  - stanovení pověření pro komunikaci,
  - dohoda o mechanismech ochrany zpráv,
  - ověření přípustnosti komunikujících parametrů,
  - tarifikace a kvalita služeb.
- Z konkrétních služeb se jedná zejména o:
  - VT (*virtual terminal*),
  - JTM (*job transfer and manipulation*),
  - DS (*directory services*),
  - FTAM (*file transfer and manipulation*),
  - MHS (*message handling system*).



Obr. 6.2: Komunikace v modelu ISO/OSI

- **prezentační vrstva** (*presentation layer*)
  - přenášené zprávy prezentovat aplikaci jednotným způsobem bez ohledu na jejich různorodost
  - 3 syntaktické verze dat:
    - použitá vysílající aplikační entitou
    - použitá přijímací aplikační entitou
    - přenosová syntaxe
  - vytvoření neutrální formy dat
  - transformace syntaxe (převod kódů a abeced, modifikace grafického uspořádání dat, adaptace operací s datovými strukturami) a výběr syntaxe

- transformace probíhá uvnitř systémů, pro jiné systémy je neviditelná a nemá vliv na normalizaci prezentačních protokolů
- žádost o vytvoření a zrušení relace, přenos dat, dohoda o syntaxi, formátování a příp. komprese dat
- OSI nedefinuje přenosovou syntaxi (dohoda komunikujících entit)
- sémantika zpráv je známá jen aplikační vrstvě
- služby *remote job entry*, *terminal emulation* apod.



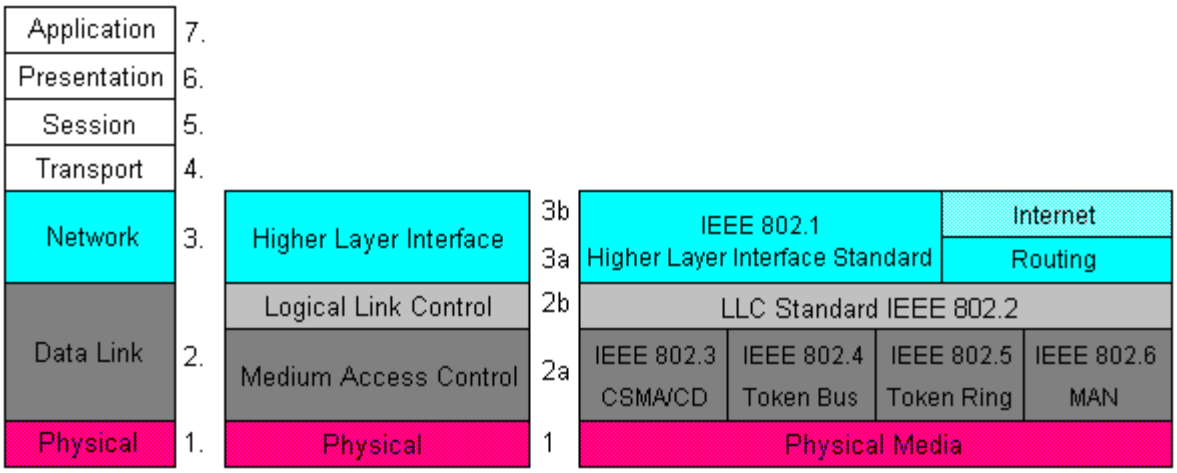
Obr. 6.3: Vztah mezi sousedními vrstvami referenčního modelu ISO / OSI

- **relační vrstva** (*session layer*)
  - zabezpečení nepřetržitosti komunikace i při přechodném výpadku komunikačního systému
  - logičtí uživatelé (tj. komunikace schopné uzly vyšších vrstev) mohou současně komunikovat přes větší počet spojení zajišťovaných transportní vrstvou
  - formy komunikace – plný duplex, poloviční duplex, simplex
- **transportní (přenosová) vrstva** (*transport layer*)
  - transportní adresy
  - zobrazení transportních adres na síťové
  - příprava zpráv pro rozdělení na pakety a naopak
- **síťová vrstva** (*network layer*)
  - realizace logické cesty od uzlu k uzlu pro nesousedící systémy
  - paketizace a depaketizace
  - řízení cesty (routing), směrování a zprostředkování cesty přes mezilehlé systémy
  - síťové adresování

- síťová služba se spojením (spolehlivá, reliable) nebo bez spojení (unreliable, datagramová)
- multiplexování síťových spojení na telekomunikační okruhy

- **linková vrstva** (*data link layer*)
  - 2 podvrstvy:
    - *Logical Link Control* (LLC) - logický spoj nezávislý na topologii
    - *Medium Access Control* (MAC) - přístup k médiím, závisí na topologii, **hardwarová adresa**
  - detekce a korekce chyb při přenosu, synchronizace
- **fyzická vrstva** (*physical layer*)
  - přenos bitů po vedení
  - mechanická (konektory) a elektrická specifikace

Souběžně s ISO/OSI probíhala normalizace jednotlivých vznikajících síťových standardů i po jiných liniích. Jednou z nich jsou normy IEEE. Vzhledem k zaměření IEEE se tyto specifikace týkají zejména nižších vrstev (konkrétně vrstev 1 – 3 dle ISO/OSI), tedy elektrických parametrů, kódování, metod přístupu k médiu, adresace apod. Vztah ISO/OSI a standardů IEEE je zachycen na obr. 6.4.



Obr. 6.4: Souvislost modelu ISO/OSI a standardů IEEE

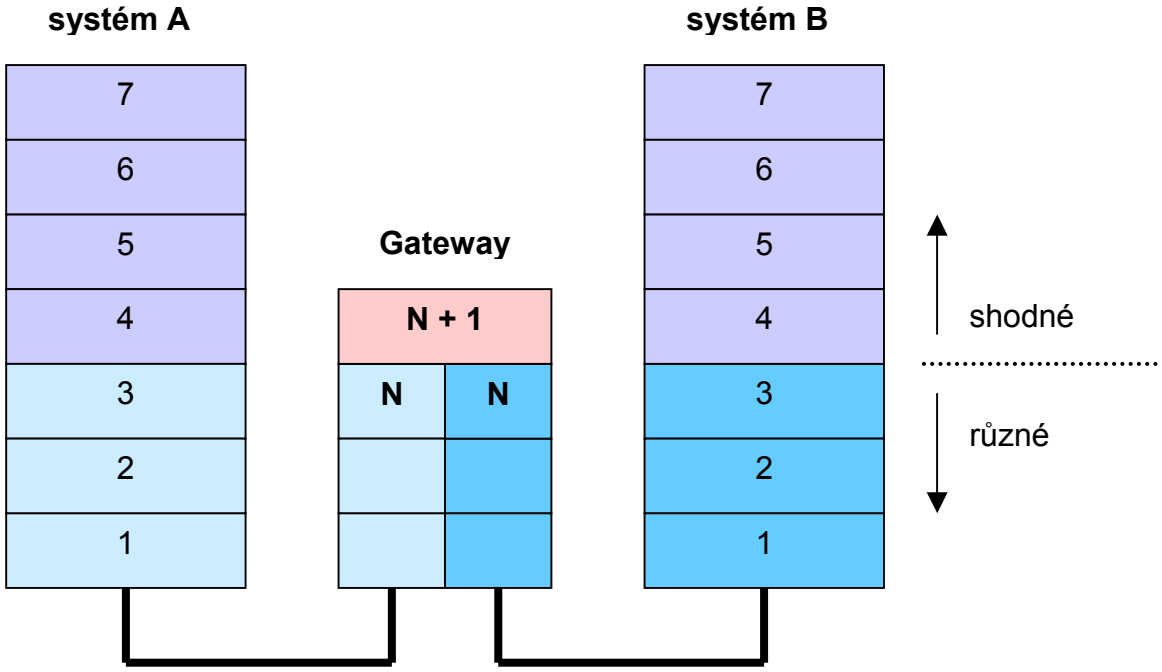
Další standard, který vznikal na ISO/OSI zcela nezávisle, představuje rodina protokolů TCP/IP, která bude popsána v kapitole 8.

7 PROPOJOVÁNÍ POČÍTAČOVÝCH SÍTÍ

Důvodů k propojování sítí je mnoho. Rozsáhlé počítačové sítě bývají obvykle řešeny jako mnoho vzájemně propojených sítí LAN, případně může existovat rozsáhlá infrastruktura (např. veřejná datová síť), ke které jsou jednotlivé LAN připojeny. Obecně se může při propojování jednat zejména o řešení následujících úloh:

- propojení dvou místně se dotýkajících LAN (stejného nebo různého typu)
- propojení dvou místně vzdálených LAN (stejného nebo různého typu)
  - pomocí pevného vedení
  - pomocí veřejné datové sítě
- připojení LAN k veřejné datové síti
- připojení LAN k velkému počítači nebo k síti velkých počítačů
- kombinace předchozích

Vzhledem k rozmanitosti úloh je zřejmé, že propojování sítí bude vyžadovat rozmanité prostředky, pomocí kterých se propojení realizuje. Obecně se propojovací prvek označuje názvem **brána** (*gateway*). Situaci při propojení dvou systémů pomocí brány v modelu ISO/OSI znázorňuje obr. 7.1. Je zřejmé, že minimálně na úrovni aplikace musí dojít k předání dat, tzn. že komunikující aplikace musejí rozumět předávaným datům. Směrem k nižším vrstvám se mohou systémy lišit, např. každý systém může být zapojen v síti jiného typu (Ethernet, Token Ring apod.). Odlišnosti těchto nižších vrstev musí vyřešit brána. Je vhodné, aby brána zpracovávala data odlišným způsobem pouze na vrstvách, které se skutečně liší, a data mezi systémy předala v nejnižší možné vrstvě, která již má shodné vlastnosti pro oba systémy.



Obr. 7.1: Propojení dvou systémů v modelu ISO/OSI

Pokud se nejvyšší různá vrstva označí jako vrstva *N*, pak předání dat se může odehrát nejníže ve vrstvě *N+1*, brána předávající data ve vrstvě N+1 se označuje jako brána úrovně *N*. Pro některé úrovně existují zavedené názvy:

- gateway úrovně 1: **repeater** (*opakovač*)
- gateway úrovně 2: **bridge** (*most*)
- gateway úrovně 3: **router** (*směrovač*), v protokolu TCP/IP se zde poněkud nešťastně v angličtině obvykle používá slovo *gateway*

7.1 Bridge

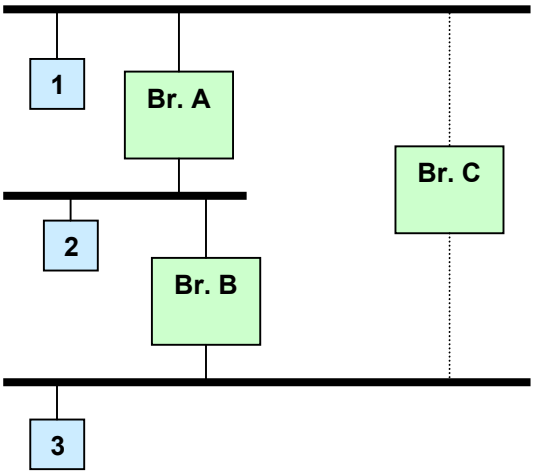
Bridge je prvek, který je určen ke spojení dvou LAN, které na vrstvě 3 a výše používají shodný (ale přitom libovolný) protokol. Často se jedná o dvě shodné sítě – pak je důvodem použití bridge překonání omezení daných fyzickou vrstvou (topologická omezení – počet stanic, vzdálenost) nebo potřeba oddělit lokální provoz na obou sítích. Bridge musí reagovat na všechny rámce v obou propojených sítích a podle jejich určení je buď předá nebo nikoliv do druhé sítě. Řízení přístupu k médiu je v obou sítích odděleno, takže bridge musí být schopen rozpoznat signály jako jam, token apod., a tyto signály pochopitelně nebude předávat do druhé sítě. Bridge je schopen pracovat s daty druhé vrstvy, v této vrstvě existuje pouze fyzická adresace, bridge se tedy řídí výhradně podle hardwarových (tzv. MAC) adres. Vyšší vrstvy obou propojených sítí o přítomnosti bridge neví (ani to nepotřebují), takže síť není nutné pro použití bridge nijak konfigurovat (konfigurovat se pro svoji základní funkci nemusí ani samotný bridge, může být ovšem vybaven doplňkovými funkcemi, které konfiguraci vyžadují).

Bridge není adresovatelné zařízení, takže jeho síťová rozhraní nemusejí mít přidělenu MAC adresu. Bridge ke svému provozu potřebuje informaci, které počítače (resp. které MAC adresy) se nacházejí v připojených sítích. Tuto tabulku si bridge vytváří sám za provozu. Bridge přijímá každý rámec. Podle cílové adresy rozhodne, zda rámec předá do druhé sítě či nikoliv. Bridge rámec nepředá v případě, kdy si je jist, že předání není třeba (adresát leží ve stejné síti, ze které rámec přišel), ve všech ostatních případech rámec předá. Vždy při příjmu rámce si bridge aktualizuje svoji tabulku – MAC adresu odesílatele doplní do seznamu MAC adres ve zdrojové síti. Tímto mechanismem je zaručeno, že síť bude pracovat správně okamžitě po zapnutí bridge, dokud se ale bridge "nenaučí" seznam počítačů v každé připojené síti, bude docházet ke zbytečnému předávání rámců do druhé sítě i v případě, kdy to není nutné.

Topologická omezení sítí se týkají první a druhé vrstvy (délka kabelů, počty opakovačů, počet stanic apod.). Bridge tedy představuje účinný prostředek k překonání topologických omezení, v tomto případě jsou propojené sítě shodné (a neliší se ani na první ani na druhé vrstvě). Podobně lze bridge použít v případech, kdy je potřeba rozdělit síť na dvě nebo více síti menších (např. v přetížených sítích, ve kterých dochází k mnoha častým kolizím). V tomto případě lze ale dosáhnout úspěchu pouze v situacích, kdy charakter provozu je pro toto řešení vhodný. Typicky nevhodný je případ sítě s mnoha stanicemi a jedním serverem, kde

všechny stanice komunikují se serverem a nikoliv spolu navzájem – potom provoz v síti, ve které je zapojen server, pochopitelně nelze použitím bridge snížit.

Zvláštní zmínku vyžaduje použití bridge v sítích s nejednoznačnou topologií (obr. 7.2). Při datových přenosech ze stanice na stanici nečiní taková topologie potíže – cílová stanice sice každý rámec obdrží vícekrát, ovšem protokoly vyšších vrstev se s touto situací dokážou úspěšně vyrovnat. Problém nastává u rámců s všeobecnou adresou (určenou všem stanicím). V tomto případě vznikne nekonečný cyklus, a tento rámec bude v mnoha exemplářích donekonečna putovat sítí až do jejího úplného zahlcení. Možné řešení je dvojí. Buď nepoužívat redundantní topologii (z důvodu zálohování linek a spolehlivosti je to ale někdy nutné). Druhá možnost představuje variantu, že bridge nejsou všechny aktivní, ale některé z nich jsou pouze v pohotovostním stavu a aktivními se stanou až v okamžiku výpadku komunikace.



Obr. 7.2: Bridge v síti s nejednoznačnou topologií

Má-li být bridge použit k propojení sítí lišících se na druhé vrstvě, je nutné, aby obě sítě používaly shodnou délku MAC adresy (a také aby byla zaručena unikátnost adres). Bridge se nejčastěji vyrábí v provedení Ethernet – Ethernet nebo Token Ring – Token Ring, méně často v provedení Ethernet – Token Ring (Ethernet i Token Ring používají shodně MAC adresu délky 48 bitů a unikátnost adres je zaručena).

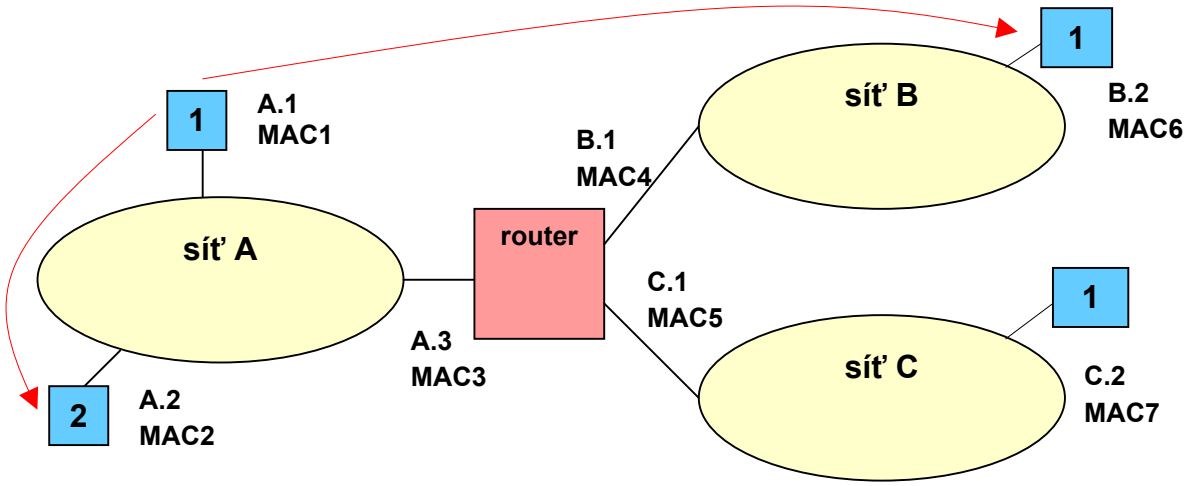
Omezením použití bridgů je jejich velké zatížení, neboť musejí reagovat na všechny rámce (nejsou adresovatelné). Ve velmi rozsáhlých sítích potom použití bridgů není možné, neboť jejich tabulky by narůstaly nad všechny rozumné meze (proto nelze bridge použít jako základní komunikační prvek např. v síti Internet, tuto roli plní routery).

Bridge by bylo možné realizovat i počítačem se dvěma síťovými kartami a vybaveným vhodným programovým vybavením, není to však obvyklé, a vzhledem k silnému zatížení bridge by to ani nebylo efektivní řešení.

Existují také víceportové bridge, které umožňují propojit více než dvě sítě, pro tato zařízení se někdy používá označení *b-router*.

7.2 Router

Router pracuje na třetí vrstvě, z hlediska datových jednotek tedy zpracovává data na úrovni paketů. Používá metodu *store and forward* (přijme rámec, zpracuje a odešle). Základní myšlenka spočívá v použití jiné adresace, než jakou nabízejí MAC adresy. MAC adresa totiž neumožňuje nijak jednoduše indikovat příslušnost počítače ke konkrétní síti. Adresace třetí vrstvy zavádí adresy sítí jako celků a adresy počítačů v rámci dané sítě. Princip činnosti routeru znázorňuje obrázek 7.3.



Obr 7.3: Princip činnosti routeru

Na obrázku 7.3 jsou tři sítě se symbolickými adresami sítí A, B a C. V rámci sítě má každý počítač svoji adresu, tato adresa musí být unikátní v rámci jedné sítě, ovšem nikoliv v rámci všech propojených sítí, úplná adresa počítače (přesněji adresa síťového rozhraní počítače, každý počítač jich může mít více) se potom skládá z adresy sítě a z adresy počítače v dané síti (v obr. 7.3 jsou počítače A.1, A.2, B.2, C.2). Router má úplnou síťovou adresu přidělenu pro každé síťové rozhraní. Každé síťové rozhraní má samozřejmě také hardwarovou adresu (na obrázku MAC1 až MAC7). Při každém vysílání vyplní odesílatel úplnou síťovou adresu příjemce (do záhlaví třetí vrstvy, tedy do hlavičky paketu). Pokud příjemce leží ve stejné síti jako odesílatel, vyplní v hlavičce rámce MAC adresu příjemce a rámec odešle, router se komunikace neúčastní (např. při komunikaci mezi počítači A.1 a A.2). Pokud příjemce leží v jiné síti než odesílatel, vyplní odesílatel do hlavičky rámce MAC adresu routeru a ten zprostředkuje předání. Komunikace mezi počítačem A.1 a B.2 proběhne tedy tak, že A.1 odešle paket adresovaný na B.2 v rámci uvede jako adresu příjemce MAC3 (rozhraní A.3 routeru), router zjistí, že síť B je k němu přímo připojená, změní v hlavičce rámce adresu příjemce na MAC6 a rámec odešle do sítě B (přes rozhraní B.1 – MAC4).

Z popsaného principu jsou patrné některé výhodné a naopak i nevýhodné vlastnosti routeru oproti bridgi. K výhodným vlastnostem patří:

- Router nemusí reagovat na všechny rámce (jako bridge), ale pouze na rámce které jsou mu adresovány (je adresovatelný). Tím je dáno menší zatížení routeru.
- Router pracuje s adresami sítí a MAC adresy počítačů musí znát pouze pro přímo připojené sítě. Tím dochází ke značné redukci tabulek (router používá tzv. *směrovací tabulku*) oproti bridgi, a router je možné použít jako propojovací prvek pro velmi rozsáhlé sítě (např. Internet).
- Protokoly třetí vrstvy mohou obsahovat algoritmy pro paralelní cesty, takže routerům nečiní potíže pracovat v sítích s nejednoznačnou topologií.
- Vzhledem k menšímu zatížení může být (a často bývá) router realizován jako běžný počítač s několika síťovými kartami.
- Pomocí routerů lze propojovat sítě, které se na druhé vrstvě liší délkou hardwarové adresy.

Jako relativně nevýhodné vlastnosti lze uvést:

- O přítomnosti routeru (na rozdíl od bridge) musí odesílatel vědět, pro komunikaci prostřednictvím routeru tedy musí být každá stanice nakonfigurována (je třeba jí přidělit síťovou adresu a sdělit jí adresu routeru) a nakonfigurován musí být i samotný router.
- Router je závislý na protokolu použitém třetí vrstvou, nemůže tedy existovat např. univerzální router pro Ethernet. (Činnost routeru je realizována softwarově, takže pro směrování více protokolů může být použit fyzicky jeden počítač s více směrovacími programy.)

Činnost routeru se označuje jako směrování (routování) a jeho podstatou je zjištění cesty mezi dvěma komunikujícími jednotkami (a v případě nejednoznačné topologie také výběr nejlepší z nich). Hovoří se o směrování **přímém** (mezi dvěma počítači na jedné síti – bez účasti routeru) a **nepřímém** (mezi dvěma počítači v různých sítích, odesílatel musí znát adresu routeru – alespoň jednoho).

Ke zjišťování cest používají routery data uložená ve směrovací tabulce (záznamy o dostupných sítích, cestách k nim a ohodnocení cest). Z hlediska způsobu vytvoření směrovací tabulky může směrování být :

- **statické –** pevně ručně zadané cesty (výhodou je bezpečnost, snížení zátěže pro nejednoznačné případy, pro případy obecné a pro velké sítě nelze reálně použít),
- **dynamické –** optimální cestu vyhledá router podle daného algoritmu s využitím ohodnocení cesty.

Cesty v síti bývají ohodnoceny pomocí tzv. **metriky**. Metrikou může být jakákoliv veličina, která vyjadřuje míru vhodnosti použití dané cesty. Často se používá např. počet směrovačů na cestě, propustnost cesty (bit/s), spolehlivost cesty (pravděpodobnost doručení na základě zkušeností s touto cestou), zpoždění, zátěž, délka podporované MTU, cena za přenos a samozřejmě také libovolná kombinace uvedených veličin.

Protokoly třetí vrstvy se z hlediska svého vztahu ke směrování dělí na:

- **směrovatelné protokoly** – protokoly, které lze směrovat, např. OSI, TCP/IP, DECNet, AppleTalk, XNS, Novell, Banyan Vines),
- **nesměrovatelné protokoly** – protokoly, které z principu nelze směrovat (nepoužívají adresu sítě), např. SNA, LAT, NetBIOS,
- **směrovací protokoly** – protokoly používané k zajištění směrování (výměně informací mezi routery).

Ve velmi rozsáhlých sítích (např. Internet) se používá tzv. **směrování s částečnou informací** (s ohledem na rozumnou velikost směrovacích tabulek není možné ani účelné, aby každý router znal všechny sítě). Síť je logicky rozdělena na **základní páteřní síť** (*core backbone network*), ve které jsou umístěny tzv. *core gateways*, a k ní jsou připojené **autonomní systémy** (*autonomous systems, AS*, dle ISO se používá pojem *administrativní doména*). Autonomní systém je skupina sítí a routerů řízených jednou administrativní autoritou, vše mimo AS je směrováno na implicitní cestu (páteř). Autonomní systém je identifikován číslem (v Internetu 16 bitů, přidělováno centrálně – podobně jako IP adresy, viz. kap. 8) jednou z následujících institucí: ARIN (*American Registry for Internet Numbers*), RIPE (*Réseau IP Européenne*), APNIC (*Asia Pacific Network Information Centre*). Směrovací protokoly se dělí na **vnitřní** (uvnitř AS) a **vnější** (propojují autonomní systémy). Problematika směrování je ve vztahu ke konkrétní síti velmi obsáhlá a složitá, další text se bude věnovat zejména vnitřním směrovacím protokolům.

7.2.1 Routovací algoritmy

Routovací (směrovací) algoritmy slouží ke zjištění nejvýhodnější cesty mezi dvěma sítěmi propojenými routery. Pro vnitřní směrovací protokoly se používají dva základní algoritmy:

- **DVA** – algoritmus vektorů vzdáleností, *Distance Vector Algorithm*
- **LSA** – algoritmus stavu spojů (linek), *Link State Algorithm*

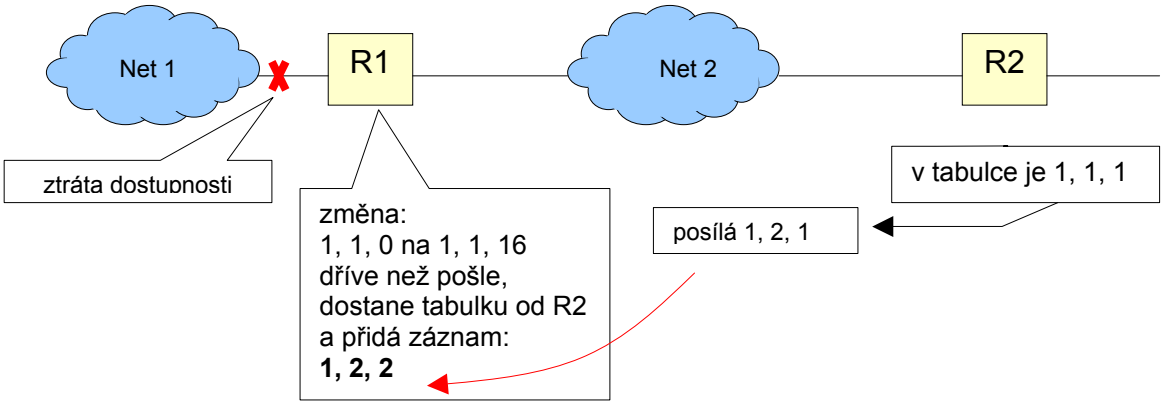
Algoritmus DVA

Tento algoritmus (zvaný též Ford-Fulkersonův nebo Bellman-Fordův) byl použit již v síti ARPANET v roce 1969, jeho implementaci obsahují protokoly RIP, RIP2 nebo IGRP. Jeho podstatu lze shrnout do následujících bodů:

- routovací tabulka je složena z uspořádaných trojic (N, R, D) – síť, router, metrika,
- metrika je vzdálenost sítí udávaná v počtu routerů na trase (přímo připojená síť má $D = 0$),
- na začátku jsou v tabulce pouze přímo připojené sítě s $D = 0$,
- router periodicky posílá celou tabulku sousedním routerům (jako R nastaví sebe)
- v každé přijaté položce se inkrementuje D a zjistí se, zda:
    - určuje cestu do nové dosud nedostupné sítě
    - nebo určuje do dané sítě kratší cestu, než je doposud známá
    - pokud ano, zařadí se do tabulky (příp. nahradí dosud známou „horší“ cestu)

- existuje hodnota D_∞ pro nedostupnou síť (nastavuje se při ztrátě dostupnosti sítě), čím je D_∞ menší, tím rychleji síť reaguje na změny topologie, ale tím více je omezen maximální rozsah sítě (a naopak),
- přenáší se celé tabulky, tedy velké množství dat, které představuje velkou zátěž sítě.

Algoritmus DVA je náchylný na vznik směrovacích smyček. Z principu tento algoritmus nedokáže podporovat paralelní cesty (pro každou cílovou síť je v tabulce jeden záznam s „nejlepší“ cestou). Značným problémem je tzv. **problém pomalé konvergence**. Tento problém se projeví v okamžiku ztráty dostupnosti některé sítě. Přímo připojený router situaci zjistí a do svojí tabulky nastaví pro tuto síť $D = D_\infty$, ovšem dříve, než tuto informaci rozešle, je nebezpečí, že dostane tabulky od sousedních routerů. Ty cestu do této sítě inzerují, takže přímo připojený router je svými sousedy přesvědčován (nepravdivě) o dostupnosti dané sítě. Negativním projevem tohoto jevu je, že namísto okamžitého zjištění a signalizace nedostupnosti sítě následuje postupné zvyšování metriky dané cesty až do D_∞. Situaci dokumentuje obr. 7.4. Existuje několik možných řešení tohoto problému: **split horizon** (rozložený horizont) – informace se neposílají tomu routeru, od kterého byly původně získány, **poison reverse update** (otrávená zpětná informace) – k původnímu zdroji se posílá metrika nastavená na D_∞, **trigger update** (spouštěná aktualizace) – tabulky se při změně posílají okamžitě, **hold-down timer** (zadržovací časovač) – po obdržení D_∞ se nějakou dobu ignorují informace o cestě k dané síti.



Obr. 7.4: Problém pomalé konvergence

Algoritmus LSA

Podstatu a hlavní vlastnosti algoritmu LSA lze shrnout do následujících bodů:

- použit později než DVA
- hlavním cílem bylo zajistit rychlou konvergenci (doba od změny do ustálení)
- každý směrovač musí mít informace o topologii celé sítě (síť je považována za graf, uzly jsou sítě, hrany cesty a ohodnocení hran je metrika)
- nepřenášejí se celé tabulky, ale:
    - aktivně se testují stavy všech sousedních směrovačů (periodická výměna krátkých zpráv – zjištění dostupnosti souseda, pravidlo *k* z *n*)

    - periodicky se šíří informace o spojích všem ostatním LSA směrovačům
- po každé změně každý router zjistí nejkratší cesty do všech sítí pomocí Dijkstrova algoritmu
- informace se vysílají prostřednictvím paketu LSP (*Link State Packet*)

K výhodám algoritmu LSA patří zejména:

- výpočet nejkratších cest provádí každý router samostatně (zaručená odolnost proti zacyklení)
- zprávy o stavu spojů obsahují pouze informace o sousedech (malý objem předávaných dat, všechny informace jsou z „první ruky“)
- prakticky okamžitá reakce na změnu topologie
- časová synchronizace (v LSP je informace o čase jeho vyslání)
- možnost autentizace dat (vyloučení záměrného napadení směrovacího protokolu)

7.2.2 Vnitřní směrovací protokoly

K nejdůležitějším vnitřním směrovacím protokolům patří:

- **RIP** (*Routing Information Protocol*)
    - jeden z prvních použitých protokolů (Xerox, 1981, implementován pro UNIX)
    - koncem 80. let de facto norma pro sítě s TCP/IP (RFC1058, RFC1582)
    - pracuje nad UDP (viz kap. 8), port 250
    - algoritmus DVA
    - metrika – počet směrovačů na cestě, $D_\infty = 16$
    - ručně se vytvoří tabulka pro přímo připojené sítě, ostatní automaticky
    - perioda vysílání tabulky: 30 s, pokud nedorazí aktualizovaná informace po dobu 6 period za sebou, prohlásí se cesta za neplatnou (3 min)
    - mechanismy pro řešení pomalé konvergence: split horizon, poison reverse, trigger update
    - omezení:
        - nejdelší možná cesta je 15
        - směrovací smyčky (počítání do nekonečna)
        - fixní metrika bez možnosti zohlednit zpoždění, zátěž, spolehlivost
        - nelze použít paralelní cesty
        - nelze použít IP masky různé délky (viz kap. 8)
- **RIP 2** (specifikován v RFC1722-1724)
    - vylepšený RIP
    - podpora subsíťových masek (pro IP masky různé délky nebo směrování podle adresových prefixů – viz kap. 8)
    - tabulky lze vysílat na skupinovou adresu
    - autentizace směrovacích informací
    - spolupráce s jinými vnitřními i vnějšími směrovacími protokoly
    - výhody (pro RIP a RIP2):
        - otevřený protokol (nezávislý na konkrétním výrobci)

        - jednoduchá implementace
        - velké rozšíření, např. Novell (perioda 60 s, metrika typu zpoždění, podpora paralelních cest se stejnou metrikou pro rozložení zátěže), AppleTalk (pod názvem RTMP – *Routing Table Maintenance Protocol*), metrika je počet skoků, perioda 10 s), Banyan Vines (pod názvem RTP – *Routing Table Protocol*), ...
    - nevýhody (pro RIP a RIP2):
        - nekvalitní metrika
        - pomalá konvergence
        - omezená max. délka cesty (15 skoků)
- **IGRP** (*Interior Gateway Routing Protocol*) (Cisco Systems)
    - vychází z DVA, odstranění nevýhodných vlastností
    - metrika: kombinované kritérium, zahrnuje zpoždění, rychlost (v nejpomalejším úseku cesty k cíli), zatížení, spolehlivost (zatížení a spolehlivost měřeny za provozu), v tabulkách je i počet routerů a MTU, na těch ale metrika nezávisí
    - perioda vysílání tabulek 90 s
    - tvoří autonomní systém, pro cestu do jiných sítí používá implicitní cestu (default route)
    - výhody:
        - kombinovaná metrika
        - možnost rozložení zátěže do paralelních cest
        - nelimitovaná maximální délka
    - nevýhody:
        - firemní protokol vázaný na směrovače Cisco
        - pomalá konvergence v rozsáhlých sítích
- **E-IGRP** (Cisco Systems)
    - snaha učinit IGRP konkurenceschopný s protokoly na základě LSA
    - spojuje výhody DVA a LSA
    - použitelný pro IP, IPX a AppleTalk
    - DUAL (*Diffusing Update Algorithm*): vylučuje vznik směrovacích smyček (výpočtem), okamžitá synchronizace při změně
    - 3 tabulky: sousedů, topologie, směrování
    - výhody:
        - rychlá konvergence i v rozsáhlých sítích
        - kombinovaná metrika (jako IGRP)
        - malá zátěž směrovačů (tzn. i sítě)
        - minimální nároky na plánování intersítě (např. oproti OSPF)
        - podpora VLSM a sumarizace adres
        - integrovaná podpora více protokolů (IP, IPX, AppleTalk)
    - nevýhody:
        - firemní protokol vázaný na směrovače Cisco

- **OSPF** (*Open Shortest Path First*)
  - algoritmus LSA
  - informace se posílají okamžitě po detekci změny, nebo periodicky po 30 min.
  - protokol normalizován IETF (RFC1247, verze 2 RFC2328)
  - metrika: skutečná propustnost (rychlost) spojů
  - podpora směrování podle typu služby (*type of service*) – několik různých cest do cílové sítě pro různé služby
  - rozdělení zátěže (*load splitting*) pro vícenásobné cesty se stejnou metrikou
  - hierarchické směrování – (sítě lze sdružovat do oblastí – area – a okolní routery nemusejí znát topologii oblasti, právě jedna oblast tvoří OSPF backbone, ke které jsou připojeny všechny ostatní oblasti)
  - kontrola autorizace (autentizačním heslem)
  - podpora podsítí s různou subsíťovou maskou (VLSM)
  - může existovat pověřený směrovač (za skupinu routerů vysílá informace o stavu routerům mimo tuto slupinu) – redukce zatížení sítě
  - virtuální spoje (*virtual links*): mezi dvěma směrovači, které nejsou ve stejné oblasti (výměna informací mezi směrovači, které nejsou fyzicky přímo napojeny na OSPF páteř)
  - několik typů směrovačů:
    - vnitřní směrovač – všechna jeho rozhraní v jedné oblasti
    - hraniční směrovač oblasti (ABR – *Area Border Router*)
    - hraniční směrovač autonomního systému (ASBR – *Autonomous System Border Router*)
  - každá oblast používá individuální kopii SPF (topologická databáze všech routerů v oblasti je totožná)
  - hraniční routery mají více databází (pro každou propojovanou oblast jednu)
  - SPF je poměrně náročný algoritmus, proto:
    - nedoporučuje se, aby routery sousedily s více než třemi oblastmi
    - doporučený rozsah oblasti max. 50 až 80 routerů
    - limity jsou podle zkušeností, neexistuje pevný limit jako např. u RIP
  - topologie oblasti (mimo hranice oblasti není známá):
    - dvoubodové sítě (přímá linka mezi routery – automaticky jsou to sousedé)
    - lokální síť propojená s okolím více routery (používá se pověřený router)
    - rozlehlé sítě (složitá topologie, obvykle manuální statická konfigurace vybraných routerů – pro routery se síť redukuje na množinu dvoubodových spojů)
  - výhody:
    - otevřený protokol nezávislý na výrobci
    - rychlá konvergence
    - používání skupinové adresy

        - paralelní cesty
        - směrování podle služby
        - podpora VLSM a CIDRautentizace směrovacích informací
    - nevýhody OSPF:
        - složitý návrh sítě,
        - kvalita směrování je závislá na použité adresaci (doporučuje se, aby oblast sdružovala souvislé rozpětí adres)

8 RODINA PROTOKOLŮ TCP/IP

Zahájení projektů, které ve svém důsledku vedly k vývoji protokolu TCP/IP a ke vzniku sítě Internet, sahá do šedesátých let 20. století. V tomto období naplno probíhala tzv. studená válka a jedním z úkolů, který bylo třeba zvládnout, bylo zajištění komunikace mezi vládními a armádními úřady během a po případné atomové válce. Bylo nutné vyvinout komunikační síť, která by byla schopná činnosti i při vyřazení některých jejích částí a která nemá žádné centrum. V té době se pro všechny datové i hlasové přenosy používalo výhradně přepojování okruhů.

V USA a Velké Británii byl zahájen výzkum paketového přenosu. V roce 1961 přednesl Leonard Kleinrock (z MIT) první referát na téma přepojování paketů s názvem *Information Flow in Large Communication Nets*. V roce 1962 byl zahájen výzkumný projekt v této oblasti, projekt byl financován agenturou DARPA (Defense Advanced Research Project Agency). V roce 1964 vychází první kniha o přepojování paketů, ve stejném roce Paul Baran (RAND Corporation) popisuje principy sítě se směrováním paketů dle požadavků Pentagonu v publikaci *On Distributed Communications Networks*. Do výzkumu byla zapojena i akademická sféra. V roce 1969 byla uvedena do provozu experimentální síť ARPANET, tato síť obsahovala čtyři uzly – UCLA (University of California Los Angeles), SRI (Stanford Research Institute), University of California Santa Barbara a University of Utah.

V roce 1972 byla u příležitosti konference ICCC (International Conference on Computers and Communications) představena síť ARPANET demo. Tato síť obsahovala cca 20 routerů a 50 počítačů a používala protokol **NCP** (*Network Control Protocol*). Protokol NCP byl určen pro experimentování a nebyl vhodný pro rutinní použití. V této síti byl zahájen provoz elektronické pošty. V roce 1973 byly k této síti připojeny první uzly ležící mimo USA (ve Velké Británii a v Norsku). (Pro představu o tehdejších technických prostředcích lze uvést, že ve stejném roce vyvíjí Bob Metcalf – Xerox – síť Ethernet.) V letech 1977 – 1979 probíhal vývoj základní architektury TCP/IP (ve spolupráci Stanford University, BBN – Bolt, Baranek and Newman a University College London), v roce 1980 bylo zahájeno experimentální ověřování TCP/IP v síti ARPANET. Ve stejném roce byl protokol TCP/IP implementován pod operačním systémem BSD UNIX (spolupráce BBN a UCB – University of California Berkeley). V roce 1983 se protokol TCP/IP stal standardem pro síť ARPANET. Ve stejném roce dochází k oddělení sítě MILNET (Military Network) od sítě APANET. Za přispění firmy SUN se TCP/IP úspěšně přenáší i do komerční sféry. V té době model ISO/OSI není ještě dopracován, jako alternativy k TCP/IP mohou ale sloužit firemní řešení – XNS (Xerox), DECNet, SNA (IBM).

V letech 1985/1986 je zahájen program NSFNET (financováno NSF – National Science Foundation) pro rychlé spojení šesti amerických superpočítačových center, do roku 1995 jenom NSF sponzorovala vývoj částkou cca 200 milionů dolarů. V roce 1993 pracovala páteř sítě NSFNET s rychlostí 44,7 Mb/s. Během let byl ukončen provoz sítě ARPANET (v roce 1990), vzniklá infrastruktura je ale samozřejmě provozována dále, a to pod názvem Internet. Ve stejném roce nastal důležitý průlom – na tuto doposud výhradně akademickou síť se dostává i komerční provoz, konkrétně se jednalo o bránu mezi Internet e-mail a MCI mail.

V roce 1995 byl ukončen provoz NSFNET a páteřní síť je v USA provozována komerčně jako síť BNS (Backbone Network Service).

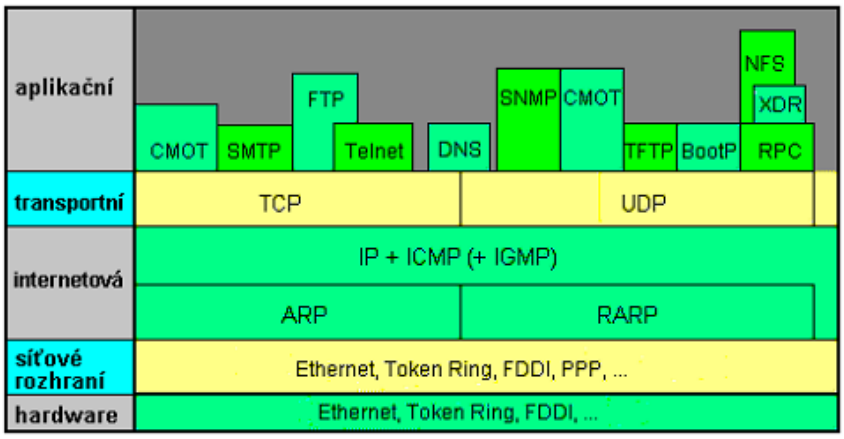
Vývoj samozřejmě pokračoval dále a stále pokračuje, mezi přelomovými daty je třeba uvést ještě alespoň rok 1992, kdy spatřila světlo světa služba www, a rok 1993, kdy byl vytvořen program Mosaic, který byl prvním grafickým www prohlížečem.

Síť Internet je obvykle definována jako informační systém, který:

- je logicky propojen v globálně jedinečném adresním prostoru založeném na protokolu IP a jeho rozšířeních,
- podporuje komunikaci založenou na souboru TCP/IP a jeho rozšířeních,
- poskytuje, používá a zpřístupňuje veřejně nebo soukromě služby založené na této infrastruktuře.

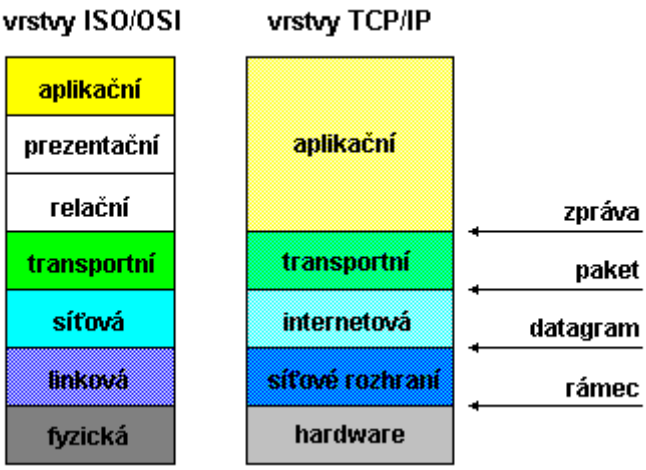
Z uvedených skutečností je patrné, že vývoj TCP/IP a sítě Internet probíhal souběžně a že Internet je s touto rodinou protokolů silně spjat. To se projevuje nejen tím, že se v Internetu protokol TCP/IP používá pro datové přenosy, ale také v tom, že běžně používané aplikace a služby Internetu (e-mail, ftp, www apod.) jsou definovanými protokoly aplikační vrstvy TCP/IP.

Architektura protokolu (často se používá pojem *rodina protokolů*, ve skutečnosti se jedná o mnoho souvisejících a navzájem se využívajících protokolů) TCP/IP je na obr. 8.1. Jak je patrné, protokol se člení do několika vrstev (ovšem členění na vrstvy je zde spíše pomocné a s čísly vrstev se příliš často neoperuje), vztah k modelu ISO/OSI je na obr. 8.2.



Obr. 8.1: Architektura a vzájemná souvislost protokolů rodiny TCP/IP

Během vývoje TCP/IP si doktorandi na UCLA zvykli publikovat své myšlenky, návrhy, názory a představy jako neformální dokumenty „*Request for Comments*" (**RFC**, žádost o komentář). Tato forma dokumentů se v oblasti protokolu TCP/IP a Internetu používají dodnes. RFC se číslují. Platí zásada, že RFC se nikdy nemění, pokud nějaký dokument zastará, je nahrazen novým dokumentem s novým číslem. Seznam a znění všech dokumentů lze nalézt na Internetu např. v umístění *http://www.rfc-editor.org/rfc.html* nebo *http://www.rfc.net/*.



Obr. 8.2: Souvislost TCP/IP a modelu ISO/OSI

8.1 Adresace v protokolu TCP/IP

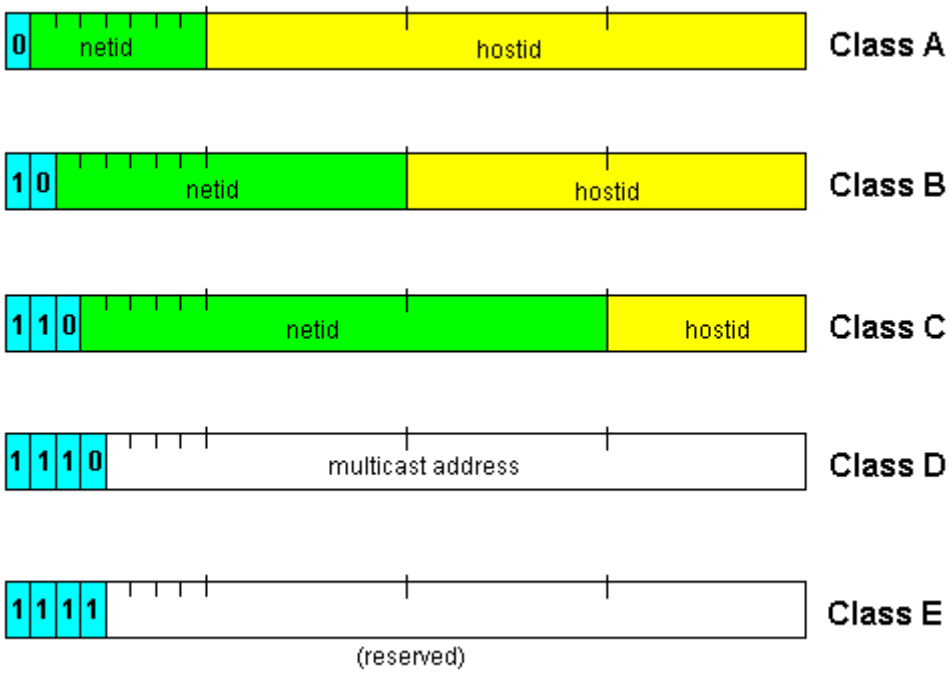
Rodina protokolů TCP/IP používá k adresaci tzv. **IP adresy** (IP je základní přenosový protokol používaný ke všem datovým přenosům všemi ostatními protokoly TCP/IP). IP adresy vycházejí z následujících zásad:

- adresa se vztahuje k síťovému rozhraní, nikoliv k počítači (ten může mít rozhraní více),
- každý uzel musí mít unikátní adresu,
- adresy jsou abstraktní (nejsou nijak předurčeny MAC adresou rozhraní),
- adresy jsou nezávislé na druhu sítě (tedy ani na tvaru a délce MAC adres),
- délka adresy je 32 bitů (zapisují se obvykle v desítkové soustavě po bytech, hodnoty jednotlivých bytů se oddělují tečkou, např. 123.12.56.7),
- struktura adres musí vyhovovat potřebám směrování, adresa se skládá ze dvou částí: **netid** (identifikace sítě) a **hostid** (identifikace uzlu v rámci sítě), router se rozhoduje pouze na základě adresy sítě (*netid*).

Obě části IP adresy (netid i hostid) tvoří souvislé úseky bitů (celkem 32 bitů), hranice mezi nimi může být na různých místech. Standardně bývá tato hranice na hranici bytů, přesná poloha je dána příslušností adresy k tzv. třídě (*address class*). Rozdělení adres do tříd je znázorněno na obr. 8.3. Příslušnost adresy ke třídě je indikována nejvyššími bity adresy (lze ji tedy poznat podle hodnoty z hlediska zápisu prvního bytu adresy). Platná adresa uzlu nesmí obsahovat v části netid ani hostid všechny bity nastavené na hodnoty 0 ani 1, tyto hodnoty jsou určeny pro speciální případy – viz dále.

Třída A je určena pro případy, kdy je málo propojených sítí a v každé síti je velmi mnoho uzlů (počítačů). Hodnoty prvního bytu adresy pro třídu A jsou v rozsahu 1 až 126, adresa třídy A poskytuje prostor pro adresování 126 sítí a v každé z nich 16 777 214 uzlů. Třída B umožňuje adresovat 16 384 sítí a v každé z nich až 65 534 uzlů, odpovídající rozsah hodnot nejvyššího bytu adresy je 128 až 191. Třída C poskytuje prostor pro 2 097 152 sítí

a v každé maximálně 254 uzlů, nejvyšší byte adresy je v rozsahu 192 až 223. Třídy D a E nejsou určeny k běžnému použití.



Obr. 8.3: Rozdělení IP adres do tříd

Jak již bylo uvedeno, některé hodnoty IP adres mají zvláštní význam (obvykle se jedná o adresy, kde jsou netid nebo hostid tvořené hodnotami zapsatelnými ve dvojkové soustavě samými nulami nebo samými jedničkami). K těmto zvláštním případům patří zejména:

hostid = 0, netid nenulový
Adresa celé sítě, nikoliv konkrétního uzlu (např. 147.229.0.0).

netid = 0, hostid nenulový
Adresa uzlu v této síti, komunikace nemůže být zprostředkována routerem (např. 0.0.0.5).

adresa 0.0.0.0
Tento počítač na této síti, používá se v případě, kdy počítač dosud nezná svoji adresu a potřebuje komunikovat po síti, používá se výhradně jako zdrojová adresa.

adresa 255.255.255.255
Limited broadcast (omezená všeobecná adresa), takto adresovaná data budou doručena všem počítačům v síti, ze které byla odeslána, přes routery data neprojdou.

netid obvyklý, hostid tvořen ve dvojkovém zápisu samými jedničkami
Directed broadcast (řízená všeobecná adresa), data budou doručena všem uzlům specifikované sítě (např. 147.229.255.255).

adresa tvaru 127.x.x.x (nejčastěji se objevuje 127.0.0.1)
Software loopback address (sw zpětnovazební adresa), používá se v případě, kdy počítač adresuje sám sebe (probíhá komunikace mezi procesy téhož počítače pomocí protokolu TCP/IP, vše se odehrává běžným způsobem, ovšem neprovádí se žádné vysílání na síť).

8.1.1 Podsíťování (subnetting)

Členění adres do tříd je zdrojem neefektivního zacházení s adresami (např. nevyčerpatelný přebytek stanic pro třídu A a obvykle i B). Mechanismus podsíťování umožňuje část hostid přidat k netid (hostid se rozdělí na adresu podsítě a adresu stanice). Pro adresy podsítí se používá souvislý tok bitů zleva. Prakticky tedy dojde k posunutí hranice mezi netid a hostid oproti původnímu stavu (podle příslušnosti ke třídě) směrem doprava. Pozice této nové hranice se udává pomocí tzv. **masky podsítě** (*subnet mask*). Podsíťová maska je 32 bitová hodnota, která má jedničky na pozicích, které odpovídají adrese sítě nebo podsítě, a nuly na pozicích určujících adresu uzlu. Vzhledem k charakteru sítě a popsanému mechanismu je maska podsítě tvořena zleva souvislým blokem bitů s hodnotou jedna následovanou souvislým blokem bitů s hodnotou nula až do konce masky. Podobně jako IP adresa se subsíťová maska zapisuje po bytech, obvykle v desítkové (někdy v šestnáctkové) soustavě a hodnoty jednotlivých bytů se oddělují tečkou. Router pro úspěšnou práci potřebuje znát nejen adresu uzlu, ale také podsíťovou masku. Vzhledem k možným kolizím s adresami se speciálním významem se doporučuje, aby adresa podsítě nebyla tvořena ve dvojkovém zápisu samými jedničkami nebo samými nulami, z toho důvodu je nevhodné používat posunutí hranice dané třídou pouze o jediný bit. Podsíťování např. umožňuje pracovat s adresou třídy B jako s blokem 254 adres třídy C.

Technika podsíťování je natolik rozšířená, že se masky podsítí uvádějí vždy, i v situacích, kdy je to zbytečné, neboť je respektována hranice daná příslušností adresy ke třídě. V těchto případech masky nabývají tzv. implicitních hodnot, tyto hodnoty jsou 255.0.0.0 pro třídu A, 255.255.0.0 pro třídu B a 255.255.255.0 pro třídu C.

8.1.2 Problém nedostatku IP adres

V době vzniku TCP/IP se předpokládalo, že 32 bitová délka IP adresy vystačí pro všechny případy na velmi dlouhou dobu a že množství adres bude prakticky nevyčerpatelné (32 bitů poskytuje více než čtyři miliardy kombinací). S nástupem osobních počítačů a všeobecným rozšířením sítě Internet se ukázalo, že tento původní předpoklad byl příliš optimistický. S ohledem na strukturu adres a jejich rozdělení do tříd se navíc s adresami zachází poměrně nehospodárně (pro každou sebemenší LAN připojenou k Internetu je nutné přidělit minimálně jednu adresu třídy C). Okamžité řešení přinesla technika podsíťování. Existují i další řešení, všechna jsou ale dočasná, neboť řeší pouze následek, nikoliv příčinu problému.

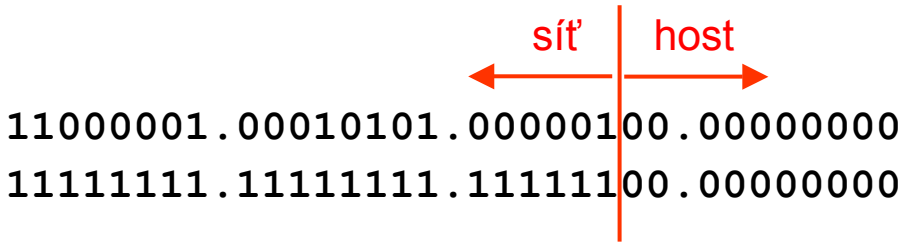
Privátní IP adresy

vycházejí z názoru, že kde nebude existovat přímá komunikace, tam nemusí být unikátní adresy (privátní sítě jsou od zbytku světa odděleny – zařízením firewall – na vyšší vrstvě, než

je síťová). Na hranicích privátních sítí je třeba zastavit šíření směrovacích informací. V privátních sítích lze teoreticky používat libovolné adresy, ale doporučuje se používat adresy k tomu určené (RFC1918). Silně se doporučuje používat tyto adresy i u izolovaných sítí (vůbec nepřipojených k Internetu). Adresy soukromých sítí podle RFC1918 byly původně určeny pro sítě nepřipojené k Internetu, z důvodu nedostatku adres se používají i pro podnikové sítě připojené přes firewall. Doručené adresy jsou: pro třídu A adresa sítě 10.0.0.0, pro třídu B adresy sítě 172.16.0.0 až 172.31.0.0 a pro třídu C adresy sítí 192.168.0.0 až 192.168.255.0.

CIDR (Classless interDomain Routing), RFC 1518 a 1519

Pro tento způsob zacházení s adresami se používá název **prefix routing**. CIDR umožňuje přidělovat koncovým sítím „přesně“ velké skupiny IP adres podle jejich potřeb. Řeší problém nárůstu směrovacích tabulek – síť jednoho providera může obsahovat mnoho adres (jisté třídy, ale směrování je do všech těchto sítí jediné, neboť je to vlastně jedna síť. Někdy se používá pojmu *supernetting* jako protiklad k subnettingu, neboť v podstatě se jedná o způsob, jak posunout hranici mezi netid a hostid směrem doleva. Agregace skupiny adres pro směrování se vyjadřuje počtem bitů prefixu za IP adresou a lomítkem (nebo nadsíťovou maskou). Např. zápis 193.21.4.0/22 (s využitím nadsíťové masky 193.21.4.0 s maskou 255.255.252.0) pokryje rozsah C adres 193.21.4.0 až 193.21.7.0. Hodnota 22 vyjadřuje počet použitých pro směrování. Situace je zachycena na obr. 8.4.



Obr. 8.4: příklad supernettingu

VLSM (Variable Length Subnet Mask), RFC 1812

Původně panoval předpoklad, že subnetting bude dostačující, proto se měla v jedné IP síti používat jedna (stejná) subsíťová maska. V praxi je třeba velký počet podsítí a na jednotlivých podsítích je značně různý počet stanic. VLSM umožňuje podsíťovat podsítě, takže router může na různých rozhraních používat různou masku podsítě.

NAT (Network Address Translation)

Překládá (mění „za chodu“) IP adresy (RFC 1631). Používá se na rozhraní mezi privátní sítí a veřejným Internetem (překládá lokální – privátní, vícenásobně použitelné – adresy na veřejné – unikátní – adresy. V případech, kdy jen část lokálních uzlů potřebuje komunikovat s vnějším světem, dochází k úspoře IP adres. Je zde možné spatřovat i jistý příspěvek k bezpečnosti, neboť lokální adresy nejsou vidět „zvenku“.

8.1.3 IP adresy třídy D

Problematiku řeší RFC 1112. Tyto adresy umožňují adresovat skupinu počítačů podle příslušnosti ke skupině. Jedná se např. o následující adresy:

224.0.0.1	skupina všech stanic připojených k lokální podsíti,
224.0.0.2	skupina všech směrovačů připojených k lokální podsíti,
224.0.0.4	všechny směrovače protokolu DVMRP,
224.0.0.5	skupina všech směrovačů podporujících protokol OSPF,
224.0.0.6	skupina všech jmenovaných směrovačů podporujících protokol OSPF,
224.0.0.9	použito pro RIP2,
224.0.1.1	použito pro NTP (Network Time Protocol).

8.1.4 IP verze 6

Protokol IPv6 byl vypracován již v roce 1995, důvodem jeho vzniku byla nedostatečná adresová (a směrovací) kapacita původního IP (tzv. IPv4). IPv6 vychází z charakteristik IP, poskytuje datagramovou službu, adresace a formát datagramu jsou odlišné. Protokol je specifikován v RFC 2460. Adresa má délku 128 bitů (RFC 2373), značná délka byla zvolena z důvodu počtu adres, jejich snadné agregovatelnosti podle příslušnosti k provozovateli, zákazníkovi, fyzickému segmentu sítě, apod. IPv6 se používá v páteřních sítích Internetu, v lokálních sítích se prakticky nevyskytuje (na hranicích mezi IPv4 a IPv6 se provádí překlad adres).

8.2 Datový komunikační model

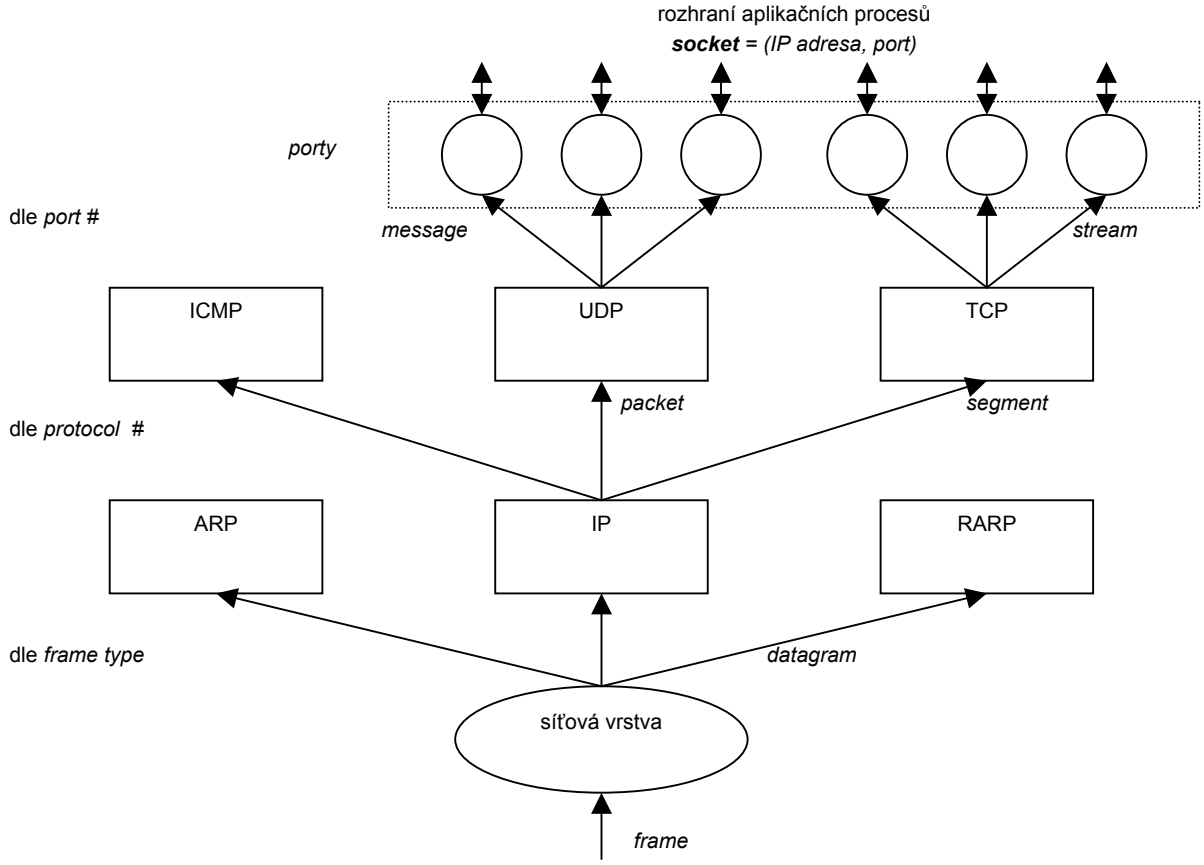
Jedná se o vrstvový model, vzhledem ke vzhledu nakresleného modelu se používá termín **protocol stack**. V jedné vrstvě může být více protokolů (např. mail, ftp jsou ve stejné vrstvě). Každý protokol komunikuje se svým partnerem (tzv. **peer** = druh, osoba stejného stavu, rovný), kterým je implementace stejného protokolu v ekvivalentní vrstvě ve vzdáleném systému. Neexistuje obecně platná dohoda o popisu TCP/IP pomocí vrstvového modelu, obvykle se považuje za složený z méně vrstev než ISO/OSI (3 až 5 úrovní), nejobvyklejší struktura je následující:

1. **aplikační vrstva**
2. **transportní vrstva** (doručení dat mezi dvěma účastníky)
3. **internetová vrstva** – *Internet Layer* (definuje datagram, zajišťuje směrování)
4. **síťová vrstva** – *Network Access Layer* (procedury pro přístup k fyzické síti)

Pro přenos dat se v TCP/IP používají dva protokoly – TCP a UDP, názvosloví používaných datových struktur jsou v tabulce 8.1. Tok dat datovým modelem je na obr. 8.5.

Vrstva / protokol	TCP	UDP
aplikační	stream	message
transportní	segment	packet
internetová	datagram	
síťová	frame	

Tab. 8.1: Datové struktury protokolu TCP/IP



Obr. 8.5: Tok dat v modelu TCP/IP

Čísla protokolů (obr. 8.5) identifikují protokol ve vyšší vrstvě (nad IP), kterému mají být předána data. Délka čísla protokolu je 8 bitů. V operačním systému UNIX jsou čísla protokolů definovaná v souboru */etc/protocols* (běžný textový soubor).

Čísla portů slouží k identifikaci aplikace v rámci systému. Transportní protokol předává data procesu na základě čísla portu. Čísla portů mají délku 16 bitů. Aplikace má zdrojový port pro vysílání a cílový port pro příjem. Existují tzv. *well-known ports* – cílové porty síťových služeb mají standardní čísla, aby jim bylo možné posílat data z libovolného místa v síti (bez nutnosti znát detailně konfiguraci cílového systému). V operačním systému UNIX jsou čísla portů definovaná v souboru */etc/services* (běžný textový soubor). Pro zdrojové porty se často používá dynamické přidělování čísel portů – nově spuštěný proces (např. klient nějaké služby) musí mít zajištěno unikátní číslo portu.

Jako **soket** (*socket*) se označuje kombinace IP adresy a čísla portu, tato dvojice tvoří jednoznačnou identifikaci procesu v rámci celého Internetu.

8.2.1 Síťová vrstva

Síťová vrstva (*Network Access Layer*)

- prostředek, kterým systém doručuje data jiným zařízením na přímo připojené síti.
- definuje způsob přenášení IP datagramů po síti
- musí znát detaily o síti (adresování apod.)
- z OSI může zahrnovat 3 dolní vrstvy, částečný překryv – IP se typicky uvádí jako záležitost síťové vrstvy
- známější protokoly (TCP, UDP, IP) jsou záležitostí vyšších vrstev
- funkce: zapouzdření IP datagramů na framy, mapování IP adres na fyzické a naopak (provádí protokoly ARP a RARP, které jsou obvykle řazeny do vyšší vrstvy, neboť pro přenos dat používají protokol IP)
- vrstva tvořena kombinací ovladačů a souvisejících programů

8.2.2 Internetová vrstva

Internetová vrstva obsahuje protokoly IP, ARP, RARP, ICMP a IGMP. Pro všechny tyto protokoly se jako základní komunikační protokol používá protokol IP.

- **IP** (*Internet Protocol*), RFC 791
    - základní protokol doručování paketů, v TCP/IP použit vždy bez ohledu na zdroj a cíl
    - používá se i pro ARP a RARP, ICMP, IGMP
    - *connectionless protocol* (nemá handshake) – opak by byl *connection-oriented protocol*
    - *unreliable protocol* (neobsahuje kód pro detekci ani opravy chyb)
    - doručuje datagramy
    - fragmentace datagramu, MTU (maximum transmission unit) – gateway může datagram fragmentovat
    - •předání datagramu transportní vrstvě podle čísla protokolu
- **ARP** (*Address Resolution Protocol*), RFC 826
    - pro komunikaci na síti je nutné znát hw adresy (adresují se jimi rámce)
    - převod IP na hardwarovou adresu
    - postup zjištění hw adresy:
        1. žadatel vyšle žádost – vyplní hw adresu odesílatele (tzn. svoji), IP adresu odesílatele (tzn. svoji) a IP adresu cíle a pošle na všeobecnou hw adresu
        2. žádost akceptuje počítač s cílovou IP adresou a pošle odpověď, současně si dvojici adres žadatele zařadí do svojí tabulky (minimalizace provozu)
        3. žadatel přijme odpověď, zařadí ji do tabulky ARP cache
        4. pokud hledaný je v jiné síti, odpovídá svojí hw adresou router (jako jeho zástupce – proxy ARP)

- **RARP** (*Reverse ARP*)
  - zjištění IP adresy při znalosti hardwarové
  - nejčastěji při startu systému ke zjištění vlastní IP (např. u bezdiskových stanic)
  - Postup:
    1. stanice vyplní svoji fyzickou adresu a pošle RARP na všeobecnou adresu
    2. RARP server zjistí z databáze adresu a pošle odpověď
    3. formát zpráv je shodný s ARP
  - pro komunikaci v IP sítích je znalost pouze vlastní IP adresy nedostatečná (je třeba znát masku podsítě, router, DNS server, ...), proto se místo ARP častěji používají komplexnější protokoly (BootP, DHCP)
- **ICMP** (*Internet Control Message Protocol*), RFC 792
  - protokol řídících hlášení, zprávy o chybách a zvláštních okolnostech při přenosu
  - často se vysílají v situaci zahlcené sítě nebo jiných problémů, proto zprávy koncipovány tak, aby co nejméně zatěžovaly síť (negenerují se v určitých situacích, např. při problémech s doručováním na všeobecnou nebo skupinovou adresu)
  - funkce:
    - řízení přenosu (pozastavení vysílání)
    - detekce nedosažitelných cílů
    - přesměrování trasy (posílá router, radí použít jiný router – zdroj i oba routery musí být na jedné síti)
    - kontrola vzdálených hostů (ping)
    - zjištění komunikační cesty (traceroute)

8.2.3 Transportní vrstva

Úkolem **transportní vrstvy** je doručení dat mezi dvěma účastníky. Nabízí přístup ke službě doručení datagramů (IP).

- **UDP** (*User Datagram Protocol*), RFC 768
  - connectionless protocol,
  - unreliable protocol,
  - nespolehlivá nespojovaná transportní služba,
  - nízká režie, jednoduchý,
  - typicky pro aplikace „dotaz/odpověď“, pro aplikace nevyžadující vysoké zabezpečení, aplikace požadující jednoduchost a malou režii,
  - podporuje i vysílání na všeobecnou adresu (255.255.255.255).
- **TCP** (*Transmission Control Protocol*), RFC 793
  - poskytuje virtuální okruh mezi koncovými aplikacemi,
  - vykonává i řízení koncového zabezpečení a datového toku, řízení koncového spojení,

- spolehlivá (reliable) transportní služba (doručí adresátovi data tak, jak je uživatel odeslal – bez ztráty nebo zkreslení dat a duplicitních paketů),
- využívá pozitivní potvrzování a opětovné přenosy (*Positive Acknowledgement with Retransmission – PAR*) – opakuje se tak dlouho, až přijde potvrzení,
- předávaná jednotka dat je segment, TCP dělí data (stream) na segmenty,
- kontrolní součet, když souhlasí, příjemce potvrdí příjem, jinak segment ignoruje,
- služba se spojením (navázání spojení, přenos dat, ukončení spojení),
- efektivní využití přenosových kanálů (bufferování, zahájení vysílání až po nashromáždění dostatečného množství dat, ...),
- full duplex (potvrzení příjmu segmentu je součástí segmentu vysílaného opačným směrem),
- přenášená data chápána jako posloupnost bytů, nikoliv jako pakety (proto stream),
- řízení zahlcení (RFC 2581) – ztráta paketů např. v důsledku malé vyrovnávací paměti příjemce, obdržení segmentu mimo pořadí apod.

8.2.4 Aplikační vrstva

Aplikační vrstva (*Process/Application Layer*) je nejvyšší vrstvou síťové architektury Internetu. Protokoly této vrstvy specifikují pravidla komunikace a formáty datových struktur pro jednotlivé síťové služby. Některé služby jsou vázány na konkrétní komunikační protokol, jiné mohou volit mezi TCP a UDP (podle implementace a/nebo konfigurace). Přehled vybraných protokolů je v tabulce 8.2.

Protokol:	HTTP	FTP	telnet	SMTP	DNS	TFTP	NTP	RPC	DHCP	SNMP
RFC:	2616	959	854	821	1035	1350	1305	1831	2131	11557
port:	80	20/21	23	25	53	69	123	111	546/547	161/162
použitý komunikační protokol:	TCP, RFC 793, číslo protokolu 6				TCP nebo UDP	UDP, RFC 768, číslo protokolu 17				

Tab. 8.2: Základní vlastnosti vybraných protokolů aplikační vrstvy

- **TELNET** (RFC854, TCP, port 23)
  - virtuální terminál pro vzdálený přístup
  - možnost přihlásit se ze vzdáleného počítače pro interaktivní práci na jiném počítači
  - klient zřídí spojení se serverem a posílá mu jednotlivé znaky (zadané z klávesnice), server je zpracovává jakoby byly napsané na jeho terminálu, vzniklé výstupní znaky pošle klientovi, který je zobrazí
  - definuje síťový virtuální terminál (NVT, *Network Virtual Terminal*), jednotné standardní rozhraní pro přístup ke vzdáleným systémům
  - *option negotiation* - volitelné režimy (sedmi- nebo osmibitový přenos apod.)

    - symetrické spojení – nerozlišuje mezi terminály a procesy (klientem se může stát jakýkoliv proces)
- **FTP** (*File Transfer Protocol*), RFC 959, TCP, port 20/21
    - jeden z nejstarších protokolů, počátky v r. 1971
    - klient - server
    - přenos vzdálených souborů na lokální počítač a opačně
    - interaktivní přístup
    - specifikace formátu (binary, ASCII, EBCDIC, ...)
    - řízení přístupu (jméno, heslo, anonymous)
    - TCP, 2 spojení - řídící (port 21, aktivní trvale) a datové (port 20, jen při přenosu dat)
    - nepříliš dobře řešená bezpečnost, existuje RFC 2228 (*FTP Security Extensions*)
- **TFTP** (*Trivial File Transfer Protocol*), RFC 1350, port 69
    - tak jednoduchý, aby implementace mohla být v ROM bezdiskových počítačů
    - použití typicky pro zavádění OS na bezdiskové počítače
    - UDP, bloky pevné délky 512 B
    - žádné zabezpečení, ani jméno/heslo
- **NFS** (*Network File System*), RFC 1813
    - transparentní sdílení vzdálených souborů (jako by byly lokální), koncový uživatel nebo aplikace neví o existenci NFS
    - architektura klient – server, server nabízí svůj lokální souborový systém, klient ho využívá
    - obvykle začleněno do operačního systému
- **Subsystém RPC a XDR** (*Remote Procedure Call* – RFC 1831, port 111 a *eXternal Data Representation* – RFC 1813)
    - oba jsou využívány NFS, mohou být použity i mimo
    - volání vzdálených procedur, distribuované programy
    - proces běžící na jednom počítači může zavolat vzdálený program na vzdáleném počítači, výsledek přenesen zpět volajícímu procesu
    - UDP i TCP
    - XDR - strojově nezávislá reprezentace dat pro přenos mezi dvěma počítači
    - vysílající provede konverzi do XDR, přijímající do svého formátu
- **SMTP** (Simple Mail Transfer Protocol) – RFC 821, 1870, 1869, port 25
    - doručení pošty formou přímého spojení TCP mezi odesílatelem a adresátem
    - adresa ve tvaru *username@mail-domain-name*
    - mail gateway
    - tvary a obsahy zpráv definovány v MIME (Multipurpose Internet Mail Extensions, RFC 2045, 2231)
    - přenos zpráv mezi serverem a osobním počítačem:
        - **POP** (*Post Office Protocol*, verze 3 RFC 1939, port 110) – stažení zpráv ze serveru na lokální počítač a odesílání

        - **IMAP** (*Internet Message Access Protocol*, RFC 2060) - manipulace se zprávami, ty zůstávají na serveru
- **BOOTP** (*Bootstrap Protocol*) – RFC 1813, port 68 klient, 67 server
    - získání základních informací při startu (např. bezdiskové stanice)
    - alternativní služba k RARP
    - využívá UDP
    - klient odešle dotaz na adresu 255.255.255.255
    - lze získat:
        - IP adresa klienta, IP adresa serveru, který odpověděl, routeru
        - jméno zaváděcího souboru (při bootování)
        - volitelně i subnet mask, jméno klienta, time servery, DNS servery, ...
    - nahrazován novějším protokolem DHCP
- **DHCP** (*Dynamic Host Configuration Protocol*), RFC 2132, RFC 2131
    - rozšiřuje možnosti BootP, zejména zavedena konfigurace serveru - přidělování IP adres klientům
    - IP adresy dočasně propůjčovány:
        - automaticky
        - dynamicky (leasing adresy na stanovenou dobu)
        - manuální (staticky přiděleno správcem sítě)
    - lze obdržet např.:
        - IP adresa, subnet mask
        - router
        - doména, server DNS
        - využívá k přenosu zprávy BootP, vzájemná slučitelnost
- **NTP** (*Network Time Protocol*), RFC 1305, port 123
    - synchronizace hodin v rámci sítě
- **NNTP** (*Network News Transfer Protocol*), RFC 977, port 119
    - zpravodajské skupiny (usenet news)
- **Gopher**, RFC 1436, port 70, TCP
    - vyhledávání distribuovaných dokumentů
    - *gopher* = sysel, je ve znaku státu Minessota,
    - služba vyvinuta na univerzitě v Minneapolis
    - historický, nepoužívá se
- **RSVP** (*Resource Reservation Protocol*), protokol č. 46, návrh RFC 2205-2210)
    - signalizační protokol umožňující přijímající stanici rezervovat šířku pásma pro přenos dat citlivých na zpoždění (hlas, obraz)
    - šířka pásma se specifikuje s ohledem na požadovanou kvalitu služby
    - požadavek budoucí přijímač pošle prvnímu routeru na trase k budoucímu zdroji
    - pokud je požadavek splnitelný, pošle ho router dalšímu routeru na trase
    - v případě úspěchu vznikne rezervovaná cesta s požadovanou šířkou pásma
    - rezervace je jednosměrná, iniciuje vždy příjemce

    - RSVP souvisí s transportní vrstvou TCP/IP, plní úlohy příslušející relační vrstvě podle OSI
    - QoS (Quality of Service)
- **RTP** (*Real-time Transport Protocol*), RFC 1889, 1890, 2435, 2508
    - přenosový protokol v reálném čase
    - podporuje spolehlivý koncový přenos interaktivního videa
    - synchronizace časového přenosu, zjištění ztrátu nebo nesprávného pořadí dat
    - identifikace přenášených dat, číslování v pořadí, časové značky
    - řídící protokol RTCP
    - může používat kompresi videa (JPEG)
    - nejčastěji používá UDP
    - neposkytuje mechanismus na zajištění doručení, včasného doručení ani doručení všech paketů ve správném pořadí
- **RTCP** (*Real-time Transport Control Protocol*)
    - řídící protokol spolupracující s RTP
    - periodické vysílání paketů od každého účastníka relace RTP všem účastníkům za účelem řízení výkonnosti a pro diagnostiku
    - informace o kvalitě vysílaných dat
    - identifikace zdroje RTP (přes kanonické jméno)
    - řízení intervalu vysílání RTP
    - přenos minimální informace o řízení relace
- **Real-time Streaming Protocol**
    - podporuje multimediální přenosy
    - proudový protokol v reálném čase
    - proudování rozděluje data do mnoha paketů o velikosti vhodné pro danou šířku pásma
    - po obdržení dostatečného počtu paketů může klient přehrávat jeden paket, dekomprimovat druhý a přijímat třetí (nemusí mít celý soubor)
- **SNMP** (*Simple Network Management Protocol*), RFC 1157, port 161/162
    - přenos informací pro management sítí
    - konfigurace síťových prvků po síti
    - předchůdcem byl **CMOT** (*Common Management Information Protocol over TCP/IP*), ten je zastaralý a již se nepoužívá

8.3 Služba DNS

DNS je zkratka pro *Domain Name System* (někdy se také interpretuje jako *Domain Name Services* nebo *Domain Name Server*). DNS umožňuje používat textová jména počítačů.

Jedinečná IP adresa poskytuje 2^{32} kombinací, v Internetu tedy může být asi $4{,}295 \cdot 10^9$ síťových rozhraní. Software při práci s číselnými adresami nemá potíže, člověku se ovšem lépe než čísla pamatují jména, která mohou mít při vhodné volbě i vypovídací hodnotu.

Výhodou důsledného používání jmen je také možnost přesunout jistou síťovou službu na jiný počítač (s jinou adresou), při zachování jména se pro uživatele zdánlivě nic nezmění. Pro většinu služeb a situací jsou jméno a adresa libovolně zaměnitelné (síť pracuje vždy s IP adresou, v případě použití jména je třeba provést konverzi – vyhledání IP adresy pro dané jméno v tabulce). K překladu jmen na adresy (a opačně) se používají dva mechanismy:

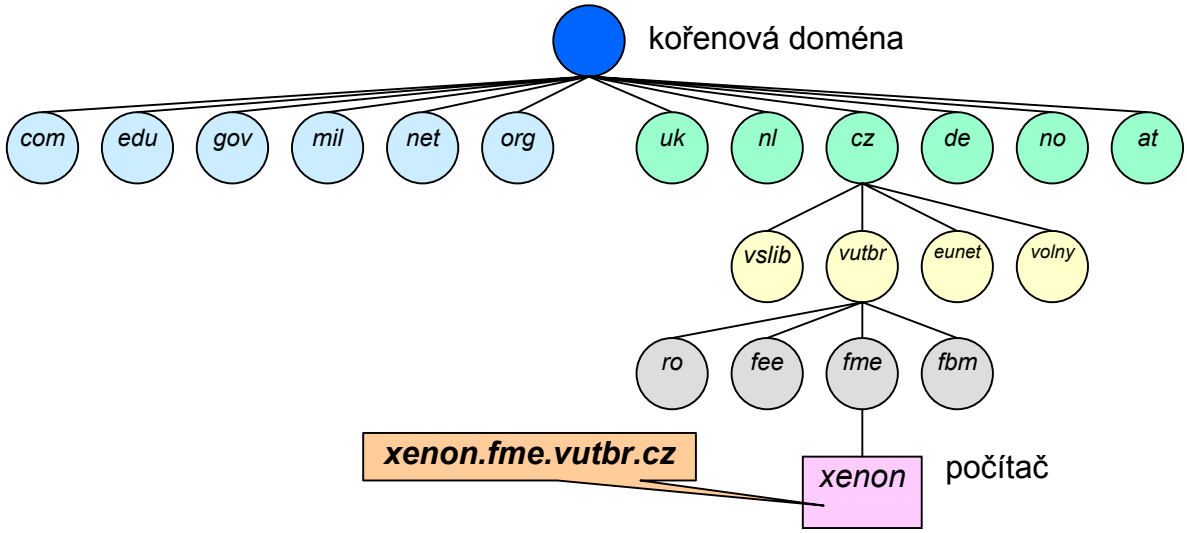
- **tabulka hostů**
- **DNS**

Tabulka hostů (*host table*) je řešení staré a již dávno překonané. V jednoduchém textovém souboru byly na počítači umístěna tabulka obsahující vždy IP adresu a textové jméno. V této tabulce musel být záznam pro všechny počítače, které měly být uživatelem počítače, na kterém je tabulka, identifikovány jménem. Výhodou byla jednoduchost. Nevýhod je ale mnohem více. Jednak bylo možné, aby si stejný počítač pojmenoval každý uživatel jinak, jednak, a to hlavně, tabulka obsahovala pouze omezený počet záznamů a nikdy nemohla obsahovat aktuální údaje pro celou velkou síť. Používala se také pouze pro malé sítě, ve kterých si uživatelé pojmenovali pouze několik důležitých počítačů. Pokusem o zlepšení popsaného mechanismu byla tabulka hostů NIC (*Network Information Center*). Původně byla tato tabulka tvořena souborem */netinfo/host.txt* na počítači *nic.ddn.mil*. V této tabulce se nacházely tzv. registrované hosty a záměrem bylo mít v této tabulce jména všech počítačů připojených do Internetu. Je zřejmé, že vzhledem k vývoji Internetu tato snaha neměla šanci na úspěch, NIC jako takové ale svoji roli zcela neztratilo (center je dokonce více) a hraje roli i ve spojení se systémem modernějším.

DNS pracuje jako hierarchický distribuovaný databázový systém, neexistuje tedy jediná tabulka ani jediná databáze s jedním centrálním správcem. Síť je členěna na domény, v každé z nich je autorita pro přidělování jmen. V každé doméně je alespoň jeden **autoritativní** server DNS, který je autoritou pro přidělování a rozpoznávání jmen ve svojí doméně. Struktura domén (jmenného prostoru sítě) je **stromová** (tedy nesouvisí s topologií sítě, která je v Internetu neomezená). Existuje **kořenová doména** (*root domain*) obsluhovaná **kořenovými servery** (*root servers*), tato kořenová doména je nepojmenovaná. Pod kořenovou doménou jsou **domény nejvyšší úrovně** (*top level domains*), členění na tyto domény je jednak geografické (podle států, výjimkou jsou USA, které geografickou doménu nepoužívají) a jednak organizační podle typu instituce (vzdělávací, vládní, vojenská, komerční, …), toto organizační členění se používá v USA. Pod těmito doménami nejvyšší úrovně jsou zřizovány domény další, úroveň dalšího větvení není omezena. Je samozřejmě nutné, aby jména všech subdomén každé domény byla unikátní. Přidělování jmen počítačům v každé doméně probíhá samostatně, jména počítačů v rámci domény musejí být unikátní. Úplné síťové jméno počítače se zapíše textovým řetězcem, který začíná jménem počítače a dále jména všech domén na cestě ke kořenové doméně, jednotlivá jména se oddělují tečkou. Struktura prostoru jmen je znázorněna na obr. 8.6.

Každý DNS server (tzv. *nameserver*) zná IP adresy nameserverů všech podřízených domén a IP adresu kořenových serverů (je jich více). Při potřebě konverze jména na IP nebo opačně se počítač dotáže některého známého nameserveru (obvykle ve svojí doméně, každý počítač musí mít v konfiguraci uvedenu IP adresu alespoň jednoho nameserveru). Dotázaný

nameserver buď odpověď zná (a tedy ji poskytne), nebo ji nezná, a pak je nutné ji zjistit od jiného nameserveru. Zde je možný dvojí mechanismus: buď se nameserver sám dotáže jiného (např. kořenového nebo některého podřízeného) nameserveru a získanou odpověď sám oznámí požadující stanici (**rekurzivní odpověď**), nebo nameserver pouze poskytne stanici odkaz na vhodný nameserver (**iterativní odpověď**). Aby se omezil provoz na síti a zrychlily odezvy, vytváří si každý nameserver dočasnou paměť pro údaje, které se v rámci poskytování rekurzivní odpovědi dozvěděl od jiných nameserverů – tzv. DNS cache. Platnost údajů v této dočasné tabulce je časově omezená (koncepce systému počítá je se zřídka nastávajícími změnami a tomu je podřízeno právě časování cache tabulek a výměn informací mezi servery). Pokud je dopověď přímo získána od serveru, který je autoritou v dané zóně, pak se jedná o **autoritativní odpověď** (bez ohledu na to, že byla zprostředkována jiným serverem v rámci rekurzivní odpovědi), pokud je zdrojem odpovědi DNS cache, jedná se o odpověď neautoritativní.



Obr. 8.6: Struktura jmenného prostoru Internetu

Nejpoužívanějším operačním systémem pro nameservery je UNIX. V systému UNIX je DNS implementováno softwarem *Berkeley Internet Name Domain* (BIND). BIND pracuje v režimu klient/server. Klientské části se říká *resolver*, server je implementován jako démon *named*. Pokud na počítači není zřízen nameserver, používá se pouze resolver. Server named se používá ve třech režimech (typech konfigurace):

- **caching-only** – neobsahuje žádnou databázi, není autoritou pro žádnou doménu,
- **primární nameserver** – autoritativní zdroj informací o konkrétní doméně, obsahuje databázi s údaji o jménech a adresách počítačů svojí autoritativní zóny,
- **sekundární nameserver** – všechny informace přebírá z primárního serveru, v konfiguraci má zjednodušeně řečeno jediný údaj – adresu primárního serveru, poskytuje autoritativní odpovědi o autoritativní zóně. Důvod pro zřizování sekundárního serveru je současný požadavek na existenci záložního serveru a možnost udržovat pouze jednu databázi.

Nameservery jsou schopny provádět převod oběma směry – z jména na IP adresu a z adresy na jméno (tzv. zpětný převod). K tomu si nameserver udržuje dvě tabulky (pro každý směr

převodu jednu), údaje pro každý počítač jsou tedy v databázi nameservery dvakrát. Již bylo uvedeno, že struktura jmenného prostoru nemusí odpovídat topologii sítě. To se projeví při potřebě převodu oběma směry – převod z adresy na jméno a z jména na adresu při nesouladu jmenné a fyzické topologie budou provádět různé servery – normální převod (z jména na IP adresu) bude provádět autoritativní server dané jmenné domény, opačný převod nameserver příslušný k dané oblasti sítě dle adres. Proto je zapotřebí pro každý směr převodu zvláštní soubor.

9 SLUŽBA WWW

Služba **www** (*World Wide Web*) byla vyvinuta v instituci CERN (*Conseil Européen de Recherche Nucléaire*) sídlící v Ženevě, a sice z potřeby šířit informace ke geograficky různě lokalizovaným badatelům v oboru vysokoenergetických fyzikálních polí. *Tim Berners-Lee* navrhl hypertextový systém, který umožňoval spojovat dohromady dokumenty uložené v počítačové síti (na různých počítačích). K přenosu navrhl protokol, který pojmenoval **http** (*Hyper Text Transfer Protocol*). V březnu 1991 byl stejným autorem navržen jazyk pro popis vzhledu zobrazovaných stránek **html**. V lednu 1992 byla služba poprvé veřejně předvedena a do dubna 1993 existovalo již asi 60 www serverů. V březnu 1993 studenti NCSA (*National Center of Supercomputer Applications*) představili první grafický prohlížeč nazvaný *Mosaic*.

S rozšiřováním služeb sítě Internet vyvstala nutnost vytvoření logicky jednotného formátu adresy pro celou paletu služeb. Tato adresa se nazývá **URL** (*Uniform Resource Locator*) a jeho struktura je následující:

`typ://uživatel:heslo@počítač:port/cesta;parametry?dotaz`

Typ znamená označení služby (např. http, ftp, telnet, file, gopher. mailto, …), **uživatel** a **heslo** jsou přihlašovací jméno a heslo uživatele, **počítač** je identifikace počítače (jméno nebo IP adresa), **port** je číslo komunikačního portu TCP/IP, **cesta** je označení požadovaného souboru včetně cesty k němu, **parametry** a **dotaz** jsou předávány serveru a jejich význam se pro různé aplikace liší.

WWW je služba typu klient/server. Klientem je prohlížeč (Netscape, MS Internet Explorer, Mosaic, …), který zasílá požadované URL na server a server zasílá klientu požadovaná data, komunikace probíhá v protokolu http. Protokol http je bezstavový (pro každou http operaci se vytváří a ruší spojení, stav posledního spojení si server ani klient nepamatují). Jedna http operace se nazývá *http transakce*. Protokol podporuje dynamické formáty (klient může poslat serveru seznam podporovaných formátů). Protokol http je čitelný (textově orientovaný). Obsahuje tři základní operace: vyhledání zdroje (ustavení spojení, odeslání požadavku - URL), získání zdroje a komentování zdroje (stavové zprávy). Transakce se skládá z ustanovení spojení, odeslání požadavku klientem, zaslání odpovědi serverem a ukončení spojení (serverem).

9.1 Jazyk html

Jazyk html (*Hyper Text Markup Language*, hypertextový jazyk s příznaky) je popisný jazyk stránky. Jazyk sám je popsán pomocí jazyka SGML (*Standard Generalized Markup Language*). SGML je metajazyk (jazyk určený primárně k popisu dalších jazyků), a je normalizován v ISO (schváleno 1986), HTML je tedy aplikací v SGML. Jazyk html popisuje, jak budou jednotlivá data zobrazena prohlížečem. V době vzniku autor jazyka html nepředpokládal, že by se stránky vytvářely přímo v html, uvažoval o existenci generátoru stránek, jehož výstupem bude popis stránky v html. V dnešní době existuje řada progra-

mových produktů schopných úlohu takového generátoru více či méně úspěšně zastávat, vytváření stránek přímo v jazyce html však není výjimkou.

Jazyk html prošel a stále ještě prochází bouřlivým vývojem. V roce 1994 bylo založeno *www konsorcium* (WWWC, W3C), které má vývoj jazyka na starosti. Vzhledem k tomu, že řadu rozšíření zavedli do jazyka přímo výrobci prohlížečů, není úloha konsorcia jednoduchá a jsou časté případy, kdy stejně popsanou stránku (a napsanou v souladu s oficiální verzí jazyka) zobrazují různé prohlížeče různě.

Jazyk html je popisným jazykem stánky, má tedy podobnou úlohu jako např. postscript. Protože ale cílovou plochou pro zobrazení je obrazovka (resp. okno), neobsahuje html prostředky pro přesný popis zobrazení, ale pouze doporučení typu „zde začíná odstavec“, „tohle je nadpis“, „zde je centrovaný obrázek“ apod. V novějších verzích jazyka sice jsou prostředky pro poměrně přesné ovlivnění vzhledu výstupu, využití těchto prostředků může být ale problematické vzhledem k tomu, že každý počítač – prohlížeč – používá jiné rozlišení, jiný počet současně zobrazitelných barev, podporuje různé fonty, velikost okna prohlížeče si může každý uživatel nastavit zcela libovolně atd.

Příkazy jazyka html (položky, příznaky, tagy, značky) se zapisují ve tvaru **<xxx>**, jsou tedy uzavřené v úhlových závorkách. Značky existují párové a nepárové, párových značek je většina a označují začátek platnosti značky a konec platnosti (ukončovací značka se zapisuje jako **</xxx>.** Dokument html je koncipován jako nezávislý na platformě a aplikaci. Struktura dokumentu html je na obr. 9.1.

```
<HTML>
<HEAD>
<TITLE>Nadpis</TITLE>
</HEAD>
<BODY>
text dokumentu<!-- komentář -->
</BODY>
</HTML>
```

Obr. 9.1: Formát html dokumentu

Přehled značek jazyka html lze nalézt na Internetu, vhodná URL jsou například: *http://www.w3.org/pub/WWW/MarkUp* nebo *http://www.fee.vutbr.cz/info/WWW/.*

9.2 Statické a dynamické www stránky

Nejobyčejnější způsob vytvoření a zobrazení stránek je takový, že stránka je vytvořena v jazyce html, na serveru je uložena v souboru (textovém), při požadavku na zobrazení příslušné stránky server pošle obsah tohoto souboru, klient interpretuje příznaky html a na jejich základě dokument naformátuje a zobrazí. Tento jednoduchý mechanismus se hodí pouze pro

stránky, které se mají zobrazit vždy stejně a nereagují na žádné akce uživatele. Má-li být chování stránek složitější (např. mají-li umožňovat přístup do databáze apod.), musí být tento proces složitější. Potřebný mechanismus poskytují *dynamické www stránky*. Stránka může být dynamická na straně serveru nebo na straně klienta (nebo na obou), každá z variant poskytuje jiné možnosti a je vhodná v různých případech.

9.2.1 WWW stránky dynamické na straně serveru

V tomto případě server posílá html text, který na serveru přesně v té podobě, v jaké je posílán, v žádném souboru neexistuje. Server jeho text vygeneruje až po obdržení požadavku od klienta. Pro klienta není žádný rozdíl v tom, zda stránka na serveru existuje jako statická nebo byla vygenerována jako dynamická.

Jednou z běžných možností je naprogramování aplikace (v jakémkoliv programovacím jazyce), URL odpovídající stránky pak neukazuje na textový html soubor, ale na spustitelný soubor této aplikace. Server aplikaci spustí, předá jí kompletní URL (včetně polí *parametry* a *dotaz*), aplikace jako svůj výstup vygeneruje popis stránky v html a odvysílá jej ke klientovi. K předání parametrů a přesměrování výstupu na síť se používá rozhraní **CGI** (*Common Gateway Interface*) na serveru. Takto spouštěným aplikací se říká *CGI-aplikace*. Obvykle se tyto programy realizují v jazyce C nebo PERL.

Jinou možností je použití tzv. **SSI** (*Server Side Include*). V tomto případě je stránka napsaná jako html text, ve kterém jsou ale vloženy příkazy pro server, server tyto příkazy provede a jejich výstup vloží na odpovídající místo v textu html. Tímto způsobem lze např. do textu stránky přidávat datum a čas poslední modifikace stránky, realizovat různá počítadla přístupů, začleňovat do stránky obsahy celých jiných souborů nebo provést obecný příkaz na serveru a do stránky zahrnout jím produkovaný výstup.

Široké možnosti poskytují tzv. skriptovací jazyky na straně serveru, k nejrozšířenějším patří **php** a **ASP**. Na serveru existuje soubor (textový, formálně se jedná o soubor obsahující html text), v html textu jsou (podobně jako u SSI) vloženy příkazy pro server, v tomto případě se ale jedná o možnost psát celé programy, které server interpretuje a jejich výstup začleňuje do webovské stránky zasílané klientu. Tato varianta je v současné době velmi rozšířená.

Dynamické www stránky se většinou požívají v případech, kdy je nutné reagovat na speciální požadavky uživatele. Ty se projevují v URL v polích *dotaz* a *parametry*. V jazyce html je podpora tzv. *formulářů*, které umožňují na www stránce zobrazovat běžné editační prvky (vstupní textová pole, výběry ze seznamů, zaškrtávací políčka apod.). Formulář má vždy jedno odesílací tlačítko, po jehož stisknutí je klientem odesláno URL definované ve formuláři a do pole *dotaz* URL jsou přidány hodnoty editačních prvků (existuje i jiný způsob předání parametrů na server).

9.2.2 WWW stránky dynamické na straně klienta

Klient (www prohlížeč) může od serveru dostat v zásadě data dvojího druhu: text v jazyce html nebo kód programu v jazyce **Java** (tzv. *Java applet*).

V případě Java appletu zasílaným dokumentem není text, ale program v binární podobě (jedná se ovšem o metakód, nikoliv strojový kód, applet musí být nezávislý na platformě). Klient namísto zobrazení stránky podle html popisu provádí program, který píše a kreslí na obrazovku (do okna prohlížeče). Applet může samozřejmě reagovat na události na straně klienta (akce uživatele, např. pohyby myší apod.), nemá ale přístup k serveru (spojení je po odeslání appletu ukončeno). Java je objektově orientovaný jazyk podobný jazyku C++. Na straně serveru se obvykle jedná o statickou stránku (generovat programem – třeba CGI – kód jiného programu je obtížné, i když ne nemožné). Stránkám napsaným v jazyce Java je připisována velká budoucnost. Je ovšem pravda, že většinu toho, co tyto stránky poskytují, lze realizovat i jednodušším způsobem, a navíc je provádění Java appletů na straně klienta zatím dosti pomalé. Zajímavá je multimediální podpora obsažená v jazyce Java. U stránek dynamických na straně klienta je třeba vždy řešit bezpečnost, neboť se jedná o proces prováděný na počítači klienta. Java má tuto otázku vyřešenou velmi dobře a potenciálně nebezpečné operace nepodporuje (má např. silně omezený přístup k souborům na straně klienta).

Jinou možnost poskytují tzv. skripty. Jedná se o vkládání úseků programů do html textu. Server tyto vsuvky ignoruje (nejsou určeny jemu), klient je potom vykonává (interpretuje). Pro tyto účely byl vyvinut skriptovací jazyk *JavaScript* a *VBScript*. JavaScript vychází z jazyka Java (objektový jazyk podobný C++) a je podporován nejrůznějšími prohlížeči. VBScript je zvláštním klonem jazyka Visual Basic a je podporován výhradně MS Internet Explorerem, takže jeho použití je omezeno na platformu Microsoft. Protože Internet je síť, ve které jsou zapojeny počítače různých výrobců, architektur a kategorií, pracující s různými operačními systémy, nelze použití VBScriptu označit za příliš dobrou volbu.

10 VYSOKORYCHLOSTNÍ SÍTĚ

Motivací k vytváření stále rychlejších sítí je mnoho. Mezi nejdůležitější patří:

- nárůst počtu počítačů a uživatelů,
- změna charakteru aplikací (původně hlavně e-mail, který má dávkový charakter, dnes zejména www s nutností přenosu obrázků, vzdálený přístup k souborům, vzdálený přístup k databázím, multimediální aplikace),
- zvýšení výkonu počítačů (s rostoucím výkonem počítačů – zejména sběrnic – nastal nepoměr mezi datovou propustností sběrnice počítače a počítačové sítě, síť, která úspěšně pracovala s jistým počtem připojených starých počítačů bude moderními počítači o stejném počtu zahlcena).

KE ZRYCHLENÍ SÍTÍ LZE POUŽÍT DVĚ STRATEGIE:

- zvýšení přenosové rychlosti (redukce času na přenesení jednoho bitu),
- změna organizace provozu na síti (rozčlenění sítě na několik menších s cílem snížit pravděpodobnost vzniku kolize nebo zvýšit pravděpodobnost obdržení tokenu).

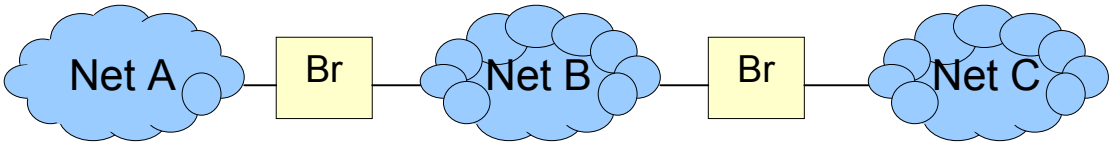
V praxi se používají oba zmíněné přístupy. První z nich se projevuje zejména ve specifikaci nových výkonnějších síťových platforem, druhý je aplikován v tzv. přepínání.

10.1 Přepínání

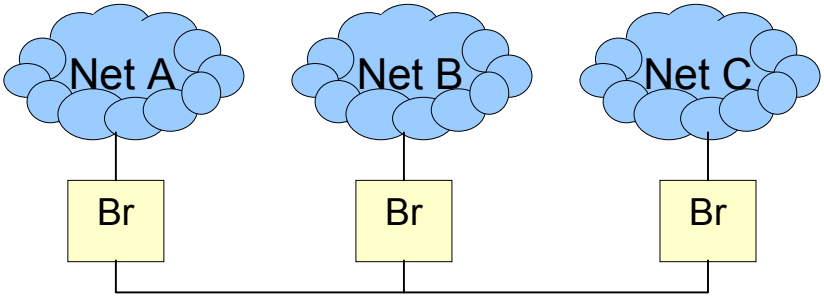
Přepínání bylo nejprve k dispozici pro síť Ethernet, neboť se tam nejsnadněji implementuje a jeho myšlenka dokonale odpovídá filozofii Ethernetu. Základní ideou je zmenšení tzv. kolizní domény (oblast sítě se společným řízením přístupu k médiu, tzn. oblast sítě, ve které při současném vysílání dvou stanic dojde ke kolizi). Toho lze dosáhnout používáním vhodných aktivních síťových prvků (a hlavně nepoužívat repeatery – tedy ani huby). Ideálním stavem by bylo mít na jednom segmentu zapojenu pouze jednu stanici, pak by vznik kolize byl vyloučen. Základním aktivním prvkem vhodným pro dosažení požadovaného cílového stavu je tzv. **přepínač** (*switch*), který je možné si v nejjednodušší podobě představit jako rychlý víceportový bridge (tato představa je velmi zjednodušená a silně nepřesná až nepravdivá, viz dále). Použití přepínačů a omezení počtu kolizí vede k opuštění topologie páteře a sběrnice, a nakonec vůbec koaxiálního kabelu – jednak vyžaduje „nevhodné“ topologie, jednak nepodporuje přenosy vysokými rychlostmi u moderních vysokorychlostních sítí.

Rozdělování sítě na několik menších kolizních domén obvykle vede ke změně topologie, hovoří se o tzv. **zborcené páteři** (*collapsed backbone*). Přechod k této topologii ukazují obr. 10.1 až 10.3. Na obr. 10.1 je znázorněna síť, která byla za účelem zmenšení kolizní domény rozdělena na tři sítě propojené pomoci bridgů. Protože provoz mezi sítí A a C jako tranzitní zatěžuje síť B, jeví se jako výhodnější použít další bridge a přejít k páteřní topologii (obr. 10.2), zde ovšem jakákoliv komunikace mezi sítěmi prochází přes dva bridge. Definitivní řešení je na obr. 10.3, vzhledem k tomu, že vzniklo jako důsledek odstranění páteře, označuje se tato topologie jako zborcená páteř (ve skutečnosti je to hvězda). Postup

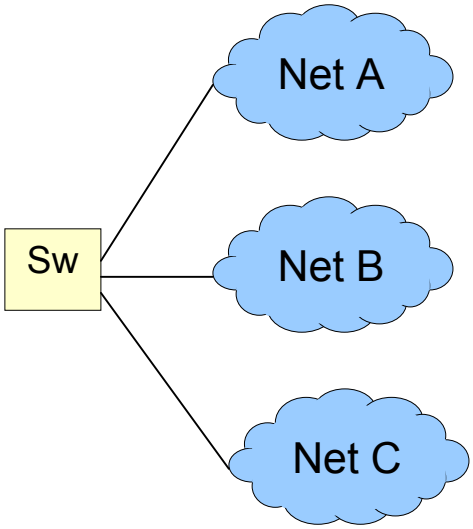
naznačený na obr. 10.1 až 10.3 lze aplikovat dále až do okamžiku, kdy vznikne síť s topologií hvězdy v jejíchž vrcholech budou jednotlivé počítače a uprostřed bude centrální přepínací prvek. S ohledem na topologická omezení bude tato topologie reálně použitelná pouze v malých sítích, jinak se bude jednat nejspíše o topologii stromovou (více vzájemně propojených hvězd).



Obr. 10.1: Síť rozdělená na tři kolizní domény



Obr. 10.2: Síť z obr. 10.1 s odstraněním tranzitního provozu v síti B



Obr. 10.3: Síť z obr. 10.1 s topologií zborcené páteře

Charakteristickým rysem přepínaných sítí je použití vysokorychlostních přepínacích zařízení, poskytujících dedikované připojení jednotlivých uzlů, podporujících agregovanou přenosovou šířku pásma všech portů (tzn. že switch je schopen přenášet paralelní komunikace – po vzájemně nekolidujících dvojicích portů až do jejich maximálního možného počtu).
K výhodám přepínaných sítí patří:

- možnost snadného přechodu k plně přepínané síti (lze připojovat stanice i segmenty sítí, postupně se nahradí stávající huby),

- využití stávajících směrovačů (není nutné měnit konfiguraci routerů, adresy apod.),
- zvětšení agregovaného přenosového výkonu,
- zvýšení a stabilita přenosového pásma dostupného uživateli,
- různé přístupové rychlosti na různých portech přepínačů,
- podpora různých topologií, modularita zařízení
- podpora VLAN (virtuální LAN)
- vyšší bezpečnost (nižší možnost odposlechu dat)

Podle principu přepínání (druh informací, podle kterých se switch rozhoduje, kam poslat data) se rozlišují různé kategorie přepínání:

- na fyzické vrstvě (v zásadě možnost rozdělení hubu na několik menších),
- na MAC vrstvě (jako bridge, na základě MAC adresy),
- na síťové vrstvě (na základě adresy v paketu, např. podle IP adresy)

Existuje i přepínání na vyšších vrstvách (např. podle služby).

Podle toho, jaké datové elementy jsou přepínány, se rozlišuje **přepínání rámců** a **přepínání buněk**.

Existují tři základní režimu přepínání:

- *cut through-mode*
  - nejmenší zpoždění
  - přečtení adresy (MAC adresa v rámci), vyhledání portu a přímý přenos na výstupní port
  - nevýhoda: přenáší se i vadné pakety (kontrolu lze vyhodnotit až pro celý paket)
  - použitelné pouze pro porty stejné rychlosti
- *modified cut-through mode*
  - prvních 64 bytů načteno do paměti a analyzováno, pak teprve přenos
  - projdou pouze nekolizní pakety (platí pro Ethernet při dodržení topologických omezení)
  - pracuje pouze s porty stejné rychlosti
- *store and forward mode*
  - jako klasický bridge
  - načte se adresa, nalezne port a současně je celý frame uložen do paměti, po kontrole CRC se vyšle
  - umožňuje používat porty s různými rychlostmi
  - největší zpoždění

10.1.1 Virtuální sítě

Při provozu (a zejména správě) počítačových sítí je potřeba přeřazovat počítač mezi segmenty bez zásahu do kabeláže. Řešení je hned několik:

- strukturovaná kabeláž, ručně přepojit v rozvaděči,
- přepínání na fyzické vrstvě,
- použití VLAN

Termínem VLAN (virtual LAN) se označuje logický segment LAN, který obsahuje uzly připojené k různým fyzickým segmentům. K největším výhodám použití VLAN patří:

- možnost seskupování uživatelů podle logických kritérií, nejen podle umístění,
- vyrovnání síťové zátěže,
- zvětšení dostupné šířky pásma,
- zjednodušení konfiguračních změn

Možnost existence VLAN těsně souvisí s přepínáním, používají se následující druhy přepínání:

- přepínání portů,
- přepínání rámců,
- přepínání buněk

Z hlediska souvislosti s ISO/OSI modelem se hovoří o třech úrovních VLAN:

- 1. úroveň: sdružování portů hubů a přepínačů,
- 2. úroveň: přiřazování uzlů do VLAN na základě MAC adres,
- 3. úroveň: dle síťové adresy (IP)

10.2 Fast Ethernet

Fast Ethernet byl odvozen ze standardního Ethernetu redukcí bit-time faktorem 10. Práce na novém rychlejším standardu byly zahájeny v roce 1992, vývoj byl poznamenán soupeřením technologií Fast-Ethernet a 100VG-AnyLAN (viz dále), 14. července 1995 byl přijat standard IEEE802.3u popisující 100 megabitový Ethernet (zabývá se 1. a 2. vrstvou ISO/OSI).

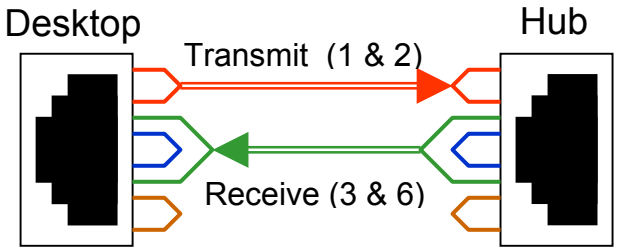
Očividnou změnou oproti Ethernetu klasickému je ukončení podpory koaxiálního kabelu a tím i sběrnicové topologie – tyto již v novém Ethernetu nelze použít. Typickou topologií se stala hvězda (podobně jako u desetimegabitového Ethernetu s použitím UTP kabelu). Pro Fast Ethernet je umožněno používat UTP kabely a optická vlákna. Metoda přístupu k médiu je převzata z původního Ethernetu (CSMA/CD). Formát rámců zůstal rovněž zachován (včetně minimálního a maximálního limitu délky a adresace). Podporované typy kabelů včetně označení a maximálních délek jsou v tabulce 10.1.

specifikace	kabel	max. délka segmentu
100 BASE-TX	UTP cat. 5, STP type 1 a 2 (2 páry)	100 m half/full duplex
100 BASE-T4	UTP cat. 3, 4, 5 (4 páry)	100 m half duplex
100 BASE-FX	62,5/125 MM optické vlákno	412 m half duplex 2000 m full duplex

Tab. 10.1: Kabely Fast Ethernet

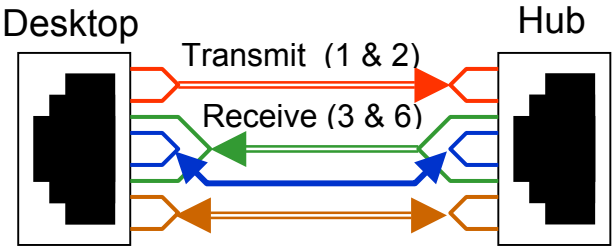
Fast Ethernet zavádí dva způsoby použití UTP kabelů ve specifikacích 100 BASE-TX a 100 BASE-T4. 100 BASE-T4 umožňuje použít "horší" druh kabelu (původně určený pro desetimegabitové sítě, aby bylo možné využít kabeláž vybudovanou pro klasický Ethernet), ovšem s tím, že na tomto kabelu nelze použít přenos v režimu full duplex. To je dáno tím, že přenos využívá vždy tři páry pro každý směr vysílání – jeden pár je použit vždy pro jeden směr, druhý vždy pro vždy druhý směr, zbývající dva páry se používají pro oba směry

(v jednom okamžiku ovšem pouze pro jeden). Zapojení přímého kabelu pro specifikaci 100 BASE-TX je na obr. 10.4, pro specifikaci 100 BASE-T4 na obr. 10.5.



100 BASE-TX
(100 Mb/s = 1 pár x 125 MHz x 80 %)
(kódování 4B5B)

Obr. 10.4: Přímý kabel pro 100 BASE-TX



100 BASE-T4
(100 Mb/s = 3 páry x 25 MHz x 133 %)
(kódování 8B6T)

Obr. 10.5: Přímý kabel pro 100 BASE-T4

Pro Fast Ethernet jsou definovány dva druhy hubů (rozbočovačů) – class 1 a class 2. Hub class 1 (Translational Repeater) opakuje signál po jeho konverzi do digitální podoby, maximální počet hubů v kolizní doméně je jeden. Hub class 2 (Transparent Repeater) konverzi signálu neprovádí, má menší zpoždění a v kolizní doméně mohou být huby dva (ovšem propojené kabelem maximální délky 10 m). Důvodem pro existenci hubu class 1 je možnost koexistence obou typů UTP kabelů – TX i T4.

Topologická omezení pro stomegabitový Ethernet (pro jednu kolizní doménu) jsou v tabulce 10.2. Topologická omezení lze překonat rozdělením sítě na více kolizních domén, tedy aplikací přepínání.

kombinace kabelů / propojení	T4 nebo TX	TX & FX	FX	T4 & FX
DTE – DTE (žádný repeater)	100 m	–	412 m	–
jeden repeater class 1	200 m	260,8 m	272 m	231 m
jeden repeater class 2	200 m	308 m	320 m	–
dva repeatery class 2	210 m	216 m	228 m	–
propojení hub – bridge, router nebo switch	100 m	–	228 m	–
propojení switch – switch	100 m	–	412 m half duplex 200 m full duplex	–

Tab. 10.2: Topologická omezení pro Fast Ethernet

10.3 Gigabit Ethernet

V březnu 1998 byla publikována specifikace IEEE 802.3z, která standardizuje síť na bázi Ethernetu s přenosovou rychlostí 1000 Mb/s. Tento standard se týkal pouze optických kabelů, u metalických kabelů byla maximální možná délka velmi malá (25 m). Koncem téhož roku ale byla přijata specifikace IEEE 802.3ab, která obsahuje možnost použít UTP kabel o max. délce 100 m. Síť používá přístupovou metodu odvozenou z CSMA/CD (došlo k úpravě časových poměrů s ohledem na možnost spolehlivého vyhodnocení kolizí). Síť používá na všech médiích přenosový režim full duplex. 1000 Mb Ethernet rovněž obsahuje podporu virtuálních sítí. Topologií je opět hvězda, základním aktivním prvkem je switch pracující na 2. nebo 3. vrstvě a tzv. **buffered distributor** (v zásadě víceportový repeater, pro možnost práce v režimu full duplex jsou všechny rámce před vysláním přijaty a uloženy do vyrovnávací paměti – bufferu). Topologická omezení jsou v tabulce 10.3.

specifikace	kabel	max. délka segmentu
1000 BASE-SX	50/100 nebo 62,5/125 MM	550 nebo 275 m
1000 BASE-LX	SM optické vlákno	5000 m
1000 BASE-CX	STP nebo twinax	25 m
1000 BASE-T	UTP cat. 6 (větš. vyhoví i cat. 5)	100 m

Tab. 10.3: Topologická omezení pro Gigabit Ethernet

10.4 100VG-AnyLAN

Při zahájení prací na vývoji sítě rychlejší než klasický desetimegabitový Ethernet se skupina výrobců (hlavně Hewlett-Packarda AT&T) snažila nejen zvýšit rychlost sítě, ale také odstranit některé nevýhodné vlastnosti sítě Ethernet (zejména některá topologická omezení a náhodnou metody řízení přístupu k médiu). Tato snaha byla korunována úspěchem, ovšem pouze technickým, obchodně se síť neprosadila a od jejího používání se velmi brzy upustilo. Síť je standardizována v IEEE 802.12 (Přijato v červnu 1995, tedy o něco dříve než Fast Ethernet).

100VG-AnyLAN nepoužívá přístupovou metodu CSMA/CD. Základní technické údaje jsou následující:

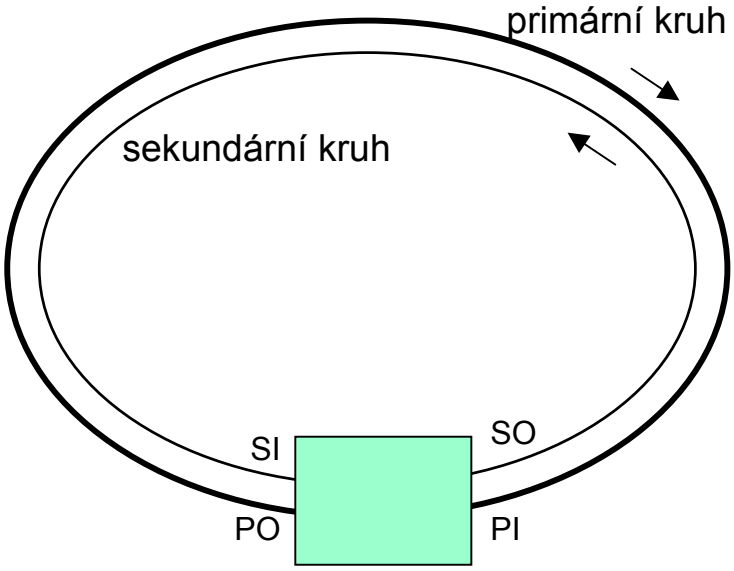
- stromová topologie,
- umožňuje přenos rámců 802.3 i 802.5 (Token Ring), nikoliv oba současně v jednom segmentu,
- přes bridge lze připojit i 10 Mb/s, 4 Mb/s nebo 16 Mb/s segmenty,
- používá half duplex (data) i full duplex (řídící informace),
- základním aktivním prvkem je opakovač (koncentrátor, hub, rozbočovač) má dva typy portů:
    - **down-link** port (výstupní) - připojení koncových zařízení nebo opakovačů nižší úrovně,
    - **up-link** port (vstupní) - spojení s opakovačem vyšší úrovně,
- režimy práce portů:
    - **private mode** (pouze pakety určené připojenému koncovému zařízení),
    - **promiscuous** mode (všechny pakety),
- segmentace (podobně jako Ethernet), ale oddělení zajišťují kaskádně řazené huby,
- přístupová metoda DPA (deterministická metoda, na žádost), dvě úrovně priority požadavku, dále priorita dána číslem portu,
- podpora zaručené šířky pásma,
- maximální rozlehlost 600 m pro kabel UTP cat. 3, 900 m pro UTP cat. 5, při použití optického kabelu (62,5/125 MM) až 4000 m.

10.5 FDDI

Fiber Distributed Data Interface (FDDI) je nejstarším standardem řazeným mezi vysokorychlostní sítě. Standardem je ANSI norma X3T9.5, která byla přijata již v roce 1989. Síť používá topologii dvojitého kruhu, ke kterému lze připojit pobočné stromy (původní anglický termín je *dual ring of trees*) a pracuje s rychlostí 10 Mb/s. FDDI byla zejména v první polovině devadesátých let 20. století dosti rozšířená, neboť jako jediná dostupná technologie umožňovala vysokorychlostní řešení i pro poměrně rozlehlé sítě, typickou oblastí použití byly metropolitní a campusní sítě. FDDI byla dosti drahá síť a byla postupně vytlačena jinými levnějšími nebo perspektivnějšími platformami (nejdříve sítí ATM, v současné době její roli převzal gigabitový Ethernet).

FDDI používá základní topologii dvou kruhů, každý kruh má jiný směr toku dat. Jeden z kruhů je primární, a v běžných situacích se pouze tento používá pro datové přenosy. Ve zvláštních situacích se do přenosů zapojí i sekundární kruh – např. v situaci, kdy dojde k přerušení kruhu (přerušení kabelu) dojde k tzv. fragmentaci kruhu, kdy připojené aktivní prvky dokážou kruh uzavřít s využitím sekundárního kruhu a práce sítě může pokračovat (při porušení kabelu na dvou místech se ovšem síť rozpadne na dvě izolované sítě). Topologie sítě je na obr. 10.6. Zkratky v obrázku 10.6 mají význam: PI – primary (ring) in, PO – primary (ring) out, SI – secondary (ring) in, SO – secondary (ring) out.

Metoda přístupu k médiu využívá předávání příznaku oprávněnosti k vysílání (token), oproti síti Token Ring jsou zde ale podstatné odchylky: stanice, která potřebuje vysílat, počká na token, na síť vloží svoje data a hned za nimi vysílá token (na kruhu se tak může objevit za sebou několik datových rámců následovaných tokenem – někdy se používá termín *tlačná lokomotiva*). Tato úprava byla přijata s ohledem na značnou rozlehlost sítě – součtová délka obou kruhů (obvod) může dosáhnout až 200 km.



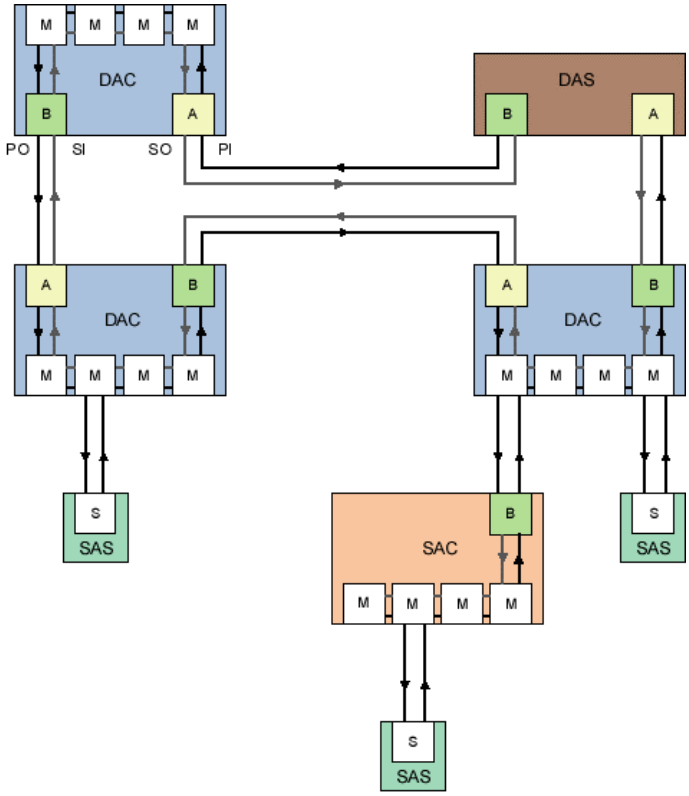
Obr. 10.6: Topologie FDDI

Do sítě se zapojují dva základní typu zařízení – stanice a koncentrátor, každé z nich může být připojeno k jednomu, oběma a koncentrátor také k žádnému kruhu. Používají se zkratky DAC (dual attached concentrator), SAC (single attached concentrator), NAC (null attached concentrator), DAS (dual attached station) a SAS (single attached station). Tato zařízení jsou opatřena několika typy portů: A,B – porty pro připojení ke dvojitému kruhu (A vstupní, B výstupní), M – Master Port pro připojení stanic nebo rozbočovačů nižší úrovně, S – Slave Port pro připojení zařízení k portu M. Příklad možného zapojení sítě FDDI je na obr. 10.7.

10.6 ATM

Technologi nazvaná **Asynchronous Transfer Mode** (ATM) byla vyvinuta v průběhu osmdesátých let dvacátého století. Původně byla tato síť vyvinuta pro digitální multimediální přenosy (např. video on demand), postupně se rozšířila i do běžných datových sítí. Technologie ATM navzdory značné technické pokročilosti a eleganci byla pronásledována některými nešťastnými (nezaviněnými) okolnostmi, které zavinily, že nikdy nebyla a není tolik rozšířená, jak by technické vyspělosti odpovídalo. Projekt digitální kabelová televize se nikde na světě nerozvíjel takovým tempem, jako se původně předpokládalo, v oblasti datových sítí nevládly tak přísné požadavky, které by nutily k nasazení ATM ve velkém měřítku. Významnou aplikační oblastí ATM tak zůstaly zejména rozsáhlé páteřní sítě

(campusní, metropolitní i celoevropské). Tato oblast nasazení ale nebyla schopna odebrat takové množství aktivních prvků, aby došlo k jejich výraznému zlevnění. Se zrychlením sítě Ethernet je ATM v současné době vytlačována prakticky ze všech aplikací. ATM má vlastní standardizační orgán – ATM fórum (založeno 1991).



Obr. 10.7: Příklad sítě FDDI

Základním aktivním prvkem sítě ATM je ATM přepínač. Technologie ATM využívá k přenosu buňky o pevné délce 53 bytů, což je kompromisní hodnota pro přenos různého typu informací. Každá buňka má hlavičku o délce 5 bytů, která nese identifikační, směrovací a řídící informace. Obsah hlavičky se při každém průchodu ATM přepínačem mění. Malá velikost a pevná délka ATM buňky umožňuje optimalizaci technického vybavení přepínacích matic, takže lze minimalizovat zpoždění buněk. Přenosová rychlost dosahuje teoreticky až 2,4 Gb/s, v praxi se používá rychlost do 622 Mb/s. Typickým přenosovým médiem jsou optická vlákna, podporovány jsou však i UTP a koaxiální kabely.

Technologie ATM podporuje virtuální sítě, je schopna garantovat šířku pásma, je schopna spolupracovat s ostatními síťovými technologiemi a v době své největší slávy poskytovala nejvyšší přenosovou rychlost při minimálních topologických omezeních K nevýhodám je třeba řadit zejména vysokou cenu a dále fakt, že ATM je poměrně složitou technologií.

V rámci evropského projektu TEN-155 byla vytvořena a v současné době je provozována evropská páteřní síť o rychlosti 155 Mb/s založená právě na technologii ATM. Na tuto páteřní síť je připojena i Česká republika.

11 BEZDRÁTOVÉ SÍTĚ

Bezdrátové sítě (*wireless networks*) lze podle používaného způsobu přenosu rozdělit na rádiové, radioreléové a družicové, do této kategorie se řadí i sítě využívající optický přenos na přímou viditelnost s využitím IR světelného paprsku (optické směrové spoje).

Jestliže dříve byla základním požadavkem síťové komunikace rychlost, v dnešní době se k tomuto kritériu připojuje mobilita. Propojení jednotlivých stanic elektromagnetickými vlnami poskytuje větší pružnost při připojování stanice do sítě a podporuje pohyblivost koncových uživatelů a jejich přenosných počítačů. Využití bezdrátové technologie je zvlášť vhodné pro dočasné pracovní prostory, oblasti s obtížným přístupem ke kabelům, pro tovární prostory, skladové prostory apod. Technologie v této oblasti se rychle vyvíjejí, jedná se např. o standardy IEEE 802.11, HiPerLAN, Bluetooth a různé typy optických směrových spojů.

Bezdrátové řešení není zdaleka bez problémů. Rádiové vysílání je náchylné na rušení, a to všemi zařízeními, která mohou na příslušných kmitočtech pracovat. Může také dojít k nežádoucímu překrytí dvou nebo více takových lokálních sítí. Bezpečnosti vysílání je třeba věnovat prvořadou pozornost a svoji roli v kvalitě komunikace hraje i vzdálenost komunikujících zařízení. Přestože existuje schválená mezinárodní norma pro tento typ sítí, je zvolený kmitočet lokální sítě potřeba porovnat s pravidly stanovenými pro používání příslušných pásem. Regulace a přidělování kmitočtů se liší u jednotlivých států. Jako nevýhoda je vnímána i (zatím?) nízká přenosová rychlost, omezený dosah, nižší kvalita vlivem rušení a omezená podpora jiných než datových služeb.

Mezi výhody bezdrátových sítí lze zařadit minimální nároky na pokládku, překládku a údržbu kabelových tras, podporu mobilních uživatelů a možnost zcela náhodné topologie počítačové sítě.

11.1 Architektura technologie IEEE 802.11

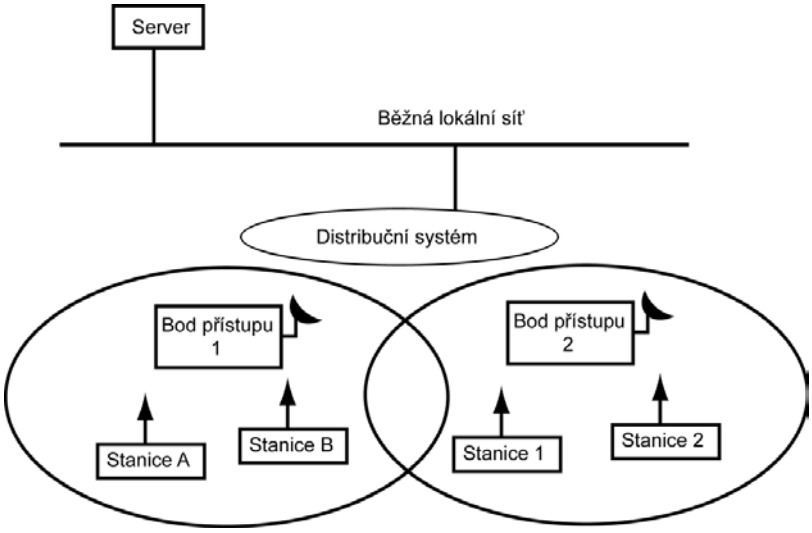
Podvýbor IEEE 802.11 zahájil svoji práci na funkčních požadavcích, specifikaci požadované šířky pásma a protokolu řízení přístupu k bezdrátovému přenosu v roce 1990. V roce 1997 byl schválen návrh normy IEEE 802.11 specifikující příslušnou podvrstvu MAC a tři typy fyzické vrstvy bezdrátových lokálních sítí (tradičně se využívá podvrstva LLC). Jedná se o FHSS (1 Mb/s), DSSS (1 a 2 Mb/s) a sítě s přenosem v infračerveném pásmu. Později došlo k rozšíření o specifikaci vyšších rychlostí (až 11 Mb/s pro DSSS).

Topologie bezdrátových sítí se zásadně liší od topologie klasických sítí. Stanice bezdrátové lokální sítě vybavená příslušným adaptérem může pracovat ve dvou konfiguracích:

- **Nezávislá konfigurace** (ad hoc) – stanice mezi sebou komunikují přímo a není potřeba instalovat žádnou podpůrnou infrastrukturu. Taková konfigurace je mimořádně výhodná pro náhodná uspořádání, ale nehodí se pro rozsáhlé sítě.
- **Konfigurace s distribučním systémem** (DS) – jsou komplikovanějším případem bezdrátových sítí. Stanice komunikují s distribučním systémem prostřednictvím bodu

přístupu (obr. 11.1). Přístupový bod je vlastně komunikačním mostem vybaveným patřičným transceiverem a řídící úlohou, zajišťuje také propojení bezdrátové sítě s okolními sítěmi (případně s jinou základnovou stanicí). Počet přístupových bodů souvisí s požadovaným rozsahem příslušné sítě. Každá stanice si vybere jeden přístupový bod a s ním udržuje relaci. Norma definuje způsob řešení přesunu stanice z dosahu jednoho přístupového bodu do pole působnosti jiného (roaming).

Distribuční systém si lze představit jako páteřní síť, která může být realizována nejrůznějším způsobem. Norma definuje jen bezdrátové rozhraní, tj. rozhraní mezi stanicemi a přístupovými body. S distribučními systémy se rozsah lokální sítě rozšiřuje. Vnitřní uspořádání distribučního systému může být řešeno běžnou drátovou lokální sítí připojenou prostřednictvím mostu.



Obr. 11.1: Bezdrátová lokální síť s distribučním systémem

V bezdrátové lokální síti není řešena možnost směrování přes několik skoků, tedy mezilehlých systémů. Každá stanice může komunikovat buď přímo s jinou stanicí (v obou konfiguracích) nebo může stanice vysílat rámce přístupového bodu, s nímž navázala relaci.

Každé rádiové zařízení sestává ze dvou základních částí. První z nich je rádiový modem, který se stará o vlastní modulaci a vysílání dat na dané frekvenci a o příjem rádiového signálu. Hlavními charakteristikami modemu jsou pracovní frekvenční pásmo, přenosová rychlost, typ modulace a výstupní výkon. Druhým základním prvkem je MAC řadič, který má za úkol řízení přístupu k médiu, předávání informací na výstup a zajištění spolupráce vlastního rádiového zařízení s počítačem přes společnou sběrnici. Parametry fyzické vrstvy určuje především modem a linkové vrstvy MAC řadič.

Pro komunikaci se využívá rádiových vln v kmitočtovém pásmu 2,4 GHz. Jde o bezlicenční pásmo ISM (průmyslové, vědecké a lékařské). Vedle rádiových vln se používají také infračervené paprsky. Bezdrátové lokální sítě poskytují rychlost 1 Mb/s (volitelně 2 Mb/s) a mohou být řešeny jedním ze tří definovaných způsobů:

1. Rádiové rozložené spektrum v přímém pořadí **DSSS**. Rozložené spektrum znamená, že se energie rádiových vln rozkládá do širokého kmitočtového pásma tak, že se každý datový bit určený k přenosu moduluje pomocí jedenáctibitového kódu (Barkerova posloupnost). V přijímači je signál získán z přijatého rozprostřeného signálu jeho demodulací stejným kódem. Tento způsob zpracování se používá z důvodu co největšího rozložení původního signálu, při kterém klesá náchylnost k rušení z jiných rádiových zařízení sdílejících stejné pásmo. Vhodnou volbou příslušného převodního kódu lze snadno instalovat i několik sítí vedle sebe, aniž by docházelo k vzájemnému rušení. Pro přenosovou rychlost 2 Mb/s je výsledný signál rozprostřen při použití jedenáctibitové modulace na 22 MHz. Objeví-li se úzkopásmové rušení, nebude jeho vliv na rozprostřený signál znatelný, protože úroveň užitečného signálu je mnohem vyšší. Procedura kódování je výpočetně náročná, proto jsou modemy DSSS obecně komplikovanější a vyžadují použití výkonných signálových procesorů. Pracují však na konstantním kmitočtu, což zjednodušuje práci MAC řadiče. V pásmu ISM jsou tři nepřekrývající se pásma. Použití jednoho kódu pro všechny signály snižuje možnost použití více rádiových sítí v jedné lokalitě bez nebezpečí snížení kvality přenosu.
2. Rádiové rozložené spektrum s přeskakováním mezi kmitočty **FHSS**. Tento přístup je velmi podobný předchozímu typu rozložení původní energie, tentokrát však mezi různé kmitočty. Obvykle se na jednom kmitočtu přenese několik datových bitů, pak se pokračuje na dalším přiděleném kmitočtu. Rušení se tak minimalizuje krátkou dobou, po kterou systém vysílá na daném kmitočtu. Kmitočet se změní minimálně 2,5 krát za vteřinu (změna kanálu každých 20 - 400 ms), takže je nepravděpodobné, že by dva vysílače současně využívat tutéž frekvenci. Navíc jenom oprávněný příjemce zná posloupnost kmitočtů, na nichž se vysílá. Přeskakování kmitočtů umožňuje efektivní využití vysílacího spektra pro 22 lokálních sítí vedle sebe. Každá z nich má vlastní pořadí kmitočtů pro vysílání prostřednictvím 79 kanálů o šířce 1 MHz, na nichž se vysílá. Tento typ bezdrátové komunikace poskytuje větší počet kanálů než DSSS, proto je vhodný pro prostředí s vyšší hustotou vysílání a vyšší náchylností k rušení. Změna pracovní frekvence však zvyšuje složitost MAC řadiče, který musí být schopen nalézt signál s proměnnou frekvencí. Složitější je i struktura záhlaví přenášených paketů, což omezuje efektivní přenosovou rychlost.
3. Použití infračervených paprsků – umožňuje dvě rychlosti přenosu modulací 16-PPM, respektive 4-PPM. Pro tyto systémy se používá vlnová délka od 850 do 950 nm s maximálním výkonem 2 W. Infračervené paprsky se mohou vyslat koncentrovaně přímo k příjemci nebo rozptýleně, kdy se paprsky vyšlou různými směry a odrazem od stěn se dostanou k cíli.

Komunikující stanice v rádiové lokální síti se musí předem dohodnout na použité přenosové rychlost 1 Mb/s nebo 2 Mb/s, které mohou být sdílené jediným kanálem. Rádiové lokální sítě mohou dosáhnout průměru až 100 m, ve vnitřním prostředí přitom záleží na topologii. Infračervená varianta lokální datové komunikace je zásadně omezena na souvislý prostor, neboť infračervené paprsky se odráží od překážek. Řešení na bázi infračerveného provozu je cenově méně výhodné.

Uživatelé požadují stále vyšší datové rychlosti, čehož lze dosáhnout použitím širšího kmitočtového pásma. V případě omezeného kmitočtového pásma (1 MHz pro FHSS) je nutné použít složitější modulaci.
Jako protokol řízení přístupu ke sdílenému médiu se využívá protokol mnohonásobného přístupu s nasloucháním nosné a vyvarování se kolizí CSMA/CA. Náhodný přístup CSMA/CD použitý u standardu Ethernet je u rádiových systémů nepraktický, protože rádiové systémy nejsou schopny detekovat kolize nasloucháním kanálu při vlastním vysílání. Zatímco Ethernet je náchylný ke kolizím těsně po uvolnění média, protože se všechny stanice snaží vyslat čekající rámce, předchází CSMA/CA takovému krátkodobému přetížení přenosového média. Po určité povinné době od uvolnění kanálu si stanice náhodně zvolí svoji vlastní dobu čekání, která je násobkem dohodnutého časového úseku. Pokud skutečně nezačnou vysílat dvě stanice ve stejný okamžik, jedna detekuje rádiový signál druhé a odloží svoje vysílání. Jelikož je soutěžení založeno na náhodně zvolené časové prodlevě, statisticky mají všichni účastníci stejnou možnost přístupu k přenosové trase. Rozdělení časové základny do slotů bylo zvoleno v důsledku konečného času nutného k přepnutí mezi vysílacím a přijímacím režimem. Vysílání může být zahájeno pouze na začátku slotu, který trvá 50 μs u FHSS a 20 μs pro DSSS. Tímto způsobem se výrazně snižuje nebezpečí kolizí za cenu pomalejší komunikace. Detekce obsazeného kanálu se provádí měřením signálu na anténě. Pokud je jeho hodnota menší než specifikovaný práh, je kanál považovaný za volný. Protože pro bezdrátové vysílače neexistuje žádná možnost detekovat kolize vzniklé ve vzduchu průnikem rádiových vln, využívá se pro detekci kolizí systém potvrzování. Existencí nebo výpadkem potvrzení na úrovni MAC je stanice vyrozuměna o vzniklé chybě v přenosu. Protokol navíc umožňuje přednostní vysílání pro rámce s nejvyšší prioritou či časové rámce, které mají možnost být vyslány před vypršením jinak povinné doby po konci vysílání rámce.

V roce 1999 byly definovány organizací IEEE standardy 802.11a a 802.11b. Hlavní hybnou silou pro jejich definici byly firmy Lucent Technologies a Intersil Corp. Vzorem pro přijetí standardů byl Ethernet, který je definován pro přenosové rychlosti 10, 100 a 1000 MB/s pro optická i metalická vlákna. Standard 802.11b je definován v pásmu ISM pro frekvenci 2,4 GHz s použitím rozloženého spektra v přímém pořadí. Podporuje rychlosti přenosu 5,5 a 11 Mb/s a v dnešní době splňuje jeho požadavky většina dostupných zařízení.

Standard 802.11a pracuje v pásmu UNII na frekvenci 5 GHz s použitím rozloženého spektra s přeskakováním mezi kmitočty. Přenosová rychlost je definována v několika úrovních 6, 12, 24, 36, 48 a 54 Mb/s.

Nejnovější standard, který vznikl díky kompromisu mezi dvěma vedoucími představiteli výrobců obvodů pro rádiová zařízení (Intersil, Texas Instruments) pracuje v pásmu ISM na frekvenci 2,4 GHz s datovou propustností 54 Mb/s. Zařízení, která splňují tuto normu by měla být zpětně kompatibilní se zařízeními standardu 802.11b.