Lokální sítě

Jan Janeček, Martin Bílý

Prosinec 2003

Předmluva

Tento text je učební pomůckou pro studenty denního studia Elektrotechnické fakulty ČVUT, kteří si zapsali předmět Lokální sítě. Jeho studium předpokládá základní znalosti z přenosu dat, technologie přepojovacích sítí a operačních systémů, v některých partiích je užitečná znalost chování systémů hromadné obsluhy.

Text je směrován jako přehled principů současných technologií využívaných v lokálních sítích, od metod přístupu, přes komunikační protokoly po současná řešení systémové podpory aplikací. Rozsah problematiky se sice poněkud projevil v nemožnosti věnovat se na omezeném prostoru podrobnostem jednotlivých technologií, zde však můžeme čtenáře odkázat na standardy.

Text vychází ve druhém vydání. Od doby, kdy vyšla jeho prvá verze, tedy od roku 1996 došlo v technologii lokálních sítí k podstatným změnám. Převahu získala technologie Ethernet, i když pod tímto označením už zdaleka nerozumíme jen sítě opírající se o sdílené médium s metodou přístupu CSMA/CD. Rozvoj nastal v oblasti rádiových lokálních sítí. Úprava textu tyto změny respektuje, a zahrnuje i některé technologie, které dosud nejsou v konečné fázi normalizace a kde ještě může dojít ke změnám.

Myslíme si, že na toto místo patří i jazyková poznámka. Náš text se zabývá oblastí, ve které se objevuje řada nových termínů v jazyce současné techniky - v angličtině. Při psaní tohoto textu jsme se snažili respektovat pravidla a duch češtiny. Tam, kde existuje zavedený, nebo dokonce standardizovaný český odborný termín, užíváme ten a vyhýbáme se oborovému slangu (např. používáme standardizovaný termín *slabika* a *oktet*, nebo kde nemůže dojít ke dvojznačnosti termín *znak*, tam kde dnes řada publikací používá dost nehezký termín *bajt*). Tam, kde alespoň částečně akceptovaný český termín neexistuje, a kde doslovný překlad anglického termínu není dostatečně výstižný a/nebo přetížení českého termínu z nějakého důvodu není výstižné nebo by vedlo ke dvojznačnosti, jsme raději zůstali u původních termínů anglických (pochopitelně bez pokusů o problematický fonetický zápis, české skloňování nebo dokonce časování) a u zkratek (kterými ostatně specifikace v oblasti počítačových komunikací silně hýří). Z čistě praktických důvodů (využitelnost pro výuku v angličtině) jsou anglické termíny použity v obrázcích.

Autoři se o zpracování textu podělili takto: kapitolu 17 napsal Ing. Martin Bílý, ostatní kapitoly doc. Jan Janeček. Chceme poděkovat všem, kteří nám s přípravou textu pomohli, poskytli potřebné materiály a firemní informace, zvláště Ing. Martinovi Červenému, jehož připomínky přispěly k přehlednosti a užitečnosti předkládaného materiálu.

Text se proti prvému vydání v řadě kapitol změnil a autoři uvítají poznámky pečlivého čtenáře k jeho formě a obsahu.

Praha, prosinec 2003 autoři

Obsah

1. Úvod

Pojmem *lokální síť* zpravidla označujeme komunikační systém schopný propojit desítky až stovky počítačů na vzdálenost stovek metrů až jednotek kilometrů. Lokální sítě jsou využívány v administrativě, v inženýrských systémech (CAD, CAE) a v technologickém řízení.

Bez lokálních sítí si současné nasazení kvant osobních počítačů nelze představit. Zatímco rozsáhlé počítačové sítě jsou nejužitečnější v těch aplikacích, kde zajišťují přenosy dat (elektronická pošta, sběr dat), typickou aplikací pro lokální sítě je zajištění přístupu k systémovým prostředkům, které jsou spravovány jen některými počítači sítě (označujeme je obvykle jako *servery*) a využívány počítači ostatními (označujeme je obvykle jako *uživatelská* nebo *klientská pracoviště*). Takovými systémovými prostředky jsou nejčastější drahá zařízení (rychlé a speciální tiskárny), velké a sdílené soubory a databáze.

Lokální počítačové sítě jsou vhodným prostředkem i tam, kde je třeba rozložit výpočetní kapacitu tak, aby poskytované služby byly snáze dostupné, aby bylo možné specializovat jednotlivé počítače na konkrétní funkce a abychom zvýšili spolehlivost výpočetního systému. Aplikacemi jsou měřící a sledovací systémy ve vědě a zdravotnictví, řízení technologických procesů v průmyslu a automatizace administrativy.

Problematika lokálních sítí zahrnuje řadu oblastí. Patří sem vytvoření vlastního fyzického spoje mezi počítači, tedy technologie kabelových propojení a komunikačních řadičů (karet). Obvykle se rozhodujeme mezi několika řešeními, která odpovídají zavedeným standardům. Hrubému přehledu technologií, jejich vlastnostem, prvkům a možnostem spolupráce je věnována první část tohoto textu.

S potřebou rozumět komunikačním protokolům se setká každý, kdo bude nucen implementovat aplikační program nebo službu, která komunikačních schopností lokální sítě využívá nad rámec funkcí souborového serveru. Popis komunikačních protokolů, se kterými se v lokálních sítích setkáváme, je obsahem druhé části.

A konečně, i pro běžného uživatele počítačů má svůj význam přehled služeb, která mu síť poskytne. V nejjednodušší formě jde o rozšíření operačního systému jeho pracoviště o přístup ke sdíleným souborům a zařízením serverů. Modernější systémy pro lokální sítě podporují rozklad takových aplikací jako je přístup k databázím nebo elektronická pošta formou označovanou jako *Client-Server*. Přehledu současných systémů podporujících provoz lokálních sítí a vývoj síťových aplikací je věnována závěrečná část textu.

Lokální sítě za krátkou dobu svého rozvoje prošly řadou proměn. Klasické sdílení jediného přenosového kanálu je u lokálních sítí opírajících se o kabeláž (elektrickou nebo optickou) stále více nahrazováno *přepojováním*. Jako přenosové médium jsou stále častěji využívána *optická vlákna*. S rozvojem přenosných počítačů (a o počítačovou techniku se opírajících přenosných zařízení) roste význam *rádiových lokálních sítí*. Mění se požadavky kladené na vlastnosti lokálních sítí; nejen že roste množství vyměňovaných dat mezi zvyšujícím se počtem počítačů, ale zvyšují se i požadavky na kvalitu komunikačních služeb (isochronní provoz, rozumná degradace služeb při přetížení sítě). Klasické technologie jsou přizpůsobovány novým požadavkům tak, že z nich často zbývá pouhé rozhraní koncových účastníků; jako příklad může sloužit rozhraní Ethernetu, využívané technologiemi širokopásmových sítí (CATV) nebo přístupovou technologií EFM (Ethernet for the First Mile). Takový přístup, spolu s využíváním formátů Ethernetu i na vysokorychlostních dálkových spojích gigabitového a desetigigabitového Ethernetu, usnadňuje *integraci* lokálních sítí a digitálních spojů sítí rozsáhlých a globálních. Moderní řešení lokálních sítí dovolují oddělit vlastní komunikační systém od uživatelské struktury sítě, nastupují řešení označovaná jako *virtuální lokální sítě*.

2. Architektura, topologie a média

Lokální sítě se od sítí přepojovacích liší hlavně tím, používají pro propojení stanic vícebodových kanálů. U těchto kanálů hraje, vzhledem k jejich sdílení vzdálenými stanicemi, podstatnou roli zpoždění signálu při průchodu médiem.

Rozlehlost

Přívlastek *lokální* vyjadřuje také skutečnost, že síť pokrývá malé území. Rozměry sítě přitom nejsou omezené našimi potřebami, ale teoretickými vlastnostmi přístupových metod, které lokální sítě používají.

Budeme-li se snažit vyjádřit *rozlehlost* sítě numericky, můžeme ji definovat jako poměr a mezi zpožděním signálu τ a střední dobou potřebnou pro vyslání jednoho paketu t_0 při dané přenosové rychlosti

$$a = \frac{\tau}{t_0} \ .$$

Pro sítě, které označujeme jako *rozlehlé*, platí $a > 1$. Sítě, které budeme označovat jako *lokální* (nebo *soustředěné*), mají $a < 1$. Přenosové médium je využito v daném okamžiku pro přenos jediného paketu, v rozlehlých sítích může být média využito pro přenos více paketů současně.

Obrázek 2.1: Přenos v soustředěné a rozlehlé síti

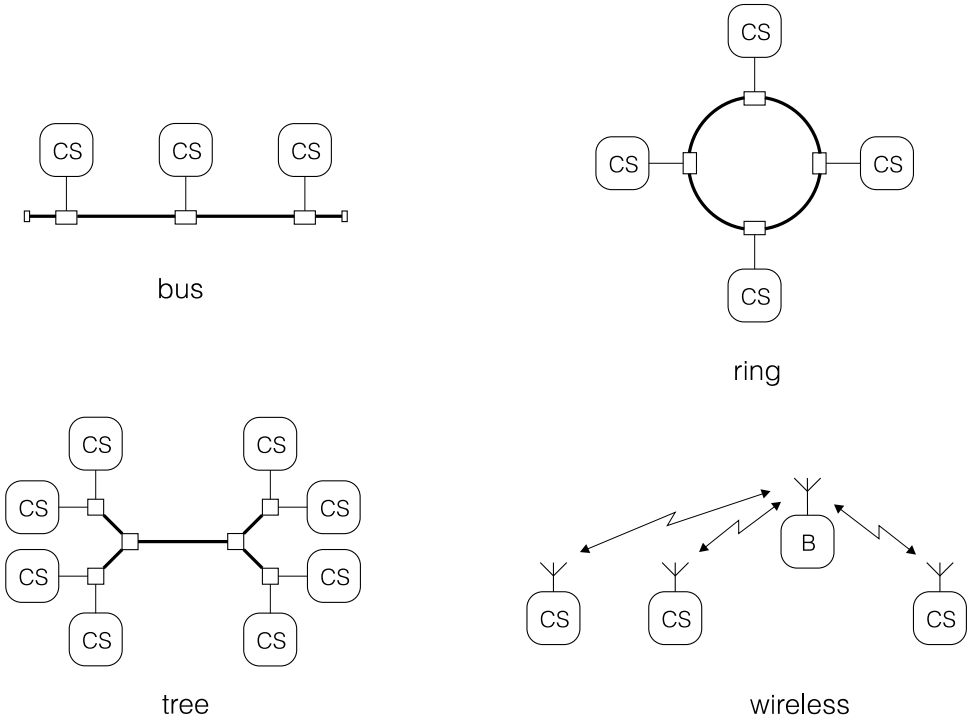
Mezi sítě, které takto charakterizujeme jako rozlehlé, patří i sítě s vysokou rychlostí přenosu a středními překonávanými vzdálenostmi (optické městské sítě). Soustředěné sítě zahrnují běžné sítě lokální a sítě rádiové (pro jejich malou přenosovou rychlost). Pro řadu metod řízení musíme zajistit velmi malou hodnotu parametru a, typicky $a \ll 0.1$.

2.1 Topologie

Topologií se klasické lokální sítě liší od rozsáhlých počítačových sítí. Ty se opírají o přepojování paketů nebo zpráv – postupné předávání zpráv mezi uzly po dvoubodových spojích (technika *"store-and-forward"*) a jsou *polygonální*. Klasické lokální sítě využívají přímého propojení komunikačních stanic sdíleným kanálem, signál vyslaný jednou ze stanic je přijímán ostatními stanicemi sítě. Takové lokální sítě jsou někdy označovány jako *"broadcast"* sítě. Volba topologie má vliv na řadu vlastností lokální sítě :

- rozšiřitelnost – možnost a snadnost doplňování stanic do existující sítě,
- rekonfigurovatelnost – možnost modifikovat síť při závadě komponenty nebo spoje,
- spolehlivost – odolnost sítě proti výpadkům komponent nebo spojů,
- složitost obsluhy a správy,
- výkonnost – využití přenosové kapacity média, zpoždění zpráv.

V praxi se setkáváme s topologií sběrnicovou, hvězdicovou, stromovou a kruhovou, některé sítě jednotlivé topologie kombinují (např. ARCNet nebo dnešní Ethernet).



Obrázek 2.2: Topologie lokálních sítí

Sběrnice

Základním prvkem sběrnicové sítě je úsek přenosového média – *segment* sběrnice, ke kterému jsou připojeny stanice sítě. Přenosovým médiem je nejčastěji koaxiální kabel nebo symetrické vedení (kroucený dvoudrát). U optických vláken je realizace odboček obtížná. Vlastnosti sběrnicové sítě lze shrnout do těchto bodů:

- pasivní médium,
- snadné připojování stanic,
- odolnost proti výpadkům stanic.

Pro řízení sběrnicových sítí je využívána řada deterministických i nedeterministických metod, které využívají faktu, že signál vysílaný jednou stanicí je přijímán ostatními stanicemi jen s velmi malým zpožděním.

Hvězda

Stanice sítě jsou připojeny k centrálnímu uzlu samostatnými linkami. Centrální uzel označovaný jako *hub* (v překladu "střed loukoťového kola") signál přicházející z jedné linky rozděluje do ostatních linek hvězdy. Rozlišujeme *pasivní hub*, ve kterém je signál pouze dělen (odporovým děličem), a *aktivní hub* (vícevstupový opakovač), ve kterém je přijatý signál upravován tak, aby měl na výstupních linkách požadovanou úroveň a časování. Vlastnosti topologie *hvězda* lze shrnout takto:

- dvoubodové spoje mezi stanicemi a centrálním uzlem lze snadno realizovat,
- síť je odolná proti výpadku jednotlivých stanic a linek,
- síť je citlivá na poruchu centrálního uzlu.

Sítě s topologií hvězda, jak jsme si ji právě popsali, se tím, že signál jedné stanice mohou přijímat současně stanice ostatní, blíží sítím sběrnicovým a lze u nich použít i obdobné metody řízení. Topologie hvězda s pasivním centrálním uzlem často nacházíme u optických sítí.

Strom (hvězdice)

Stromová topologie je přirozeným rozšířením topologie typu *hvězda*. Setkáváme se s ní u širokopásmových sítí a u sítí využívajících pro přenos světlovody. Vlastnosti stromové topologie jsou podobné jako u sítí typu *hvězda* :

- odolnost sítě proti výpadkům jednotlivých stanic a linek,
- citlivost na výpadky uzlů (hubů),
- snadná rozšiřitelnost,
- dvoubodové spoje.

Lokální stromové/hvězdicové sítě používají podobných metod řízení jako sítě sběrnicové. U přístupových sítí převládá deterministická rezervace kanálu realizovaná centrálním prvkem.

Kruh

U kruhových sítí jsou komunikační stanice propojeny spoji, které jsou využívány pouze jednosměrně. Signál vyslaný jednou stanicí je postupně předáván ostatními stanicemi kruhu (základní prvkem stanice je krátký posuvný registr) a po oběhu sítí se vrací ke stanici, která jej odeslala. Vlastnosti kruhových sítí lze shrnout do těchto bodů:

- dvoubodové jednosměrné spoje lze snadno realizovat i na světlovodech,
- v síti lze kombinovat různá média (pro krátké spoje elektrická vedeni, pro dlouhé spoje světlovody),
- síť je citlivá na výpadek libovolného prvku (stanice nebo spoje).

U kruhových sítí jsou pravidelně používány deterministické metody řízení, zvýšení spolehlivosti lze dosáhnout použitím dvou protisměrných kruhů nebo kombinací kruhové topologie s přepojováním.

Uvedené dělení sítí na sítě sběrnicové, stromové a kruhové je opřeno o *elektrickou topologii* (signálovou topologii), tedy o způsob vzájemného propojení stanic. Z hlediska vlastností sítě má velký vliv i *topologie fyzická* (způsob vedení kabelů) a *topologie logická* (metoda spolupráce stanic u deterministických metod).

2.2 Přenosová média

Jedním z důležitých prvků, který charakterizuje konkrétní lokální síť, je použité přenosové médium. Kromě malého počtu historických sítí, které používaly paralelní přenos po vícevodičových kabelech (např. sběrnicová síť Cluster One nebo kruhová síť Twentenet), jde u naprosté většiny dnešních sítí o přenos sériový. U některých technologií ještě najdeme nesymetrické vedení (*koaxiální kabel*), většina dnešních technologií se opírá o symetrické vedení (*kroucený dvoudrát – twisted pair*). Řada sítí se opírá o optická vlákna a ta jsou alternativním médiem i pro klasické technologie. Významnou pozici získavají lokální sítě využívající vysokofrekvenčních rádiových a vzdušných světelných spojů.

Koaxiální kabely

Nesymetrická vedení (koaxiální kabely) dovolují využití pásma 0 – 150 Mhz v základním pásmu (kódovaný datový signál) a pásma 50 – 750 MHz přeloženém pásmu (modulovaný signál). V základním pásmu lze dosáhnout přenosové rychlosti v rozmezí 1 – 50 Mb/s, v přeloženém pásmu lze vytvořit skupinu přenosových kanálů s přenosovou rychlostí až 40 Mb/s (pro kanál s televizní šířkou pásma 6 MHz). Při přenosu v základním pásmu omezují elektrické vlastnosti vedení překlenutou vzdálenost na stovky metrů, proto jsou často používány drahé speciální kabely (jako je tomu např. u sítě Ethernet 10BASE5). Přeložené pásmo lze využít pro přenos

na kilometrové vzdálenosti, podstatnou výhodou je možnost použít kabely a další prvky určené pro kabelovou televizi. Koaxiální kabel byl po dlouhou dobu typickým médiem lokálních sítí, má relativně dobrou odolnost proti rušení. Setkáme se s několika typy kabelů, které se liší charakteristickou impedancí (50 Ω, 75 Ω a 93 Ω), útlumem, ale i dalšími vlastnostmi, které ovlivňují jeho použitelnost.

Symetrická vedení – UTP,STP

Symetrické vedení ve formě *krouceného dvoudrátu* (twisted pair), jak ho známe z telefonních kabelů, je nejlevnějším přenosovým médiem. Ve většině případů jde o stíněný (*STP – Shielded Twisted Pair*) nebo nestíněný (*UTP – Unshielded Twisted Pair*), jednoduchý nebo dvojitý dvoudrát, který dovoluje bez problémů přenášet signály rychlých sítí, jako jsou sitě Ethernetu 100BASE-T, 100VG-AnyLAN, FDDI nebo ATM, na vzdálenost 100 m, přenosové rychlosti jsou zde až 155 Mb/s. Symetrické vedení je používáno pro přenos kódovaných signálů v základním Pásmu. V průmyslových aplikacích se často setkáme s použitím napěťových úrovní odpovídajících standardním rozhraním RS-422 EIA a RS-485 EIA, varianty sítí Ethernet, 100VG-AnyLAN, FDDI a ATM mají své vlastní standardy kódování, časování a úrovní datového signálu.

Vlastnosti kabelů s kroucenými páry jsou definovány normami, nejpoužívanější standard *EIA/TIA 586* (z roku 1991) definuje vlastnosti kabelů UTP se čtyřmi dvoudrátovými vedeními. Dělí je podle mezního přenášeného kmitočtu (pro zvuk a obraz) nebo přenosové rychlosti do následujících kategorií (*UTP Category*):

3 - do 16 MHz nebo 10 Mb/s, je označován jako Voice Grade Cable,
4 - do 20 MHz nebo 20 Mb/s,
5 - do 100 MHz nebo 100 Mb/s, je označován jako Data Grade Cable.

V současné době jsou používány téměř výlučně kabely odpovídající UTP Cat.5, starší instalace používaly kabely UTP Cat.3. Moderní technologie dovolují vyrábět kabely, které překračují parametry vyžadované pro kategorii 5 (zadaný rozdíl mezi přeslechem na blízkém konci em NEXT a útlumem na mezní frekvenci). Takové kabely jsou označované jako kabely Cat.5e nebo Cat.5+.

Pro vyšší kvalitativní třídy kabelů byly navrhovány další standardy - Cat.6 a Cat.7. Frekvenční limity měly být podstatně vyšší - mezní frekvence 200 Mhz pro Cat.6 na kabelech UTP/FTP a 600 Mhz pro Cat.7 na kabelech STP. Vysoké nároky na řadu nových parametrů a citlivost na instalaci ukázaly, že v této oblasti již metalická vedení nejsou schopna konkurovat optice.

Poněkud odlišným standardem pro vlastnosti kabelů je firemní *norma IBM*, ta definuje vlastnosti symetrických kabelů *STP* používaných v sítích IBM Token Ring. Pro toto použití jsou definovány jejich parametry, firemní standard dělí kabely na třídy (*Type*):

Type 1 - dva dvoudráty (0.6 mm), samostatně stíněné,
Type 2 - jako Type 1, navíc čtyři nestíněné dvoudráty pro telefon,
Type 3 - pro telefon, dva nestíněné dvoudráty,
Type 5 - světelná vlákna 100/140 μm,
Type 6 - jako Type 1, ale slabší vodiče (0.4 mm),
Type 8 - jako Type 6, ale v plochém provedení.

Víceméně raritou jsou sítě, které pracují s nižší přenosovou rychlostí, v oblasti 9.6 – 115.2 kb/s. Takové sítě jsou však velice snadno realizovatelné bez speciálních komunikačních řadičů; opírají se o použití běžného sériového rozhraní podle RS-232C EIA (V.24 CCITT), kterým je dnes vybaven prakticky každý osobní počítač. Dovolují propojit osobní počítače na vzdálenost jednotek metrů (hvězdicové sítě EasyLAN, propojení počítačů Laplink).

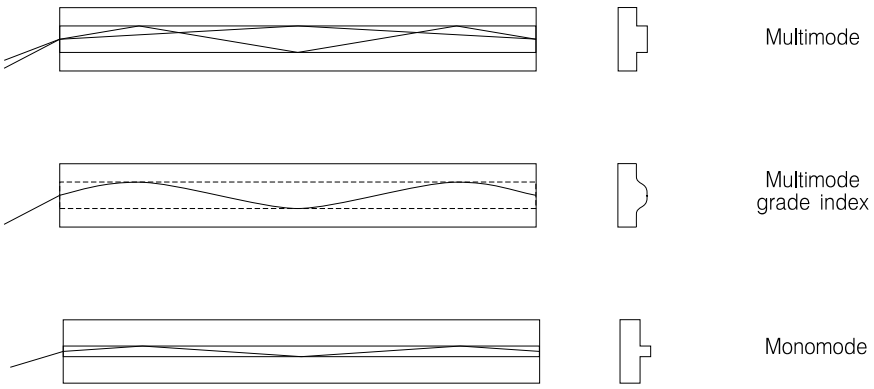
Strukturovaná kabeláž

V současnosti používané kabely *UTP Cat.5* dovolují přenos signálu do kmitočtu 100 MHz. Kabely UTP se stávají i alternativou ke kabelům *STP* (Shielded Twisted Pair) pro kruhové sítě IBM Token Ring. Čtyřpárové kabely se společným stíněním označované jako *FTP* (Foiled Twisted Pair – fólií stíněné zkroucené páry) nebo *SFTP* (Screened Foiled Twisted Pair – FTP s ochranným opletením) odolnější proti vlivu vnějšího rušení a omezující vyzařování přenášených signálů.

Kabely UTP (a jejich modifikace FTP a SFTP) jsou dnes považovány za univerzální materiál pro kabeláže, které kombinují přenos dat s přenosem telefonních signálů (analogových i digitálních) a videosignálů. Konkrétní lokální síť lze vystavět poměrně jednoduše s využitím vedení takové univerzální *strukturované kabeláže* příslušným propojením na konektorových panelech (*patch-panelech*) v uzlech její většinou hvězdicové struktury.

Světlovodná vlákna

Světlovodná vlákna využívají infračervené a viditelné oblasti světelného spektra pro přenos dat rychlostmi do 10 Gb/s na vzdálenost jednotek až desítek kilometrů. Výhodou optických vláken je vysoká přenosová kapacita při nízké ceně média a velká odolnost proti rušení, nevýhodou je vysoká cena prvků rozhraní, konektorů a náročné spojování kabelů. S optickými vlákny se setkáváme v lokálních sítích s kruhovou nebo stromovou topologií.



Obrázek 2.3: šíření signálu v optickém vlákně

Mnohavidová optická vlákna jsou tvořena vnitřním *jádrem* (*Core*) o průměru do 100 μm a vnějším *obalem* (*Cladding*) z materiálu o nižším indexu lomu. Na rozhraní obou materiálů dochází k poměrně dokonalému odrazu přenášeného signálu. Materiálem jádra je převážně speciální sklo, obalem bývá sklo nebo plastická hmota. V technologických aplikacích jsou používána vlákna s plastovým jádrem i obalem. Vlákna jsou označována jako mnohavidová, protože světelné paprsky se médiem šíří ve více videch charakterizovaných různými úhly odrazu. Takových diskrétních hodnot jsou u mnohavidových vláken tisíce. Důsledkem odlišných úhlů odrazu je rozdíl v absolvované délce cesty paprsku vláknem a z toho vyplývající rozptyl světelného výkonu v čase na výstupu z vlákna. Mluvíme o *vidové disperzi*, ta je hlavním limitem překlenutelné vzdálenosti. Limit vzdálenosti je uváděn jako součin délky vlákna a kmitočtu (MHz.km, GHz.km).

V praxi rozlišujeme historická mnohavidová vlákna se skokovou změnou indexu lomu a modernější vlákna *gradientní*, u nichž je změna indexu lomu plynulá. Výhodou gradientních vláken je zvýšení podílu energie přenášené módy s většími úhly odrazu, zachování většího průměru jádra usnadňuje propojování vláken (ve srovnání s vlákny jednovidovými). Gradientní vlákna s průměrem 65/125 μm používaná v lokální síti FDDI mají větší vidovou disperzi než vlákna 50/125 μm používaná v telekomunikační technice a dnes běžná v optických variantách Eth-

	50/125	62.5/125	100/140	
NA	0.23	0.275	0.29	
Min. attenuation				
850 nm	2.6	3.4	3.7	dB/km
1300 nm	0.48	0.63	0.67	dB/km
Bandwidth	1400	1000	500	MHz.km

Obrázek 2.4: Parametry mnohavidových vláken

ernetu. Ve starších sítích IBM Token Ring se můžeme setkat s vlákny 100/140 μm (IBM je označuje jako kabel typu 5). Porovnání teoretických parametrů mnohavidových vláken (útlum pro používané vlnové délky 850 a 1300 nm a omezení na dosažitelnou šířku pásma danou vidovou disperzí) uvádí obr. 2.4. Výběr používaných vlnových délek je omezen vlastnostmi materiálu vlákna, vlnové délky 850, 1300 a 1550 nm odpovídají minimům útlumu v materiálu jádra.

Jednovidová optická vlákna se vyznačují tím, že se při šíření světelného signálu uplatňuje jediný mód (nebo chceme-li být přesní, jde o dva módy lišící se polarizací). Potřebného snížení počtu módů lze dosáhnout zvýšením vlnové délky světla (na 1300 nebo 1550 nm), snížením poměru mezi indexy lomu jádra a obalu a snížením průměru jádra. Používaná jednovidová vlákna mají průměr vnitřního světlovodu kolem 10 μm (typicky používanými jsou vlákna 9/125 μm, horním limitem pro vlnové délky 1300 a 1550 nm a realizovatelné poměry indexu lomu je zhruba 15 μm). Jejich útlum bývá nižší než u mnohavidových vláken a pohybuje se kolem 0.55 dB/km na vlnové délce 1300 nm a až kolem 0.25 dB/km na vlnové délce 1550 nm. Překlenutelná vzdálenost je až 100 km, šířka pásma až 100 GHz.km. Důležitým parametrem je zde *chromatická disperze* – závislost zpoždění signálu na vlnové délce signálu; ta se projeví více při použití světloemitujících diod LED než při použití monochromatičtějších laserových diod ILD.

Optické kabely obsahují více vláken opatřených primární ochranou. *Primární ochrana* zvyšuje průměr vlákna typicky na 0.25 mm, je na vlákno nanášena bezprostředně po jeho vytažení a chrání materiál jádra před vlhkostí. Jako materiál primární ochrany je obvykle používán ultrafialovým světlem tvrditelný akrylát. Při potřebě práce ve větším teplotním rozsahu bývá akrylát nahrazen tenkou vrstvičkou polyimidu. Pro zvýšení odolnosti proti vlhkosti může být primární doplněna o tenoučkou uhlíkovou vrstvu nanesenou pod ní na vlákno.

Těsná *sekundární ochrana* vláken pro vnitřní použití má průměr typicky 0.9 mm a je tvořena vhodnou plastickou hmotou (polyamid, nylon). Kabely pro vnitřní použití pak ve své konstrukci ještě mají, obvykle kevlarové, prvky zachycující podélný tah, jako materiál vnějšího pláště vnitřních kabelů jsou používány materiály s nízkým obsahem halogenidů.

Kromě kabelů s těsným uložením vlákna v materiálu sekundární ochrany (většinou pro vnitřní použití) existují kabely s volným uložením vláken v konstrukci kabelu (většinou pro vnější použití). Vnější plášť kabelů pro vnější použití je obvykle polyetylénový, případně vyplněný gelem zabraňujícím přístupu vlkosti.

Spojování vláken poněkud komplikuje instalaci optických spojů, přesně zakončená vlákna lze spojovat vzájemným přiložením konců, jejich slepením ve speciálních držácích nebo svařením. Je potřeba speciálních zařízení, realizované spoje je nutné proměřit (změřit útlum a případně odrazy ve spojích). Pro rozebíratelná spojení přesně zakončených vláken existuje škála různých konektorů, vedle starších typů ST a SC jsou dnes pro připojování koncových zařízení k dispozici rozměrově úsporné konektory LC, MT-RJ a VF-45. Starší připojování již ve výrobě nakonektorovaných úseků vlákna (*pigtails*) je nahrazováno konektorováním při montáži. Potřebná úprava konce vlákna a montáž konektoru je však na technologii náročnější operací.

Jako zdroj světla pro světlovodné kabely jsou používány světloemitující diody *LED* (Light Emitting Diode) nebo rychlejší laserové diody *ILD* (Injection Laser Diode) – materiálem je GaAs nebo AlGaAs (850 nm), InGaAs (1300 nm) a InGaAsP (1550 nm). Jako přijímače jsou používány fotodiody *PIN* nebo citlivější lavinové diody *APD* (Avalanche PhotoDiode) – materiálem je Si (850 nm), Ge a InGaAsP (1300 a 1550 nm).

Efektivitu napojení zdroje světla na vlákno ovlivňuje souhlas mezi průměrem zdroje světla a průměrem jádra. Do vlákna navíc mohou vstoupit pouze paprsky pod takovými úhly, které po průchodu rozhraním zdroj světla – jádro odpovídají rozsahu úhlů přenášených vláknem. Příslušné rozmezí úhlů definuje *numerická apertura* definovaná jako NA = $sin\Theta$. Jak vysílače, tak přijímače jsou dodávány buď s úsekem připojeného vlákna (*pigtail*) nebo s připojeným optickým konektorem.

Kapacita přenosového kanálu

Základním parametrem, který omezuje přenosovou rychlost kanálu, je šířka použitého kmitočtového pásma. Spojitý signál, který neobsahuje složky s vyšším kmitočtem než W, lze plně charakterizovat $2W$ vzorky za sekundu a z těchto vzorků signál opět rekonstruovat. Obráceně, spojitým signálem s kmitočtovým spektrem omezeným kmitočtem W nemůžeme přenést více než $2W$ vzorků za sekundu. Může-li každý vzorek nabývat V diskrétních hodnot, pak pro přenosovou rychlost C platí *Nyquistova věta*

$$C = 2W.log_2(V) \qquad [\mathrm{b/s, Hz}].$$

Počet úrovní signálu V nelze s ohledem na poškození spojitého signálu při přenosu (obvykle toto poškození charakterizujeme přídavným signálem – šumem) libovolně zvyšovat; teoretický limit přenosové rychlosti C kanálu s pásmem o šířce W a odstupem signálu od šumu S/N udává *Shannonova věta*

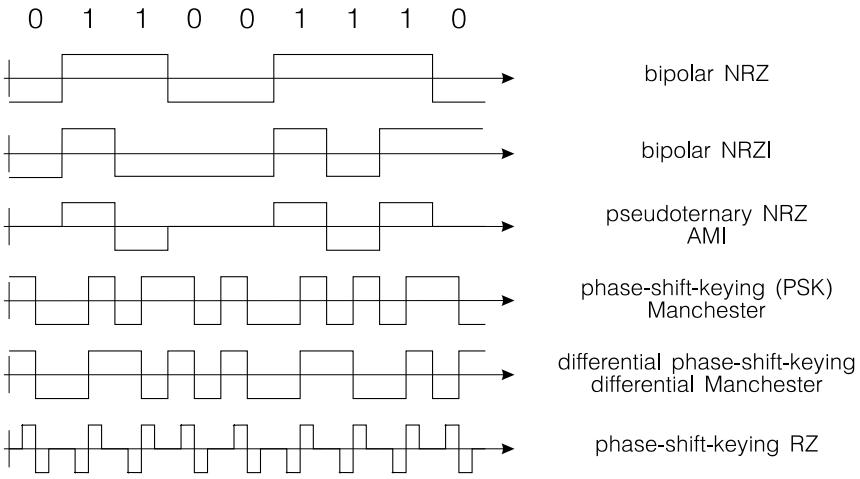
$$C = W.log_2(1 + S/N) \qquad [\mathrm{b/s, Hz}].$$

Kódování a modulace

Neupravený datový signál není vhodný pro přímý přenos datovým kanálem. Obsahuje stejnosměrnou složku, jejíž přenos je v některých případech obtížné zajistit, ať už pro elektrické vlastnosti kanálu nebo pro nutnost galvanického oddělení kanálu transformátorem. Další nepříjemnou vlastností původního datového signálu je nezaručený výskyt elektrických změn, o které se lze opřít při vzorkování na straně přijímače.

Datový signál můžeme zbavit stejnosměrné složky a doplnit o změny usnadňující jeho příjem vhodným *kódováním*. Kód NRZI je používán u sítí pracujících v základním pásmu a ve spojení s modulací i v sítích širokopásmových. Fázovou modulaci NRZ (označovanou jako PSK nebo kód *Manchester*) používá například síť Ethernet. Diferenciální fázová modulace NRZ (označovaná také jako DPSK nebo *diferenciální Manchester*) je použita v lokálních sítích podle doporučení IEEE 802.5. Dalším možným úkolem kódování je dát signálu na médiu pseudonáhodný charakter, příslušný postup označujeme jako *scrambling*.

Zajistění vzájemné synchronizace vysílače a přijímače mají za úkol metody *bitové synchronizace*. Tu lze zajistit několika způsoby. Mohli bychom například vedle vlastního datového signálu přenášet signál hodinový, který označuje místa, ve kterých máme vzorkovat. Rozumnější je však vybavit přijímač samostatným generátorem hodin a tento generátor fázově synchronizovat s přijímaným signálem. Podmínkou správné funkce fázového závěsu je dostatečný výskyt změn v přenášeném signálu, což zajistí vhodné kódování (např. kódy Manchester používané u starších lokálních sítí, nebo kódy 4B5B a 5B6B používané u moderních rychlých sítí).



Obrázek 2.5: Kódování datového signálu v lokálních sítích

Dalším úkolem, který musí obvody přijímače řešit, je určení začátku jednotlivých rámců v přenášené bitové posloupnosti. Mluvíme o *rámcové synchronizaci* a u starších sítí ji obvykle zajišťujeme porovnáváním úseku přijímané bitové posloupnosti se synchronizačním znakem nebo rámcovou značkou (křídlová značka, flag). Novější řešení jsou založena na použití nedatových prvků v signálu (chybějící hrany u signálu IBM Token Ring) nebo o nedatové kombinace bitů v kódech 4B5B a 5B6B.

Přenos kódovaného datového signálu označujeme jako přenos v *základním pásmu*. Pokud chceme pro přenos využít kmitočtového pásma, které neobsahuje základní harmonické přenášeného datového signálu, musíme sáhnout k modulaci. Je-li nosným signálem harmonický signál

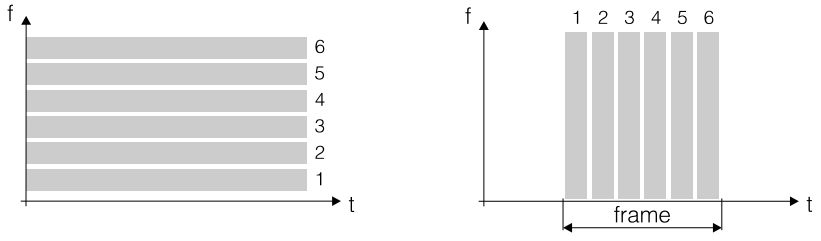
$$u(t) = U sin(\omega.t + \varphi) \quad ,$$

můžeme modulací ovlivnit jeho amplitudu U, kmitočet ω, nebo fázi φ. V lokálních sítích využívajících elektrických signálů používáme nejčastěji kmitočtovou nebo fázovou modulaci, v lokálních sítích optických používáme modulaci amplitudovou.

Kmitočtové spektrum modulovaného harmonického signálu leží v jiné kmitočtové oblasti než spektrum signálu modulačního – mluvíme o přenosu v *přeloženém pásmu*.

Sdílení přenosového média

Pokud přenosové médium poskytuje větší šíři pásma (větší přenosovou rychlost) než je potřebné pro realizaci jediného přenosového kanálu, lze médium sdílet více přenosovými kanály. V lokálních sítích se používá jak *kmitočtový* (frekvenční) *multiplex*, tak *časový multiplex*. U moderních radiových sítí (str. 123) se setkáme s *multiplexem kódovým* (CDMA – Code Division Multiple Access).



Obrázek 2.6: Kmitočtový a časový multiplex

Kmitočtový multiplex

Kmitočtový multiplex (*FDMA – Frequency Division Multiple Access*) využívá skutečnosti, že pro přenos dat s danou přenosovou rychlostí vystačíme s určitou šíří frekvenčního pásma. Je-li šíře pásma, kterou nám poskytuje přenosový kanál, větší, lze kanál rozdělit na více podkanálů a každý z nich použít nezávisle. Pro převod datového signálu do daného frekvenčního pásma a zpátky používáme *modemů* vybavených selektivními filtry. Kmitočtový multiplex je základem širokopásmových lokálních sítí.

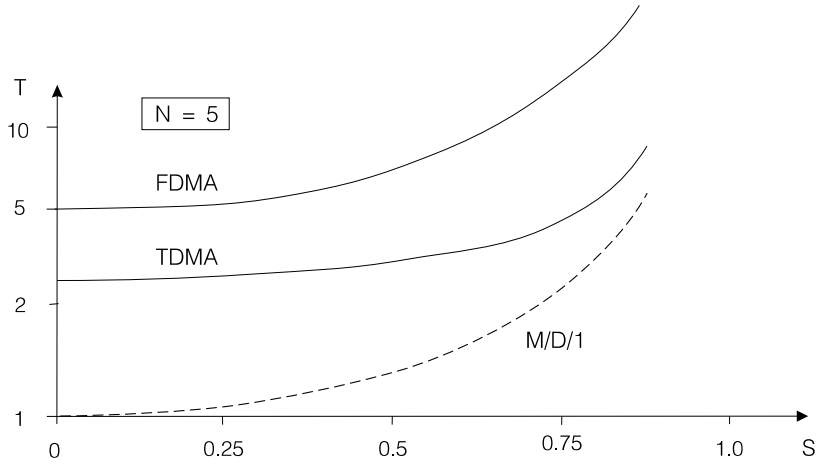
Časový multiplex

Při časovém multiplexu (*TDMA – Time Division Multiple Access*) přidělujeme přenosový kanál postupně jednotlivým stanicím. Každé stanici je vyhrazen časový úsek (*slot*), ve kterém může vyslat paket určité délky. časové úseky jednotlivých stanic se pravidelně střídají s periodou, kterou obvykle označujeme jako rámec (*frame*).

Pro přenos dat zřejmě nelze plně využít kapacitu kanálu, v každém časovém slotu je nutné věnovat čas na sfázování přijímače a rámec je nutné doplnit synchronizačním slotem. Metoda je použitelná pro lokální sítě s malou rozlehlostí $a < 0.1$.

Nevýhodou pevného rozdělení kapacity sdíleného kanálu TDMA (synchronní časový multiplex) je neschopnost přizpůsobit využití kanálu nárazovému charakteru požadavků jednotlivých stanic. Optimálního využití kapacity bychom dosáhli v případě, že bychom měli k dispozici algoritmus, který by evidoval požadavky jednotlivých stanic a přiděloval podle nich stanicím médium. V ideálním případě bychom dosáhli chování obslužného systému $M/M/1$ (označujeme ho tak v případě náhodně přicházejících požadavků na přenos náhodně dlouhých bloků dat po jednom kanálu). Tomu se můžeme vhodnými metodami řízení do určité míry přiblížit – mluvíme o asynchronním časovém multiplexu (*ATDMA – Asynchronous TDMA*, *Adaptive TDMA*). Porovnání středního zpoždění, ke kterému dojde při přenosu sítí s frekvenčním multiplexem, sítí se synchronním časovým multiplexem a sítí s ideálním přidělováním typu $M/M/1$ uvádí obr. 2.7.

Časový multiplex je dnes snadněji realizovatelný než multiplex kmitočtový, a jeho adaptivní formy (sdílení datového kanálu takovým způsobem, aby bylo maximálně využito jeho kapacity) jsou principem převážné většiny lokálních sítí a sítí integrovaných služeb (ISDN).



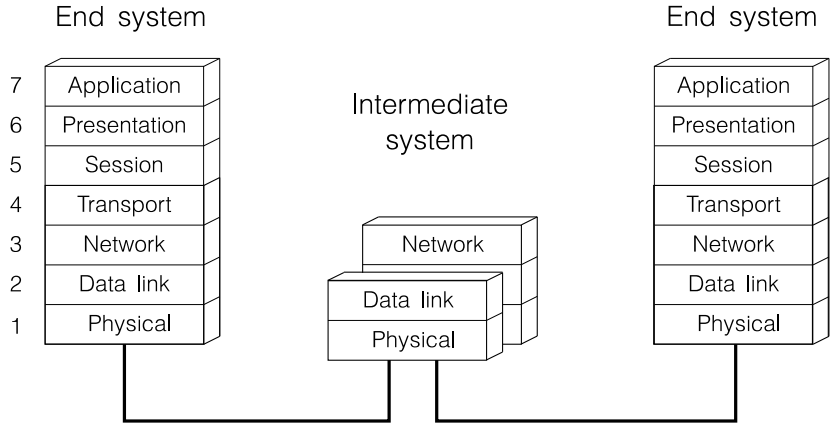
Obrázek 2.7: Závislost zpoždění paketu na zátěži

2.3 Architektura komunikačních funkcí

Současné lokální sítě se opírají o technologie, které jsou vesměs definovány standardy normalizačních organizací jako jsou *IEEE* (Institute of Electrical and Electronics Engineers), *ETSI* (Europian Telecommunications Standards Institute), *ITU-T* (International Telecommunication Union - Telecommunication Standardization Sector), *ANSI* (American National Standards Institute) a *ISO* (International Organization for Standardization). Patří sem varianty Ethernetu a kruhové sítě IBM Token Ring a FDDI. Dobře definované a zavedené jsou standardy popisující použití sítí ATM (Asynchronous Transfer Mode) jako páteří lokálních sítí a standardy bezdrátových sítí.

Architektura ISO OSI

Na síťové vybavení, technické a programové, jsme zvyklí se dívat jako na systém funkčních vrstev, ve kterém každá vyšší vrstva rozšiřuje možnosti vrstvy nižší. Důvodem takového rozkladu je složitost problémů, se kterými se v sítích setkávme a které je třeba řešit pokud možno odděleně. Pro přepojovací počítačové sítě, ze kterých se na počátku osmdesátých let vyvinuly dnes provozované veřejné datové sítě, byl vytvořen standardní model síťové architektury označovaný jako *ISO/OSI* (*ISO Open Systems Interconnection*). Architekturu vrstev modelu OSI ilustruje obr. 2.8.



Obrázek 2.8: Architektura vrstev ISO OSI

Fyzická vrstva (Physical Layer) definuje fyzické propojení mezi prvky sítě, mechanické vlastnosti těchto propojení (konektory, typ média), elektrické vlastnosti (napěťové úrovně, způsob kódování a modulace) a u lokálních sítí i topologii propojení jednotlivých prvků a metodu přístupu k přenosovému médiu.

Linková vrstva (Data Link Layer) definuje pravidla pro předávání bloků dat. Zprávy jsou sítí přenášeny v pevně definovaných rámcích, rámce dovolují chránit předávaná data proti chybám při přenosu. U vícebodových spojů (a o ty se lokální sítě opírají) je nutné zajistit *linkovou adresaci* stanic. Struktura rámce (ale spíš potřeba zajistit rozumné přidělování média) často limituje délku bloků dat.

Síťová vrstva (Network Layer) definuje způsob, jakým se sítí pohybují pakety, jak si je jednotlivé prvky sítě předávají na jejich cestě od odesílatele k adresátovi. Opírají se přitom o *síťovou adresaci* stanic, ta může být odlišná od adresace linkové. Mechanismy vrstvy se starají i o ochranu sítě proti nadměrné zátěži (*Flow Control*).

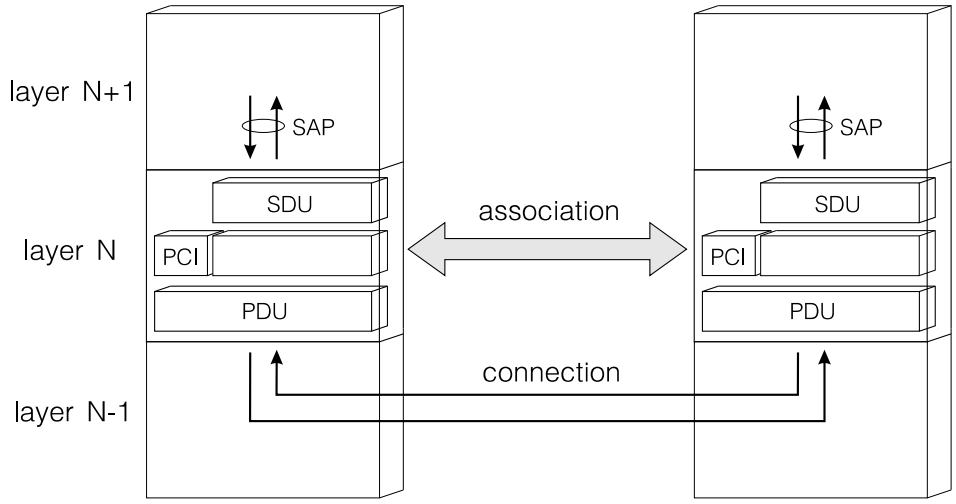
Transportní vrstva (Transport Layer) umožňuje současnou komunikaci více aplikačních programů na jednom počítači v síti, zajišťuje vytváření dočasných komunikačních spojení mezi aplikacemi a rozklad zpráv do paketů a skládání paketů do zpráv.

Relační vrstva (Session Layer) vytváří logické rozhraní pro aplikační programy, které používají služeb sítě. Definuje způsob komunikace programů a uživatelský pohled na komunikační kanál.

Presentační vrstva (Presentation Layer) transformuje přenášená data – zajišťuje převody kódů a formátů dat pro nekompatibilní počítače, kompresi a utajování přenášených dat.

Aplikační vrstva (Application Layer) je vrstvou standardních aplikačních rozhraní a aplikačních programů, které síť využívají.

Model OSI se stal základem i pro lokální sítě, které používají jiných přenosových médií, potvrzovacích technik a způsobů předávání zpráv, než starší sítě přepojovací.



Obrázek 2.9: Vnitřní struktura vrstvy ISO OSI

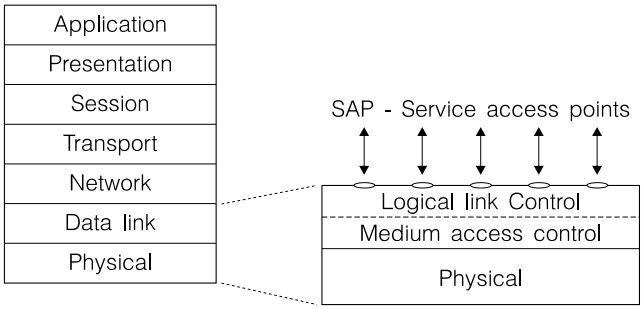
Standardy jednotlivých vrstev definují služby, které vrstva poskytuje (přenos bloků dat *SDU – Service Data Unit*), a způsob, kterým lze těchto služeb využívat (*SAP – Service Access Point*). Popisuje komunikaci uvnitř vrstvy (s protistanicí) a způsob využití služeb nižší vrstvy (přenos bloků dat *PDA – Protocol Data Unit*) pro realizaci této komunikace. Cenou za zprostředkování služby je předávání řídící informace, obr. 2.9 ji uvádí jako *PCI – Protocol Control Information*.

Architektura lokálních sítí IEEE 802

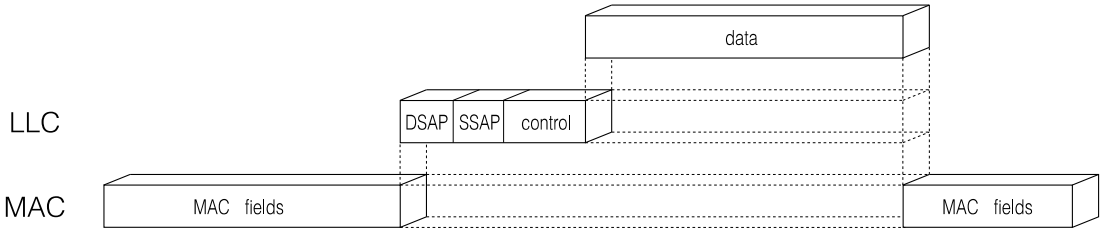
Normalizační úsilí v oblasti lokálních sítí se ujala organizace IEEE, jejíž pracovní skupiny si vzaly za úkol definovat univerzální standard pro lokální datové komunikace, označený jako IEEE 802. Na počátku (do roku 1983) se definice omezovaly na technologie Ethernetu, na sítě sběrnicové s deterministickým řízením a na sítě IBM Token Ring. V průběhu let byla normami pokryta řada dalších technologií a jejich modifikací. Model IEEE 802 pokrývá tři nejnižší vrstvy architektury OSI, vrstvu fyzickou, linkovou a částečně i síťovou, a je členěn na samostatná doporučení, týkající se jednotlivých technologií.

Doporučení IEEE 802 člení nejnižší vrstvy poněkud odlišně od architektury ISO (obr. 2.10). Vytváří vrstvu fyzickou, která definuje média, konektory, signály, a nad ní staví vrstvu řízení přístupu ke sdílenému komunikačnímu kanálu *MAC* (Medium Access Control). Ta definuje formáty rámců, adresaci stanic, zabezpečení proti chybám. První dvě vrstvy jsou vlastní každé konkrétní popisované technologii. Nad nimi je postavena na technologii nezávislá vrstva linková *LLC* (Logical Link Control). Ta dovoluje násobně využít kanálu jedné stanice (vytváří nezávislá místa přístupu *SAP – Service Access Point*) a podporuje potvrzovací schémata.

Každá z vrstev architektury IEEE 802 definuje řídící informace nutné pro její činnost. Jejich rozložení ve struktur rámců uvádí obr. 2.11.

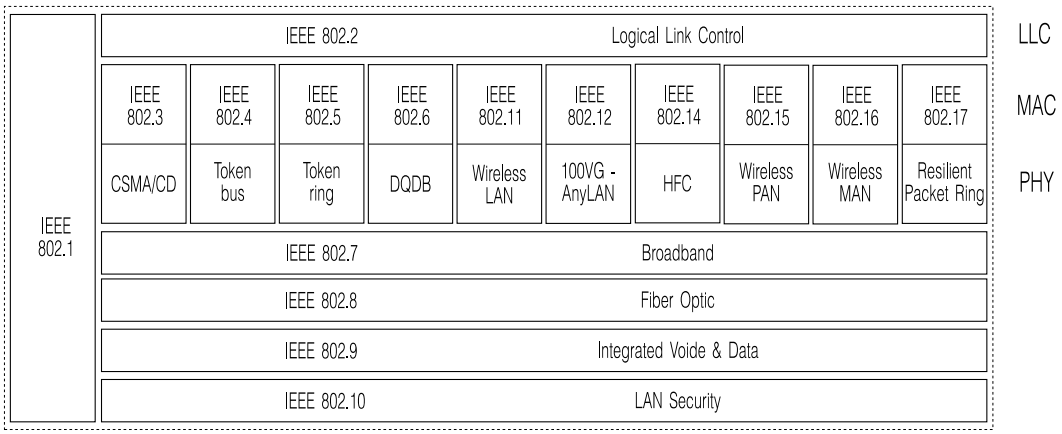


Obrázek 2.10: Architektura lokálních sítí IEEE 802



Obrázek 2.11: Struktura rámců IEEE 802

Již jsme si uvedli, že současná doporučení IEEE pokrývají mnohem více technologií, než tomu bylo v době zahájení prací. Zhruba současnou situaci (v obrázku chybí standard IEEE 802.14 HFC) uvádí obr. 2.12.



Obrázek 2.12: Technologie IEEE 802

Doporučení *IEEE 802.1* zastřešuje ostatní doporučení řady, definuje jejich strukturu a vzájemnou vazbu. Popisuje také propojení lokálních sítí opřené o MAC adresaci – *mosty* (*bridges*).

Doporučení *IEEE 802.2* definuje funkce linkové vrstvy a definuje služby, které lokální síť poskytuje. Jde o dva základní druhy služeb, o nepotvrzovanou datagramovou službu (Connection-less Service), virtuální spojení (Connection-oriented Service) a potvrzovanou datagramovou službu. Nepotvrzovaná datagramová služba využívá vysoké kvality přenosových kanálů lokálních sítí a nezajišťuje potvrzovací mechanismus, ten nechává na vyšších vrstvách a aplikačních programech. Potvrzovaná datagramová služba a virtuální spojení naproti tomu potvrzování zajišťují.

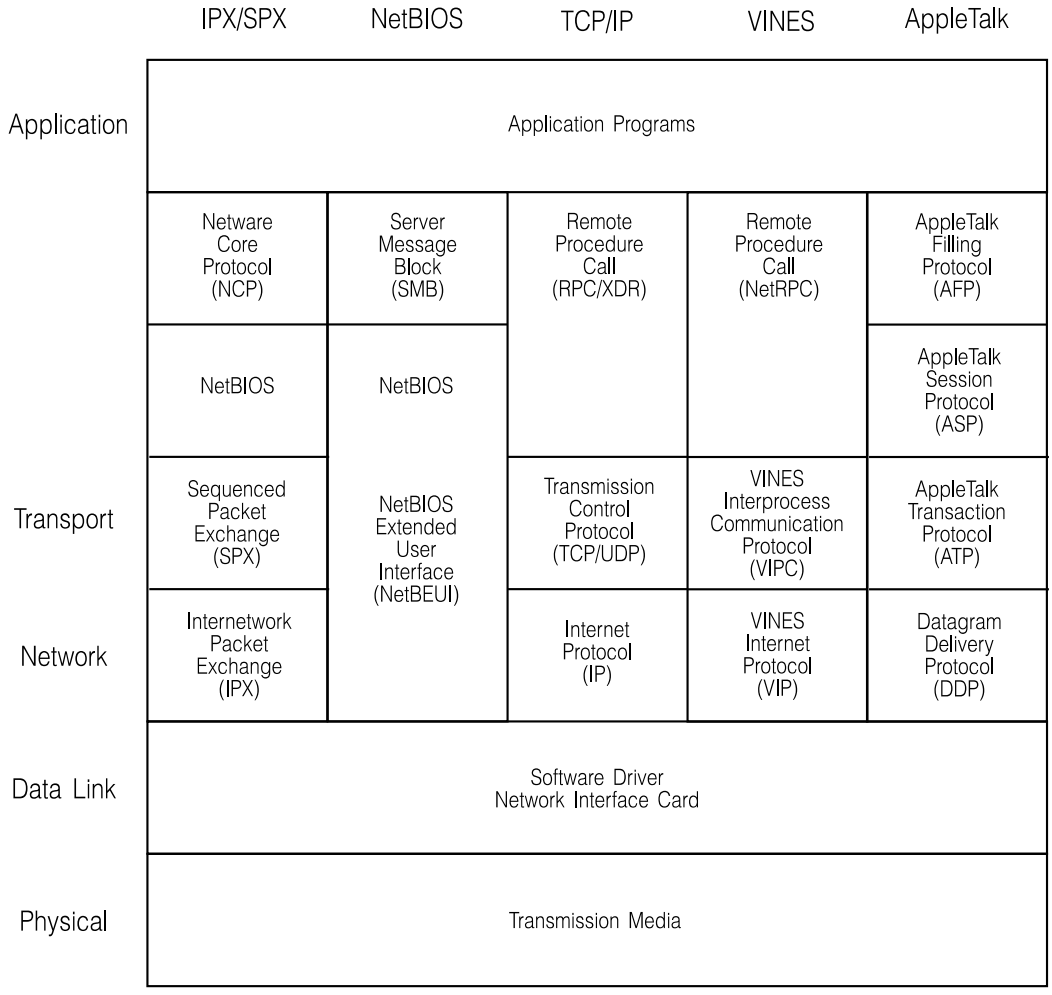
Doporučení *IEEE 802.3, 802.4, 802.5, 802.6, 802.11, 802.12, 802.14, 802.15, 802.16 a 802.17* popisují fyzickou vrstvu a přístup k médiu pro lokální sítě různého typu – pro sběrnicové lokální sítě s náhodným řízením metodou CSMA/CD Ethernet, lokální sítě s deterministickým řízením, kruhové lokální sítě IBM Token Ring, rozhraní metropolitních sítí DQDB, bezdrátové

sítě WLAN, síť 100 VG-AnyLAN, kombinované širokopásmové sítě, personální bezdrátové sítě, metropolitní bezdrátové sítě a virtuální kruhové sítě.

Doporučení *IEEE 802.7, 802.8, 802.9 a 802.10* jsou věnována využití širokopásmových kanálů, optických vláken, zajištění přenosu isochronních dat a bezpečnosti v lokálních sítích. Podobně jako doporučení IEEE 802.1 a IEEE 802.2 se neomezují na jedinou technologii, ale vztahují se jistým způsobem ke všem.

Architektura TCP/IP, IPX/SPX, NetBIOS a VINES

Specifikace IEEE 802 popisují způsob, jak přenést konkrétní lokální sítí bloky dat – rámce. Využití obsahu těchto rámců pro data aplikací a pro řízení vyšších síťových služeb je záležitostí vyšších vrstev architektury (síťové, transportní, relační, presentační a aplikační).



Obrázek 2.13: Architektura TCP/IP, IPX/SPX, NetBIOS, VINES a AppleTalk

V oblasti vyšších protokolů není shoda, pokud jde o používaná řešení, tak výrazná, jako u vrstev nižších. Každý z důležitých síťových systémů se opírá o poněkud odlišnou sadu protokolů, dnes však již běžně zjišťujeme, že jednotlivé produkty dovolují použít protokolových sad několik, a to buď alternativně nebo i souběžně.

Obr. 2.13 uvádí protokolové sady typické pro architektury TCP/IP (dnes převažující), IPX/SPX, NetBIOS, VINES a AppleTalk. Tyto sady většinou zahrnují síťový protokol (IP, IPX, VIP, DDP), transportní protokol (TCP, SPX, NetBIOS, VIPC, ATP) a aplikační rozhraní (RPC/XDR, NCP, NetBEUI, NetRPC, AFP).

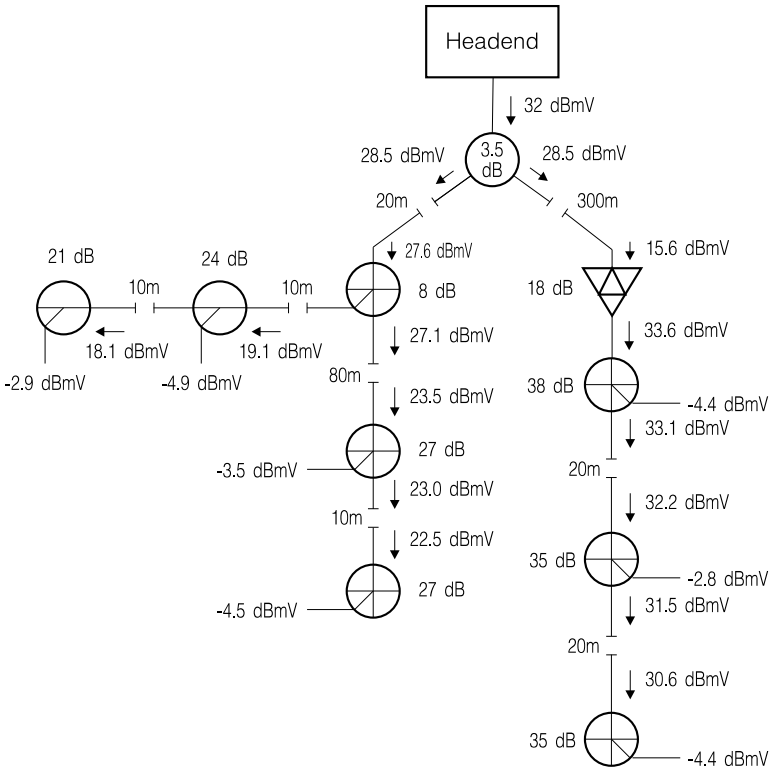
3. Širokopásmové sítě

Zajímavou skupinou sběrnicových lokálních sítí jsou sítě využívající přenosu v přeloženém pásmu. Toto pásmo je v případě koaxiálního kabelu dostatečně široké, aby ho bylo možné rozdělit na více podkanálů *frekvenčního multiplexu*.

Přenosové médium

Přenosovým médiem širokopásmových sítí je zpravidla koaxiální kabel o průměru půl palce s charakteristickou impedancí 75 Ω používaný pro rozvody kabelové televize (*CATV – Community Area TeleVision*). Jeho výhodou je postačující kvalita a nižší cena než cena kabelů u sítí pracujících v základním pásmu (Ethernet). Současně lze využít celou škálu prvků používaných pro instalaci kabelové televize – rozbočovače, odbočovače a pásmové zesilovače.

Logickou strukturou širokopásmových sítí je dvojice kanálů. Na jeden z nich jsou připojeny vysílače stanic, na druhý jsou připojeny přijímače. Oba kanály širokopásmové sítě jsou propojeny v jediném místě zesilovačem nebo retranslátorem. Zesilovač je používán u sítí, které pro vysílací a přijímací kanál používají samostatné kabely – systémy označujeme jako *Dual-Cable Systems* (příkladem takové sítě je Wangnet). Retranslátor používají sítě s jediným kabelem pro přenos obou kanálů v různých frekvenčních pásmech – *Split-Channel Systems* (nebo, vzhledem k symetrickému rozdělení pásma jako *Mid-Split Systems*, příkladem jsou sítě Localnet, IBM PC LAN). Retranslátor převádí signály z pásma kanálu vysílacího do pásma kanálu přijímacího. Příklad rozdělení kmitočtového pásma v širokopásmové síti typu Split-Channel uvádí (pro síť Localnet) obr. 3.2.



Obrázek 3.1: Širokopásmová síť

Rozbočovače (*splitters*) dovolují rozvětvit síť, do všech větví vkládají stejný útlum (obvykle 3.5 dB pro dvoucestný rozbočovač). Odbočovače (*directional couplers*) mají průchozí útlum

mnohem menší (kolem 0.5 dB), útlum odbočky je volitelný v rozsahu 10 až 40 dB. Odbočovače sloužící k připojení stanic k médiu jsou označovány jako *taps* a bývají často vícenásobné.

U rozsáhlejších sítí je nutné útlum kabelů, rozbočovačů a odbočovačů krýt zesílením linkových zesilovačů se zesílením v rozsahu 20 až 30 dB, stejnou velikost mívá i zesílení retranslátoru. Důsledkem nutnosti respektovat útlumy v širokopásmových sítích je nutnost výpočtu kabelových rozvodů pro konkrétní rozmístění pracovních stanic. Příklad širokopásmové sítě uvádí obr. 3.1.

Řízení přístupu

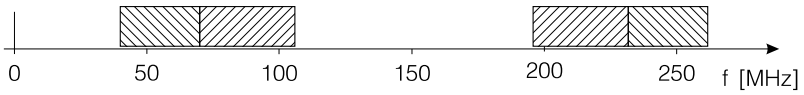
V širokopásmových lokálních sítích jsou využívány metody řízení, které poznáme u sběrnicových sítí s náhodným a deterministickým přístupem. Metody náhodného přístupu CSMA/CD jsou použitelné pro menší lokální sítě, u rozsáhlejších sítí z principu klesá jejich efektivita. Důvodem je jednak doba šíření signálu mezi stanicemi – signál je přenášen přes retranslátor, jednak nižší účinnost detektoru kolize, který musí pracovat na jiných principech než u sítí s přenosem v základním pásmu. Jako příklad řešení detekce kolize si můžeme uvést porovnání odeslaného a přijatého signálu, jak ho používá technologie IEEE 802.3 10BROAD36 (str. 69). Častěji se setkáváme s deterministickým řízením (Token-Passing Bus), síť pracující v přeloženém pásmu s deterministickým řízením je základem doporučení IEEE 802.4 (str. 43).

Pozn.: V uvedených příkladech (IEEE 802.3 10BROAD36 a IEEE 802.4) se nejedná o širokopásmové sítě, protože je využíván jediný přenosový kanál. Princip metod řízení je však týž.

Širokopásmové sítě jsou vhodné pro aplikace, na které jsou kladeny větší požadavky. Mají větší přenosovou kapacitu, zajišťují větší odolnost proti vnějšímu rušení a dovolují využít přenosového média pro další přídavné služby (telefon, TV signál). Prvky kabelových rozvodů mají vysokou spolehlivost, jsou provozně ověřené z kabelové televize a snadno dostupné. Nevýhodou je poněkud vyšší složitost komunikačních stanic, které obsahují výrobně náročný modem.

Localnet

Jedna z nejznámějších technologií širokopásmových lokálních sítí typu Split-Channel Localnet firmy Sytek se opírá o technologii kabelové televize (kabely, odbočovače, rozbočovače). Využívá kmitočtového pásma 40 – 106 MHz pro vysílání a pásma 196 – 262 MHz pro příjem. Signály pásma 40 – 106 MHz převádí do pásma 196 – 262 MHz retranslátor umístěný v kořeni stromové sítě. Na jedné kabeláži mohou současně pracovat dvě, vzájemně slučitelné varianty sítě označené jako System 20 a System 40.



Obrázek 3.2: Rozdělení kmitočtového pásma sítě Localnet

Localnet System 20 využívá úseků 70 – 106 MHz a 226 – 262 MHz rozdělených do 120 kanálů frekvenčního multiplexu o šířce 300 kHz. Jednotlivé kanály lze využít pro dvoubodová spojení nebo jako sběrnicové kanály s řízením typu TDMA nebo CSMA/CD. Přenosová rychlost kanálů je 128 kb/s, vzdálenost koncových stanic může být až 56 km.

Localnet System 40 využívá úseků 40 – 70 MHz a 196 – 262 MHz. K dispozici je pět kanálů o šířce 6 MHz, kanály lze využít jako sběrnicové kanály s řízením CSMA/CD, přenosovou rychlostí 2 Mb/s a vzdáleností stanic až 8 km.

Síť Localnet je široce koncipovaný systém, který zahrnuje řadu speciálních zařízení pro napojení na jiné lokální sítě, veřejné datové sítě, telefonní ústředny, ap. Technologie Localnet byla použita firmou IBM pro propojení personálních počítačů IBM PC a dodávána pod označením PC LAN. Řízení sítě PC LAN odpovídá metodě CSMA/CD, přenosová rychlost je 2 Mb/s. Data v kódu NRZI jsou ve vysílači stanice frekvenčně modulována na kmitočet 50.75 MHz, přijímací kanál má střední kmitočet 219 MHz. Pro ovládání komunikačních stanic byl vytvořen programový ovladač známý jako NetBIOS (str. 145).

Wangnet

Jako příklad sítě se strukturou kabeláže Dual-Cable si uvedeme síť Wangnet. Má stromovou topologii, pro přenos je využívána dvojice koaxiálních kabelů. Na jeden jsou připojeny vysílače stanic, na druhý přijímače. Kabely, rozbočovače, odbočovače a zesilovače odpovídají běžné kabelové televizi.

Pro přenos je využíváno pásmo o šířce 340 MHz (10 – 350 MHz) rozdělené do tří částí. Nejdůležitější částí spektra je Wangband – vytváří sběrnicový kanál CSMA/CD s přenosovou rychlostí 12 Mb/s. Kmitočty mezi 10 a 82 MHz jsou využity pro pomalé synchronní a asynchronní kanály. Prvá část tohoto pásma dovoluje vytvořit 32 pevných dvoubodových nebo vícebodových kanálů s rychlostí přenosu do 9.6 kb/s, druhá část 16 pevných dvoubodových nebo vícebodových kanálů s rychlostí přenosu do 64 kb/s. Kanály ve třetí části pásma jsou přidělovány na žádost, pro jejich využití je nutný přeladitelný modem (*Frequency Agile Modem*). Do poslední části pásma (*Utility Band*) na kmitočtech 174 – 216 MHz lze umístit až sedm televizních kanálů využitelných například pro telekonferenci nebo bezpečnostní systémy.

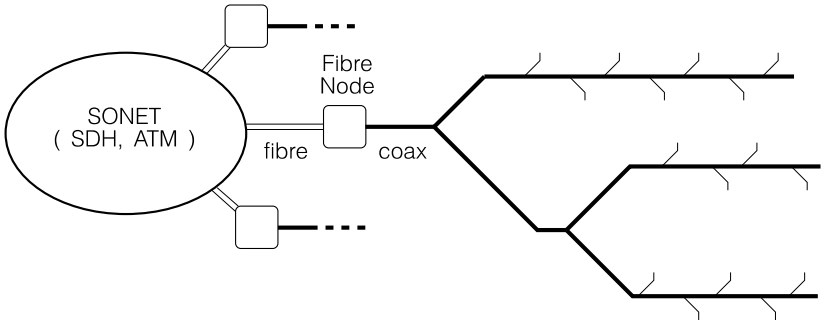
Pozn.: Topologii, podobnou širokopásmovým sítím typu Dual-Cable používají i optické sítě. I u těch jsou často vysílače napojeny na optická vlákna vedoucí do středu hvězdicové sítě odkud je optický signál distribuován jinými vlákny k přijímačům.

3.1 Využití sítí CATV

Z předchozích příkladů by se mohlo zdát, že širokopásmová technologie opírající se o koaxiální kabely CATV je spíše otázkou minulosti, alespoň v příkladech, které jsme si zde uvedli, se jedná o poměrně stará řešení. Opak je však pravdou. Využití kabelů CATV pro zpřístupnění moderních telekomunikačních služeb je zajímavou technologií přístupových sítí.

HFC – Hybrid-Fibre-Coax

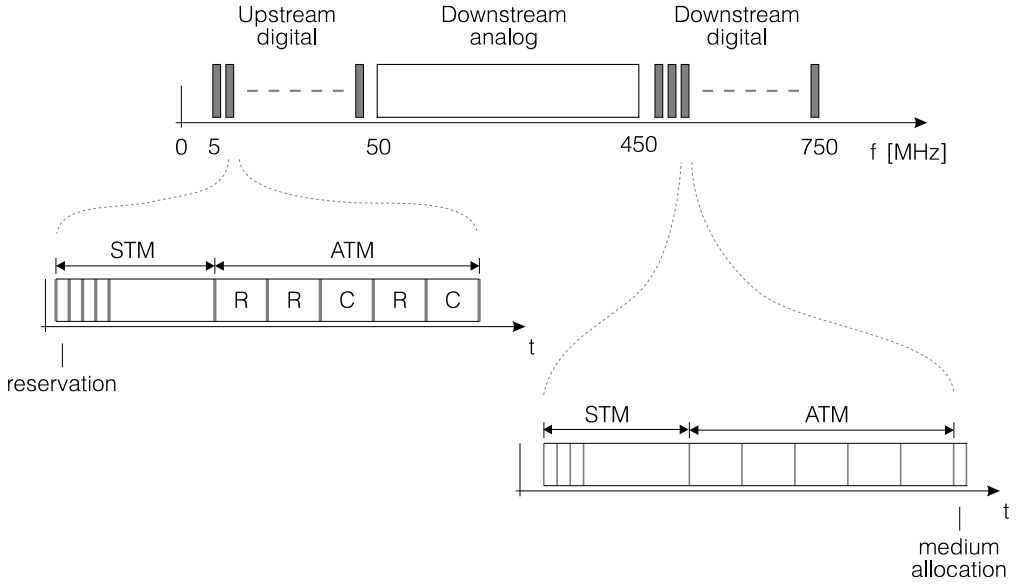
Jedním ze systémů umožňujících datovou komunikaci v přeloženém pásmu na kabeláži CATV je systém definovaný doporučením IEEE 802.14 pod označením *Hybrid-Fibre-Coax System*.



Obrázek 3.3: Struktura sítě IEEE 802.14 Hybrid-Fibre-Coax System

Jedná se o systém, jehož topologii ilustruje obr. 3.3, a který dovolí zpřístupnit síťové služby široké veřejnosti. Kořenem kabelových sítí jsou namísto konvertorů nebo opakovačů prvky označované jako *Fibre-Node*. Ty připojují stromové širokopásmové sítě dvoubodovými optickými spoji k vlastní vnitřní struktuře, kterou tvoří plesiochronní optická přepojovací síť SONET (v Evropě SDH). Výsledkem poměrně komplikované kombinované struktury je systém, který minimalizuje náklady na připojení velkého množství koncových účastníků (připojení koaxiálním kabelem je levnější než připojení optickým vláknem, ale hlavně lépe udržovatelné) a přitom zachovává velkou průchodnost pro data i analogové signály.

Pro připojení koncových stanic je použit širokopásmový systém typu s rozdělením kmitočtového pásma podle obr. 3.4. Na rozdíl od předcházejících sítí je rozdělení pásma do obou směrů asymetrické.



Obrázek 3.4: Rozdělení kmitočtového pásma sítě IEEE 802.14 Hybrid-Fibre-Coax System

Z pásma využívaných frekvencí 5 – 750 MHz je vyčleněno pásmo 50 – 450 MHz pro distribuci analogového TV signálu. Frekvence v rozsahu 5 – 45 MHz jsou využívány k digitálnímu přenosu od stanic k síti (*dostředné kanály*), frekvence v rozsahu 450 – 750 MHz k distribuci digitálního signálu ze sítě ke stanicím (*odstředné kanály*). Kanály mají šířku od 1 MHz do 6 MHz a dovolují přenos dat rychlostmi od 1.6 Mb/s do 10 Mb/s. Na jednotlivých kanálech může být realizován časový multiplex. Časové rámce jsou rozdělené na časové sloty vyhrazené pro *synchronní přenos* (telefonní hovorové a video kanály) a na sloty přidělované *buňkám ATM* (str. 102). Rámce dostředného kanálu mají vyhrazen prvý slot pro signalizaci a pro žádosti o přidělení kanálů, v posledním slotu rámců odstředných jsou rezervace potvrzovány.

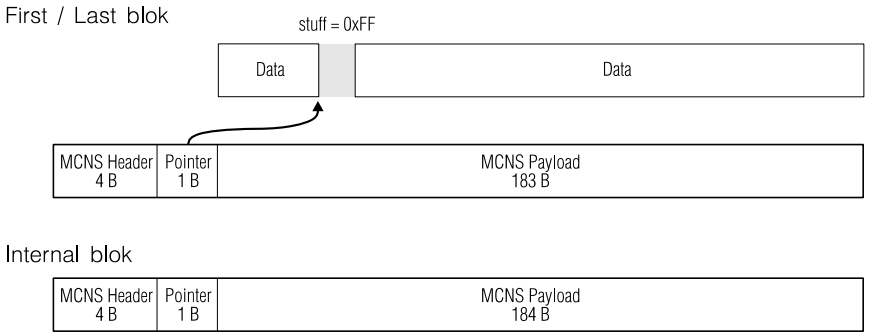
Rozhraní mezi synchronními kanály a prostorem pro buňky ATM je pohyblivé, s možným limitem. O sloty pro buňky ATM mohou stanice soupeřit (metodou taktovaná Aloha, str. 26), jsou pak označovány jako kolizní (C). Druhou možností je ponechat stanici slot, který obsadila (opět metodou taktovaná Aloha), i v dalších rámcích. Takové sloty jsou označovány jako rezervované (R).

Obrázek 3.4 ilustruje i skutečnost, že mezi jednotlivými sloty je nutné ponechat ochranné prodlevy, respektující dobu šíření signálu v kabelové síti.

MCNS – Multimedia Cable Network Systém

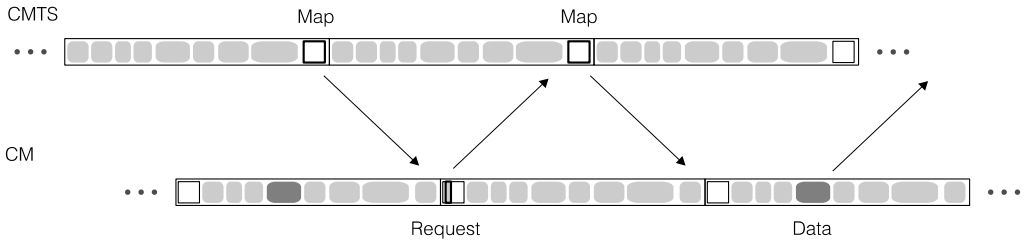
Využití kabeláže CATV pro přenos dat popisuje vedle IEEE 802.14 také norma vypracovaná kosorciem MCNS (Multimedia Cable Network System), využívaná provozovateli systémů CATV.

Architektura sítě MCNS je shodná s architekturou sítě HFC (obr. 3.3) Přenos dat po síti MCNS se podřizuje formátům základní služby sítě, distribuce digitalizovaného televizního signálu. Datové bloky (např. fragmenty rámců Ethernetu) jsou v režimu *DOC* (*Data over Cable*) vkládány do rámců pevné délky (obr. 3.5), pozici začátku datového bloku určuje pointer následující za krátkou hlavičkou.



Obrázek 3.5: Formát rámců systému DOC MCNS

Přístup k dostřednému Uplink kanálu zajišťuje jednotlivým stanicím rezervační přístupová metoda (obr. 3.6). Centrální řídící stanice informuje koncové stanice o rezervaci kanálu pro jejich vysílání speciální řídící zprávou - *mapou*, ta je vysílána na začátku časového rámce distribučního kanálu. Součástí mapy je i informace o pozici rezervačních slotů, v nich koncová stanice může (metodou taktovaná Aloha) zažádat o rezervaci dostředného kanálu. Výsledek rezervace je stanici sdělen v následující mapě, rezervovaný časový slot stanice využije k odeslání dat.



Obrázek 3.6: Přidělování kanálu v systému DOC MCNS

Kritickým místem metody je respektování zpoždění signálu na médiu. Technologie proto zahrnuje dvoustupňový mechanismus dovolující změřit zpožění signálu na médiu pro každou ze stanic. Mechanismus předpokládá během provozu neměnné umístění stanice, což je u fyzického média snadno akceptovatelný požadavek. V prvé fázi mechanismu dává centrální stanice nově se přihlašujícím koncovým stanicím široký interval respektující možné vzdálenosti v síti. Druhá fáze mechanismu dovoluje zpřesnit informaci o vzdálenosti koncové stanice a o nutném časovém předstihu, se kterým musí koncová stanice zahajovat vysílání.

4. Náhodný přístup ke sdílenému médiu

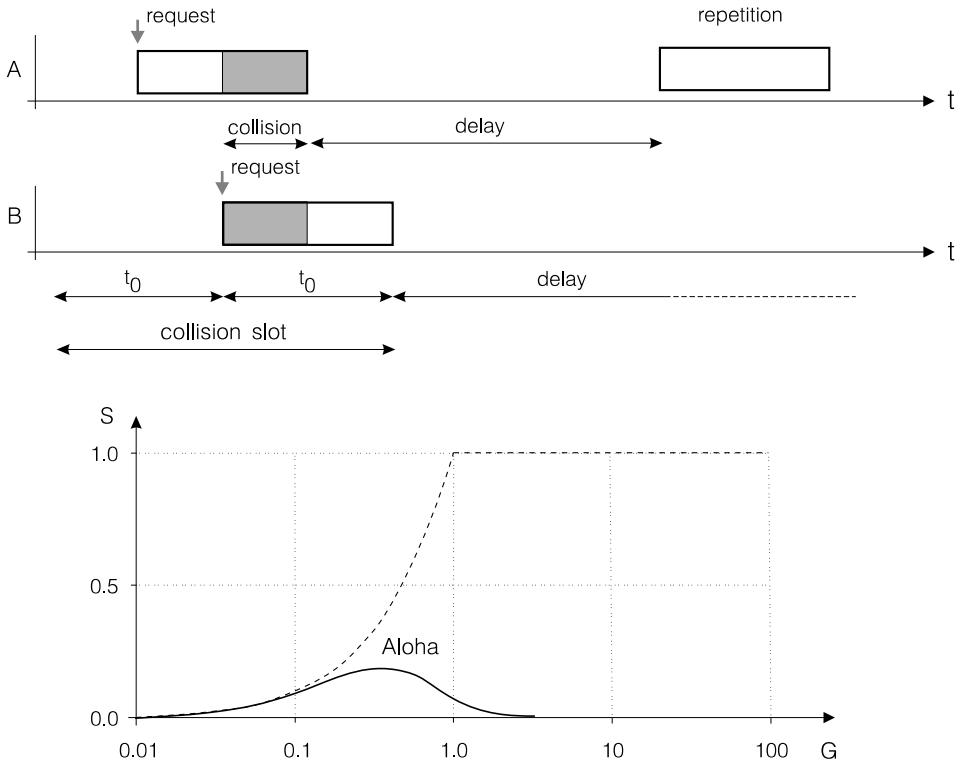
Náhodný přístup ke sdílenému přenosovému kanálu můžeme považovat za nejjednodušší techniku přístupu a za protipól deterministických metod, které si popíšeme později. Jednotlivé stanice podřizují přístup na kanál pouze svému odhadu nebo pozorování.

4.1 Aloha

Logickým předchůdcem metod řízení, které používají dnešní lokální sítě nasazované v administrativě, jsou metody náhodného přístupu, které byly vyvinuty pro komunikaci na sdíleném rádiovém kanále – metody označované jako metody *Aloha*.

Prostá Aloha

Nejjednodušší metodou náhodného přístupu je *prostá Aloha*, která byla poprvé použita v roce 1971 pro řízení rádiové sítě na Havajské universitě. Stanice, která má rámec připravený k odeslání, začne vysílat bez ohledu na případné obsazení kanálu jiným přenosem. Důsledkem jsou pochopitelně kolize; situaci, ve které dochází ke kolizi, uvádí obr. 4.1.



Obrázek 4.1: Prostá Aloha

Rámce poškozené při kolizi je nutné opakovat (v praxi je tato skutečnost indikována vypršením časového limitu, do kterého měl být příjem potvrzen), prodleva před zahájením dalšího pokusu musí být volena náhodně, aby nedošlo k opakování kolize.

Budeme-li měřit vstupní tok sítě počtem rámců, které mají být přeneseny, a tento tok označíme S, je zřejmé, že v ustáleném stavu je tento tok roven toku výstupnímu (rámce přenesené sítí). V důsledku kolizí a z toho vyplývající nutnosti opakovat poškozené rámce je celkový tok vnucovaný stanicemi kanálu vyšší, označujeme ho G. Vztah obou toků, průchozího S

a celkového G lze (za předpokladu, že opakující stanice nesmí generovat nový rámec) vyjádřit analyticky jako

$$S = G.e^{-2G} \quad .$$

K tomuto výsledku se lze dostat poměrně jednoduše, neboť vztah vyjadřuje počet paketů nezasažených kolizí, tedy

$$S = G.P_0 \quad ,$$

kde P_0 je pravděpodobnost, že během vysílání jednoho rámce nepřijde další požadavek na vysílání. Předpokládáme-li, že stanice jsou Poissonovské zdroje (a je jich buď nekonečně mnoho nebo mohou poškodit násobným vysíláním své vlastní rámce) pak pro pravděpodobnost příchodu dalších k požadavků během vysílání rámce platí

$$P_k = (2G)^k.e^{-2G}$$

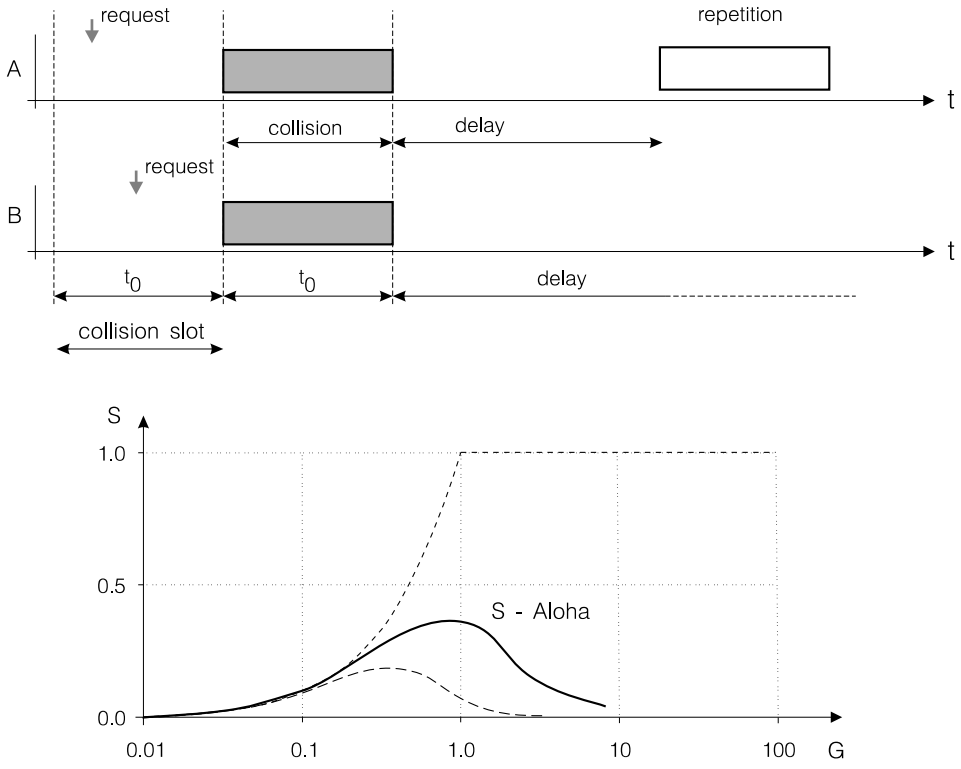
a tedy jednoduchým dosazením

$$P_0 = e^{-2G}.$$

Průběh této závislosti uvádí obr. 4.1. I u metody prostá Aloha lze dosáhnout využití kapacity kanálu až 18.4 %, při dosažení odpovídající zátěže je každý rámec v průměru vyslán třikrát. Za povšimnutí stojí pokles průchodnosti pro rostoucí celkový tok, této oblasti je nutné se vyhýbat vhodným řízením.

Taktovaná Aloha

Podstatného zvýšení průchodnosti sítě lze dosáhnout jednoduchou modifikací metody Aloha. Stanicím dovolíme zahájit vysílání pouze v okamžicích, které definují začátky časových úseků postačujících pro odeslání jednoho rámce. Metodu označujeme jako *taktovaná Aloha* (Slotted Aloha).



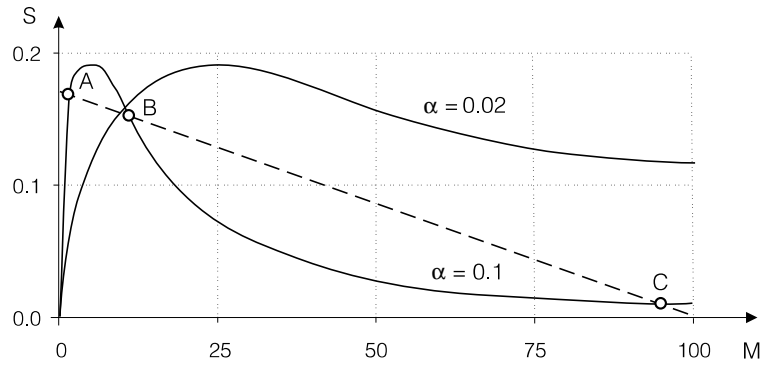
Obrázek 4.2: Taktovaná Aloha

Důvodem zlepšení, které je patrné z grafu na obr. 4.2, je zkrácení tzv. kolizního slotu, jehož délka odpovídala v případě prosté Alohy dvojnásobku doby potřebné pro odeslání jednoho rámce, na polovinu. Pro závislost průchodnosti na celkovém toku platí

$$S = G.e^{-G} \quad .$$

Výhodou metod Aloha je okamžité odvysílání rámce. Překročí-li však zátěž určitou mez, zvýší se počet opakovaných rámců a silně poklesne pravděpodobnost přenosu nepoškozeného kolizí. Síť přechází do tzv. *zablokovaného stavu*, ze kterého se nelze bez modifikace parametrů sítě dostat.

Situaci vystihuje obr. 4.3, ve kterém jsou vyjádřeny závislosti průchodnosti sítě S na počtu zablokovaných stanic M pro konečný počet stanic v síti (v našem případě 100 stanic) a dvě intenzity opakování α. (Vyšší intenzitě opakování odpovídají kratší prodlevy mezi pokusy.) Průběhy vynesené pro dvě intensity opakování α udávají výstupní tok sítě v závislosti na počtu zablokovaných stanic (při menší intenzitě opakování α výstupní tok klesá). Čárkovaně je vyznačen pokles toku vstupujícího do sítě, pokles je způsoben snížením počtu stanic schopných generovat vstupní tok. Průsečíky A a C křivky pro $\alpha = 0.1$ s přímkou odpovídají stabilním rovnovážným stavům, bod B je rovnovážným stavem nestabilním. Z pracovního bodu sítě A síť přejde po jisté době do bodu C, cesta zpět je možná pouze snížením intenzity opakování α, které změní průběh závislosti výstupního toku a dovolí vrátit se do bodu blízkého bodu A a k původní hodnotě intenzity opakování.



Obrázek 4.3: Stabilita u metod Aloha

Metody, které přizpůsobují intenzitu opakování α zátěži, označujeme jako metody řízené.

Řízená Aloha

Pakety, které kolidovaly, jsou u metod Aloha opakovány po náhodně volené době. Dynamickou volbou intenzity opakování α lze dosáhnout toho, že metoda Aloha pracuje s výhodnější charakteristikou (s větší intenzitou opakování vedoucí k rychlejšímu předání rámce), ale při překročení zátěže, které by vyvolalo zablokování, se charakteristika změní na charakteristiku s jediným bodem stability (stabilní charakteristika).

Pro změnu parametru α existuje řada heuristik. Nejjednodušší je snížení intenzity opakování α na hodnotu odpovídající stabilní charakteristice po zadaném počtu neúspěšných pokusů. Velice účinnou metodou je řada postupně klesajících hodnot parametru α, které stanice postupně používá při určení okamžiku dalšího opakování, mluvíme o *ustupování*.

Zajímavou metodou používanou v rádiových sítích je sledování provozu na kanále a nastavování intensity opakování na hodnotu tak, aby celková zátěž G nepřesáhla hodnotu $G = 1$. Protože pro pravděpodobnost klidového stavu na kanále platí

$$P_0 = e^{-G}$$

(pro taktovanou Alohu), může stanice sledováním poměru neobsazených slotů určit celkovou zátěž a z ní odvodit intenzitu opakování. Vhodnou funkcí je například

$$\alpha = \frac{e^{-G}}{(N+1)} = \frac{P_0}{(N+1)} \quad .$$

řízené opakování kolizí poškozených rámců má podstatný význam nejen pro metody Aloha, ale i pro metody, které uvádíme dále (metody CSMA a jejich modifikace); bez řízení nelze ani u těchto metod zajistit trvalou efektivní činnost. Jednoduchou variantu metody s prodlužováním střední doby prodlevy po každém neúspěšném pokusu na dvojnásobek známe například u Ethernetu jako *exponenciální ustupování* (exponential back-off).

Rezervační Aloha

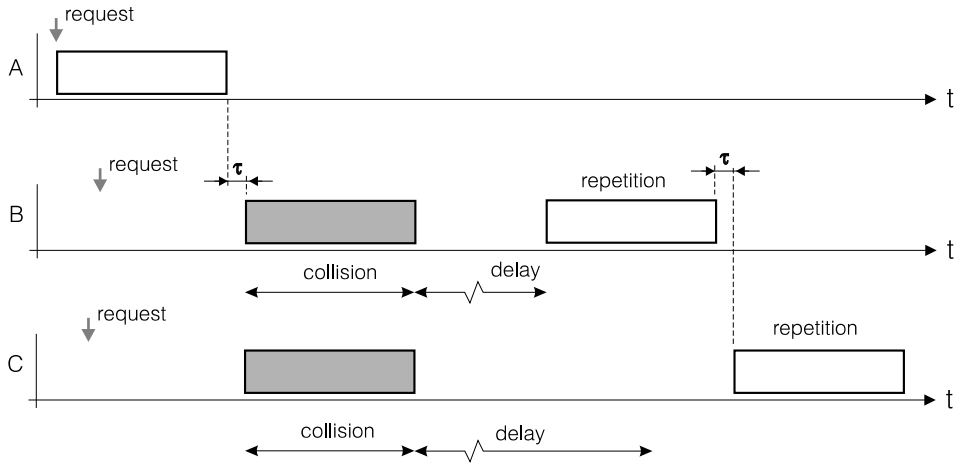
Metody Aloha jsou často využívány pro rezervaci kanálu časového nebo frekvenčního multiplexu, stanice pak může kanálu využívat po delší dobu. S tímto postupem se setkáváme u rádiových sítí, příklad použití metody Aloha pro bezdrátové sítě najdeme na str. 133.

4.2 Metody CSMA

Metody Aloha byly navrženy pro rádiové sítě a nevyužívaly možnosti zjistit obsazenost přenosového kanálu před zahájením vlastního vysílání. U lokálních sítí, které se vyznačují malým zpožděním signálu a dokonalou slyšitelností stanic, však taková informace dovolí podstatně omezit pravděpodobnost kolize. Metody, které znalost obsazení kanálu využívají, nazýváme metodami náhodného přístupu s příposlechem nosné, zkráceně metodami *CSMA* (Carier Sense Multiple Access).

Naléhající CSMA

Stanice, která používá metodu *naléhající CSMA* (persistent CSMA, 1-persistent CSMA), před odesláním rámce testuje stav kanálu. Je-li kanál obsazen, stanice odloží vysílání na okamžik, kdy se kanál uvolní.

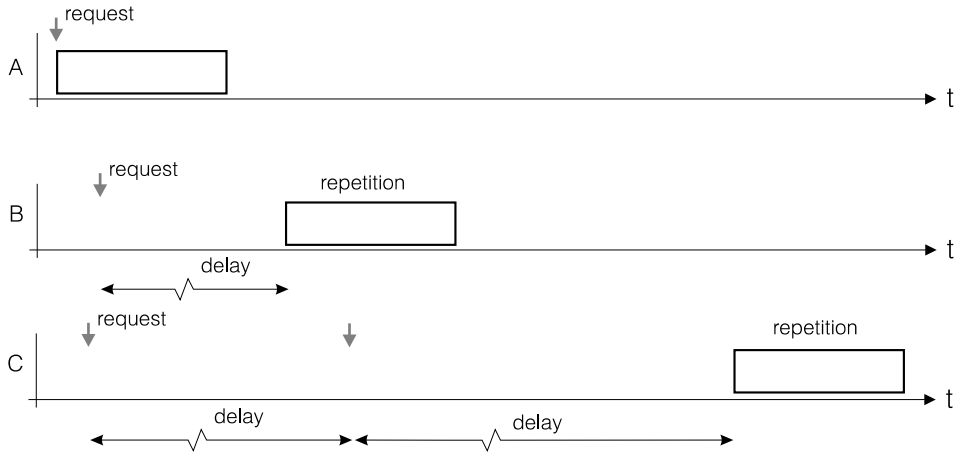


Obrázek 4.4: Naléhající CSMA

Zjevnou nevýhodou této jednoduché metody je riziko kolize stanic, které čekají na uvolnění kanálu. Poměrně vysoké riziko se projeví nižší průchodnosti kanálu (zhruba 53 %, obr. 4.7).

Nenaléhající CSMA

Stanice, která používá metodu *nenaléhající CSMA* (non-persistent CSMA), před odesláním rámce testuje stav kanálu. Je-li kanál volný, stanice zahájí vysílání. Pokud je kanál obsazen, stanice počká náhodně zvolenou dobu a znovu testuje stav kanálu. Postup opakuje do odeslání rámce.

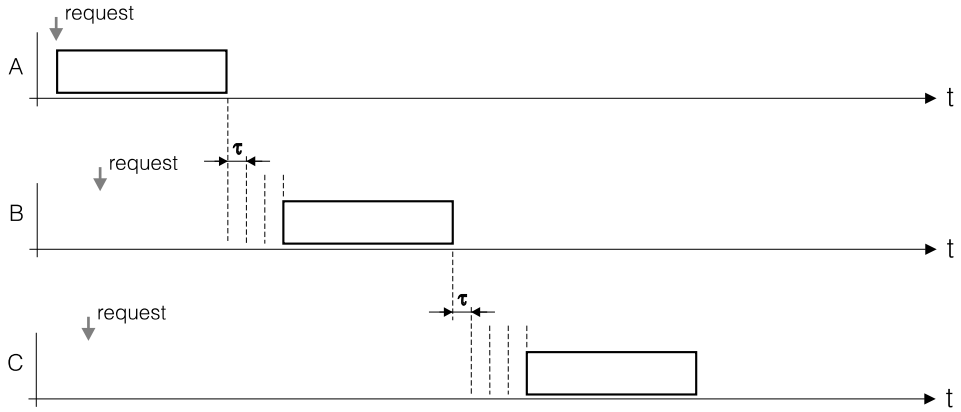


Obrázek 4.5: Nenaléhající CSMA

Volbu náhodné prodlevy obvykle převádíme na volbu náhodného násobku taktu, který obvykle vybíráme tak, že odpovídá době průchodu signálu sběrnicí. Závislost průchodnosti na zátěži uvádí obr. 4.7, z grafu je patrná schopnost metody využít velice dobře kapacitu kanálu, cenou je však velký počet nutných pokusů a tedy i velké zpoždění při přenosu.

p-naléhající CSMA

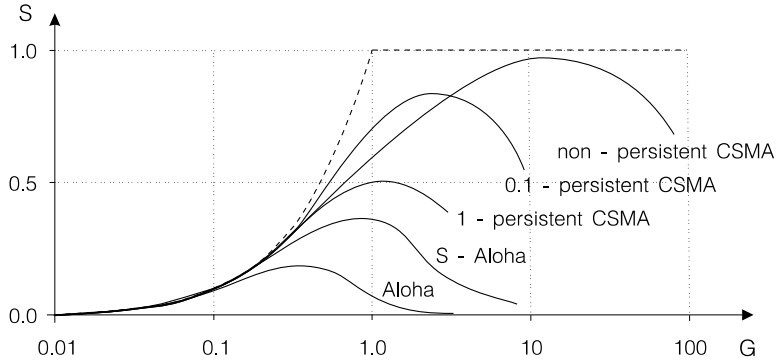
Stanice, která používá metodu *p-naléhající CSMA* (p-persistent CSMA), před odesláním rámce testuje stav kanálu. Je-li kanál volný, stanice zahájí vysílání. Pokud je kanál obsazen, stanice počká na uvolnění kanálu. Byl-li kanál volný nebo se právě uvolnil, začne stanice s pravděpodobností p vysílat a s pravděpodobností $q = 1 - p$ odloží další činnost o krátký časový interval (může odpovídat délce šíření signálu médiem). Po uplynutí této doby celou činnost opakuje až do úspěšného odeslání rámce.



Obrázek 4.6: p-naléhající CSMA

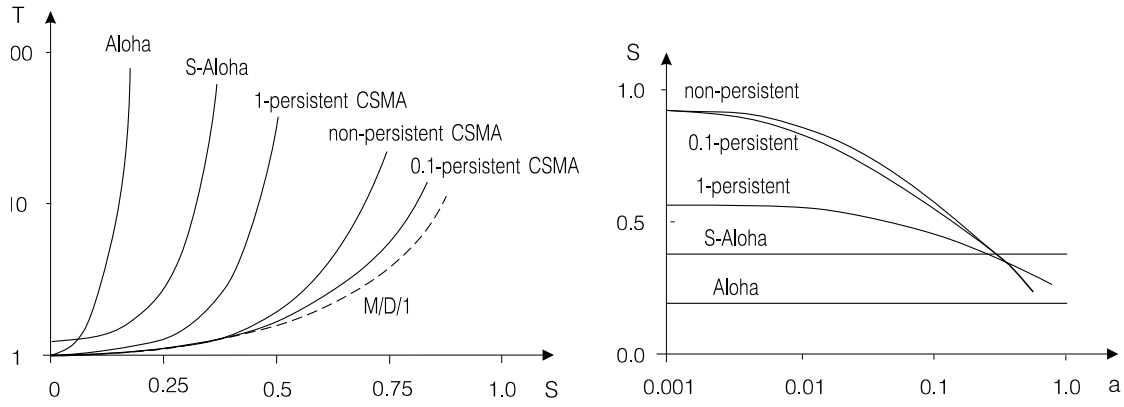
Volba parametru p dovolí optimálně nastavit využití kanálu a střední zpoždění rámce vzhledem k zátěži. Pro $p = 1$ metoda přechází v naléhající CSMA, pro $p \to 0$ se sice průchodnost kanálu blíží hodnotě $S = 1$, ale střední doba přenosu rámce roste nade všechny meze.

Metody CSMA samy o sobě nezajišťují stabilitu. Pro udržení kanálu v pracovním bodě je stejně jako v případě metod Aloha nutné použít vhodnou metodu řízení (například snižovat intenzitu opakování nebo hodnotu parametru p u metody p-naléhající CSMA).



Obrázek 4.7: Propustnost u metod CSMA

Metody CSMA dovolují ve srovnání s metodami Aloha podstatně zvýšit propustnost kanálu. Závislost propustnosti S na celkovém toku G u těchto metod uvádí obr.4.7. Propustnost u naléhající CSMA není nejvyšší, je to důsledek vysoké pravděpodobnosti kolize stanic čekajících na uvolnění kanálu. U nenaléhající CSMA je nevýhodou vysoký počet pokusů o přístup ke kanálu. Vhodné nastavení koeficientu p u p-naléhající CSMA dovoluje najít vhodný kompromis mezi těmito extrémy. Graf však ilustruje i skutečnost, kterou je chybějící limit pro doručení paketu. Ustupování navíc znevýhodňuje stanice po kolizích, metody proto nejsou vhodné pro aplikace v oblasti technologického řízení.



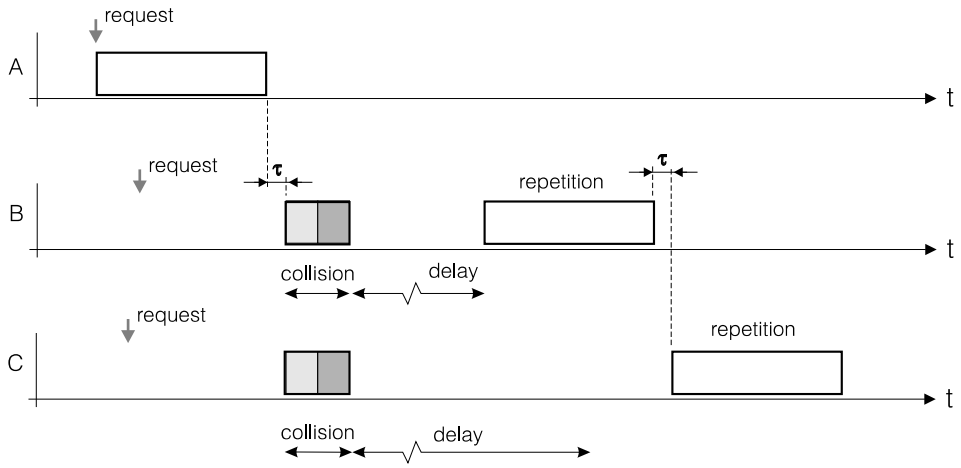
Obrázek 4.8: Zpoždění a efektivita u metod CSMA

Metody CSMA jsou použitelné pouze v sítích s malým rozsahem, ve kterých se koeficient a pohybuje v mezích $0 < a < 0.1$. Pro rozsáhlé lokální sítě efektivita metod klesá a pro hodnoty $a \to 1$ je dokonce horší než pro metody Aloha (obr. 4.8).

U dosud popisovaných metod jsme neuvažovali potřebu potvrzování přijatých rámců (přesněji řečeno, neuvažovali jsme, že potvrzení budou muset soupeřit o přidělení kanálu). Na potvrzení se konečně můžeme dívat jako na nutnou přídavnou zátěž, která pouze v určitém poměru sníží čistou průchodnost sítě. Chceme-li tuto přídavnou zátěž eliminovat, můžeme pro potvrzení rezervovat časový interval bezprostředně navazující na vyslání rámce a zajistit, že žádná ze stanic nesmí v tomto intervalu zahájit vysílání nového datového rámce. Taková modifikace bývá označována jako *CSMA/CA* (*Collission Avoidance*), popis najde čtenář na str. 36.

4.3 Metody CSMA/CD

Metody CSMA nejsou schopné zabránit kolizi, je-li časový interval mezi zahájením vysílání dvou stanic menší než jistá mez, daná konečnou rychlostí šíření signálu v kanále, vzdáleností stanic a rychlostí reakce detekčních obvodů. U naléhající CSMA je navíc při větší zátěži velice nepříjemné, že dojde-li během vysílání rámce více než jeden další požadavek, je výsledkem kolize (bezprostředně po uvolnění kanálu). Kolize, které u dlouhých rámců blokují po dlouhou dobu přenosový kanál, snižují dosažitelnou průchodnost. Zlepšení lze dosáhnout, dokážeme-li je detekovat a předčasně zastavit vysílání. Příslušné metody označujeme jako *CSMA/CD* (Carrier-Sense Multiple Access with Collision Detection).



Obrázek 4.9: Metoda CSMA/CD

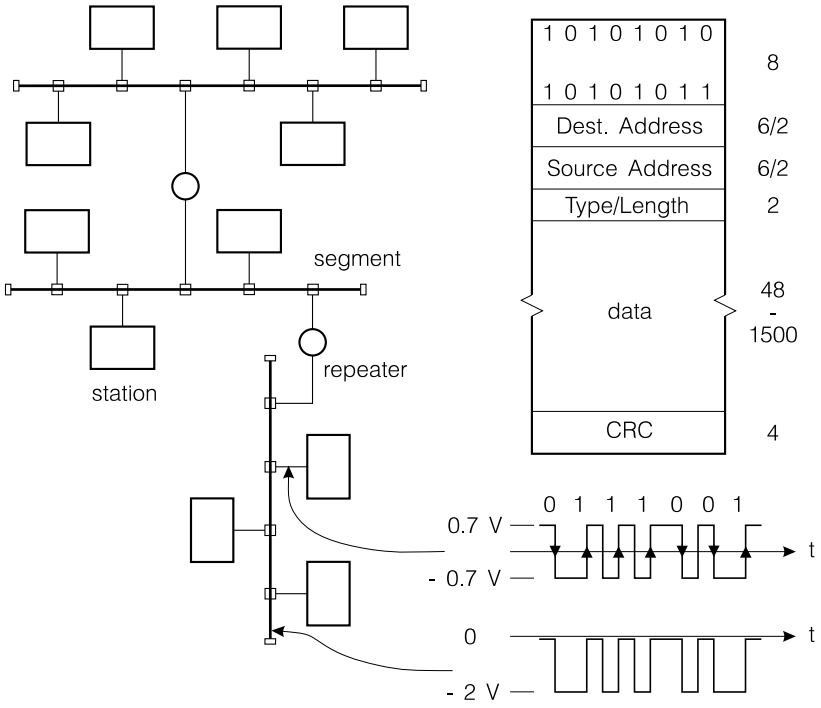
Použití metod CSMA/CD vyžaduje použít kanálu, na kterém lze kolizi zjistit. Nejjednodušším kanálem, který detekci kolize umožňuje, je sběrnice typu otevřený kolektor. V praxi však obvykle kolizi detekujeme jinak, například sledováním napětí na médiu, které je buzeno proudovými zdroji vysílačů (Ethernet 10BASE5) nebo sledováním signálu na krouceném páru přijímače (10BASE-T).

Stanice, která má připravený rámec k vyslání a detekuje klid na sdíleném kanále po definovanou dobu označovanou jako *kolizní slot*, zahájí vysílání synchronizační posloupnosti a odešle vlastní rámec. Stanice, která chce vysílat, ale indikuje provoz na médiu, musí počkat na uvolnění média a uplynutí ochranného intervalu (kolizního slotu). Teprve potom může stanice zahájit vysílání, uvedený postup odpovídá *naléhající CSMA*. Je však samozřejmě možné opřít se i o *p-naléhající CSMA* nebo o *nenaléhající CSMA*.

Pokud stanice vstoupila do kolize a tuto skutečnost rozpoznala, přeruší vysílání rámce, ale ještě před uvolněním média odešle *kolizní posloupnost* (jam). Tato posloupnost zajistí, že kolizi rozpoznají všechny kolidující stanice. O opakované vysílání se stanice pokusí až po určité, náhodně zvolené době. Náhodná volba odmlky brání periodickému opakování kolize. Pokud by se kolize opakovala a stanice další pokus zahájila po sice náhodně zvolené době, ale se stejnou střední hodnotou prodlevy, mohlo by při větším počtu stanic dojít k situaci, kdy kolize zcela zablokují užitečnou činnost kanálu a síť se z tohoto stavu bez vnějšího zásahu nedostane. Jde o situaci, kterou jsme si popsali jako bistabilní chování (str. 28). U metod CSMA/CD musíme, stejně jako u všech metod CSMA, zajistit stabilitu režimu práce řízením intenzity opakování.

4.3.1 Ethernet

Lokální síť Ethernet se sběrnicovou architekturou byla vyvinuta v první polovině 70-tých let firmou Xerox pod označením Ethernet II a později byla standardizována firmami Xerox, Intel a DEC (jako norma DIX) a normami IEEE 802.3 a ISO 8802/3 pro sítě v administrativě (těmto modifikacím se budeme věnovat na str. 65). Dnes se zřejmě jedná o nejrozšířenější technologii využívající širokou škálu přenosových médií a lze očekávat, že bude používána i k připojování stanic k rozsáhlým přenosovým sítím využívajícím vnitřně technologii jinou.



Obrázek 4.10: Ethernet

Přenosovým médiem sítě Ethernet II je speciální koaxiální kabel o charakteristické impedanci 50 Ω. Výhodou kabelu s nižší charakteristickou impedancí než je běžnějších 75 Ω je vyšší odolnost proti parazitním kapacitám konektorů a proti vnějšímu rušení. Data jsou přenášena v základním pásmu v kódu Manchester, rychlost přenosu je 10 Mb/s. Originální návrh (z roku 1972) počítal s rychlostí přenosu 2.9 Mb/s, pracoval se segmentem koaxiálního kabelu o impedanci 70 Ω a délce do 1 km a měl poněkud jinou strukturu rámce.

Základem sítě je *segment* – sběrnice o délce nejvýše 500 m, na kterou lze připojit až 100 stanic. Rozsáhlejší sítě lze vytvořit propojováním segmentů pomocí *opakovačů* (rozbočovačů, Repeater) – limitem je 1024 stanic a vzdálenost mezi nejvzdálenějšími stanicemi (měřeno po médiu) 2.5 km.

Stanice je k segmentu připojena prostřednictvím *transceiveru* (kombinace vysílače a přijímače signálu média), který je připevněn přímo na kabel. Transceiver je spojen se stanicí pětinásobným krouceným dvoudrátem na vzdálenost až 50 m. Rozhraní je označováno jako *AUI* (Attachment Unit Interface), kabel jako *AUI kabel* (Drop Cable).

Řízení sítě odpovídá metodě CSMA/CD. Stanice, která během vysílání zjistí kolizi na médiu, přeruší vysílání rámce a odešle speciální posloupnost (jam). Tato posloupnost je navržena tak, aby vyvolala indikaci kolize i u ostatních stanic (vysílajících, případně i přijímajících). Výsledkem je uvolnění média všemi stanicemi nejpozději do doby odpovídající součtu dvojnásobku doby šíření signálu sítí a doby vysílání kolizní posloupnosti. Tento součet je označován jako *kolizní slot* a má délku 51.2 μs.

Zajímavé je řízení intenzity opakování. Při zjištění kolize je další pokus plánován na r-tý kolizní slot, kde r je náhodně zvolené číslo z intervalu $0 < r <= 2^k$. Exponent k je odvozen z počtu neúspěšných pokusů o odeslání rámce a, $k = min(n, 10)$. Po šestnácti pokusech je o nemožnosti odeslat rámec (zřejmě jde o poruchu média nebo stanice) informován ovladač a/nebo aplikační program. Tato metoda řízení je označována jako *"exponential back-off"*.

Struktura rámce v síti Ethernet odpovídá obr. 4.10. Adresa má délku 48 bitů a je pro každou stanici jedinečná. Datová část rámce má délku 46 až 1500 znaků, délka nejkratšího rámce odpovídá délce kolizního slotu (512 bitů). Zabezpečení zajišťuje cyklický kód s dvaatřicetibitovým generačním polynomem.

Lokální síť Ethernet dovoluje využít kapacitu média na 80 až 95 % (podle délky zpráv), při zátěži větší než 40 % však silně roste doba přenosu (jde o důsledek 1-naléhání). Podstatnou nevýhodou původní sítě Ethernet je použití drahého speciálního koaxiálního kabelu, který je nutný pro spolehlivou funkci detektoru kolize.

4.3.2 Appletalk

Algoritmus metody CSMA/CD není nutně vázán na použití detektoru kolize v zapojení stanice. Příkladem je síť Appletalk firmy Apple navržená jako komunikační prostředek pro osobní počítače Apple a MacIntosh.

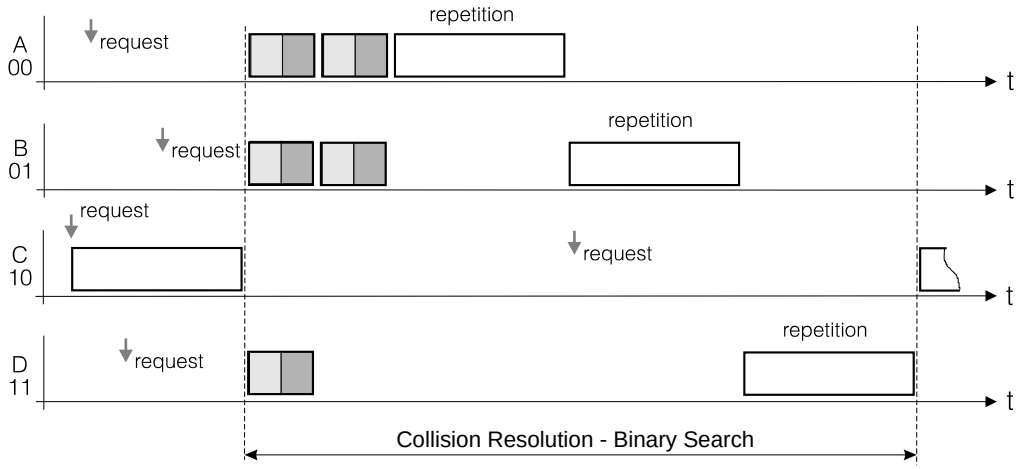
Funkci speciálního detektoru kolize v této síti nahrazuje zvláštní způsob rezervace kanálu pro přenos zprávy. Stanice, která chce získat neobsazený kanál (to zjistí detektorem signálu média stejně jako u metod CSMA), vyšle krátký rámec adresátovi zprávy a vlastní zprávu vysílá až po potvrzení tohoto rámce. Pokud dojde ke kolizi více stanic v této fázi, projeví se to poškozením žádosti nebo odpovědi; stanice, která neobdrží odpověď do časového limitu, předpokládá kolizi a odloží další pokus o náhodně zvolený interval. Zjednodušená metoda CSMA/CD použitá u sítě Appletalk má podobné vlastnosti jako základní CSMA/CD pouze v případě sítí s menší přenosovou rychlostí a malým rozměrem. Síť Appletalk používá přenosové rychlosti 230.4 kb/s na krouceném dvoudrátu se signály podle doporučení RS-422 EIA (s možností práce více vysílačů), délka jednoho segmentu sběrnicové sítě je 300 m, do sítě je možné propojit nejvýše 32 stanic. Po dlouhou dobu bylo rozhraní AppleTalk standardní výbavou počítačů Macintosh.

4.4 Deterministické řešení kolize – CSMA/DCR

Metoda CSMA/CD není posledním krokem v oblasti metod náhodného řízení. Dalšího zlepšení vlastností (zvýšení průchodnosti a snížení doby doručení zprávy) dosahují metody, které po zjištění kolize nejdříve zajistí přenos zpráv pro stanice, které se kolize zúčastnily, a teprve potom dovolí přístup stanic ostatních. Metody jsou označovány jako *CSMA/DCR* (Carrier-Sense Multiple Access with Deterministic Collision Resolution), my budeme mluvit o deterministickém řešení kolize.

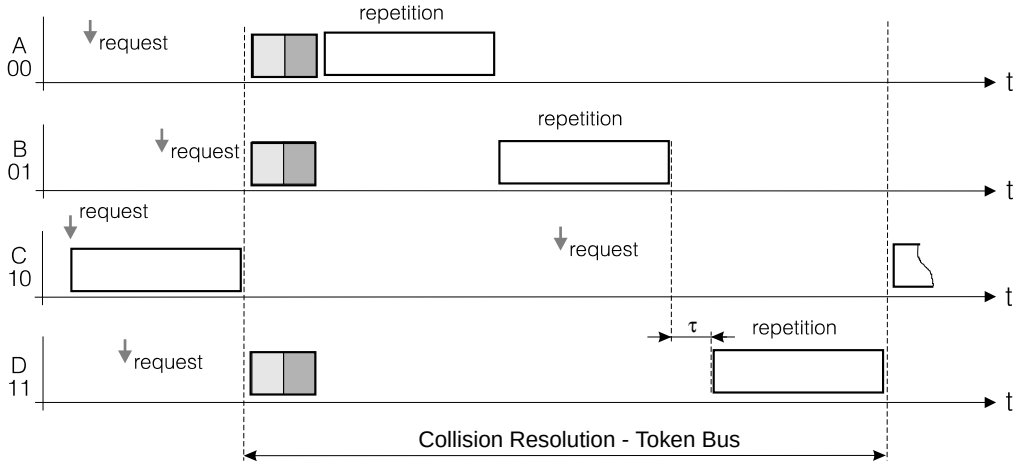
Nejjednodušší metodou řešení kolize je vyhledávání aktivních stanic v binárním stromu. Dojde-li ke kolizi v režimu CSMA/CD, stanice, které se kolize účastnily, se rozdělí do dvou skupin (například podle nejvýznamnějšího bitu adresy). Stanice z prvé skupiny se pokusí o vyslání zprávy, stanice druhé skupiny počkají na ukončení přenosů stanic v prvé skupině. Dojde-li v prvé skupině opět ke kolizi, postup dělení skupiny se opakuje. Po konečném počtu kroků je ve skupině jediná stanice, která odvysílá svůj rámec (obr. 4.11).

Modifikací metody, při které rozdělíme v každém kroku soupeřící stanice na větší počet skupin, můžeme dosáhnout rychlejšího řešení kolize; krajním případem je rozdělení stanic na skupiny o jediné stanici, který připomíná deterministickou rezervaci kanálu metodou "round-



Obrázek 4.11: Deterministické řešení kolize – binární výběr

robin" nebo virtuální logický kruh (obr. 4.12). Takového řešení například použila firma Intel pro komunikaci mezi jednočipovými mikropočítači i80132, přenosová rychlost je 2 Mb/s.

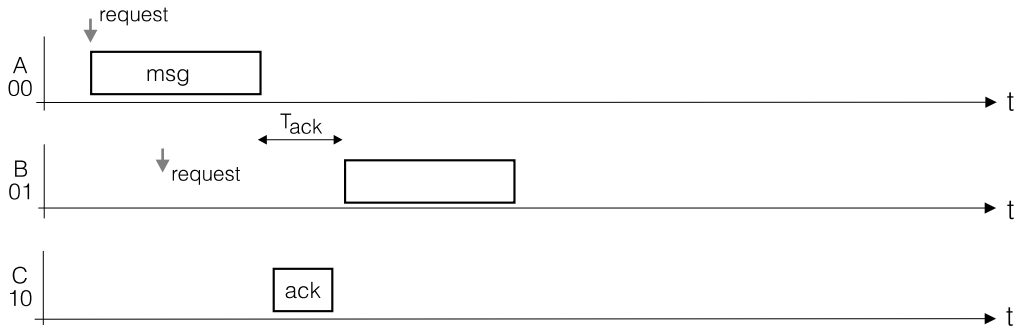


Obrázek 4.12: Deterministické řešení kolize – logický kruh

Prvý uvedený postup (binární vyhledávání aktivních stanic) je výhodnější pro malé zátěže, druhý (postupné vyhledávání) pro zátěže velké. řada modifikací se pokouší o nalezení kompromisu mezi těmito extrémy na základě informací o okamžitém zatížení sítě.

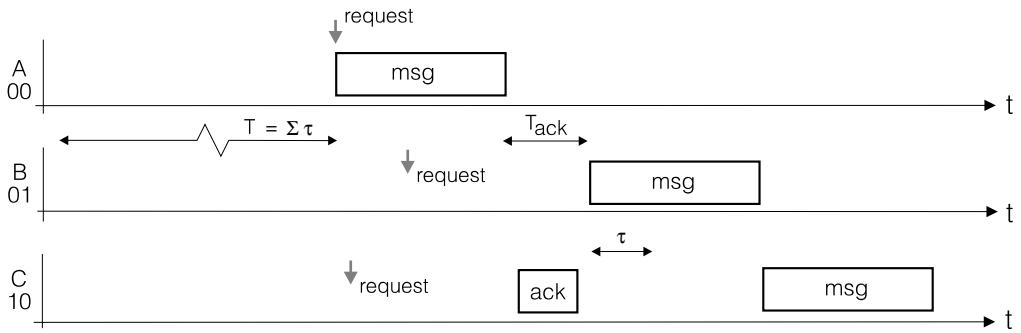
4.5 Metody CSMA/CA

U dosud popisovaných metod jsme neuvažovali potřebu potvrzování přijatých rámců (přesněji řečeno, neuvažovali jsme, že potvrzení budou muset soupeřit o přidělení kanálu). Na potvrzení se můžeme dívat jako na nutnou přídavnou zátěž, která pouze v určitém poměru sníží čistou průchodnost sítě. Chceme-li eliminovat nepříjemný vliv této přídavné zátěže na soupeření stanic o kanál, můžeme pro potvrzení rezervovat časový interval bezprostředně navazující na vyslání datového rámce a zajistit, že žádná ze stanic nesmí v tomto intervalu zahájit vysílání rámce nového. Taková modifikace bývá označována jako *CSMA/CA* (Collission Avoidance).



Obrázek 4.13: Metody CSMA/CA – bezkolizní potvrzování

Modifikací postupu i pro datové rámce je modifikace metody CSMA, u které povolíme stanici s adresou m zahájit vysílání rámce nejdříve po době $((m-n)$ **mod** $N).\tau$ po uvolnění média stanicí s adresou a (A je celkový počet stanic sítě a τ je doba šíření signálu médiem).



Obrázek 4.14: Metody CSMA/CA – virtuální logický kruh

Pokud stanice indikovala na médiu klid po dobu delší, než je tato minimální prodleva (nebo po době $N.\tau$ pokud stanici chybí informace o adrese posledního vysílače), smí zahájit vysílání okamžitě. Případná kolize je řešena opakováním po náhodně volené prodlevě, po bezkolizním průchodu prvého rámce se rozběhne *"virtuální kruh"* . Podobnou metodu označujeme proto také jako *virtuální logický kruh* (str. 41).

Další úpravu CSMA/CA nalezneme u rádiových sítí podle IEEE 802.11 (str. 120). Zde je vyčleněna vedle potvrzování ještě prioritní komunikace s prodlevou kratší než pro běžný provoz. Protože se stanice nemusí navzájem slyšet, lze navíc pro vysílání delších rámců využít mechanismus označovaný jako RTS/CTS. Stanice před startem vlastního vysílání požádá o přidělení kanálu krátkým rámcem RTS a dostane od základnové stanice souhlas CTS. Ten slyší všechny stanice. Podobný postup je používán u sběrnice AppleTalk.

5. Deterministický přístup ke sdílenému médiu

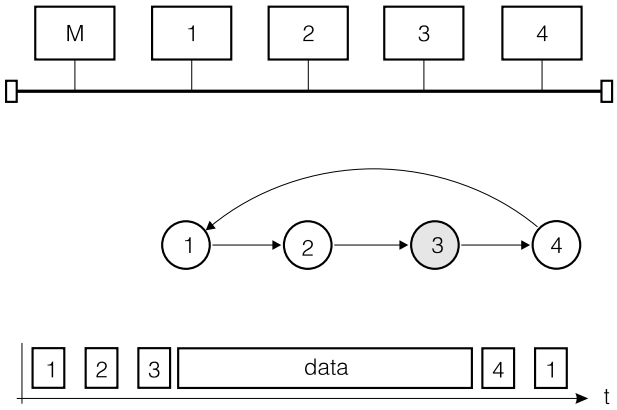
5.1 Centralizované řízení

Nejjednodušší cestou, jak přizpůsobit řízení přístupu jednotlivých stanic ke sdílenému kanálu náhodnému charakteru jejich požadavků, je vyhradit jednu ze stanic jako *stanici řídící*. Řídící stanice přiděluje kapacitu kanálu ostatním – *podřízeným stanicím*. Výhodou je efektivita blížící se ideálnímu obslužnému systému, ta je narušena potřebou obětovat část kapacity kanálu (nebo speciální podkanál) pro vyřízení žádostí nebo pro vyhledání aktivních stanic. Další nevýhodou je závislost sítě na spolehlivosti řídící stanice.

Přidělování na výzvu

Přidělování na výzvu je nejstarším způsobem adaptivního přidělování kapacity přenosového kanálu (používají ji například linkové protokoly jako BSC nebo HDLC NRM). Nejjednodušší modifikací metody je *cyklická výzva*.

Řídící stanice postupně vyzývá stanice podřízené. Pokud má podřízená stanice připravená data k odeslání, pak je odešle, jinak pouze potvrdí výzvu nebo neodpoví. Cyklická výzva je výhodná pro malý počet stanic a malé zpoždění signálu ($a < 1$). Příklad přenosu dat po kanále řízeném cyklickou výzvou uvádí obr. 5.1.



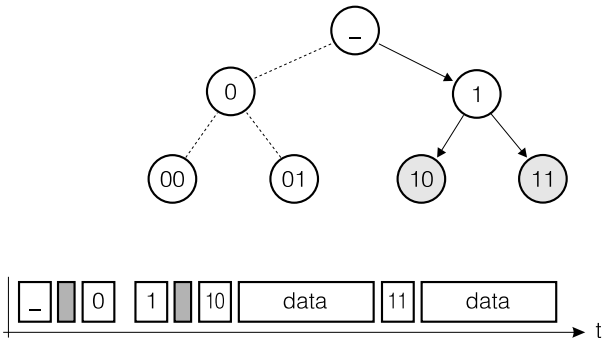
Obrázek 5.1: Řízení kanálu cyklickou výzvou

Cyklická výzva má rozumné chování při vysokém rovnoměrném využití kapacity kanálu, pro malé zatížení kanálu a velký počet stanic je střední zpoždění paketu zbytečně dlouhé.

Zlepšení přináší modifikace metody použitelná u speciálního typu kanálu, který dovolí stanici rozpoznat, zda v daném okamžiku vysílá jedna nebo více stanic. Je založena na faktu, že při malém zatížení a velkém počtu stanic lze aktivní stanici podstatně rychleji nalézt *binárním vyhledáváním*.

Pro binární vyhledávání stanice rozdělíme do dvou přibližně stejně velkých skupin, a každou skupinu dále rozdělíme do dvou přibližně stejně velkých skupin, atd., až máme v každé skupině jedinou stanici. Příklad rozdělení stanic do skupin uvádí obr. 5.2.

Řídící stanice při vyhledávání aktivní stanice postupně vyzývá skupiny stanic počínaje od kořene binárního stromu, aktivní stanice odpovídají signálem po sdíleném kanále. Pokud je ve vyzývané skupině jediná aktivní stanice, pak může zahájit přenos paketu. Je-li aktivních stanic více, řídící stanice sestoupí ve stromu o jednu úroveň a výzvu opakuje.



Obrázek 5.2: Binární vyhledávání

Algoritmus binárního vyhledávání je rychlejší pro malé zátěže, algoritmus cyklické výzvy pro zátěže velké. Přizpůsobíme-li úroveň, od které procházíme binární strom, změřené zátěži, lze dosáhnout optimálních výsledků; metodu označujeme jako metodu *adaptivní výzvy*.

Bitbus

Jako příklad sítě s centralizovaným řízením si uvedeme síť známou pod jménem Bitbus. Byla navržena firmou Intel jako levná lokální síť pro distribuované systémy řízení využívající jednočipové mikropočítače. Obdobná řešení najdeme u všech výrobců řídící techniky. Přenosovým médiem je kroucený dvoudrát, elektrické signály odpovídají doporučení RS-485 EIA, což je modifikace sériového rozhraní RS-422 EIA pro sběrnici s více vysílači. Na segment sběrnice o délce až 330 m lze připojit nejvýše 28 stanic, jednotlivé segmenty je možné propojovat opakovači, je však nutné dodržet dvě omezení – nejvýše 250 stanic v síti a nejvýše tři opakovače mezi libovolnými dvěma stanicemi.

Data jsou přenášena rychlostí 375 kb/s v kódu NRZI. Při menších požadavcích lze volit pomalejší variantu sítě s rychlostí 62.5 kb/s, která dovolí prodloužit segment na 1300 m. Struktura rámce sítě Bitbus je odvozena od bitově orientovaných linkových procedur (transparence je zajištěna vkládáním bitů, řídící pole je obdobou řídícího pole HDLC protokolu). (Jiné firemní protokoly vytvářejí formát rámce z asynchronně přenášených znaků.)

Řízením sítě je pověřena jedna stanice, která vyzývá k vysílání jednotlivé stanice podřízené, algoritmus výzvy je podřízen potřebám konkrétní aplikace. Citlivost metody na výpadek řídící stanice není paradoxně u sítí pro technologické řízení kritická, protože veškerá komunikace probíhá právě mezi řídící stanicí a stanicemi podřízenými.

Přidělování na žádost

Alternativou k přidělování na výzvu je *přidělování na žádost*, žádosti stanic jsou řídící stanici předávány po samostatném kanále. Realizace samostatného fyzického kanálu asi nepřichází u lokálních sítí v úvahu (najdeme ho např. u počítačových sběrnic pro předání žádosti o přerušení nebo o DMA cykl), s využitím podkanálu časového multiplexu se setkáme u distribuovaných metod řízení přístupu v rádiových sítích. Zajímavé využití neaktivních vedení hvězdicové sítě pro předání žádosti uvidíme u sítě 100VG-AnyLAN (str. 95).

5.2 Distribuované řízení

Nevýhodou centralizovaného přidělování je závislost na funkci centrální stanice, výhodou (proti dále popisovaným metodám náhodného přístupu) je limitovaná doba předání paketu adresátovi. Tuto vlastnost zachovávají i *deterministické metody distribuovaného řízení*, které odstraňují závislost na jediné řídící stanici. Patří sem řada metod, které mají spíše teoretický charakter, praktické použití má rezervační metoda, metoda binárního vyhledávání (prioritního přístupu) a metoda logického kruhu (Token-passing Bus).

Rezervace kanálu

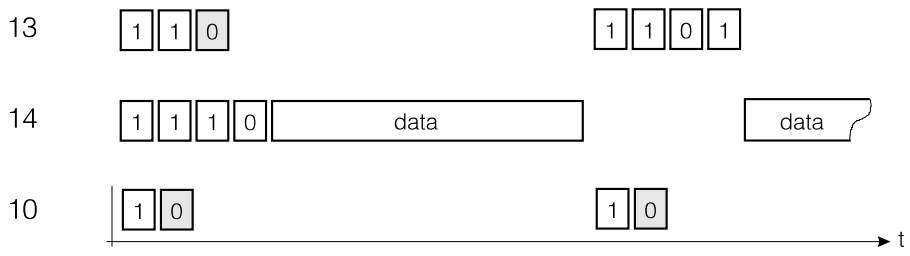
Rezervační metody jsou distribuovanou variantou přidělování kanálu na žádost. Vyčleňují z přenosového kanálu *rezervační rámec*, ve kterém si aktivní stanice rezervují přidělení kanálu datového. Rezervační rámec má charakter *bitové mapy* – každé stanici je přidělen slot o délce větší (alespoň dvojnásobně) než je doba šíření signálu médiem, v něm může stanice požádat o přidělení datového kanálu (například vysláním nosné). Po ukončení rezervačního rámce mají všechny stanice informaci o všech žádostech. Přístup ke kanálu dat jim může být poskytnut v pořadí rezervačních slotů. Algoritmus rezervace a přidělování běží synchronně na všech stanicích, jeho nevýhodou je nízká efektivita pro rozsáhlé sítě s velkým počtem stanic při malé zátěži.

Obrázek 5.3: Distribuované rezervační metody

Obr. 5.3 uvádí dvě modifikace rezervační metody, popsanou metodu *bitové mapy* a její modifikaci *"round-robin"* u které jsou rezervační sloty vloženy mezi bloku přenášených dat (datový kanál je stanici přidělen okamžitě, jakmile si ho ve svém slotu rezervuje).

Binární vyhledávání

Přidělíme-li jednotlivým stanicím jednoznačně binární adresy, můžeme je využít pro bezkolizní přidělování kanálu. Předpokládejme, že zprávu má připravenou k vyslání několik stanic. Stanice zahajuje svou činnost vysíláním adresy počínajíc od nejvyššího bitu a vyhodnocuje situaci na médiu. Pokud stanice zjistí na médiu bit shodný s vyslaným bitem adresy, může ve vysílání pokračovat, pokud tomu tak není musí vysílání zastavit. Po odvysílání adresy může právě jedna ze stanic pokračovat odesláním připravené zprávy a celý postup se cyklicky opakuje.

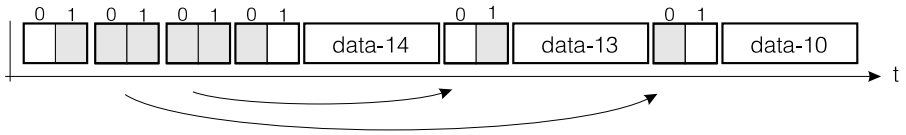


Obrázek 5.4: Prioritní přístup

Adresace stanic definuje jejich prioritu, a metoda je proto označována jako *prioritní přístup* (obr. 5.4). Vyhledávání aktivní stanice využívá speciální schopnosti některých přenosových kanálů – realizovat funkci logického součtu nebo součinu signálů více stanic (takovým kanálem je například sběrnice s otevřenými kolektory). V praxi se často jako signál sloužící k vyhledávání používá náhodný signál – šum.

Proti metodám rezervačním je prioritní přístup efektivnější (v rozsáhlých sítích s velkým počtem stanic), algoritmus vyhledávání odpovídá prohledávání binárního stromu. Není však spravedlivý ke všem stanicím, spravedlnosti lze dosáhnout například tak, že umožníme (třeba cyklické) změny adres stanic po každém přidělení kanálu.

Pozn.: V řídících systémech je adresa často nahražována identifikátorem funkce, kterou má zpráva aktivovat. Priorita přístupu ke kanálu může být u takových systémů vítanou vlastností.

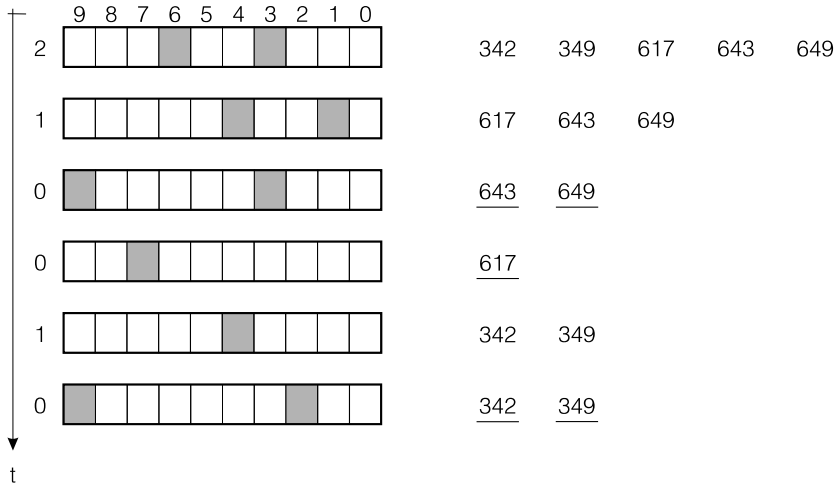


Obrázek 5.5: Binární vyhledávání

Jednodušší možností, jak zajistit spravedlnosti algoritmu vyhledávání, je prohledat celý binární strom a podle výsledku přidělovat kanál podobně jako u rezervace s binární mapou. Postup, který si označíme jako *binární vyhledávání* ilustruje obr. 5.5, jeho implementace vyžaduje například použití slotů se dvěma poli, které dovolí předat informaci o aktivitě stanic v obou větvích.

MLMA – dekadické vyhledávání

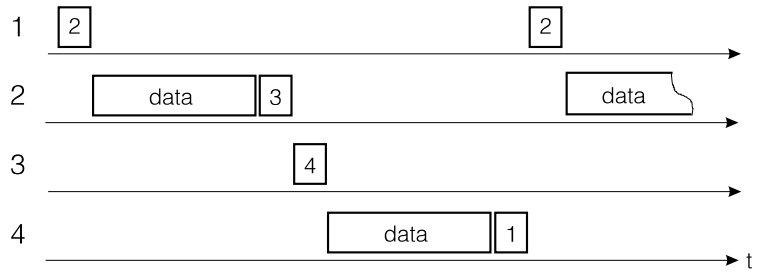
Další možnou úpravou vyhledávání je použití adres (a stromu vyhledávání) s jinou aritou. Příklad vyhledávání aktivních stanic v systému s třímístnou dekadickou adresou uvádí obr. 5.6. Metoda je uváděna pod názvem *MLMA* (Multiple Level Multiple Access), pro předání informace o aktivitách stanic v jednotlivých větvích stromu jsou potřebné sloty o délce deseti polí.



Obrázek 5.6: MLMA – dekadické vyhledávání

Logický kruh (Token Passing Bus)

Prakticky univerzálně využívanou metodou distribuovaného přidělování kanálu je metoda logického kruhu nebo některá její modifikace. Jde o obdobu "round-robin" vyhledávání, postup je však asynchronní.

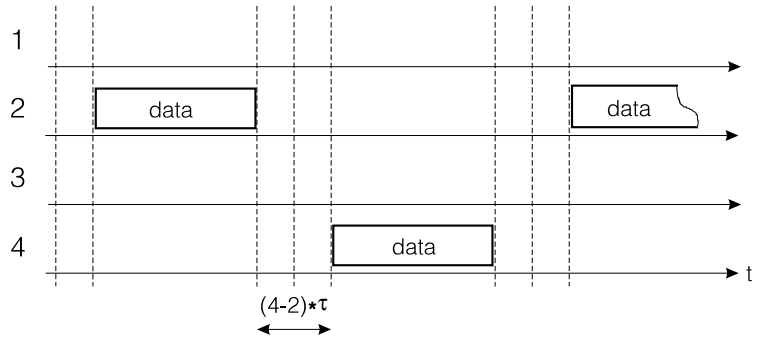


Obrázek 5.7: Logický kruh

Stanice sdílející přenosový kanál jsou označeny adresou a tyto adresy tvoří cyklickou posloupnost. Každá ze stanic zná svou vlastní adresu a adresu stanice, která smí vysílat po ní. Jedna ze stanic je vždy aktivní, v tomto stavu smí odvysílat datový paket, nebo předat řízení následující stanici speciálním paketem – *pověřením* (označovaným jako *Token* – pešek). Metoda je podle předávání pověření mezi stanicemi na sběrnici označována jako *Token-Passing Bus* nebo zkráceně *Token Bus*. Určitým problémem metody je její startování a změna posloupnosti stanic pro stanice, které během provozu sítě z logického kruhu odstupují nebo se do něj naopak chtějí zapojit. Metody pro modifikaci posloupnosti stanic v těchto případech jsou označovány jako metody *rekonfigurace*, příklady rekonfigurace si uvedeme pro síť ARCNet a pro sítě podle doporučení IEEE 802.4.

Virtuální logický kruh

Nevýhodou logického kruhu může být zbytečně velké zpoždění při malé zátěži na malé síti s velkým počtem stanic. Snížení režie způsobené předáváním pověření řadou neaktivních stanic dosahuje metoda řízení označovaná jako *virtuální logický kruh*. Chování stanic na virtuálním logickém kruhu uvádí obr. 5.8.



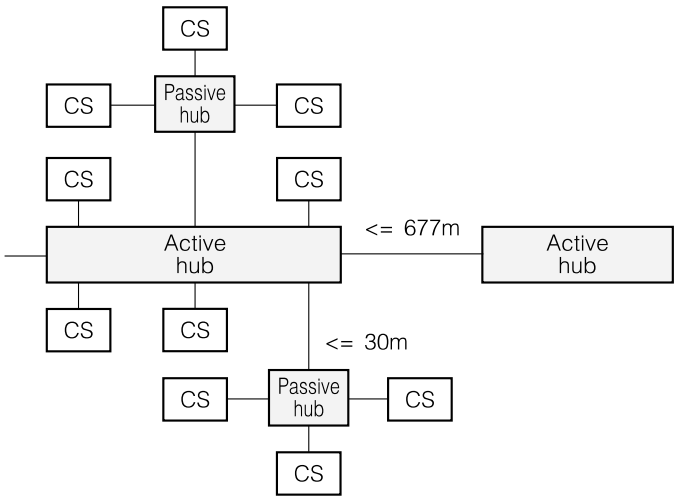
Obrázek 5.8: Virtuální logický kruh

Stanice (nechť má adresu m) sleduje provoz na médiu a dojde-li po ukončení vysílání stanice s adresou n k uvolnění média na dobu $((m-n)\ \mathbf{mod}\ N).\tau$, kde N je počet stanic a τ doba šíření signálu médiem, pak stanice, má-li zprávu k vyslání, může začít vysílat. Metoda má v oblasti malých zátěží lepší chování než metoda logického kruhu (záleží na poměru mezi dobou šíření signálu na sběrnici a dobou potřebnou k předání pověření).

Metoda vyžaduje dobrou vzájemnou synchronizaci stanic, kterou je někdy obtížné spolehlivě zajistit. Pokud uvolníme pravidla pro převzetí kanálu tak, že stanice smí zahájit vysílání do kanálu, který byl po dobu N.τ neobsazený, dostáváme kanál s možností kolize – obdobu v další části textu popisované metody CSMA/CA (str. 36).

5.3 ARCNet

Síť *ARCNet* (Attached Resource Computer) byla vyvinuta firmou Datapoint v roce 1976 a rychle se stala jednou z nejrozšířenějších lokálních sítí. Dnes již má spíše historický význam, používána je jen v sítích technologických. Síť má stromovou topologii (obr. 5.9), stanice jsou propojeny s opakovači (active hub) úseky koaxiálního kabelu o charakteristické impedanci 93 Ω a maximální délce 677 m, stejné omezení délky kabelů platí i pro vzájemné propojení opakovačů. K jednomu opakovači lze připojit až 8 sousedů (opakovačů nebo stanic), na cestě mezi dvěma stanicemi smí být nejvýše 9 opakovačů.



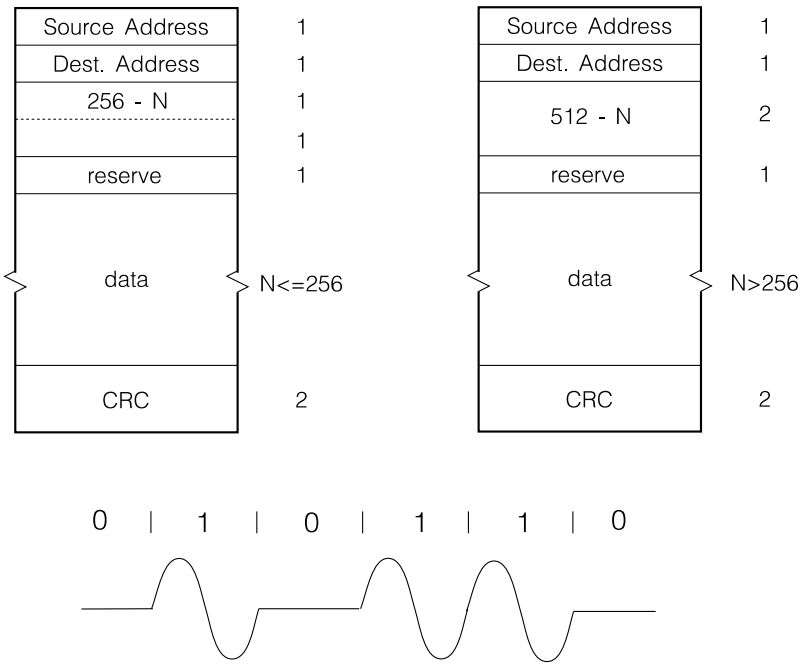
Obrázek 5.9: ARCNet – topologie

Malý počet stanic, nejvýše čtyři, lze propojit pasivním rozbočovačem (passive hub) do hvězdy, vzdálenost mezi stanicí a rozbočovačem je nejvýše 30 m. Použití rozbočovače v síti s opakovači se nedoporučuje. Někteří výrobci dovolují i sběrnicovou strukturu sítě, použití symetrických kabelů (do 133 m) nebo optických vláken (do 3.8 km).

Síť má přenosovou rychlost 2.5 Mb/s, lze propojit nejvýše 255 stanic, které smí být vzájemně vzdálené nejvýše 6.5 km. Pro řízení sítě je použita metoda logického kruhu a dále popsaná metoda rekonfigurace. Adresy stanic volí správce sítě (nastavením přepínačů), pro přenos dat jsou definovány dva formáty rámců.

V běžném provozu stanice, která přijme pověření, odvysílá datový paket (má-li nějaký připravený) a předá řízení svému následníkovi. Ten pověření převezme a do časového limitu, který je dán dobou šíření signálu v síti, síť obsadí, buď přenosem datového paketu, nebo předáním pověření další stanici.

Vyprší-li časový limit, který svou hodnotou 31 μs odpovídá nejrozsáhlejší konfiguraci sítě, považuje stanice svého následovníka za neaktivního. V takovém případě stanice použije nejblíže vyšší adresu (posloupnost adres v logickém kruhu je vzestupná) a pokusí se nalézt dalšího možného následovníka. To opakuje, až se podaří logický kruh opět navázat.



Obrázek 5.10: ARCNet – signál na médiu a formáty rámců

Výpadek aktivního držitele pověření vyvolá klid na médiu po ještě delší dobu. Libovolná stanice, která indikuje klid po dobu delší než 78 μs zahájí algoritmus výběru nového držitele pověření. Pokud se do doby (255 - adresa_stanice)*147 μs logický kruh neobnoví, stává se stanice aktivním držitelem pověření a obnovuje provoz na logickém kruhu. Podobně probíhá i počáteční spustění sítě, při kterém stanice, která takto dostává právo síť zkonfigurovat, vyhledá svého následovníka.

Pokud se chce dosud neaktivní stanice zapojit do logického kruhu, počká 840 ms na pověření (které pravděpodobně neobdrží) a potom posloupností 756 jednotkových bitů naruší funkci kruhu a vyžádá si tak znovuspuštění podle předchozího odstavce.

V roce 1990 byla uvedena na trh modifikace sítě Advanced ARCNet, která použitím šestnáctistavové fázově-amplitudové modulace dosahuje rychlosti přenosu 20 Mb/s při zachování původní modulační rychlosti.

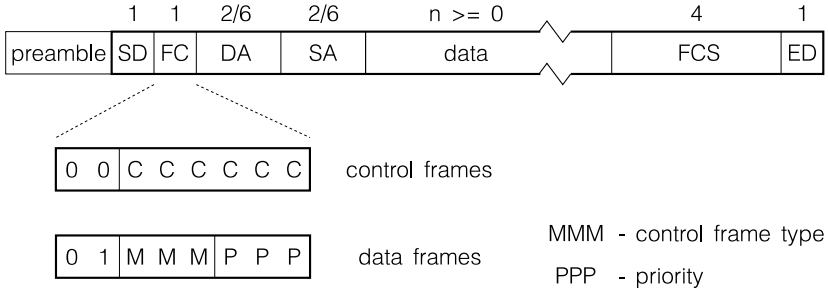
5.4 IEEE 802.4

Doporučení ANSI/IEEE 802.4 definuje sběrnicovou síť s řízením typu logický kruh určenou pro aplikace v automatizovaných systémech řízení výroby. Předchůdcem specifikace byla síť *MAP* (*Manufacturing Automation Protocol*) firmy General Motors, ta využívá jen některých způsobů přenosu definovaných doporučením IEEE 802.4. Sítě mohou vedle přenosu v základním pásmu po optických vláknech ve hvězdicové topologii (přenosové rychlosti 5, 10 a 20 Mb/s) využívat i koaxiální kabel o charakteristické impedanci 75 Ω (velký výběr typů) v pásmu základním i přeloženém. Pro přenos v základním pásmu se používá kmitočtová modulace se spojitou změnou fáze (Phase-Continuous FSK – 1 Mb/s), a kmitočtová modulace s koherentní fází (Phase-Coherent FSK – 5 a 10 Mb/s). Pro přenos v přeloženém pásmu je využívána amplitudově-fázová modulace (1, 5 a 10 Mb/s).

Stejně jako pro jiné sítě typu logický kruh je pro síť IEEE 802.4 definován algoritmus předávání pověření a algoritmus rekonfigurace.

	Phase Continuous Baseband	Phase Coherent Baseband	Broadband	Optical Fiber
Data rate	1Mb/s	5Mb/s 10Mb/s	1Mb/s 5Mb/s 10Mb/s	5Mb/s 10Mb/s 20Mb/s
Bandwidth			1.5MHz 6MHz 12MHz	
Frequency	5MHz	7.5MHz 15MHz		850nm 850nm 850nm
Modulation	Manchester FSK	Phase Coherent FSK	Multilevel duobinary AM/PSK	Manchester AM
Topology	Bus	Bus	Directional Bus	Star
Medium	Coax 75Ω	Coax 75Ω	Coax 75Ω	Optical fibre
Scrambling	no	no	yes	no

Obrázek 5.11: Média IEEE 802.4



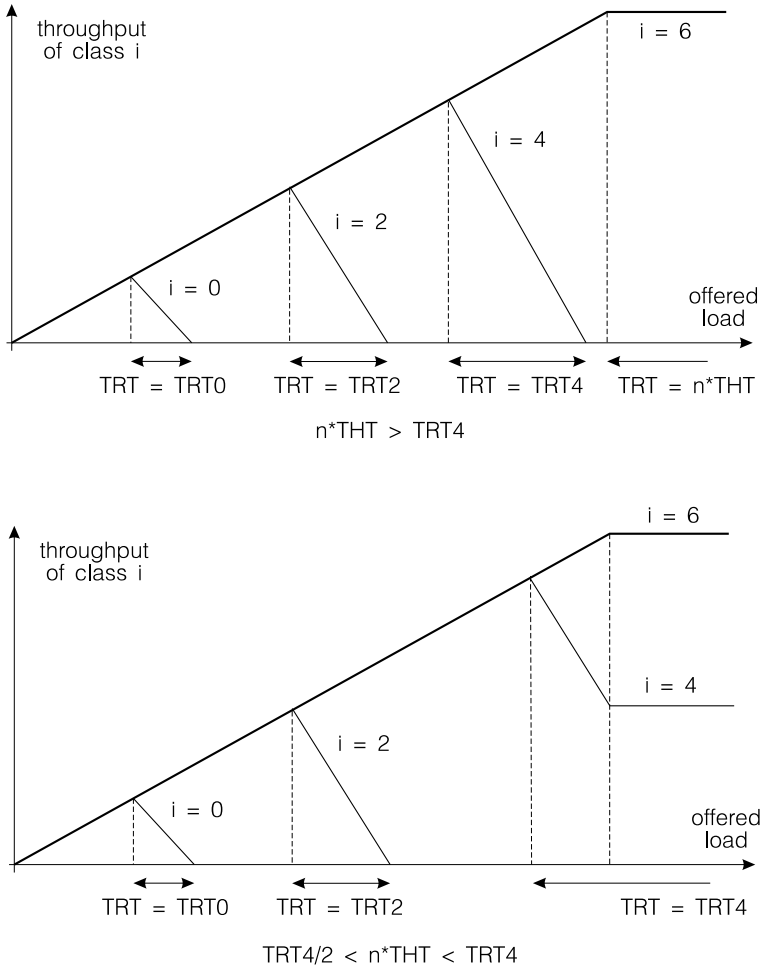
Obrázek 5.12: IEEE 802.4 – formáty rámců

Na rozdíl od ARCNetu je posloupnost adres sestupná, každá stanice si uchovává adresu svého předchůdce a adresu svého následníka. Stanice, která přijme od svého předchůdce pověření, se stává stanicí aktivní a může odeslat jeden paket. Po odeslání paketu, nebo bezprostředně po příjmu pověření (pokud nemá co vysílat) předá aktivní stanice pověření svému následníkovi. Toto předání musí proběhnout do určeného časového limitu, jinak je stanice považována za porouchanou a je startován algoritmus, který ji z logického kruhu vyjme.

Začlenění stanice do logického kruhu probíhá následovně. Každá aktivní stanice před předáním pověření periodicky vysílá výzvu *Solicit-Successor* (ve skutečnosti existují dvě varianty výzvy *Solicit-Successor-1* a*Solicit-Successor-2*), určenou stanicím s adresami ležícími v intervalu mezi její vlastní adresou a adresou jejího následovníka. Pokud na výzvu nedojde do časového limitu odpověď *Set-Successor*, aktivní stanice předá řízení následovníkovi. Pokud na výzvu odpoví jediná stanice, je zařazena do logického kruhu a aktivní stanice jí předá řízení jako svému následníkovi. Konečně, pokud na výzvu odpoví více stanic, dochází ke kolizi, aktivní stanice kolizi rozpozná (chybná odpověď) a spouští algoritmus vyhledání nejbližšího následovníka. Výběr je obdobou binárního vyhledávání, v každém kroku vyzývající stanice vyšle rámec *Resolve-Contention*, odpovídající stanice využívá hodnotu dvou bitů adresy ke stanovení prodlevy pro svou odpověď (strom, ve kterém vyhledáváme následníka má aritu rovnu čtyřem).

O *vyjmutí* z logického kruhu žádá aktivní stanice svého předchůdce rámcem *Set-Successor* a předává řízení svému následovníku. Pokud stanice neodpoví na příjem pověření vysláním zprávy nebo pověření do časového limitu (Response Window) ani na druhý pokus, je považována za porouchanou a její předchůdce vysílá dotaz *Who-Follows* na jejího následovníka. Pokud se následovník ozve alespoň po opakování rámce *Who-Follows*, je logický kruh opět navázán, v opačném případě stanice vyzývá libovolnou stanici rámcem *Solicit-Successor-2* a binárním vyhledáváním najde nejbližšího následovníka.

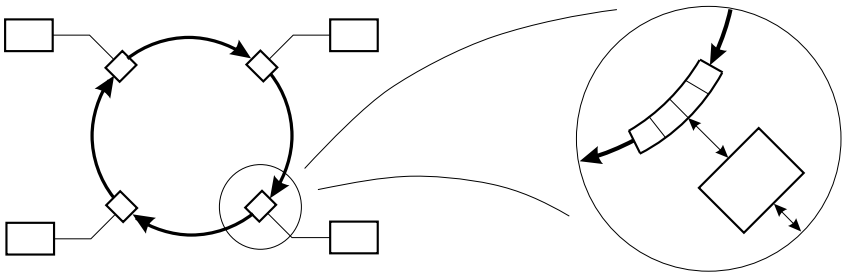
Spuštění logického kruhu je realizováno vysláním rámce *Claim-Token* stanicí, která indikuje klid na médiu. Délka rámce závisí na dvou nejvýznamnějších bitech adresy, pokud stanice po ukončení vysílání zjistí signál na médiu je to důsledek kolize a přenechá spustění kruhu soupeři. V dalším kroku použije pro určení délky rámce Claim-Token další dva bity adresy, až konečně po vyčerpání všech bitů adresy zůstává jediná stanice, která odstartuje kruh vysláním rámce *Solicit-Successor-2*. Zajímavým způsobem je u sítě MAP řešena priorita. Každému datovému rámci může být přidělena jedna ze čtyř úrovní priority (označených jako 0, 2, 4 a 6, přičemž úroveň 6 je nejvyšší). Prioritní schéma je řízeno časovými limity THT (Token Holding Time) a TRT0 (Token Rotation Time) až TRT4. Stanice měří čas od odeslání pověření, do vyčerpání limitu TRT0 smí vysílat rámce s prioritou 0, do vyčerpání TRT2 rámce s prioritou 2 a do vyčerpání limitu TRT4 rámce s prioritou 4. Při překročení limitu TRT4 smí vysílat již pouze rámce s nejvyšší prioritou 6, přičemž celková doba, po kterou smí stanice podržet pověření, je určena parametrem THT. Obrázek 5.13 uvádí chování sítě při zvyšující se zátěži pro různá nastavení parametrů.



Obrázek 5.13: IEEE 802.4 – řízení priority

6. Kruhové sítě

Alternativou k sítím využívajícím sdíleného přenosového kanálu (sběrnicové sítě a hvězdicové sítě s logicky pasivními uzly) jsou kruhové sítě. Kruhová síť je tvořena stanicemi, které jsou vzájemně propojené jednosměrnými dvoubodovými spoji do kruhu (obr. 6.1).



Obrázek 6.1: Struktura kruhové sítě

Stanice kruhu obsahují posuvný registr (o délce alespoň jednoho bitu); celou síť si lze představit jako kruhový posuvný registr, ve kterém data postupují od vysílající stanice a po oběhu kruhem se k ní opět vracejí a jsou z kruhu odebrána. Doba, kterou data k průchodu sítí potřebují, závisí na "délce" tohoto "registru" a na rychlosti přenosu.

Pro dobu oběhu dat kruhovou sítí platí

$$t = \frac{N.l_R}{C} + \frac{\Sigma l_C}{c}$$

kde A je počet stanic, l_R délka registru jedné stanice, C kapacita kanálu, l_C délky jednotlivých spojů a konečně c rychlost šíření signálu v přenosovém médiu.

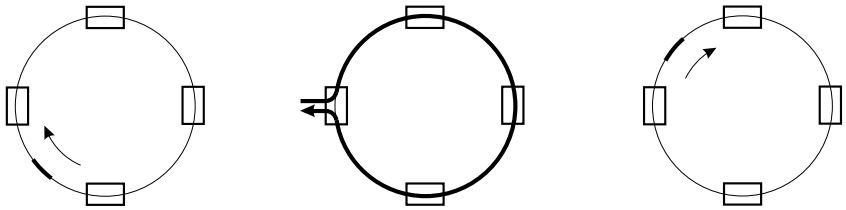
Kruhové sítě mají mnoho výhodných vlastností. Zjednodušují nasazení metod distribuovaného deterministického řízení přístupu i v případech, kdy stanice jsou velmi vzdálené (desítky kilometrů). Náhodný přístup se využívá pouze okrajově, například pro rozběh sítě. Metody zajišťují ohraničenou dobu zpoždění rámce a vysoké využití kapacity kanálu, jedinou nevýhodou může být neodstranitelné malé zpoždění i při malé zátěži. Spoje lze snadno realizovat jako světlovody, síť je potom velmi odolná proti vnějšímu rušení. Jedinou vážnou nevýhodou kruhových sítí je jejich závislost na správné činnosti všech komponent, výpadek kteréhokoliv uzlu nebo spoje přeruší komunikační kanál. Součástí každé konkrétní technologie je proto i definice postupu, který dovolí chránit síť proti výpadkům spojů a stanic – síť rekonfigurovat.

Další funkcí nutnou pro praktický provoz kruhové sítě je její monitorování. Některá ze stanic kruhu (*aktivní monitor*) sleduje průchody rámců kruhem, a pokud dojde k opakovanému průchodu téhož rámce (což může způsobit poškození adresy odesílatele nebo výpadek odesílatele) kruhem, pak rámec z kruhu odebere. Bez monitorování by došlo k omezení průchodnosti sítě nebo k jejímu úplnému zablokování (záleží na použité metodě přístupu).

Pro kruhové sítě se v praxi využívá tří základních metod řízení; podle použité metody mluvíme o sítích Newhallova typu (Token-Passing Ring, předávání pověření), sítích Pierceova typu (pevný časový multiplex) a o sítích s vkládáním rámců.

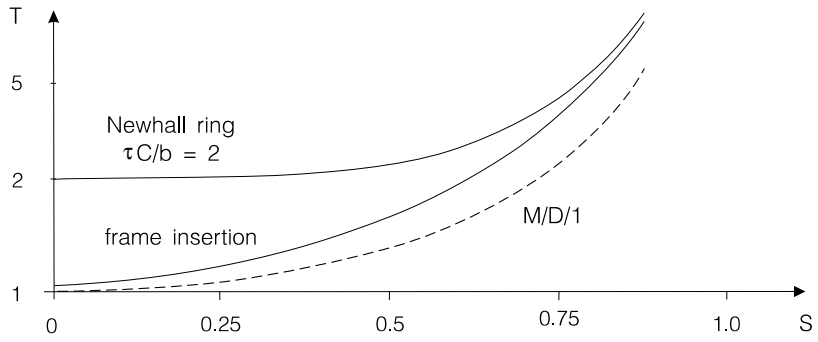
6.1 Newhallův kruh

V síti Newhallova typu obíhá v klidovém stavu, kdy žádná stanice nepotřebuje vysílat, pouze speciální datový blok – *pověření* (token, pešek). Postupné předávání pověření na kruhu zajistí, že v konkrétním okamžiku má pověření jediná stanice. Stanice, která má data k vyslání a převezme pověření, může data ve formě rámce do kruhu vyslat. Vyslání rámce spočívá ve změně pověření na znak (posloupnost znaků) identifikující počátek rámce a v odeslání vlastního rámce. Po odvysílání rámce odevzdá stanice řízení předáním pověření svému sousedu. Přenos jednoho rámce kruhovým spojem ilustruje obr. 6.2.



Obrázek 6.2: Přenos rámce Newhallovým kruhem

Zpoždění rámce v síti je pro malou zátěž dáno dobou, kterou musí stanice čekat na obíhající pověření, a dobou vlastního přenosu. Doba oběhu pověření závisí na rychlosti přenosu, počtu stanic a délce jejich registrů a konečně také na délce propojovacích spojů. Pro velké zátěže se zpoždění v síti blíží ideálnímu přidělování kanálu. Závislost zpoždění na počtu stanic a délce registrů uvádí obr. 6.3.



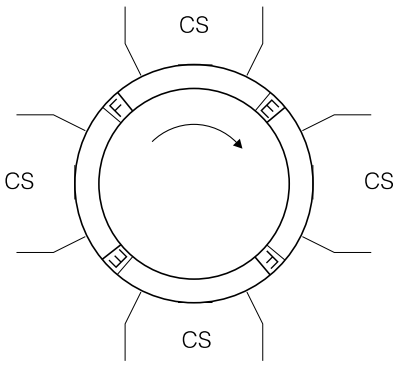
Obrázek 6.3: Zpoždění v kruhové síti

Správná funkce Newhallovy sítě je závislá na obíhání jediného pověření. Duplicitní pověření může způsobit kolizi. Ta se projeví příjmem jiného rámce, než který byl odeslán. Nechceme-li odstartováním sítě nebo jejím znovuspuštěním po ztrátě pověření pověřit jedinou stanici, můžeme realizovat distribuovaný algoritmus. Příklad řešení uvidíme u sítě IBM Token Ring.

Síť Newhalova typu je pro své chování a poměrně snadnou realizaci (obvodovou podporu – volitelné propojení přijímače a vysílače jednobitovým posuvným registrem najdeme u řady obvodů pro synchronní komunikaci) často používána jako komunikační prostředek distribuovaných řídících systémů. Na principu sítě Newhallova typu je založena síť IBM Token Ring a síť FDDI, obě si popíšeme ve zvláštních odstavcích.

6.2 Pierceův kruh

Rozdělením paměťové kapacity kruhové sítě na krátké segmenty – minipakety dostáváme sít Pierceova typu (obr. 6.4). Minipakety přenášejí jediné šestnáctibitové slovo. Obsazení minipaketu je indikováno nastavením bitu E/F (Empty/Full). Stanice, která má data k vysílání a volný minipaket ve svém registru, minipaket obsadí a po jeho oběhu sítí (a po potvrzení adresátem) jej opět uvolní.



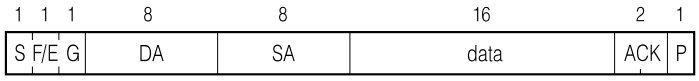
Obrázek 6.4: Kruhová síť Pierceova typu

Problémem sítě je likvidace minipaketů s poškozenou adresou odesílatele, počáteční naformátování segmentů a kontrola správnosti formátu. Tyto činnosti jsou pravidelně realizovány jednou ze stanic, tuto stanici označujeme jako řídící stanici kruhu.

Sítě Pierceova typu patří k nejdéle využívaným lokálním sítím a přes malé využití kapacity kanálu jsou často používány.

Cambridge Ring (Planet)

Kruhová lokální sít Cambridge Ring byla vyvinuta na univerzitě v Cambridge v roce 1975 pro spojení počítačů a koncentrátorů terminálů. Přenosovým médiem sítě je dvojice symetrických vodičů (slouží současně pro napájení obvodů kruhového rozhraní stanic), lze však použít i světlovodů. Pro symetrické vodiče je maximální vzdálenost mezi stanicemi 100 m, přenosová rychlost je 10 Mb/s. Data jsou přenášena v minipaketech o délce 38 bitů, jejich struktura odpovídá obr. 6.5.



Obrázek 6.5: Minipaket lokální sítě Cambridge Ring

Vedle šestnáctibitového pole dat a dvou osmibitových adres (Destination Address, Source Address) zde najdeme bit S sloužící rámcové synchronizaci, bit F/E (Full/Empty) indikující obsazení rámce a bit P zajišťující přenášená data jednoduchou paritou.

Bit G slouží řídící stanici sítě k rozpoznání a likvidaci minipaketu s poškozenou adresou odesílatele, který by jinak blokoval obsazený slot. Tento bit je v odesílaném minipaketu nastavován na hodnotu G=0. Řídící stanice bit přestaví u obsazeného rámce na hodnotu G=1 a odesílatel zprávy ho při uvolnění rámce opět vrátí na hodnotu G=0. Kombinaci odpovídající obsazenému rámci (F/E=1) a hodnotě G=1 rozpozná řídící stanice jako chybu a rámec uvolní.

Pole ACK slouží přijímači k uložení potvrzení, odesílatel nastavuje pole na hodnotu ACK=11. Vrácené hodnoty pole ACK indikují, že příjemce nemohl data převzít (ACK=00),

že data byla přijata (ACK=01) nebo že data byla odmítnuta (ACK=10). Původní hodnota ACK=11 indikuje, že příjemce neodpovídá (je mimo provoz, adresa je chybná).

Velmi podobnou strukturu rámce jako Cambridge Ring má i síť Planet (Private Local Area Network) firmy Racal Milgo (byla po dlouhou dobu využívána pro páteře rozsáhlých sítí Ethernet, její přenosová rychlost je 80 Mb/s), a síť Domain firmy Apollo (dnes součást firmy Hewlett-Packard). Síť se odlišuje přenosovým médiem, kterým je koaxiální kabel, a strukturou rámce, který má 42 bitů.

6.3 Vkládání rámců

Metoda vkládání rámců byla vyvinuta firmou Hasler v roce 1974 a má dobré chování v oblasti malých i velkých zátěží. Její nevýhodou je složitější technická realizace, přenos rámce sítí ilustruje obr.3.33.

Obrázek 6.6: Kruhová síť s vkládáním rámců

Stanice sítě, která chce vyslat rámec, ho uloží do zvláštního registru. Počká na konec rámce, který stanicí prochází, a přepnutím přepínače prodlouží síť o svůj registr. Odeslaný rámec oběhne sítí, je převzat adresátem a vrací se do registru stanice, která registr ze sítě opět odepne.

Kruhová síť SILK, která na tomto principu pracuje, používá pro přenos rychlostí 16 Mb/s koaxiální kabel 75 Ω. Datové pakety přenášejí šestnáctibitová slova.

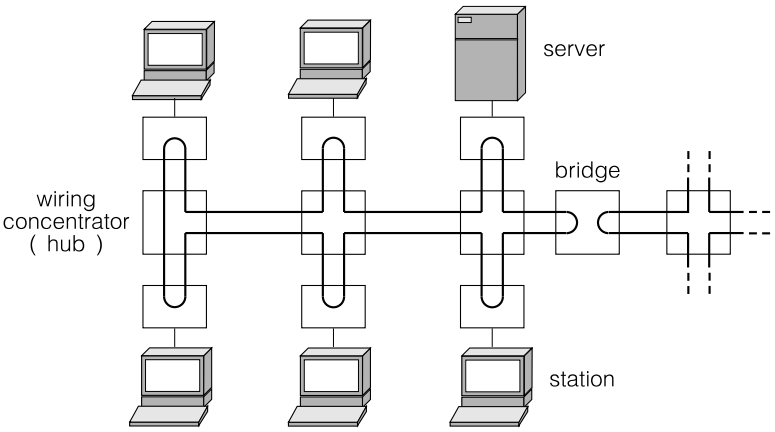
6.4 IBM Token Ring (IEEE 802.5)

Nejběžnější kruhovou sítí je síť definovaná normou IEEE 802.5, známá pod názvem (IBM) Token Ring. Je tvořena stanicemi propojenými jednosměrnými dvoubodovými spoji do jednoduchého kruhu. Spoje mezi stanicemi jsou vedeny přes *koncentrátory* (Cabling Concentrator, někdy je označujeme jako rozbočovače) tak, že síť tvoří fyzicky strom (takovou strukturu někdy označujeme jako lalokovou síť) – obr. 6.7. Vedení spojů přes koncentrátory dovoluje detekovat nefunční stanice a spoje a vyřadit je z kruhu.

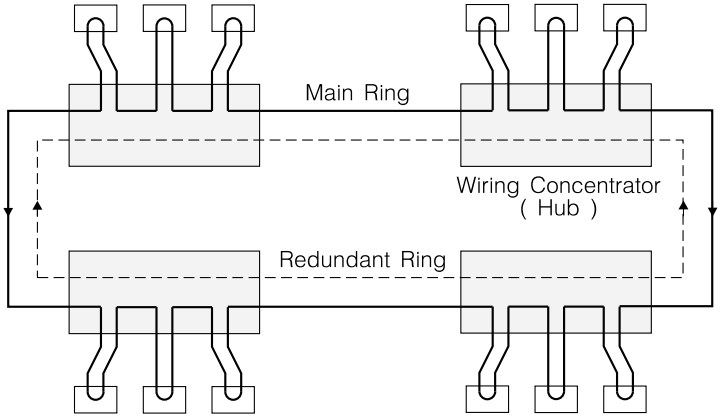
Sítě Token Ring pracují s přenosovými rychlostmi 1 Mb/s (historický standard) a 4 nebo 16 Mb/s. Rychlejší varianta s přenosovou rychlostí 16 Mb/s je určena pro páteřní sítě propojující sítě pracovišť s rychlostí 4 Mb/s s výkonnými servery. Přenosovou rychlost určuje jedna ze stanic kruhu plnící funkci monitorovací stanice, ostatní stanice v kruhu se řídí hodinami odvozenými z přijímaného signálu. Synchronní provoz kruhové sítě (při normou definovaných vlastnostech stanic) dovoluje propojit nejvýše 260 stanic.

Originálním přenosovým médiem sítě byl *kabel STP* a *optické vlákno* 100/400 μm. Dnes je běžně využíván i kabel UTP a FTP a standardní optické vlákno 62.5/125 μm. Symetrickým kabelem lze propojit dvě stanice až na vzdálenost 770 m, světlovodné úseky sítě mohou být dlouhé 2 km. Při větší překonávané vzdálenosti a při přechodu na jiné médium je nutné vřadit do spoje opakovač.

Rozbočovače, dnes standardně používané pro výstavbu sítí Token Ring, mají takovou vnitřní strukturu (obr. 6.8), že kromě možného odpojování jednotlivých stanic dovolují vytvořit záložní



Obrázek 6.7: Struktura sítě Token Ring



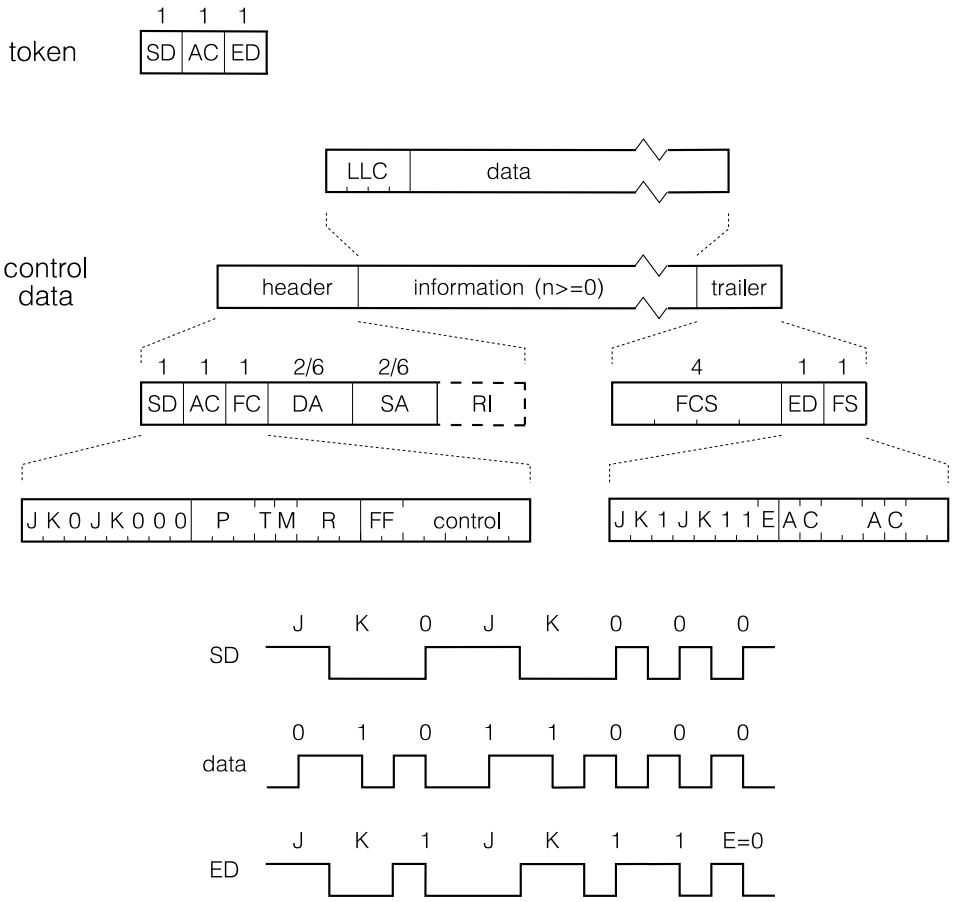
Obrázek 6.8: Redundantní kruh Token Ring (Ring of Stars)

kruh mezi rozbočovači a v případě vážnějšího výpadku na něj převést provoz. Jde o uzavření kružnice v původní stromové síti, jež prochází (pokud možno) všemi rozbočovači. V běžném provozu je využívána tato kružnice (přesněji jedno z jejích vedení), při výpadku kteréhokoliv spoje nebo aktivního prvku přecházíme na původní strom.

Kód použitý pro přenos dat je označován jako diferenciální Manchester. Přenášenému bitu odpovídá významná hrana signálu, nula je kódována jako zachování orientace předcházející významné hrany, jednotka jako změna orientace (obr. 6.9). Díky kódování není problémem prohození vodičů v páru. Transparence dat je dosaženo použitým nedatových prvků označovaných jako J a K, těmto prvkům chybí významná hrana (prvek J zachovává předchozí úroveň signálu, prvek K ji mění) a jsou využívány pro vytvoření omezovačů rámců.

Stanice si během provozu předávají pověření (Token) tvořené počátečním (Start Delimiter – SD) a koncovým (End Delimiter – ED) omezovačem, mezi omezovači je přenášeno jednoslabičné řídící pole AC (Access Control). Jednotlivé bity pole AC odlišují pověření od datového rámce (bit T – Token), označují okamžitou prioritu rámce nebo pověření (PPP – Priority) a dovolují rezervovat přenos se zadanou prioritou (RRR – Reservation). Bit M (Monitor) využívá řídící stanice k detekci rámců (datových rámců nebo pověření s nenulovou prioritou), které oběhly síť více než jedenkrát a které je nutné likvidovat (nahradit pověřením s nulovou prioritou).

Datové rámce a rámce sloužící správě kruhové sítě vkládají mezi pole AC a ED další informace. Řídící pole FC (Frame Control) dovoluje odlišit datové rámce (LLC Frames, FF=01) od rámců, které jsou využívány pro správu kruhové sítě (MAC Frames, FF=00). Adresní pole DA (Destination Address) a SA (Source Address) mají běžně délku 48 bitů a strukturu většinou



Obrázek 6.9: Diferenciální Manchester a struktura rámce IEEE 802.5

odpovídající adresnímu poli Ethernetu (individuální nebo skupinová adresa, univerzálně nebo lokálně definovaná), první bit v poli SA však určuje, zda se za polem SA objeví posloupnost adres RI (Routing Information). Posloupností polí RI určuje odesílatel konkrétní mosty na cestě rámce k příjemci, směrování typu *Source Routing* používané mosty Token Ring dovoluje (na rozdíl od Ethernetu) vytvářet sítě s alternativními cestami.

Délka datového pole není definována přímo, ale zprostředkovaně časovým limitem, po který si smí stanice podržet pověření. Ten je 10 ms, odpovídající největší využívané délky rámců jsou 4 kB (pro rychlost 4 Mb/s) a 16 kB (pro 16 Mb/s). Pole FCS (Frame Check Sequence) zabezpečuje část rámce počínaje polem FC, dvaatřicetibitový cyklický kód se opírá o standardní generační polynom.

Koncový omezovač ED (End Delimiter) ve svém posledním bitu (Error – E) dovoluje indikovat chybu ve formátu rámce (nedatový prvek uvnitř rámce, necelistvý počet znaků) nebo chybu v kontrolním součtu. Konečně pole FS (Frame Status) dovolí odesílateli v bitech A (Address Recognised) a C (Frame Copied) sdělit odesílateli výsledek přenosu. Zabezpečení této informace proti chybám při přenosu se dosahuje duplikací.

Stanice může vyslat datový rámec do sítě pouze po přijetí pověření, přesněji po přijetí nastaveného bitu T, a to tak, že změní hodnotu bitu T a odvysílá datový rámec. Stanice smí odvysílat i více rámců, nesmí však obsadit kruh na dobu delší než 10 ms. Po ukončení vysílání stanice počká na příjem pole AC odeslaného rámce (obsahuje informaci o rezervaci prioritního přenosu) a předá pověření další stanici na kruhu.

Základní funkci stanice poněkud komplikuje osmiúrovňový prioritní mechanismus, který dovoluje upřednostnit přenos pro časově kritické aplikace. Stanice, která má rámec k vysílání,

smí převzít pověření s prioritou nižší nebo rovnou prioritě odesílaného rámce, jinak musí předat pověření dál. Po odeslání rámce a jeho oběhu sítí stanice odešle pověření s hodnotu priority rovnou maximu z původní hodnoty priority v pověření a nové hodnoty zjištěné v poli rezervace. Stanice, která přijala pole AC datového rámce, a sama chce odeslat rámec s prioritou nižší než udává pole PPP ale vyšší než udává pole RRR, nastaví svůj požadavek na prioritu v poli RRR. Konečně, stanice, která zareaguje na požadavek v poli RRR odesláním pověření s touto prioritou, po návratu pověření sníží prioritu na hodnotu předcházející odeslání jejího vlastního rámce.

Čekání stanice na návrat pole AC odeslaného rámce může vést u sítí s více stanicemi a krátkými rámci na snížení průchodnosti sítě. Situaci lze zlepšit využitím režimu *Early Token Release* (*ETR*), u kterého stanice může předat pověření bez čekání na oběh sítí. Stanice v režimu ETR mohou bez problémů spolupracovat se stanicemi v základním režimu, nevýhodou režimu ETR je oslabení prioritního mechanismu.

Aktivní monitor kruhu dohlíží na to, aby datové rámce a pověření s vyšší prioritou neoběhly síť více než jedenkrát. Současně o své funkci informuje ostatní stanice na kruhu MAC rámcem *Active Monitor Present*. Po výpadku aktivního monitoru nebo po startu sítě jednotlivé stanice kruhu indikují nepřítomnost monitoru a vysílají do kruhu MAC rámce *Claim Token*. Stanice, která přijme nepoškozený rámec Claim Token, porovná svou adresu s adresou odesílatele a odešle rámec Claim Token s adresou vyšší. Stanice, která přijme z kruhu rámec Claim Token se svou vlastní adresou, se stává aktivním monitorem kruhu.

Důležitou funkci plní další MAC rámec – *Beacon*. Stanice, které vyprší časový limit No-Token, začne vysílat rámce Beacon. Na příjem rámce Beacon reaguje stanice, podobně jako u rámce Claim Token vysláním rámce Beacon s vyšší adresou. To dovolí identifikovat místo závady a síť rekonfigurovat. Pokud je vše v pořádku, jedna ze stanic (ta s nejvyšší adresou) přijme svůj vlastní rámec Beacon a vyšle rámec Claim Token.

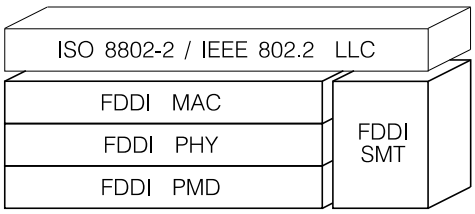
Další MAC rámce jsou používány při připojování stanic (Lobe Test, Duplicate Address Test, Request Initialization) a při zjištění rozpojeného kruhu (Beacon).

6.5 FDDI

Kruhová síť FDDI (Fiber Distributed Data Interface) byla navržena pro přenos dat vysokou rychlostí (přenosová rychlost 100 Mb/s) s možností pokrýt i rozsáhlejší území. Jeden kruh může propojit až tisíc stanic, limit délky spojů v kruhu je 200 km. Je definována standardem ANSI X3T9.5 a pozdějším ISO 9314 a určena pro propojení vysoce výkonných stanic a pro vytváření páteřních sítí propojujících pomalejší, ale levnější, sítě Ethernet nebo Token Ring.

V názvu sítě se obráží fakt, že primárním přenosovým médiem jsou optická vlákna provozovaná na vlnové délce 1350 nm. Běžně používaná mnohavidová optická vlákna 62.5/125 μm (nebo někdy i levnější 50/125 μm) dovolují dosáhnout vzdálenosti mezi stanicemi až 2 km (limit útlumu mezi stanicemi je 11 dB, včetně ztrát ve spojích a konektorech), standard FDDI však předpokládá i použití alternativních médií. Architektura sítě FDDI (obr. 6.10) odděluje protokol fyzické vrstvy (PHY) (přenosová rychlost, synchronizace, kódování) od vlastností závislých na médiu (PMD – Physical Medium Dependent). Jako alternativní média lze použít levný kabel UTP Cat.5 (na vzdálenost do 100 m, standard je označován jako CDDI – Cooper Distributed Data Interface), jednovidová vlákna 8/125 μm (až do 60 km), nebo synchronní telekomunikační kanály (STM-1/OC-3 s přenosovou rychlostí 155.52 Mb/s).

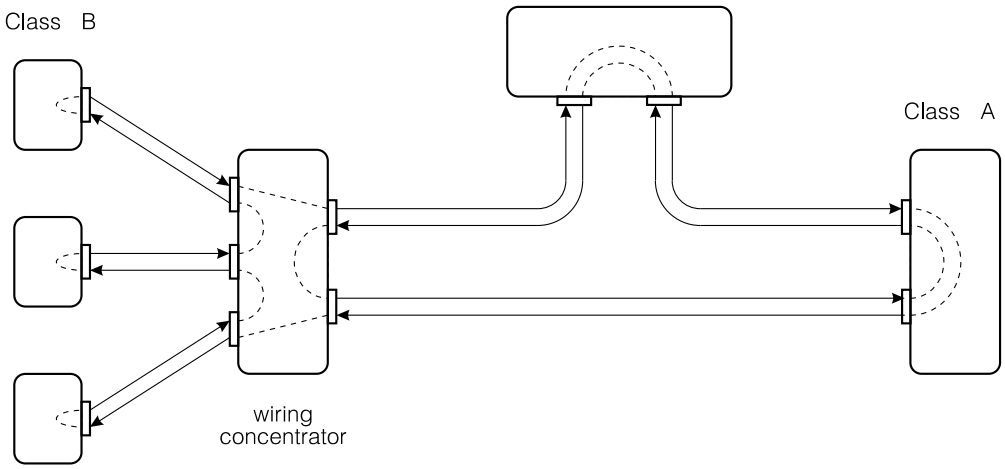
Síť FDDI se od sítě Token Ring v řadě vlastností liší. Podobně jako síť Token Ring se opírá o hvězdicové vedení spojů s koncentrátory (Wiring Concentrator) mezi stanicemi. Na rozdíl od



Obrázek 6.10: Architektura sítě FDDI

základní sítě Token Ring však předpokládá zdvojení přenosového média. Ze dvou protisměrně orientovaných kruhů je při běžném provozu pro přenos dat využíván jediný (Main Ring), druhý (Secondary Ring) dovoluje rekonfigurovat přenos při výpadku stanice, spoje nebo koncentrátoru. Stanice připojená ke zdvojenému kruhu je označována jako *Double Attachment Station* (DAS), stanice připojená k jednoduchému kruhu jako *Single Attachement Station* (SAS).

Základní konfigurací sítě (třída A) je dvojitý kruh. Při detekovaném přerušení kruhu stanice sousedící s poruchou automaticky rekonfigurují kruh – využijí sekundární kruh pro přenos dat. Pro méně náročná nasazení lze použít zjednodušené sítě (třída B) s jediným kruhem, tato síť ovšem není schopna takovéto rekonfigurace. Typickou strukturou sítě FDDI je dvojitá páteř třídy A propojující menší kruhy třídy B. Vysoká přenosová rychlost vyžaduje použití efektivnějšího způsobu kódování než je Manchester kód (u kterého je modulační rychlost, pokud bychom přenášený signál chápali jako NRZ, dvojnásobkem přenosové rychlosti). Síť FDDI využívá kódování 4B/5B, čtveřice bitů (označujeme je jako *symboly*) jsou překódovány na pětice a ty jsou přenášeny v kódu NRZI. Výsledná modulační rychlost je pouze 125 Mb/s, z pětibitových posloupností jsou pro přenos dat vybrány ty, které obsahují nejméně dvě změny (hrany signálu) a u kterých se neobjeví více než trojice nul za sebou (i přes hranici pětic). Zbývající kombinace jsou využity pro signalizaci (mezirámcová synchronizace – Idle, klid na médiu – Quiet), jako omezovače rámců nebo jako logické hodnoty přenášené vně struktury rámců (nula – Reset, jednotka – Set).

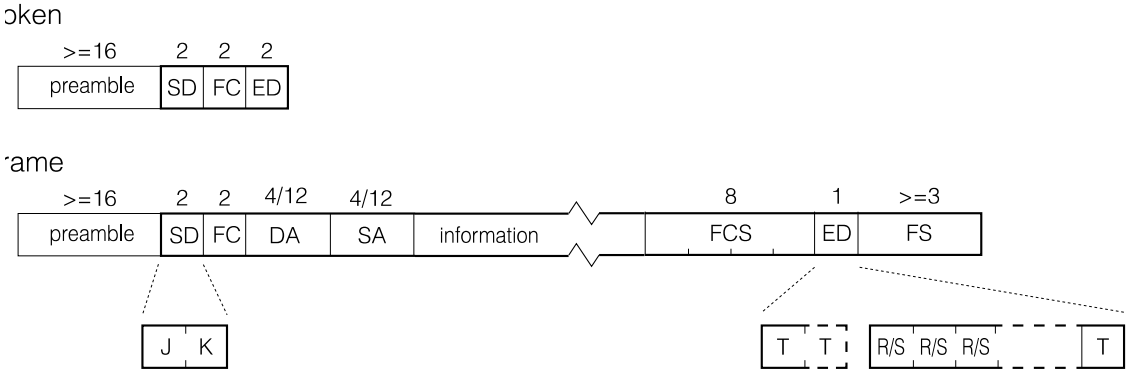


Obrázek 6.11: Struktura sítě FDDI

Povolená délka kruhu FDDI (200 km) a vysoká přenosová rychlost (100 Mb/s) vylučují synchronizaci stanic v kruhu způsobem použitým u sítě Token Ring. U sítě FDDI je použit princip označovaný jako *plesiochronní* přenos. Každá stanice má vlastní hodinový zdroj s definovanou odchylkou a stabilitou, nesouhlas přenosové rychlosti na vstupu stanice a na jejím výstupu je kompenzován posuvným registrem s proměnnou délkou (minimální délka je 10 bitů). Limitní parametry dovolují zajistit přenos rámců o maximální délce 4.5 kB, síť FDDI lze bez větších problémů použít jako páteřní síť pro Ethernet i pro Token Ring.

Dvojitý kruh FDDI dovoluje realizaci složitějších topologií než Token Ring. Příklad konkrétní struktury sítě FDDI uvádí obr. 6.11.

Rámce FDDI mají podobnou strukturu jako rámce sítě Token Ring. Vzhledem k jiné synchronizaci stanic je rámec předcházen preambulí složenou ze šestnácti čtyřbitových symbolů Idle, za počátečním omezovačem SD (Start Delimiter) obsahujícím symboly J a K následuje pole FC (Frame Control), které určuje typ datového rámce (synchronní/asynchronní), formát adresy (16/48 bitů) a odlišuje datové rámce od pověření, rámců MAC (Claim, Beacon) a rámců pro správu sítě. Přenášená data mají délku nejvýše 4.5 kB, přenos je zabezpečen 32-bitovým cyklickým kódem. Pole FS (Frame Status) za ukončujícím omezovačem ED (End Delimiter – jeden nebo dva symboly Terminate) dovoluje indikovat chybu kontrolního součtu nebo nesprávnou délku (E – Error), nalezení adresáta (A – Address Recognised) a převzetí rámce (C – Frame Copied). Pole je ukončené symbolem Terminate, což dovoluje doplnit další příznaky v konkrétních implementacích standardu. Pro zápis hodnot příznaků jsou použity symboly Set a Reset.



Obrázek 6.12: Formát rámce

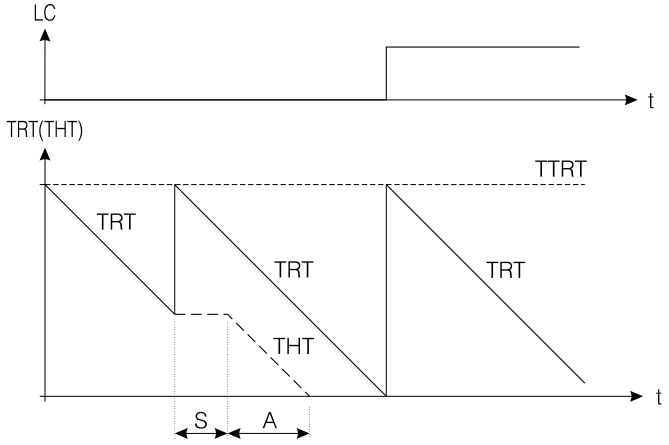
Síť FDDI používá prioritní mechanismus, stanice dělí své požadavky na ty, které je potřeba uspokojovat pravidelně (odeslat rámec při každém příjmu pověření) – označujeme je jako *synchronní*, a na ty, které mohou počkat – označujeme je jako *asynchronní*. U asynchronních požadavků je navíc možno definovat až osm úrovní priority.

Po převzetí pověření (úplného, na rozdíl od sítě Token Ring, kde může stanice změnou jediného bitu T změnit již vysílané pověření na datový rámec) může stanice odeslat více datových rámců, svou činnost uzavírá odesláním pověření. Přístup stanice k médiu je omezen mechanismem, označovaným jako *Timed Token*. Stanice se řídí časovačem TRT (Token Rotation Time), který nastaví při příjmu pověření na hodnotu TTRT (Target Token Rotation Time) a začne jeho hodnotu snižovat. Hodnotu TTRT si stanice dohodnou při konfiguraci sítě (MAC rámec Claim).

Při vlastním přenosu dat stanice po převzetí pověření přepíše hodnotu časovače TRT do časovače THT, znovu spustí TRT s hodnotou TTRT a odvysílá synchronní rámce. Spustí časovač THT a smí vysílat asynchronní rámce až do jeho vynulování. Pak musí odevzdat pověření další stanici. Pokud časovač TRT vypršel již před příchodem pověření, smí stanice odvysílat pouze synchronní rámce. Funkci čítačů TRT a THT ilustruje obr. 6.13.

Uvedené schéma zajišťuje spravedlivé rozdělení kapacity kanálu. Střední doba, kterou potřebuje pověření k oběhu kruhu, je nejvýše rovna hodnotě TTRT, konkrétní doba oběhu může dosáhnout nejvýše dvojnásobku TTRT, při překročení tohoto limitu stanice inicializuje kruh (vysílá MAC rámec Claim).

Prioritní přístup pro asynchronní provoz se opírá o hodnotu čítače THT. Pro každou úroveň priority i je definována určitá hodnota T_Pr_i nižší než TTRT. Stanice začíná vysílat



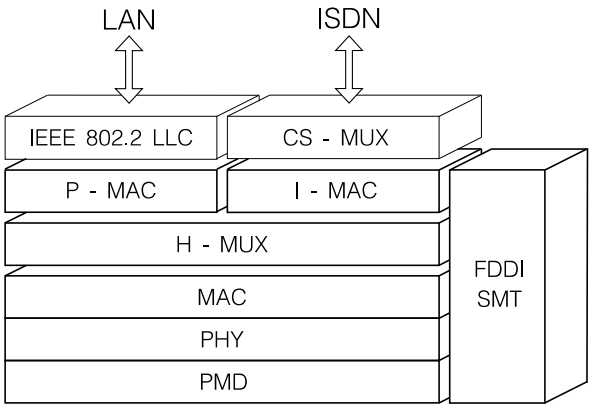
Obrázek 6.13: Přidělování kapacity

asynchronní rámce od nejvyšší priority, rámce příslušející dané prioritě smí vysílat pouze, pokud je hodnota THT vyšší než hodnota T_Pr_i . Na rozdíl od sítě Token Ring, kde je priorita definována jednotně pro všechny stanice, u FDDI si každá stanice definuje prioritu nezávisle na stanicích ostatních.

Vedle priority podporuje síť FDDI ještě speciální mechanismus, označovaný jako *Restricted Token*. V tomto režimu je veškerá kapacita asynchronního přenosu vyhrazena komunikaci dvou stanic.

FDDI II

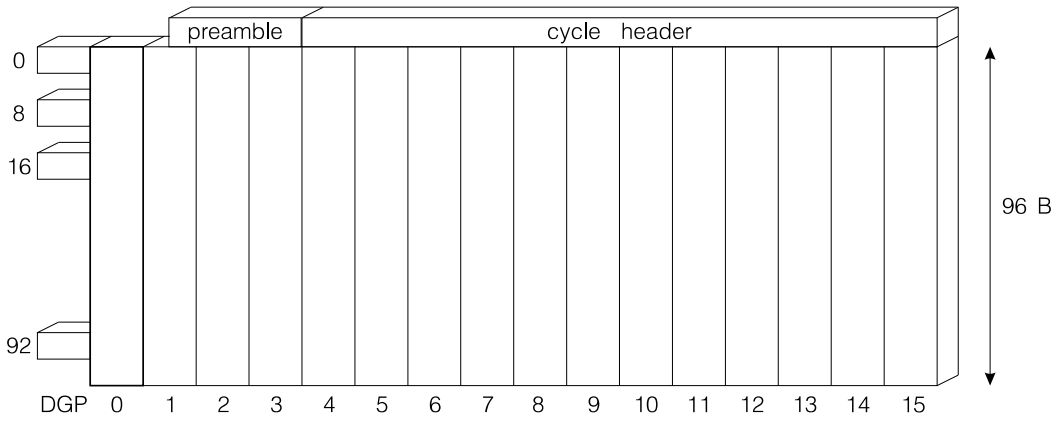
Síť FDDI podporuje provoz označovaný jako synchronní, rozumí se tím, že stanice má zaručenu možnost předání svých synchronních rámců při každém příchodu "pravidelně" přicházejícího pověření. Takové chápání pojmu "synchronní provoz" se liší od jeho definice v telekomunikačních systémech, tam synchronní přenosové kanály dovolují přenášet např. digitalizovaný zvukový signál tak, že každých 125 μs přenesou jeden osmibitový vzorek (případně větší počet vzorků za násobek intervalu). Běžná síť FDDI takovýto provoz (bez doplňkového programového vybavení a za cenu zpoždění při přenosu) podpořit neumí.



Obrázek 6.14: Architektura sítě FDDI II

Zajištění synchronního přenosu (ve smyslu výše zmíněném) po síti stanic propojených spoji FDDI do kruhu si vytkla za cíl specifikace označovaná jako FDDI II. Od základní specifikace FDDI se podstatně liší, je postavena nad časovým multiplexem na médiu kruhového kanálu (obr. 6.14) a je označována jako *isochronní FDDI*.

Specifikace FDDI II plně zachovává fyzickou vrstvu původní FDDI (přenosová média, signály, kódování 4B/5B), ale využívá ji pro pevný časový multiplex (modul H-MUX – Hybrid Multiplexer) respektující požadavky synchronní komunikace. Jednotlivé podkanály lze dále rozdělit na více synchronních podkanálů časového multiplexu (modul I-MAC – Isochronous MAC), nebo využít pro vytvoření kruhového kanálu emulujícího chování kruhu FDDI (modul P-MAC – Packet MAC). Princip přenosu použitý u sítě FDDI II je následující. Jedna ze stanic kruhu je zvolena jako řídící, tato stanice vysílá do kruhu rámce časového multiplexu, označované jako *cykl* (Cycle) s periodou 125 μs. Při přenosové rychlosti 100 Mb/s má cykl délku 12500 bitů, jeho logickou strukturu uvádí obr. 6.15.



Obrázek 6.15: Struktura cyklu sítě FDDI II

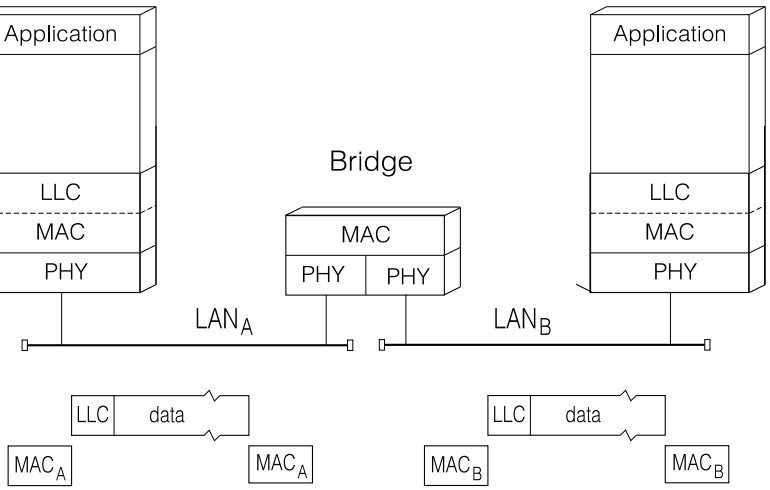
Každý cykl je tvořen preambulí o délce pěti (čtyřbitových) symbolů následovanou dvanáctislabičnou hlavičkou cyklu. Vlastní tělo cyklu je rozděleno na 16 skupin po 96 slabikách, každá skupina vytváří rychlý kanál WBC (Wide Band Channel) o přenosové rychlosti 6.144 Mb/s. Zbývajících 12 slabik tvoří kanál DPG (Dedicated Packet Group) o přenosové rychlosti 768 kb/s. Kanál DGP tvoří základ kanálu pro přenos paketů dat v režimu, který odpovídá běžnému FDDI (předávání pověření), jeho kapacitu lze rozšiřovat o jednotlivé kanály WBC po krocích 6.144 Mb/s až do celkové kapacity 99.072 Mb/s. Informaci o tom, které z kanálů WBC jsou využity pro vytvoření paketového kanálu, obsahuje hlavička cyklu.

Kanály, které nejsou využity pro přenos paketů, tedy kanály *isochronní*, lze běžnou technikou multiplexu rozdělit na kanály s přenosovou rychlostí, která je násobkem 64 kb/s, a využít je pro běžné služby, jako je např. přenos signálu ISDN (2x64 kb/s) nebo rychlý synchronní přenos dat. Přenosová rychlost jednoho kanálu WBC, která je 6.144 Mb/s, odpovídá rychlosti čtyř synchronních kanálů T1 (1.536 Mb/s) nebo tří kanálů E1 (2.048 Mb/s).

7. Propojování lokálních sítí

Lokálními sítěmi Ethernet i IBM Token Ring lze propojit pouze omezený počet stanic, častým limitem je i nejvyšší překlenutelná vzdálenost. Tu omezuje jednak délka jednoho úseku přenosového média a jednak maximální počet *opakovačů* mezi stanicemi. U sítě Ethernet je třeba dodržet nejvyšší vzdálenost mezi stanicemi 2.5 km a do sítě připojit nejvýše 1024 stanic, u sítě IBM Token Ring je limitem 260 stanic na jednom kruhu. Při větších požadavcích na rozlehlost sítě, na počet stanic nebo na kombinaci různých síťových technologií nezbývá, než jednotlivé menší sítě mezi sebou propojit prvkem, který převede komunikaci z jedné sítě do sítě druhé.

Důvody k rozdělení stanic do více sítí a k propojení těchto sítí mohou být i jiné, než překročení uvedených limitů. Rozdělení stanic do více sítí, pokud možno tak, aby se co nejvíce přenosů uskutečnilo uvnitř sítí, dovolí dosáhnout vyšší celkové *průchodnosti* (zvyšuje *kapacitu sítě*) a nižší doby odezvy. Poruchu v jedné lokální síti lze v propojovacím prvku rozpoznat, její vliv se ve zbytku soustavy neprojeví. Izolace sítě proti poruchám v jejích částech zvyšuje *spolehlivost*. Provoz mezi stanicemi jedné sítě není propojovacím prvkem zbytečně do druhé sítě přenášen, propojovací prvek tak zajišťuje ochranu komunikace stanic proti odposlechu – zvyšuje *bezpečnost*.



Obrázek 7.1: Most v architektuře lokální sítě

Lokální sítě propojujeme pomocí prvků, připojených ke dvěma nebo více propojovaným sítím, soustavu více propojených lokálních sítí obvykle nazýváme *internetwork*. Prvky propojující lokální sítě označujeme jako *mosty* (Bridges), *přepínače* (Switches) a *směrovače* (Routers). Funkce mostů a směrovačů je podobná funkci uzlů přepojovací sítě, a obvykle ji charakterizujeme termínem *"store-and-forward"*. Rámce přijaté z připojených sítí jsou analyzovány a podle výsledku buď likvidovány nebo následně vyslány do některé (některých) ze sítí. Přepínače (Switches, budeme se jim věnovat podrobněji na str. 73) dovolují zahájit vysílání bezprostředně po analýze hlavičky rámce, funkci charakterizujeme termínem *"cut-through"*.

Mosty, přepínače a směrovače se od sebe liší rozsahem informace, kterou při směrování využívají. Mosty se opírají pouze o adresační pole rámce (MAC adresy), směrovače analyzují předávaná data a využívají informací spojených s konkrétním síťovým nebo transportním protokolem. Existují i kombinované prvky – *broutery* (Bridging Routers), které pro některý síťový nebo transportní protokol fungují jako směrovače a pro jiné protokoly jako mosty, a *víceprotokolové směrovače*, které pro různé síťové nebo transportní protokoly zajišťují různé metody směrování.

Propojovacími prvky a dvoubodovým spojem mezi nimi lze propojit i vzájemně geograficky oddělené lokální sítě. Kapacita dvoubodového spoje (pronajatý datový spoj, spoj ISDN, kanál PCM, virtuální kanál ATM) pochopitelně ovlivňuje průchodnost mostu, a tím i kvalitu služeb poskytovaných aplikacím.

7.1 Most – Bridge

Most přijímá všechny rámce z propojovaných sítí a u každého z nich se rozhoduje, zda ho do druhé sítě přenese (adresát je v této druhé síti nebo je neznámý), nebo zda ho bude ignorovat (adresát je v síti, z níž byl rámec přijat).

Při rozhodování se most řídí MAC adresou příjemce a směrovacími tabulkami, ve kterých má uloženy informace o rozmístění stanic v sítích připojených k mostu (u mostu se statickými tabulkami a u mostů transparentních), nebo směrovacími údaji uloženými v MAC rámci (u zdrojového směrování – str. 62). Adresu MAC (a pochopitelně ani v MAC rámci přenášená data) běžný most nemění. Lze ho tedy použít pro propojení sítí respektujících jeden formát rámců, a lišících se nejvýše médiem.

Pozn.: Mosty mohou brát v úvahu při svém rozhodování o tom, zda rámec přenést, i další informace, například typ rámce Ethernetu, adresu odesílatele nebo adresáta. Pak mluvíme o selektivní *filtraci*, produkty jednotlivých výrobců se v této oblasti značně liší.

Pozn.: Prvky, které propojují sítě s různým formátem rámců ale se stejnou adresací (např. Ethernet, IBM Token Ring a FDDI), jsou označovány jako *translační mosty* (*translation bridges*).

Tabulky mostu by mohly být *statické*, definované například správcem sítě (příklad takového řešení uvádí obr. 7.2). Každé doplnění stanice, nebo přemístění stanice mezi sítěmi, by pak vyžadovalo zásah správce sítě.

Výhodnější je, může-li si most vytvářet směrovací tabulky během své práce sám. Most, který takto pracuje, označujeme jako *transparentní*, *učící se* nebo *inteligentní*. Modifikování směrovacích tabulek je poměrně jednoduché a je založeno na faktu, že každý rámec sítě, respektující standard IEEE 802 (Ethernet, IBM Token Ring, ale i FDDI), má ve své hlavičce uloženu MAC adresu odesílatele. Most si informaci o odesílající stanici paketu ukládá do směrovací tabulky, později ji využívá při převzetí rámců pro tuto stanici.

Funkce transparentního mostu je definována normou IEEE 802.1; most pracuje na následujícím principu:

1 Sleduje veškerý provoz v sítích, které propojuje. Vede si evidenci stanic, jejichž adresy jsou uvedené jako adresy odesílatele. Tato evidence má formu *směrovací tabulky* (Forwarding Database). Pro každou adresu, která se objevila v poli odesílatele rámce, je ve směrovací tabulce uvedena síť, ze které zpráva s touto adresou přišla. Ukládaní do tabulky je označováno jako *učení* (Bridge Learning).

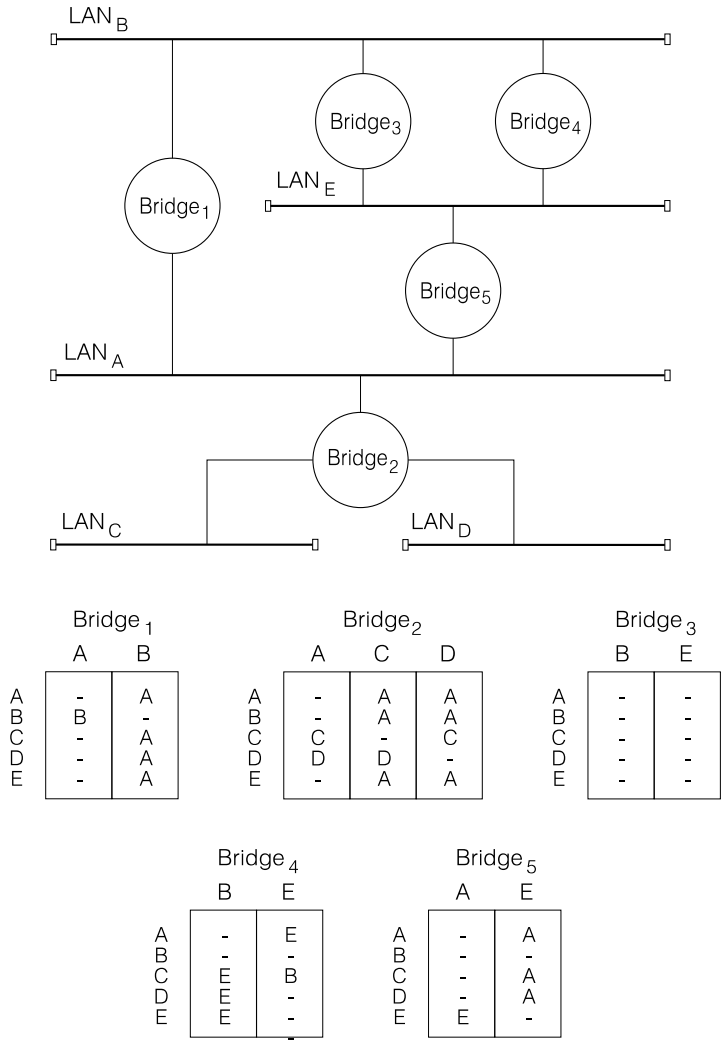
2 Na každou zprávu, která je přijata mostem z některé připojené sítě, most reaguje některým ze tří způsobů:

   a zpráva určená pro stanici, o níž most ví, že leží ve směru odkud byla zpráva přijata, je likvidována,

   b zpráva určená pro stanici, o níž most ví, že leží v jiné síti, než ze které byla zpráva přijata, je mostem převedena do této sítě,

   c zpráva určená všem stanicím (broadcast) nebo zpráva určená stanici, kterou most dosud nezná, je rozeslána do všech směrů, kromě směru, ze kterého přišla.

Pro uložení směrovacích tabulek má most vyhrazenu oblast paměti; velikostí této paměti a způsobem jejího rozdělení na jednotlivé tabulky se mosty od sebe liší. Typickou velikostí



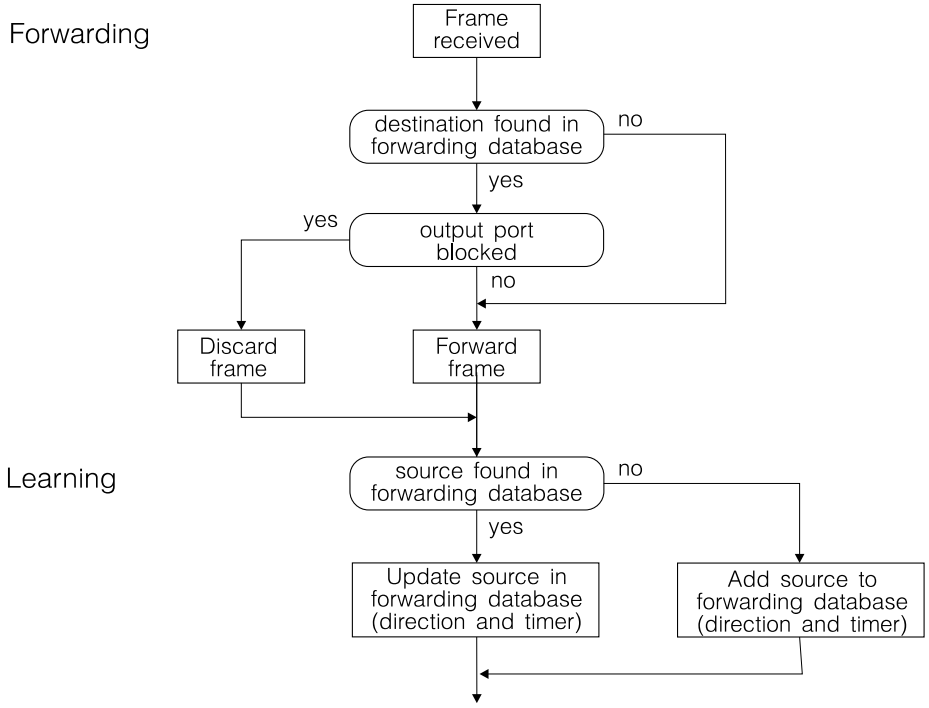
Obrázek 7.2: Mosty se statickými směrovacími tabulkami

paměti je prostor pro 4096 až 16384 položek v jediné směrovací tabulce pro všechna rozhraní. Přístup je obvykle opřen o jednoduchou adresační funkci (např. hashing, výběr pole dvanácti až čtrnácti bitů z adresy MAC), důsledkem mohou být pochopitelně kolize – opakované přepisování záznamů ve směrovací tabulce a následné zbytečné rozesílání datových rámců do sítí, do kterých nepatří.

U *přepínačů*, které mají s běžnými mosty hodně společného, jsou běžné samostatné tabulky pro jednotlivá rozhraní, v krajním případě s kapacitou omezenou až na jedinou položku.

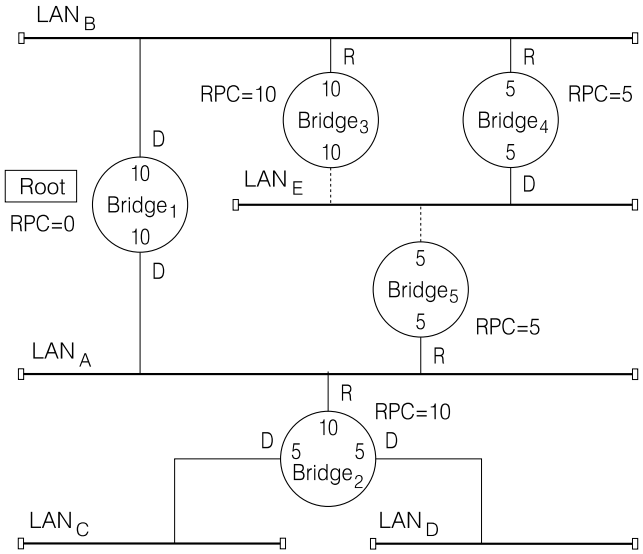
Transparentní most pracuje pouze v sítích se stromovou strukturou, v níž uzly reprezentují mosty a hrany reprezentují propojované lokální sítě. V propojených sítích nesmí vzniknout uzavřená cesta – cykl. Pokud potřebujeme propojit sítě více mosty a zajistit tak odolnost proti jejich výpadkům, musí být tyto mosty schopné vypnout některá svá rozhraní a vytvořit tak stromovou strukturu (kostru propojovací sítě). Postup, kterého mosty při takovém omezování topologie využívají, je označován jako *Spanning Tree* algoritmus.

Blokované porty mostů zůstávají v záloze pro případ výpadku některého mostu nebo sítě. Algoritmus *výběru kostry* se opírá o jednoznačnou číselnou identifikaci mostů, distribuovaný výběr fungujícího mostu s nejnižší identifikací a o nalezení stromu nejkratších cest s vybraným uzlem jako kořenem. Je standardizován specifikací IEEE 802.1d.



Obrázek 7.3: Činnost transparentního mostu

Vlastní algoritmus výběru kostry ilustruje obr. 7.4. Opírá se o již uvedenou jednoznačnou *identifikaci mostu*, opřenou např. o výrobcem přidělené adresy řadičů Ethernetu a o *cenu výstupu* (ohodnocení výstupních portů). Služební rámce, které si mosty si mezi sebou vyměňují při konstrukci kostry, mají zvláštní formát a jsou označovány jako *BPDU* (Bridge Protocol Data Unit).



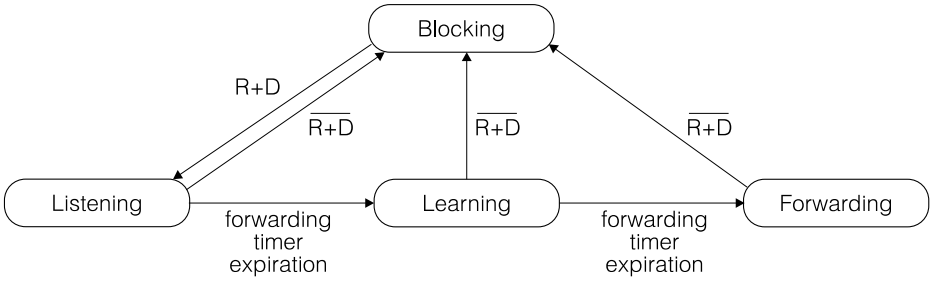
Obrázek 7.4: Spanning-Tree algoritmus

Prvním krokem algoritmu je výběr kořene. Každý z mostů může rozeslat rámec BPDU s vlastní identifikací do všech připojených sítí. Každý z mostů tak může zjistit, zda je jeho identifikace nejnižší a je tedy kořenem kostry. Most – kořen kostry rozesílání rámců BPDU periodicky opakuje.

Kořen kostry v rozesílaném rámci uvádí jako *cenu cesty* cenu přiřazenou příslušnému výstupu. Rozhraní, na kterém most sousedící s kořenem přijímá jeho rámce BPDU, označujeme jako *root port* (v obr. 7.4 je toto rozhraní označeno písmenem R). K údaji o ceně cesty v rámci BPDU most přičte cenu svého výstupu a rámec vyšle dál. Jako výsledek opakování tohoto kroku může každý z mostů určit svůj root port.

Pro každou z propojovaných lokálních sítí je dále potřeba určit most s nejnižší cenou cesty ke kořeni kostry. To je snadné vzhledem k údaji o ceně cesty v rámcích BPDU. Rozhraní tohoto mostu označujeme jako *vyhrazené* (Designated), v obr. 7.4 je označeno písmenem D.

Rozhraní R (root port) a D (designated port) vytvářejí kostru, ostatní rozhraní přecházejí do blokovaného stavu a neúčastní se přenosu datových rámců (rámce BPDU však přijímají a vysílají).



Obrázek 7.5: Stavový diagram transparentního mostu

Přechod mezi blokováním portu a jeho běžnou činností je poněkud komplikován nutností zabránit nekorektnímu přenosu datových rámců při změnách topologie. Přechod z provozního stavu do blokování proběhne okamžitě, přechod z blokovaného stavu do provozního stavu je řízen časovačem *Forwarding Timer* a navíc procházíme stavem, ve kterém si most pouze aktualizuje směrovací tabulky (obr. 7.4).

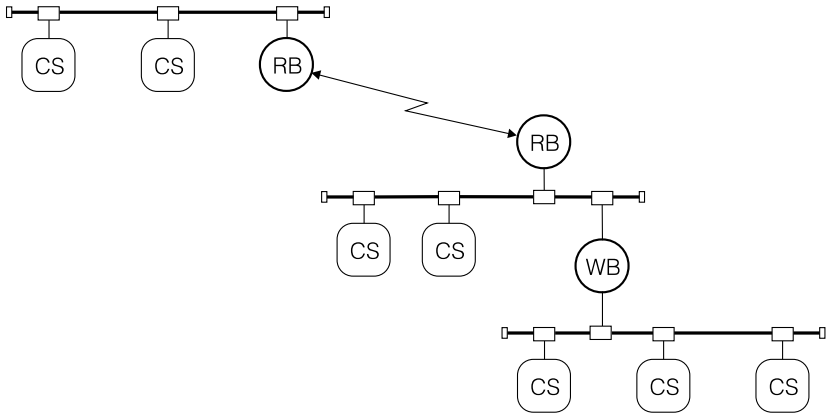
Jak už jsme uvedli, rozesílání rámců BPDU kořenem stromu je periodické (perioda je označována jako *Hello Time*). Při běžném provozu mosty evidují, že je vše v pořádku; výpadek některého z mostů nebo portů může vyvolat změnu root portu a vyhrazeného rozhraní. Každou takovou změnu most hlásí kořeni stromu zvláštním rámcem BPDU a ten hlášení po určitou dobu potvrzuje zvláštním příznakem v rozesílaných rámcích BPDU. Příjem rámce BPDU s nastaveným příznakem zneplatňuje (po zadaném čase) údaje v tabulkách mostů.

Remote Bridge

Někdy potřebujeme propojit lokální sítě na větší vzdálenost dvoubodovým spojem a pochopitelně chceme po tomto spoji přenášet pouze rámce určené vzdáleným stanicím. Řešením je umístění dvou mostů na konce dvoubodového spoje, jejich směrovací tabulky však budou identické a filtrace rámců přicházejících z dvoubodového spoje bude zbytečná. Redukce funkcí těchto dvou mostů vede na řešení, označované jako (*Remote Bridge*). Most se rozhoduje o převedení rámce lokální sítě do dvoubodového spoje, v opačném směru přenáší všechny rámce.

Podobnou redukci funkcí jako u vzdálených mostů nalezneme u mostů určených pro oddělení provozu malých skupin stanic od zbytku sítě. Takový most bývá označován jako *Workgroup Bridge*, jeho směrovací tabulka obsahuje pouze informace o adresách stanic skupiny, všechny stanice s adresami mimo skupinu leží implicitně na druhé straně mostu.

Možnost použít mostů k propojení sítí na větší vzdálenost je zajímavá, je však nutné vzít v úvahu limitovanou kapacitu dvoubodového spoje a fakt, že mosty přenášejí provoz typu *broadcast* a *multicast*. Efektivnější využití limitované kapacity proto často přináší použití směrovačů.



Obrázek 7.6: Remote-Bridge a Workgroup-Bridge

Víceportové mosty – přepínače

Víceportové mosty (připojené více než dvěma síťovými rozhraními do více než dvou lokálních sítí) jsou dnes častěji označovány jako *přepínače* – *Switches* (jejich použití v přepojovaném Ethernetu si všimneme na str. 73). Označení plně přísluší pouze těm mostům, které umožňují zahájit vysílání přenášeného rámce ještě před dokončením jeho příjmu. Metodu *"cut-through"* použila jako první firma Kalpana. Výhodou metody je snížení zpoždění rámce proti klasickému mostu při malé zátěži, nevýhodou je, že jsou přenášeny i poškozené rámce. Při velké zátěži není přínos metody podstatný a modernější označení přepínač je (spíše z reklamních důvodů) používáno i pro klasické víceportové mosty pracující s technikou *"store-and-forward"*.

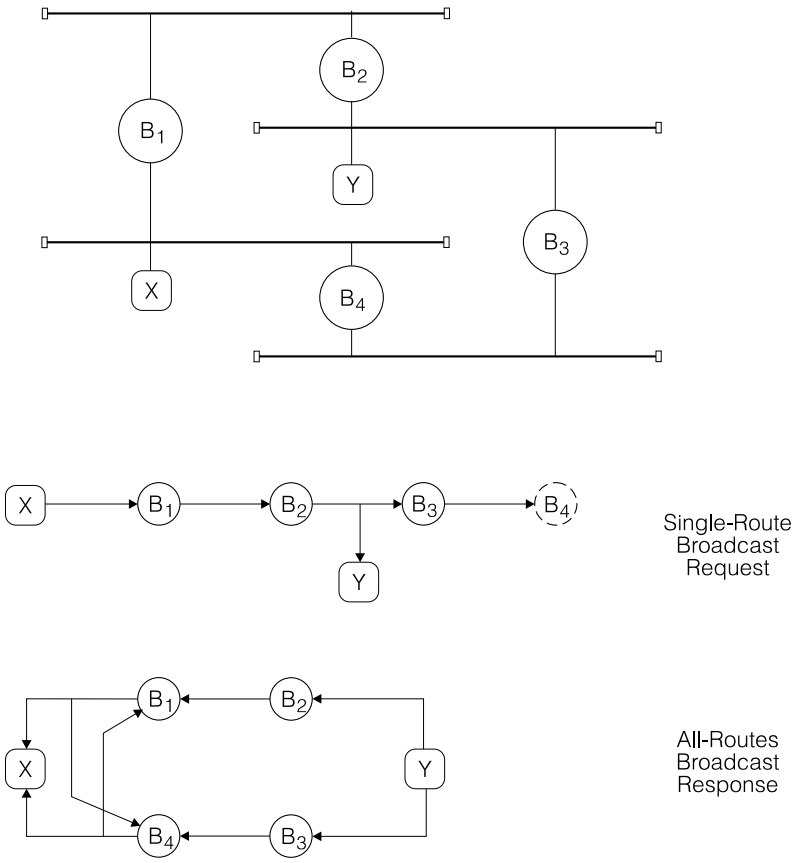
Zdrojové směrování

Vícenásobné propojení sítí mosty je zajímavé nejen proto, že zvyšuje spolehlivost sítě, ale i proto, že může zvýšit její průchodnost. Pokud však chceme takové možnosti využít, musíme se rozloučit s principem transparentního mostu. Alternativou k němu je *zdrojové směrování* (*Source Routing*), o které se opírají mosty pro sítě IBM Token Ring. Zde je každý přenášený rámec doplněn o směrovací informaci (MAC adresy mostů, jimiž rámec na cestě k cíli prochází).

Směrovací informaci můžeme všem stanicím sítě zadat staticky, předem, ve formě tabulek. A to buď tak, že tyto tabulky bude mít k dispozici každá stanice, nebo že budou k dispozici (jako služba) v jediném známém místě. Takové řešení by ale bylo nepružné a proto se setkáváme s metodami dynamického zjišťování nejvýhodnější cesty.

Než si uvedeme možné zjištění nejkratší cesty, poznamenejme, že v síti IBM Token Ring existují tři formy rozesílání rámců. Nejjednodušší je přímé rozeslání stanicím v jedné síti (označované jako *Null* – nulová směrovací informace), předání do jiných sítí přes konkrétní mosty musí být specifikováno (metoda je označována jako *Specific Route*). Rozeslání do všech sítí má dvě formy, prvou je rozesílání záplavou (*All-Route Broadcast*), druhá se opírá o znalost kostry sítě (*Single-Route Broadcast*).

Odesílatel informaci o cestě k adresátovi může získat vysláním služebního rámce – žádosti o zjištění nejkratší cesty, ten je mosty rozeslán do všech propojených sítí (např. technikou All-Route Broadcast). Tento rámec je cestou doplňován o adresy mostů a sítí, kterými prochází (ukládání informace o absolvované cestě do rámců rozesílaných úplným broadcastem je nutné i pro rozhodnutí, zda má být rámec dále rozesílán). Adresát si z přijatých kopií vybere nejkratší cestu a vrátí jedinou odpověď po této cestě.



Obrázek 7.7: Zdrojové směrování

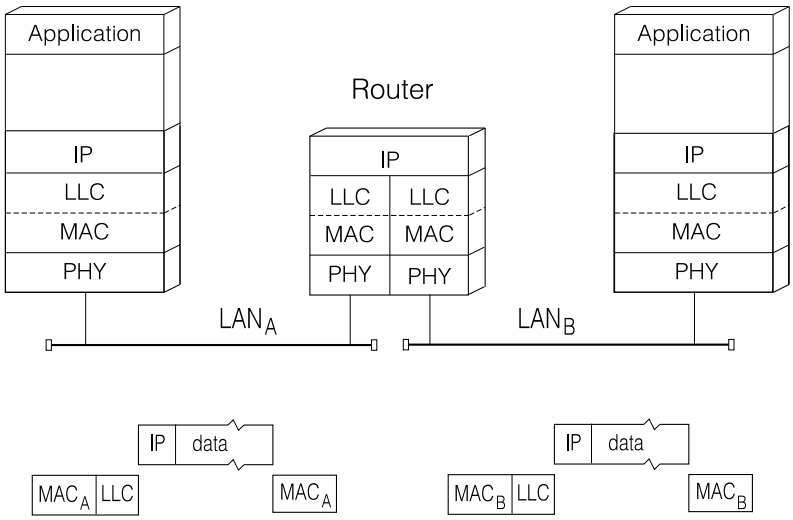
Z hlediska počtu zpráv v síti je výhodnější řešení uvedené na obr. 7.7. Žádost je rozesílána kostrou (Single-Route Broadcast), adresát vrací odpověď záplavou (All-Route Broadcast), z více odpovědí si žádající stanice vybere nejvýhodnější cestu.

Metoda zdrojového směrování je použita v síti IEEE 802.5 IBM Token Ring a označována jako *Source Routing*. Jednotlivé položky určující další most a síť na cestě k adresátovi mají délku 16 bitů, z toho vždy 4 bity určují most a 12 bitů lokální síť. Použití zdrojového směrování je indikováno jedním bitem v adrese odesílatele.

7.2 Směrovač – Router

V řadě situací nám mosty opírající se o MAC adresy pro propojení lokálních sítí nepostačí. Jedná se zvláště o situace, kdy lokální sítě vytvářejí pouhé komunikační kanály pro sítě, které původně s využitím lokálních sítí pro přenos mezi svými prvky vůbec nepočítaly. Takové sítě často mají svou vlastní síťovou adresaci, která nemá s MAC adresami nic společného. Jako příklad nám může posloužit celosvětová počítačová síť Internet, jejímiž prvky jsou nejrůznější lokální a přepojovací sítě a jejíž protokol IP se opírá o hierarchickou adresaci. Jiné sítě MAC adresy určitým způsobem využívají a rozšiřují je. Příkladem jsou sítě vycházející z protokolů firmy Xerox XNS, příkladem mohou být lokální sítě firmy Novell s protokoly IPX/SPX.

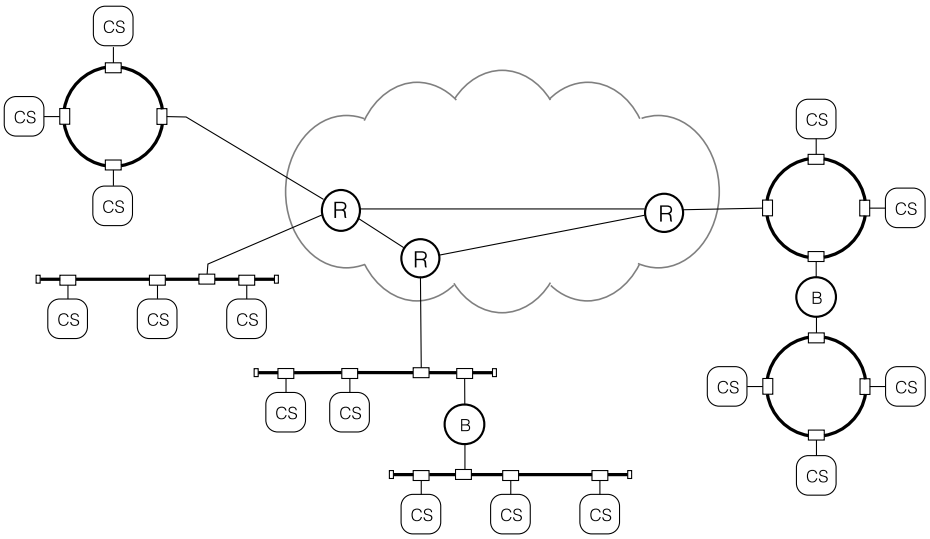
Z pohledu mostů jako součástí lokálních sítí je adresace sítí jako Internet IP nebo Novell IPX neviditelná, mosty (pokud nemají doplněnu filtraci opírající se o typ protokolu) považujeme za *protokolově transparentní*. Síťové adresy jsou přenášeny v hlavičkách *paketů*, které jsou pro prvky lokální sítě pouhými bloky přenášených dat. Pokud chceme síťovou adresaci pro směrování využít, musíme paket z rámce vyjmout a jeho hlavičku analyzovat. Analýza se může



Obrázek 7.8: Směrovač v architektuře lokální sítě

opřít o údaj o typu protokolu, který je součástí hlavičky rámce DIX Ethernetu nebo hlavičky LLC. Využití adresy z hlavičky paketu se řídí pravidly směrování Internetu, sítě Novell, ap.. Výsledkem práce takového prvku – *směrovače* (Routeru) je rozhodnutí o odeslání paketu k dalšímu prvku s obdobnou funkcí – směrovači, nebo k adresátovi. Rozdíl mezi funkcí mostu a směrovače si můžeme ilustrovat na jejich postavení v architektuře vrstev ISO OSI (obr. 2.8). Za poznámku stojí fakt, že pro směrovač je oblast sítě, tvořená lokálními sítěmi propojenými mosty, zcela transparentní. Takovou oblast (*Broadcast Domain*, broadcast doménu) směrovač vidí jako jedinou lokální síť.

Vzhledem k funkci směrovače není rozhodující o jakou síť se na jednotlivých vstupech směrovače jedná (zda jde o lokální síť konkrétního typu, nebo o síť s přepojováním paketů, nebo o pronajatý spoj s vlastním protokolem). Obálka paketu je vždy znovu vytvářena pro každou síť na cestě k adresátovi, zachován (s určitými výhradami) zůstává vlastní paket.



Obrázek 7.9: Propojení sítí mosty a směrovači

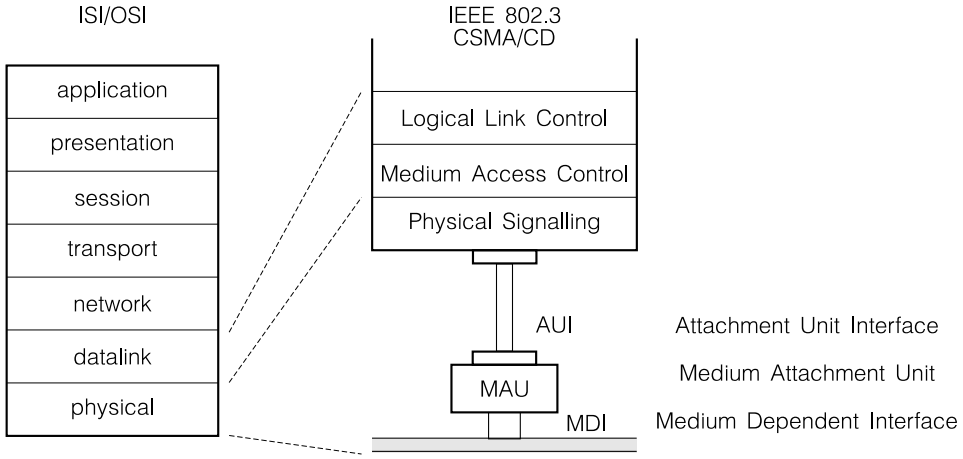
Činnosti směrovačů se budeme podrobněji zabývat v kapitole věnované síťovým protokolům, na str. 151.

8. Ethernet (IEEE 802.3)

Základy technologie, známé jako Ethernet, byly položeny ve vývojových laboratořích Xerox Palo Alto Research Center začátkem 70. let. V roce 1980 byl Ethernet standardizován konsorciem firem DEC, Intel a Xerox, standard je známý pod zkratkou DIX a Ethernet II. Současně začaly práce na standardu IEEE, jehož prvá verze byla publikována v roce 1985 pod označením IEEE 802.3 *"Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specification"*. Standard byl později podstatně rozšiřován o další média a nové způsoby provozu. Dnes je Ethernet standardizován i normou ISO 8802/3.

8.1 Ethernet 10Mb/s

Standard IEEE 802.3 definuje fyzické médium, algoritmus přístupu a formát přenášených rámců. Architektura definovaná standardem odpovídá obr. 8.1.



Obrázek 8.1: Architektura standardu Ethernetu IEEE 802.3

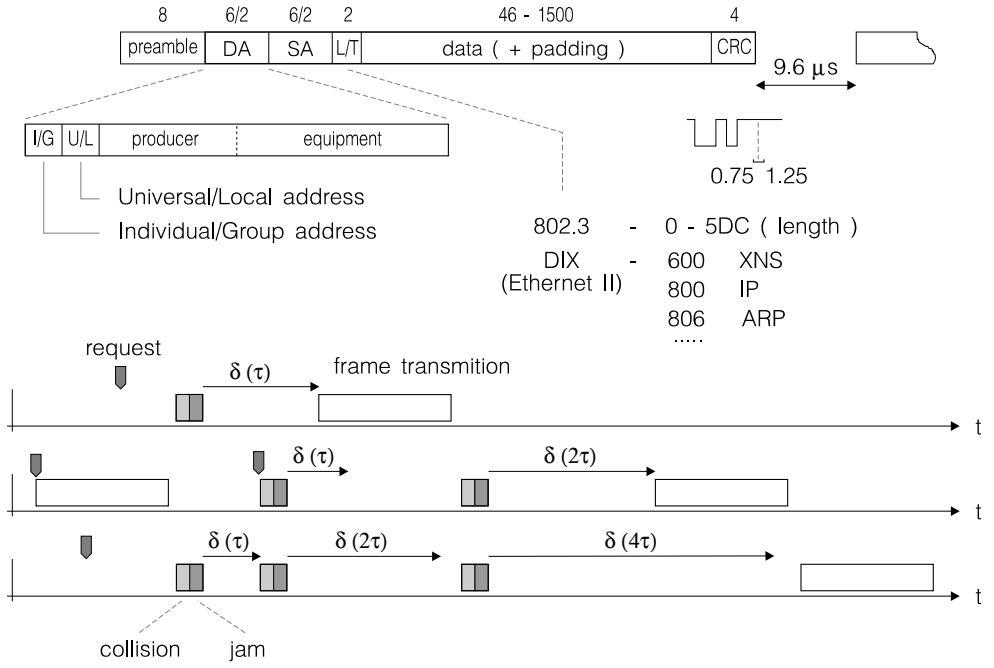
Nejnižší úroveň standardu je označována jako rozhraní *MDI* (Medium Dependent Interface) a definuje přenosové médium (tím dnes může být koaxiální kabel, kroucený dvoudrát nebo optické vlákno), signál na médiu a konektor. Přenosové médium podstatně ovlivňuje vlastnosti sítě. Jednotlivým technologiím lišícím se (hlavně) médiem jsou přidělena jména konstruovaná tak, že zahrnují informaci o rychlosti přenosu, signálech na médiu a dalších charakteristických vlastnostech. Jako příklady jmen technologií si můžeme uvést historickou technologii 10BASE5 (přenos rychlostí 10 Mb/s v základním pásmu s délkou segmentu 500m) a 100BASE-FX (přenos rychlostí 100 Mb/s v základním pásmu po optickém vlákně). Aktivní prvek, který vysílá a přijímá signál přenosového média, běžně známý jako *transceiver* (*TRANSmitter-reCEIVER*), má v normě označení *MAU* (Medium Attachment Unit).

Jednotka MAU je připojena rozhraním *AUI* (Attachment Unit Interface) k vlastní stanici, počítači vybavenému řadičem Ethernetu. Rozhraní AUI definuje:

- speciální (nepříliš ohebný) kabel, se čtyřmi kroucenými dvoudráty o impedanci 78 Ω přenášejícími signál vysílaný, signál přijímaný, signál detektoru kolize a napájecí napětí,
- konektor, kterým je upravený 15-ti špičkový Canon DB-15 s bajonetovým zámkem na místě zajišťovacích šroubků a jeho zapojení a
- elektrické signály rozhraní a zajištění izolace do 500 V (10BASE2) nebo 2000 V (10BASE5).

Rozhraní AUI může překlenout až 50 m, v konfiguracích sítí se někde musíme omezit na 25 m a v praxi se většinou setkáme s AUI-kabely (kabel transceiveru) o délce mezi dvěma a pěti metry i z méně kvalitního (ale ohebnějšího a někdy i tenčího) materiálu. U některých technologií (10BASE2, 10BASE-T) je běžná instalace MAU přímo na desce řadiče Ethernetu, na ní je i konektor přenosového média čímž AUI kabel odpadá.

Stanice, která chce po síti předat blok dat, ho opatří adresou příjemce a svou vlastní adresou. V případě Ethernetu (ale i dalších lokálních sítí, které odpovídají standardu IEEE 802) je adresa příjemce i odesílatele šestiznaková (budeme ji nadále označovat jako *MAC adresu*). Každé kartě je přidělena jedna taková adresa jednoznačně výrobcem. Vedle pevně přidělené globální adresy může karta používat adresu lokálně zvolenou správcem sítě, nebo adresu skupinovou. Další informací je údaj o vyšším protokolu, pro který je blok dat určen (u Ethernetu II), nebo údaj o délce a údaj definující přesněji odesílatele a adresáta v rámci počítače a sloužící potvrzování (u Ethernetu IEEE 802.3, strukturu a využití tohoto údaje definuje protokol logické vrstvy LLC IEEE 802.2). Ochranu proti chybám zajišťuje dvaatřicetibitový cyklický kód. Uvedenou strukturu, kterou při vlastním přenosu předchází ještě synchronizační posloupnost nul a jedniček o délce 64 bitů, označujeme jako *rámec* - obr. 8.2. Rámce kratší než 64 oktetů označujeme jako *runts*.



Obrázek 8.2: Rámec Ethernetu a přístup k médiu v síti 10BASE5

Stanice, která má připravený rámec k vyslání a detekuje klid na sdíleném kanále po dobu alespoň 9.6 μs, zahájí vysílání synchronizační posloupnosti a potom odešle vlastní rámec rychlostí 10 Mb/s. Stanice, která chce vysílat, ale indikuje provoz na médiu, musí počkat na uvolnění média a uplynutí ochranného intervalu 9.6 μs. Tento postup je označován jako *naléhající CSMA*. Stanice začíná vysílat po uvolnění média bez nějaké další podmínky, v případě sítě Ethernet je základní mechanismus ještě doplněn o detekci kolize (*CSMA/CD*). Ta dovoluje podstatně snížit ztráty způsobené kolizí stanic, které čekaly na uvolnění média a kolizi si tím "naprogramovaly" . Stanice, která vstoupila do kolize a tuto skutečnost rozpoznala, se pokusí o opakované vysílání po náhodně zvolené době se střední hodnotou rovnou délce kolizního intervalu (51.2 μs). Náhodná volba odmlky brání periodickému opakování kolize stanic. Pokud k opakované kolizi dojde, stanice prodlužuje střední dobu prodlevy na dvojnásobek. Po deseti neúspěšných pokusech přestane prodlevu prodlužovat a po šestnácti hlásí závadu vyšším vrstvám obsluhy (Může jít o odrazy na přerušeném nebo zkratovaném kabelu,

porouchanou některou ze stanic segmentu, apod.). Postup označovaný jako *exponenciální ustupování* (Exponential Back-off) je navržen tak, aby zajistil stabilitu sítě pro alespoň 1024 stanic. To je také limit, který stanovuje norma pro skupinu segmentů propojených opakovači – *kolizní doménu*.

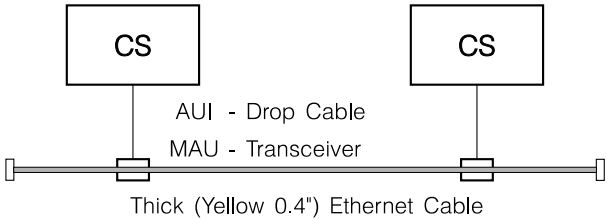
Signál přenášený po médiu je kódován tak, že jednotlivým bitům odpovídají hrany signálu, kód známe pod jménem Manchester. Vysílače fungují jako zdroje proudu, na kabelu s pevně definovanou charakteristickou impedancí, detektor kolize se pak opírá o měření střední hodnoty signálu na kabelu. Podle nastaveného limitu je schopen detekovat kolizi vysílající stanice s jinou stanicí na kabelu (Transmit Mode), nebo kolizi dvou jiných stanic na stanici v klidu (Receive Mode). Pro testování detektoru kolize může transceiver vysílat po příslušném vedení AUI kabelu indikaci kolize po odvysílání rámce (1 μs po ukončení po dobu 1 μs), funkce je označována jako *SQE Test* nebo *Heartbeat*. Další přídavnou funkcí stanice je *Jabber Control*, schopnost vypnout vysílač, pokud doba jeho vysílání překročí 20 ms, a to na dobu 500 ms. Tato funkce brání trvalému obsazení média při poruše transceiveru.

Přístupová metoda Ethernetu CSMA/CD se opírá o informace, které je stanice schopna získat pozorováním sítě. Vzhledem ke konečné době šíření signálu v přenosovém médiu a ke zpožděním v opakovačích se však jedná o informace nepřesné čímž efektivita metody CSMA/CD klesá s rostoucí vzdáleností stanic. Proto je standardem omezena jak vzdálenost po médiu tak i počet opakovačů mezi každými dvěma stanicemi. Překročení limitů může být důvodem podstatného zvýšení počtu kolizí a počtu poškozených rámců a tím i výsledného *snížení průchodnosti* sítě.

Formát rámce jsme si již popsali, za upozornění pouze stojí, že formát rámce podle normy DIX se poněkud liší od formátu rámce podle IEEE 802.3. Zatímco IEEE Ethernet uvádí v hlavičce délku LLC bloku, DIX Ethernet zde identifikuje síťový protokol (IP, IPX, ...). Odlišení obou typů rámců je možné díky tomu, že délka datového pole je omezena na 1500B a údaj o délce tak může být nejvýše $5DC_H$, zatímco označení typu využívá hodnot od 800_H (kromě některých historických identifikací protokolů, jimž se lze v praxi vyhnout).

8.1.1 10BASE5

Technologie 10BASE5 (10 Mb/s, přenos v základním pásmu, délka segmentu do 500 m) vychází z původního Ethernetu II a specifikace DIX (str. 33). (Specifikace IEEE 802.3 byla publikována v roce 1983.) Přenosovým médiem je speciální koaxiální kabel o charakteristické impedanci 50 Ω (na rozdíl od 75 Ω kabelu používaného pro rozvod televizního signálu nebo 93 Ω kabelu používaného pro připojování terminálů IBM a pro rozvody dnes již historické lokální sítě ARCNet) s dvojitým opletením a žlutou PVC nebo oranžově-hnědou teflonovou vnější izolací. Kabel o průměru 0.4" (10 mm), označovaný jako *tlustý kabel* (Thick Ethernet Cable) vytváří *segment* dlouhý až 500 m zakončený šroubovacími konektory typu N, na ně se připojují zakončovací odpory.



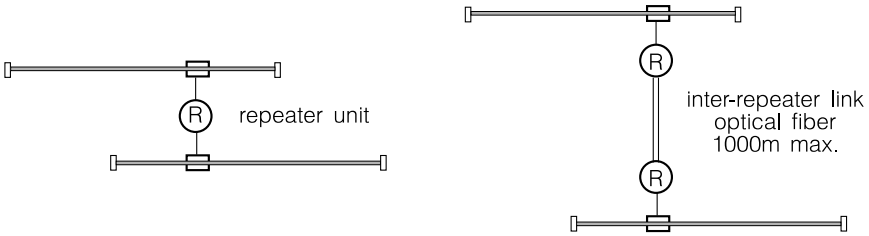
Obrázek 8.3: Prvky sítě 10BASE5

Jednotky MAU se ke kabelu připojují zvláštním způsobem - jehla konektoru jednotky přišroubované ke kabelu prochází předvrtaným otvorem ke střednímu vodiči kabelu, kabel se

nemusí při připojování jednotky MAU řezat. Alternativou je vložení jednotky MAU mezi dva úseky kabelu zakončené konektory typu N. Ke kabelu lze připojit nejvýše 100 jednotek MAU, vzdálenost mezi jednotkami smí být nejméně 2.5 m, kabel má v těchto vzdálenostech značky. Vlastní stanice je připojena AUI-kabelem. Existují i vícenásobné jednotky MAU, které dovolují připojit skupinu stanic do jednoho místa na kabelu.

Opakovač

Elektrické parametry koaxiálního kabelu nedovolují překročit délkový limit 500 m pro segment a limit 100 připojených stanic (10BASE5) na segment. Pokud potřebujeme propojit větší počet počítačů a/nebo dosáhnout větší vzdálenosti mezi stanicemi, musíme sáhnout k *aktivním* prvkům. Nejjednodušším takovým prvkem je *opakovač* (Repeater), který je připojen ke dvěma segmentům Ethernetu. Opakovač přijímá signál z jednoho segmentu, upravuje jeho časový průběh a elektrické úrovně a vysílá opravený signál do segmentu druhého. Opakovač při své činnosti rekonstruuje preambuli, prodlužuje krátké fragmenty (na minimální délku 96 bitů) a předává indikaci kolize (*Jam*). Stejnou funkci má opakovač i ve směru opačném.



Obrázek 8.4: Opakovače v síti 10BASE5

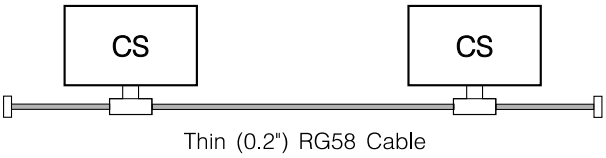
Segmenty propojené opakovačem se z pohledu připojených stanic chovají jako segment jediný, signál vyslaný jednou ze stanic lze přijmout libovolnou ze stanic na propojených segmentech. Přestože opakovače dovolují vytvářet i rozsáhlejší sítě, jejich použití má určité limity. Síť složená ze segmentů propojených opakovači může mít pouze stromovitou topologii, signál smí mezi libovolnými dvěma stanicemi sítě projít nejvýše třemi, a za splnění určitých podmínek (pouze tři z propojovaných segmentů smí být sběrnicové – Populated Segments) čtyřmi opakovači (starší normy dovolovaly pouze dva opakovače, za opakovač jediný však počítaly dvojici opakovačů propojených optickým spojem). Propojení segmentů na větší vzdálenost (například segmentů v různých budovách) a jejich dokonalou vzájemnou izolaci umožňují opakovače propojené optickým vláknem (FOIRL – Fibre Optic Inter-Repeater Link), překlenutá vzdálenost je obvykle do 1000 m. Takové prvky označujeme jako *Remote Repeater*.

8.1.2 10BASE2

Kvalita standardního kabelu u technologie 10BASE5 (specifikace IEEE 802.3b z roku 1988) je bohužel zaplacena vysokou cenou, instalace je navíc značně komplikovaná. Využijeme ho pro propojování výkonných počítačů a pracovních stanic, pro výstavbu páteřních segmentů. Pro propojení většího množství osobních počítačů je klasický rozvod speciálním kabelem zbytečně nákladný.

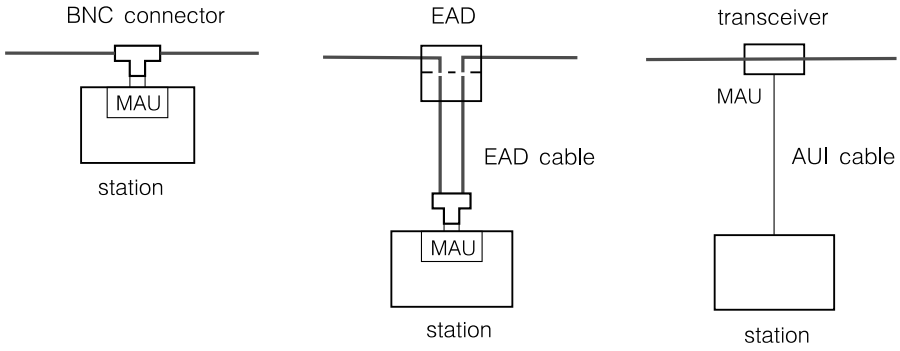
Alternativou se stalo použití *tenkého kabelu* o průměru 0.2" (5 mm) a impedanci 50 Ω s jednoduchým opletením (Thin Ethernet Cable), původně používaného v měřící technice. Síť dostala jméno CheaperNet. Dnes jsou kabel a pravidla pro výstavbu segmentu jsou definovány normou IEEE 802.3, technologie je označována jako 10BASE2. Horší parametry tenkého kabelu typu RG 58A/U nebo RG58C/U omezují délku segmentu na 185 m (pokud některé firmy dovolují pracovat se segmentem o délce až 450 m, pak předpokládají použití pouze svých prvků

na segmentu). Transceiver (MAU) je u 10BASE2 většinou integrován přímo na desce řadiče Ethernetu nebo do skříňky opakovače, pro propojení s vlastním segmentem jsou používány bajonetové *konektory BNC*. (Přesněji, na vývod desky řadiče nebo opakovače je připojena rozbočka ve tvaru písmene T, segment je tvořen propojovacími kabely mezi rozbočkami jednotlivých karet, na konce segmentu musí být připojeny zakončovací odpory.) Na jeden segment je možné připojit nejvýše 30 stanic, nejmenší vzdálenost mezi nimi je 0.5 m.



Obrázek 8.5: Prvky sítě 10BASE2

Výstavba segmentu s použitím tenkého kabelu je sice jednoduchá, přináší však jedno podstatné nebezpečí. Tím je přerušení segmentu náhodným rozpojením konektoru na volně vedených kabelech. Jeho důsledkem nemusí být pouze rozpad komunikace mezi stanicemi na rozdělených částech segmentu, ale úplné narušení komunikace odrazy na neukončeném konci kabelu. Určitým řešením problému je kabeláž, u které náhodné odpojení jednoho z osobních počítačů od sítě (vytažení kabelů, nekorektní propojení zbytku segmentu) nevede na narušení segmentu. Segment je tvořen pevně instalovanými úseky koaxiálního kabelu mezi zásuvkami označovanými jako *EAD zásuvky* (podobají se telefonním zásuvkám EAT podle normy DIN), do kterých lze zapojovat smyčky připojující jednotlivé počítače – *EAD kabely*. Odpojení počítače od pevně propojené smyčky EAD kabelu nevyvolá rozpad segmentu, vytažení EAD kabelu ze zásuvky je automaticky přemostěno spínačem v zásuvce EAD. I toto řešení však má svá úskalí: EAD kabel o délce 5 m reprezentuje 10 m délky segmentu a s tou musíme při limitní délce segmentu šetřit, i samotné zásuvky EAD jsou možným zdrojem poruch. Pokud



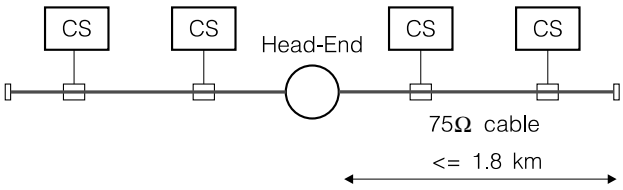
Obrázek 8.6: Varianty kabeláže 10BASE2

chceme dosáhnout co nejvyšší spolehlivosti sítě i při použití tenkého koaxiálního kabelu, je pravděpodobně nejvýhodnější realizovat pevnou kabeláž s pevně připojenými transceivery (pro tenký kabel) a jednotlivé počítače připojit k těmto transceiverům AUI-kabely podobně jako u tlustého kabelu (obr. 8.6).

8.1.3 10BROAD36

širokopásmový Ethernet (10BROAD36) je určen pro průmyslové prostředí a používá jako médium koaxiální kabel s impedancí 75 Ω pro kabelovou televizi.

Stanice jsou připojeny k segmentům koaxiálního kabelu o maximální délce 1.8 km, segmenty jsou připojené k centrálnímu prvku označovanému jako *Head-End*. Existují dvě možné funkční konfigurace sítě: Prvá používá dvojitou kabeláž (*Dual-Cable System*) – jeden kabel přenáší signál



Obrázek 8.7: Technologie 10BROAD36

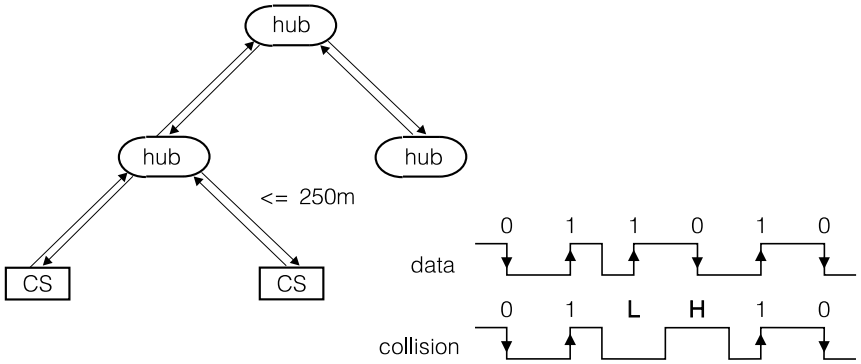
od stanice k centrálnímu prvku, druhý distribuuje signál od centrálního prvku ke stanicím. Centrální prvek pouze zesiluje signál přijatý před jeho rozesláním. Druhou konfigurací je využití oddělených frekvenčních pásem na jediném kabelu pro realizaci dostředného i distribučního kanálu (*Split-Channel System*). Centrální prvek pak převádí signál mezi oběma pásmy, má funkci konvertoru. Modemy používají diferenciální fázovou modulaci, datový signál NRZ je před vysláním skramblován. Přenosová rychlost je 10 Mb/s, využité kmitočtové pásmo (pro jeden kanál) má šířku 14 MHz. Detekce kolize se opírá o poslech vlastního vysílání ve zpětném kabelu nebo pásmu a porovnávání odeslaných a přijatých dat. Kolize je ostatním stanicím indikována po vyhrazeném kanálu o šířce 4 MHz. Celková potřebná šířka pásma je 18 MHz pro systém s dvojitou kabeláží a 36 MHz pro systém s jednoduchou kabeláží.

Výhodou technologie je délka segmentu 1.8 km, dovolující propojit stanice vzdálené až 3.6 km, a levná kabeláž opírající se o prvky kabelové televize (CATV).

8.1.4 StarLAN - 1BASE5

Předchůdcem současných stromových technologií Ethernetu byla síť *Starlan* (*1BASE5*). Používala jako média dvojici nestíněných kroucených dvoudrátů – kabel UTP Cat.3 (Voice-Grade kabel). Stanice byly připojeny hvězdicově ke koncentrátoru. Vedení mezi stanicí a koncentrátorem mělo délku do 250 m. Rozsáhlejší sítě bylo možné vytvářet propojením koncentrátorů hvězdicově mezi sebou. Limitem bylo pět úrovní koncentrátorů (největší vzdálenost mezi stanicemi je pak 2500 m).

Pro přenos dat byl použit kód Manchester, jeden dvoudrát sloužil k vysílání, druhý k příjmu. Koncentrátor opakoval přijatý signál všem připojeným stanicím, tedy i stanici vysílající. Byl současně místem, kde byla detekována kolize – při příjmu signálu z více než jednoho směru koncentrátor rozesílal kolizní posloupnost (jam), složenou z nedatových signálových prvků (chybějící hrana reprezentující bit dat).



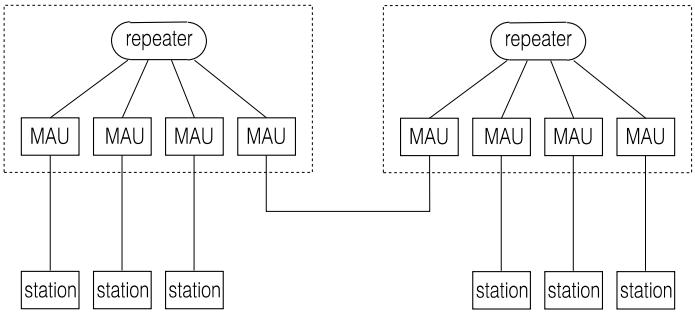
Obrázek 8.8: Síť StarLAN

Nevýhodou technologie StarLAN byla nízká přenosová rychlost – 1 Mb/s, a tím i obtížnost kombinace s jinými variantami Ethernetu. Pokus firmy National Semiconductors o zvýšení přenosové rychlosti na 10 Mb/s byl komerčně neúspěšný, standardem se stala technologie

10BASE-T.

8.1.5 10BASE-T

Koaxiální kabely jako médium pro výstavbu sítí Ethernet se stávají historií. Důvodem je přechod k "levnějšímu" a univerzálnějšímu *kabelu UTP* (Unshielded Twisted Pair) a k odlišnému způsobu vytvoření sdíleného kanálu. úseky UTP kabelu o délce do 100 m (přesněji do 90 m pevného rozvodu a dvakrát 5 m pohyblivý kabel pro připojení zařízení) propojují jednotlivé stanice s *vícevstupovým opakovačem* (Multiport Repeater, koncentrátor). Ten je středem hvězdice tvořené skupinou až osmi, dvanácti, šestnácti nebo i více stanic a vytváří anologii segmentu technologií 10BASE5 a 10BASE2. Technologie dostala název 10BASE-T (T jako Twisted Pair) a je specifikována doporučením IEEE 802.3i z roku 1990.



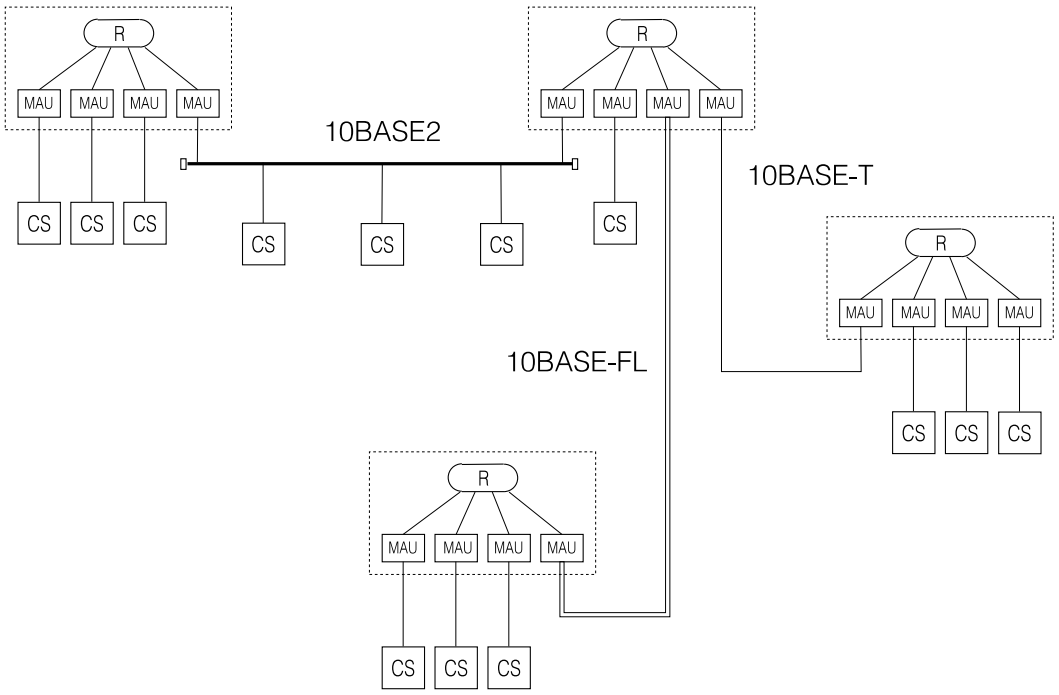
Obrázek 8.9: Struktura sítě 10BASE-T

Ze čtyř párů kabelu UTP jsou využity dva, jeden pár přenáší signál od stanice k opakovači, druhý přenáší signál ve směru opačném. Kabel UTP musí splňovat podmínky na šířku pásma, charakteristickou impedanci a přeslech. (Přeslech signálu z vysílacího vedení do přijímacího může být považován za kolizi.) Podmínky splňují kabely UTP Cat.3 (Voice Grade) a s rezervou dnes běžnější kabely UTP Cat.5 (Data Grade), ty lze při správné montáži použít i pro rychlou síť 100BASE-TX. Jako konektor (zásuvky karet, zásuvky pro pevný rozvod, zástrčky na kabel) slouží plochý konektor EIA RJ45 (podobný telefonnímu konektoru podle americké normy EIA RJ-11).

Alternativním přenosovým médiem jsou optická vlákna podle 10BASE-FL (nebo FOIRL, str. 72), ta dovolí prodloužit vzdálenosti mezi opakovači, nebo mezi stanicí a opakovačem na 400m.

Jako označení pro opakovač 10BASE-T se vžilo označení *hub*, dnes se však pod tímto názvem (připomeňme si původní význam termínu – střed loukoťového kola) často skrývají zařízení s funkcí i zcela odlišnou. Opakovač předává signál přijatý od jedné ze stanic po elektrické úpravě stanicím ostatním, kromě stanice nebo opakovače, od nichž je přijímán. Stará se tak o vytvoření sdíleného kanálu. Příjem signálu při vlastním vysílání je pro stanici indikací kolize. Opakovače lze mezi sebou propojovat, buď opět kabely UTP, segmenty koaxiálního kabelu nebo optickými spoji (obr. 8.10), pro jejich počet mezi dvěma stanicemi platí běžné limity. řada výrobců nabízí vedle opakovačů s pevným počtem rozhraní i *opakovače modulární* (s moduly pro osm, dvanáct, šestnáct UTP vedení a s moduly pro jiná média – koaxiální kabel, FOIRL nebo s univerzálním rozhraním AUI) a *stohovatelné* (Stackable Hub).

Sdílený kanál vytvářený vícevstupovým opakovačem 10BASE-T nebo strukturou z nich složenou přináší proti sběrnicovému propojení počítačů podstatnou výhodu: odpojení stanice nemůže ovlivnit chod zbytku sítě. Logika moderních opakovačů 10BASE-T dovolí odizolovat i stanici, která by u sběrnicového Ethernetu svou poruchou narušila funkci celé sítě (například trvalým vysíláním signálu).



Obrázek 8.10: Struktura kombinovan0 sítě Ethernet

Při rozhodování o volbě technologie Ethernetu pro lokální síť hraje často podstatnou roli cena řešení. "Nespolehlivý" segment Ethernetu 10BASE2 lze postavit za cenu komunikačních desek do počítačů, levného kabelu, konektorů a zakončovacích odporů. U pevné kabeláže cena roste používáním doplňkových prvků (EAD zásuvek, pevně instalovaných transceiverů a AUI kabelů, zásuvek RJ45) a náklady na instalaci. Hvězdicový rozvod 10BASE-T vyjde dráže pro větší spotřebu srovnatelně drahého kabelu UTP a pro nutnost zakoupení koncentrátoru (nejedná-li se o propojení dvou počítačů).

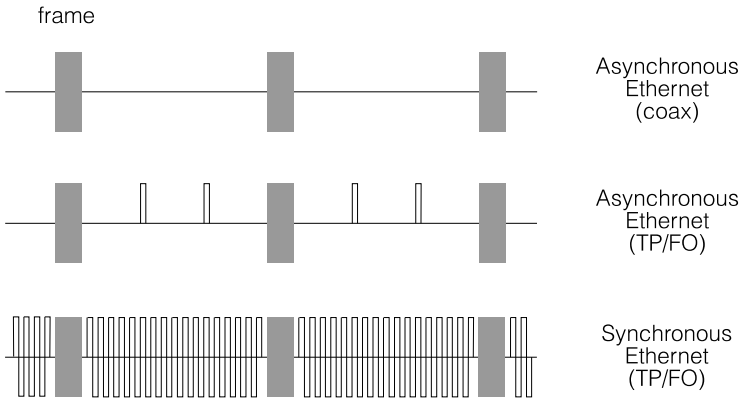
Moderní koncentrátory jsou vybavovány správou SNMP, které dovolí informovat o jejich funkci a ovládat je na dálku (str. 155). Existují i typy, které dovolují omezit přenos na jednotlivých vedeních na konkrétní adresy, takové koncentrátory zvyšují bezpečnost (ve významu "nezneužitelnost") sítě.

Synchronní Ethernet

Konfigurační pravidla sítí Ethernet omezují počet opakovačů mezi stanicemi na tři nebo čtyři. Hlavním důvodem tohoto omezení jsou ztráty bitů na začátku rámců a zpoždění vyvolaná nutností synchronizace opakovačů na přijímaný signál. Zatímco u sběrnicových konfigurací (10BASE5, 10BASE2) se nutnost synchronizace přijímače na každý přijímaný rámec nedá obejít, u dvoubodových spojů 10BASE-T lze synchronizaci sousedních opakovačů udržet i v době, kdy je médium nevyužité. Ani u běžného *asychronního Ethernetu* 10BASE-T sice není na spojích mezi opakovači klid (prvky vysílají signál dovolující zkontrolovat správné zapojení kabelů), ale u *synchronního Ethernetu* je přenášen mezi datovými rámci periodický signál o kmitočtu 2.5 Mb/s, který dovolí udržet synchronizaci a lze ho navíc využít k signalizaci.

8.1.6 Optické spoje FOIRL a 10BASE-FX

Dvoubodové spoje lze s výhodou realizovat s optickými vlákny, jejich využití přichází v sítích Ethernet v úvahu pro propojení opakovačů a pro připojení stanic v hvězdicových konfiguracích. Původní specifikace optického propojení opakovačů *FOIRL* (Fiber Optic Inter-Repeater Link)



Obrázek 8.11: Synchronní Ethernet

používá mnohavidové vlákno a dovoluje propojit opakovače na vzdálenost do 1000 m. Funkčnost optického spoje v době, kdy nejsou vysílány datové rámce je testována periodickým *idle* signálem o frekvenci 1 Mhz. Tento signál není nijak synchronizován s přenosem datových rámců.

Novější standardy označované jako 10BASE-F (IEEE 802.8) rozšiřují původní specifikaci FOIRL a definují vlastnosti dvou typů dvoubodových optických spojů a pasivní optické hvězdy.

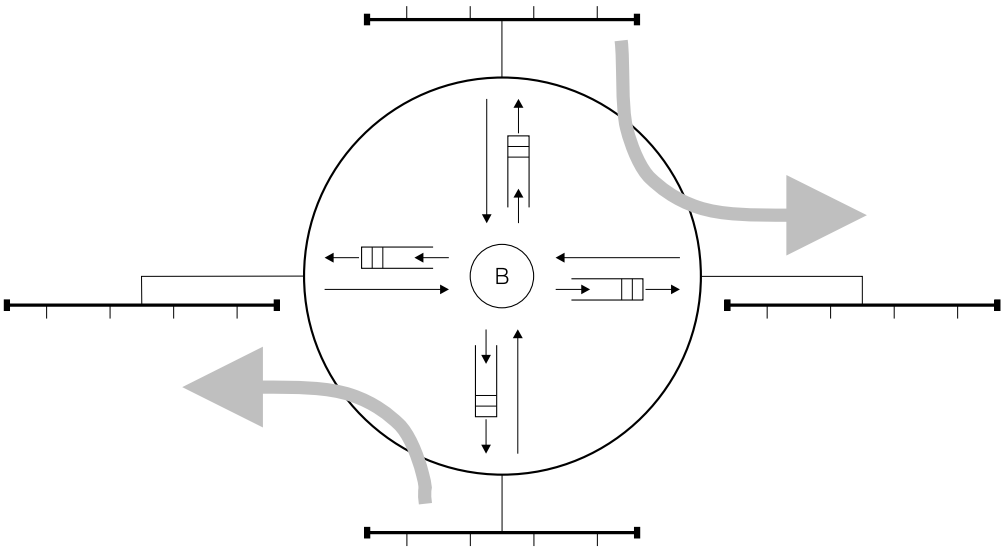
Specifikace *10BASE-FL* (Fiber Link) definuje dvoubodový spoj schopný překlenout až 2000 m určený pro propojení opakovačů a dovolující připojení stanic na vzdálenost do 400 m. Je rozšířením specifikace FOIRL, prvky 10BASE-FL mohou spolupracovat s prvky podle FOIRL (limitem je zde vzdálenost 1000 m).

Specifikace *10BASE-FB* (Fiber Backbone) definuje synchronní dvoubodový spoj, určený pro propojení opakovačů. Signál 1 Mhz indukující funkčnost spoje u 10BASE-FL je nahrazen signálem 2.5 Mhz, který však slouží k synchronizaci. Technologie dovoluje zvýšit limit počtu opakovačů mezi dvěma stanicemi, využití optického spoje 10BASE-FB mezi opakovači je obdobou *synchronního Ethernetu*. Konečně, specifikace *10BASE-FP* (Fiber Passive system) definuje pravidla pro síť se strukturou pasivní hvězdice. Segment, vytvořený podle této specifikace, dovolí překlenout až 500 m, k pasivní hvězdě lze připojit až 32 stanic.

Při použití optických spojů (ale častěji při připojování sběrnicových segmentů k moderním zařízením, která předpokládají použití UTP kabelu) se můžeme setkat s prvky, označovanými jako *převodníky signálu rozhraní* (Media Convertor). Tyto prvky, na rozdíl od opakovačů, při převodu signálu různých médií pouze upravují amplitudu signálu, neobnovují časování. Při konfiguraci sítě je musíme počítat jako opakovače, jejich použití bychom se však měli vyhnout.

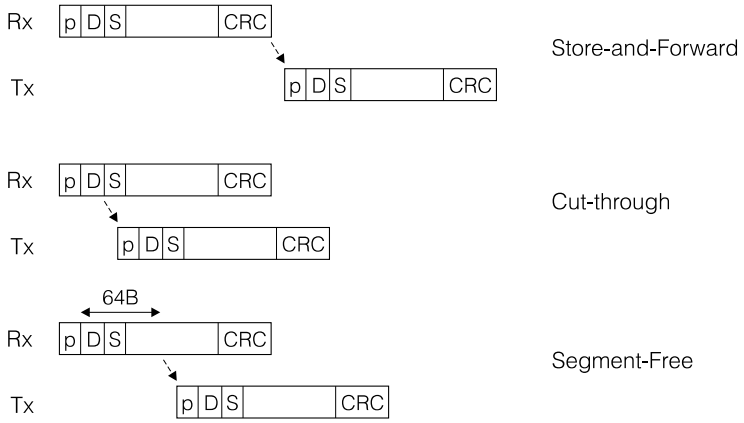
8.2 Přepojovaný Ethernet

Mosty Ethernetu dovolují rozdělit rozsáhlejší síť na *kolizní domény*, provoz v jedné části sítě nemá vliv na provoz v části druhé a součtový tok v síti může být vyšší než je limit v každé z kolizních domén. U víceportových mostů, které propojují čtyři a více kolizních domén, se objevuje další zajímavý efekt. Přenos rámců mezi dvěma kolizními doménami přes takový most neblokuje jiný přenos mezi jinými dvěma kolizními doménami přes týž most. Při větším počtu portů a možnosti rozdělit síť na menší kolizní domény (mluvíme o *segmentaci sítě*, ale tomuto termínu se budeme snažit vzhledem ke kolizi s běžně používaným pojmem segment vyhýbat) je tento efekt silnější. Takové prvky běžně označujeme jako *přepínače* (Ethernet Switches). Technologii, využívající přepínačů ke zvýšení průchodnosti sítě označujeme jako *přepojovaný Ethernet* (dáváme tomuto termínu přednost před termínem *přepínaný Ethernet*).



Obrázek 8.12: Princip přepojovaného Ethernetu

V krajním případě se můžeme dostat až k situaci, kdy na každý port přepínače je připojena jediná stanice a takto využívané přepínače jsou propojené dvoubodovými spoji (v síti nejsou víceportové opakovače ani sběrnicové segmenty s více než dvěma připojenými prvky), mluvíme o *mikrosegmentaci*. Taková síť funguje prakticky stejně jako každá jiná síť s přepojováním paketů. Pouze místo paketů (jako v X.25 nebo Internetu) jsou zde přepojovány rámce Ethernetu (a opíráme se o adresaci linkové vrstvy) a s ohledem na jednodušší topologii (pro provoz je využitelná pouze stromová podsíť získaná použitím Spanning-Tree algoritmu podle IEEE 802.1d) se zjednodušuje směrování. Rámce přijaté z jednotlivých vstupů jsou ukládány do pamětí přepínače, po rozhodnutí o způsobu odeslání a případné úpravě směrovací tabulky (přepínač se učí rozložení stanic v síti) převedeny do front na výstupech a odesílány do výstupních kanálů. Tento postup je označován jako *Store-and-Forward*.



Obrázek 8.13: Metody přepojování v přepojovaném Ethernetu

Určitou nevýhodou techniky Store-and-Forward je zpoždění, způsobené tím, že rámec může být vysílán do výstupního kanálu až po jeho dokončeném převzetí. Zpoždění lze eliminovat, dovolíme-li přepínači zahájit vysílání do neobsazeného výstupního kanálu okamžitě jakmile přepínač přečte adresu příjemce (prvních šest slabik rámce za preambulí). Využití této myšlenky (dlouho známé v teorii přepojovacích sítí jako Virtual-Cut-Through a využívané v paralelních počítačích) je známé jako technika *Cut-Through* a dovolí snížit zpoždění rámce při průchodu přepínačem až na 12 μs (proti 58-1220 μs u metody Store-and-Forward, kde záleží na délce rámce). Takové zlepšení může vypadat jako velký přínos a urychlilo rozšíření přepojovaného

Ethernetu, ale při zatížené síti, kdy v přepínačích vznikají fronty rámců, nemusí být rozdíl mezi oběma metodami podstatný.

Metoda Cut-Through má však i zápory. Patří mezi ně skutečnost, že odeslán je i rámec, u kterého bude při jeho příjmu zjištěna chyba CRC (v době, kdy přepínač zahajuje vysílání předávaného rámce, ještě nebyl zabezpečovací kód na konci rámce přijat). Další problém vyvolávají kolize na vstupech, přepínač zahájí vysílání rámce, který nebude díky zafungování detekce kolize přijat celý. Tento problém lze poměrně jednoduše řešit tak, že vysílání zahájíme až po převzetí dostatečného počtu znaků, tedy až budeme mít jistotu, že přijímaný rámec dojde celý (bylo přijato 64B a vysílání rámce již nepřeruší detekce kolize). úprava metody Cut-Through, která brání předání krátkých fragmentů rámců na výstup (a jejich dalšímu šíření sítí) je označována jako *Fragment-Free* a typické minimální zpoždění přepínače je 58 μs.

Pokud jde o reálné prvky, označované jejich výrobci jako přepínače Ethernetu, je potřeba si uvědomit, že mezi nimi existují podstatné rozdíly, které omezují jejich nasazení:

Nejširší použití mají přepínače, na jejichž vstupy lze připojovat celé kolizní domény (tvořené víceportovými opakovači nebo sběrnicovými segmenty). Takové přepínače dovolují realizovat přepínání označované termínem *Segment Switching* a bývají někdy označovány jako *Corporate Switches*. Pokud potřebujeme mít v síti náhradní spoje pro zvýšení spolehlivosti, musíme mít jistotu, že přepínač splňuje požadavky IEEE 802.1d (umí Spanning Tree Algoritmus).

Přepínačům, které počítají s připojením jediné stanice na každý vstup a které budou připojeny jediným rozhraním na zbytek sítě, stačí jednodušší směrovací tabulky (jedna adresa pro každý vstup, implicitní adresace pro rozhraní zbytku sítě). Přepojování je označováno jako *Link Switching*, přepínače bývají označovány jako *Workgroups Switches* a jsou využitelné pro mikrosegmentaci.

Pozn.: Konečně, existují zařízení označovaná jako *Configuration Switches*, která dovolí staticky připojit každý z většího množství vstupů na jeden z menšího množství výstupů. Výstupy jsou propojovány s mosty, běžnými přepínači nebo směrovači. Tyto prvky dovolují správci sítě rozdělit stanice zapojené do strukturované kabeláže do několika kolizních domén (segmentů) a toto rozdělení měnit na dálku (správou SNMP), tato funkce je označována jako *Port Switching* a nemá s přepojovaným Ethernetem mnoho společného.

Duplexní provoz

Na současné potřeby poměrně nízká přenosová rychlost běžného Ethernetu, i přes podstatné zvýšení celkové průchodnosti sítě přepojováním, vedla k hledání dalších úprav, které by chování přepojovaného Ethernetu dále zlepšily.

Nejběžnější modifikací přepojovaného Ethernetu, která dovolí zvýšit rychlost přenosu mezi samostatně připojenou stanicí a mostem/přepínačem bez velkých zásahů do funkce řadiče, je *duplexní provoz*. Náhrada sdíleného kanálu mezi dvěma silnými zdroji zátěže (například server a most/přepínač) dvojicí kanálů jednosměrných vedle zdvojnásobení kapacity (20 Mb/s) vylučuje nepříjemný vliv kolizí (je dobře si uvědomit, že i pouhé dva prvky připojené na běžný dvoubodový spoj 10BASE-T mohou vyvolat kolizi). Řešení ovšem vyžaduje upravené řadiče na obou stranách spoje, zařízení vybavená možností duplexního provozu se však mohou na přechodu na duplexní provoz po zapnutí sama domluvit. Příjemnou vlastností duplexního provozu je i to, že pro něj neplatí limit pro vzdálenost stanic (nemůže dojít ke kolizi). Při použití vhodného média (např. jednovidového optického vlákna) lze překonat i vzdálenosti desítek kilometrů.

Pozn.: Duplexní provoz se pochopitelně týká pouze přepojovaného Ethernetu, a to konfigurací, u kterých je segmentem jediný dvoubodový spoj. Vzhledem k omezenějším možnostem řízení toku musí být přepínače vybaveny dostatečně rozsáhlou pamětí.

Nepříjemné soupeření stanic na dvoubodovém spoji (i když bez využití součtu přenosové rychlosti obou vedení, kanál tedy zůstává poloduplexní) se snažila zmírnit i modifikace metody přístupu označovaná jako *PACE* (Priority Access Control). Cílem je vyloučit kolize mezi dvěma silně využívanými prvky na spoji (například server a most/přepínač) a rozdělit mezi ně spravedlivě a bezkolizně kapacitu poloduplexního kanálu. Jedná se jednoduchou úpravu, zařízení po odvysílání rámce musí počkat před vysíláním dalšího rámce výrazně delší dobu než 10 μs a dát tak šanci protistanici.

8.3 Rychlý Ethernetu (Fast Ethernet) - 100 Mb/s

Výrazně technologickou modifikací hvězdicového Ethernetu 10BASE-T se stal standard označovaný jako 100BASE-T zvyšující přenosovou rychlost na 100 Mb/s na kabelovém rozvodu UTP/FTP Cat.5 (modifikace 100BASE-T4 vystačí dokonce i s UTP Cat.3) a na vícevidových optických vláknech (62.5/125 μm a 50/125 μm). Specifikace rychlého Ethernetu pod označením IEEE 802.3u byla schválena v červnu 1995. Rychlý Ethernetu je založen na efektivnějším využití přenosového média. Kódování Manchester je u technologií 100BASE-TX/FX nahrazeno efektivnějším kódováním 4B5B, se kterým jsme se již setkali u sítě FDDI, doplněným o víceúrovňové kódování pro přenos po metalických vedeních (*MLT-3 Multi-Level Transmit*). Ještě výraznějšího zvýšení efektivity dosahují technologie 100BASE-T4 a 100BASE-T2 (obr. 8.14).

	Number of Pairs / Fibers	Encoding Method	Coding Efficiency
10BASE-T/Fx	2	Manchester	2.00 baud/bit
100BASE-TX/FX	2	4B5B	1.25 baud/bit
100BASE-T4	4	8B6T	0.75 baud/bit
100BASE-T2	2	PAM-5	0.5 baud/bit

Obrázek 8.14: Efektivita kódování u technologií rychlého Ethernetu

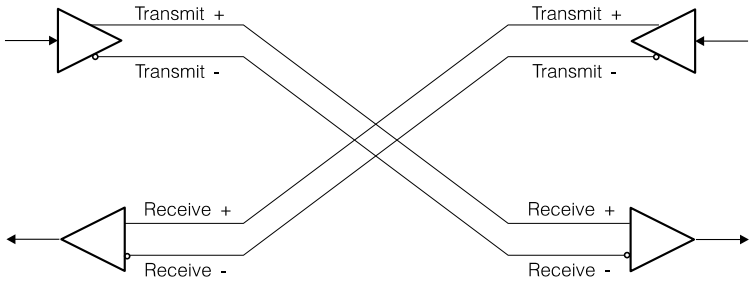
Vzdálenost mezi stanicí a koncentrátorem je, pokud použijeme metalický kabel, stejně jako u sítě 10BASE-T, do 100 m. Optické vlákno dovolí jít až na 412 m (mezi dvěma stanicemi nebo mezi stanicí a přepínačem) při poloduplexním a na 2000 m při duplexním provozu. U poloduplexního přenosu je omezením doba šíření signálu médiem: signál musí proběhnout médiem do nejvzdálenějšího místa sítě a zpět (včetně časů potřebných pro elektronice koncových prvků a opakovačů) za dobu potřebnou k odeslání 512 bitů. Při návrhu sítě rychlého Ethernetu se používá jednotka označovaná jako *bittime*. U optického vlákna odpovídá jeden metr vlákna jednomu bittime, u metalických kabelů s menší rychlostí šíření signálu jeden metr kabelu odpovídá 1.1 bittime.

Rychlý Ethernet definuje tři rozdílné realizace fyzického kanálu. Základem jsou kanály 100BASE-TX – dva páry kabelu UTP/FTP a 100BASE-FX – dvojice optických vícevidových vláken. Zajímavým doplňkem normy je kanál 100BASE-T4, který využívá tří párů kabelu UTP Cat.3 k přenosu dat a čtvrtého páru k detekci kolize. Později byl doplněn standard 100BASE-T2, který vystačí i u kabelů Cat.3 se dvěma páry.

S ohledem na různá řešení fyzického rozhraní (PMD - Physical Medium Dependent) je pro rychlý Ethernet definováno rozhraní mezi fyzickou vrstvou a vrstvou MAC. To je označováno jako *MII* (*Medium Independent Interface*) a má šířku čtyř datových bitů. Pro toto rozhraní je sice definován čtyřicetipinový konektor *rozhraní MII*, rozhraní je však, na rozdíl od AUI využíváno pouze jako standard rozhraní obvodů na desce síťového rozhraní (největší vzdálenost 0.5 m). Často je zcela skryté uvnitř obvodu.

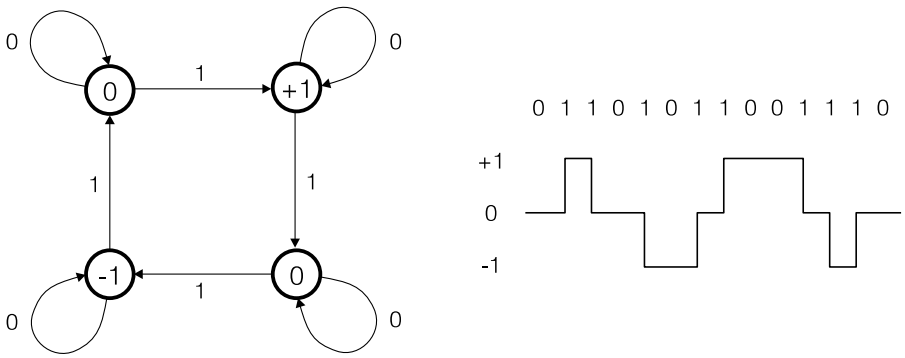
8.3.1 100BASE-TX

Základní technologií rychlého Ethernetu je 100BASE-TX. Vyžaduje použití UTP/FTP kabelu Cat. 5, jeden pár je využit pro vysílání a druhý pro příjem (obr. 8.15).



Obrázek 8.15: Využití párů u technologie 100BASE-TX

Základní kódování 4B5B je doplněné o převod na třístavový signál (*MLT-3 Multi-Level Transmit*) (obr. 8.16).



Obrázek 8.16: Kódování MLT-3

Třístavový signál MLT-3 dovolí dosáhnout na běžné kabeláži UTP/FTP Cat.5 přenosové rychlosti 100 Mb/s (vzhledem ke kódování 4B5B je modulační rychlost 125 MBd).

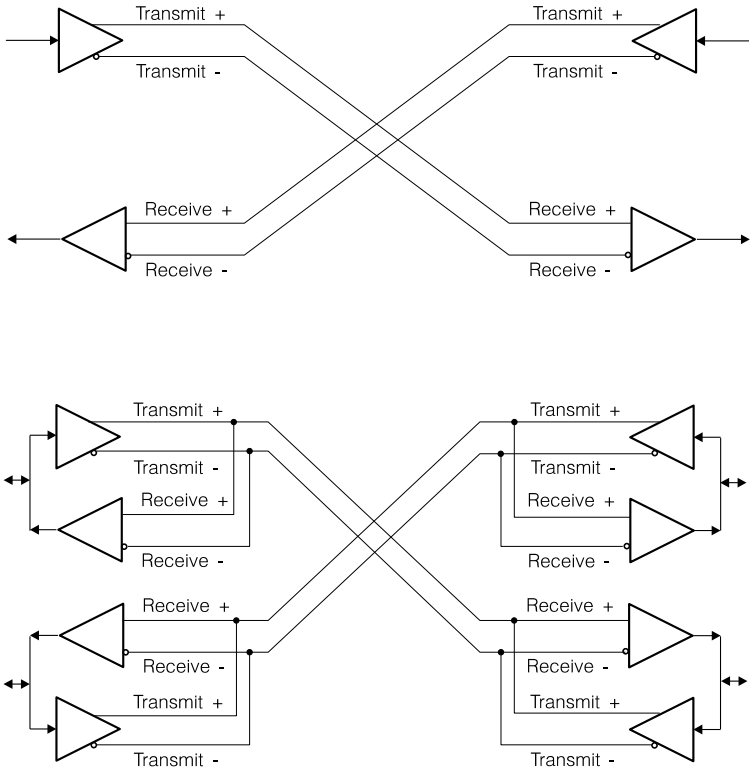
8.3.2 100BASE-T4

S příchodem technologie 100BASE-TX, která se opírá o kvalitnější UTP/FTP kabely Cat.5 se objevila snaha dovolit přechod na vyšší přenosovou rychlost i ve starších sítích, které používaly kabely UTP/FTP Cat.3.

Standard 100BASE-T4, kterému kabeláž UTP/FTP Cat.3 postačuje, využívá k vysílání (a příjmu) namísto jediného páru vodičů páry tři. Čtvrtý pár slouží k indikaci kolize, na rozdíl od ostatních technologií Ethernetu se stromovou architekturou je detekce kolize zajišťována primárně v opakovačích. Funkce všech prvků sítě je složitější než u jiných technologií, protože je na dvou vedeních nutné přepínat směr přenosu (obr. 8.17).

Snaha o co nejefektivnější přenos po trojici párů vedla k volbě kódování 8B6T, znak přenesený přes MII je vyslán jako dvě napěťové změny na každém z párů. Kódování 8B6T tak snižuje potřebnou modulační rychlost na 25 MBd, která je pro kabely UTP/FTP Cat.3 přijatelná.

Na rozdíl od ostatních technologií rychlého Ethernetu nedovoluje technologie 100BASE-T4 z principu duplexní provoz.

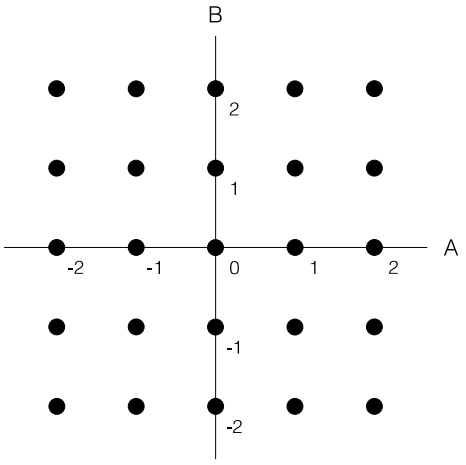


Obrázek 8.17: Využití párů u technologie 100BASE-T4

8.3.3 100BASE-T2

Snaha o další vylepšení technologie, schopné přenášet data rychlostí 100 Mb/s po jediném páru při zachování mezní modulační rychlosti 25 MBd, vedla k návrhu standardu 100BASE-T2. Tento standard má v oblasti rychlého Ethernetu okrajový význam, použitá metoda kódování však byla využita u přenosu gigabitového Ethernetu po kabelech UTP/FTP.

Princip kódování PAM-5 (5-level Pulse Amplitude Modulation) je poměrně jednoduchý (obr. 8.31).



Obrázek 8.18: Kódování PAM-5

Čtveřice bitů rozhraní MII je převedena na dvojici pětihodnotových symbolů, ty jsou jako pětiúrovňový signál přeneseny po obou použitých párech. Vedení dovoluje současný (duplexní) přenos v obou směrech, zpracování signálu, zahrnující scrambling a konvoluční kódér, se opírá

o procesor DSP.

8.3.4 100BASE-FX

Metalická vedení jsou dodnes levnější variantou kabeláže lokálních sítí, technologie rychlého Ethernetu však již předpokládá použití optických vláken, konkrétně vícevidových optických vláken datových (62.5/125 μm) nebo telekomunikačních (50/125 μm). Aby bylo možné překlenout vzdálenosti shodné s technologiemi 10BASE-FL/FB, používá 100BASE-FX světlo o vlnové délce 1300 nm.

Při poloduplexním přenosu je vzhledem k vidové disperzi a použití mnohavidových vláken nejvyšší vzdálenost omezena na 412 m. Na větší vzdálenost, až do 2 km, je nutné pracovat v duplexu, ten je však v moderních přepojovaných sítích standardně podporován.

Dvoukilometrový limit dovoluje i ve velkých budovách realizovat přepojovanou síť s architekturou jednoúrovňové hvězdy, koncová zařízení a servery sítě jsou samostatnými vlákny připojeny k centrálně umístěných přepínačům. Takové řešení často snižuje náklady, protože nevyžaduje aktivní prvky, přepínače nebo opakovače na patrech. Jeho praktické využití usnadňuje zjednodušení technologií přímého připojování maloformátových optických konektorů (LC, MT-RJ, VF-45) na optické kabely.

Datový signál je pro přenos 100BASE-FX kódován obdobně jako u 100BASE-TX, tedy nejdříve přeložen kódérem 4B5B, vlastní signál optického vlákna je z výstupu kódéru 4B5B získán překódováním NRZI (jednička je reprezentována změnou, použitý kód 4B5B zaručuje nejvýše tři nuly za sebou).

Na rozdíl od jiných technologií rychlého Ethernetu nemusí zařízení 100BASE-FX podporovat automatickou volbu přenosové rychlosti, kompatibilita s rychlejšími technologiemi Ethernetu pracujícími na vlnové délce 1310 nm je zajišťována na straně gigabitového Ethernetu.

8.3.5 100BASE-SX

Ethernet 100BASE-FX pracuje s vlnovou délkou 1300 nm a dovoluje překlenout na vícevidových vláknech v duplexním provozu vzdálenost až 2 km. Nepříjemnou vlastností této technologie je nekompatibilita se staršími technologiemi FOIRL a 10BASE-FL/FB.

Technologie 100BASE-SX je modifikací rychlého Ethernetu, pracuje na 850 nm, tedy na vlnové délce shodné se staršími technologiemi. Koncová zařízení dovolují automatickou volbu přenosové rychlosti, i když poněkud odlišnou od systému využívaného u technologie 100BASE-TX/T4. Zařízení mohou, pro omezení vidovou disperzí a tedy i při duplexu, komunikovat rychlostí 100 Mb/s na vzdálenost nejvýše 300 m.

Výhodou 100BASE-SX proti technologii 100BASE-FX jsou také poněkud levnější vysílací a přijímací diody. Technologie je proto považována za možnou alternativu metalických spojů pro připojování koncových zařízení v klasické strukturované kabeláži.

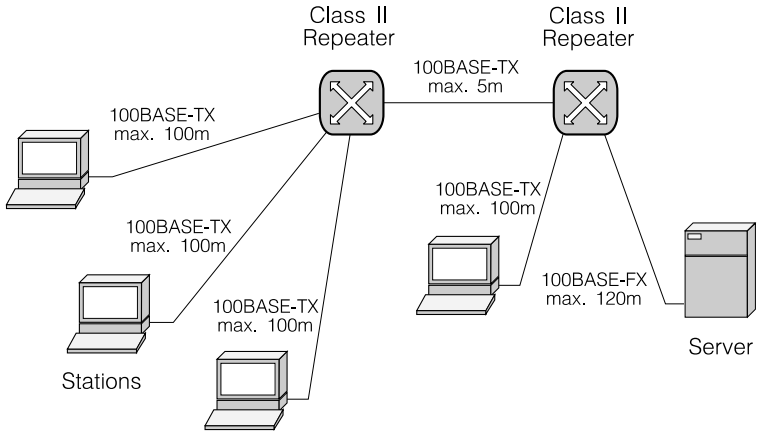
8.3.6 Sítě rychlého Ethernetu - sdílený kanál

Zvýšení přenosové rychlosti při zachování ostatních vlastností Ethernetu (metoda přístupu CSMA/CD, formáty rámců) si pochopitelně vyžádalo určitou cenu, a tou je snížení maximálně překlenutelné vzdálenosti. Ta je u sítě s opakovači omezena na o něco více než 300 m (a to pouze při použití optického vlákna). Pokud jde o vícevstupové opakovače, rychlý Ethernet definuje dva odlišné typy. První z nich (*Class I*) umožňuje použití různých fyzických rozhraní na vstupech a smí být mezi stanicemi jediný. Druhý typ opakovače (*Class II*) pracuje se stejnými fyzickými rozhraními, mezi stanicemi smí být nejvýše dva opakovače tohoto typu, navzájem propojené na vzdálenost do 5 m.

Technologie rychlého Ethernetu 100BASE-FX/TX/T4 dovoluje vytvořit sdílený poloduplexní kanál. Mezní topologie tohoto kanálu ale je, ve srovnání se základním Ethernetem 10BASE-T, podstatně jednodušší, slouží spíše pro napojení více stanic z poměrně malé lokality na jedno rozhraní přepínače, serveru nebo směrovače.

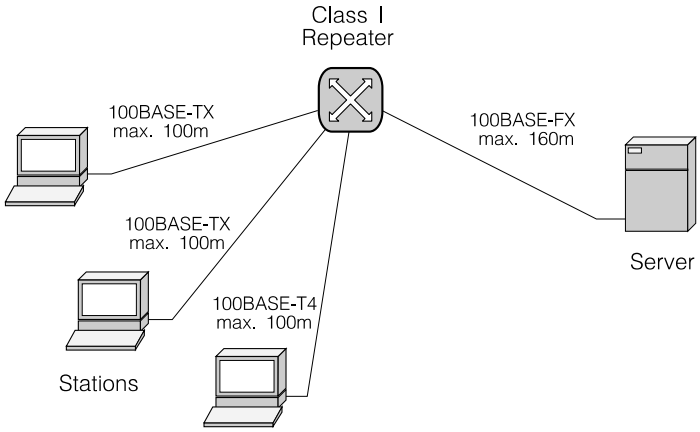
Pokud všechna rozhraní serveru využívají shodného kódování signálu, tedy buď všechna 100BASE-FX/TX (ale vzhledem ke způsobu využití spojů a použité metodě kódování i 100BASE-SX a 100BASE-T2) nebo všechna 100BASE-T4, je funkce opakovače jednodušší. Takový opakovač je označován jako *Class II* opakovač, jeho funkce je charakterizována zpožděním datového signálu kolem 90 bittime.

Pro topologii sdíleného kanálu (kolizní domény) rychlého Ethernetu platí podstatně přísnější omezení, než pro Ethernet 10 Mb/s. Zpoždění každého spoje mezi rozhraními MII musí zůstat pod 512 bittime: vlastní tranceiver koncového zařízení je charakterizován zpožděním kolem 50 bittime, opakovač třídy *Class II* zpožděním 140 bittime, metr optického vlákna zpožděním jeden bittime, a metr kabelu UTP/FTP zpožděním 1.1 - 1.2 bittime. Nejvyšší délka metalického spoje nesmí s ohledem na normu strukturované kabeláže překročit 100 m. Sdílený kanál smí mít mezi dvěma koncovými zařízeními nejvýše dva opakovače typu *Class II*, často uváděný příklad možné topologie uvádí obr. 8.19.



Obrázek 8.19: Sdílený kanál 100BASE-FX/TX s opakovači Class II

Opakovač, který musí propojit rozhraní s odlišným kódováním, tedy rozhraní 100BASE-FX/TX a rozhraní 100BASE-T4, je složitější. Je označován jako *Class I* opakovač, jeho funkce je charakterizována zpožděním datového signálu kolem 140 bittime. Omezení topologie s opakovači typu *Class I* je podstatně přísnější, mezi koncovými zařízeními smí být nejvýše jeden omezovač typu *Class I* a celkové zpoždění mezi libovolnými rozhraními MII nesmí přesáhnout 512 bittime. Příklad možné topologie sítě s opakovačem typu *Class I* uvádí Obr. 8.20.



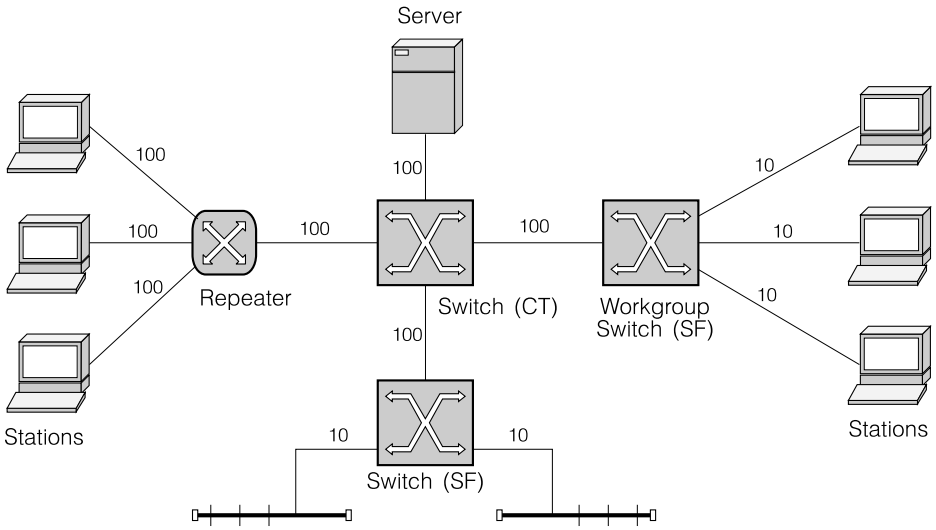
Obrázek 8.20: Sdílený kanál 100BASE-FX/TX s opakovači Class I

8.3.7 Sítě rychlého Ethernetu - přepojování

Výstavba dnešních sítí rychlého Ethernetu se nejčastěji opírá o přepínače, s opakovači se setkáváme spíše výjimečně. Běžně je přitom využívána možnost bezkolizního *duplexního provozu*; na dvoubodovém propojení přepínačů nebo na dvoubodovém připojení stanic a serverů k přepínači je tak k dispozici dvojice jednosměrných komunikačních kanálů, každý o rychlosti 100 Mb/s s možností překlenout (optickým vláknem) vzdálenost do 2000 m.

Pro řadu aplikací může stačit dvoubodové připojení pracovišť kanály o rychlosti 10 Mb/s k přepínači, na který jsou rychlými kanály připojeny servery a další části sítě. V případě takového připojení (všech) stanic sítě mluvíme o *mikrosegmentaci*. Pro náročnější aplikace je k dispozici sdílený rychlý kanál 100 Mb/s, dnes je běžné plné vyhrazení kanálů 100Mb/s jednotlivým zařízením a tím i možná práce v duplexním provozu.

Příklad možné topologie sítě na technologii 100BASE-TX uvádí Obr. 8.21.



Obrázek 8.21: Topologie sítí 100BASE-TX a 100BASE-FX

Kombinace zařízení se standardní rychlostí 10 Mb/s a zařízení pracujících se 100 Mb/s a navíc s odlišným využitím média (100BASE-TX a 100BASE-T4) a režimem provozu (poloduplex, duplex) může přinést problémy se správou a konfigurací. Pro usnadnění konfigurace jsou zařízení umožňující práci oběma rychlostmi vybavena obvody dovolujícími automatickou konfiguraci při zahájení provozu. Mechanismus respektuje i fakt, že jedno ze zařízení nemusí být

obvody pro automatickou konfiguraci vybaveno.

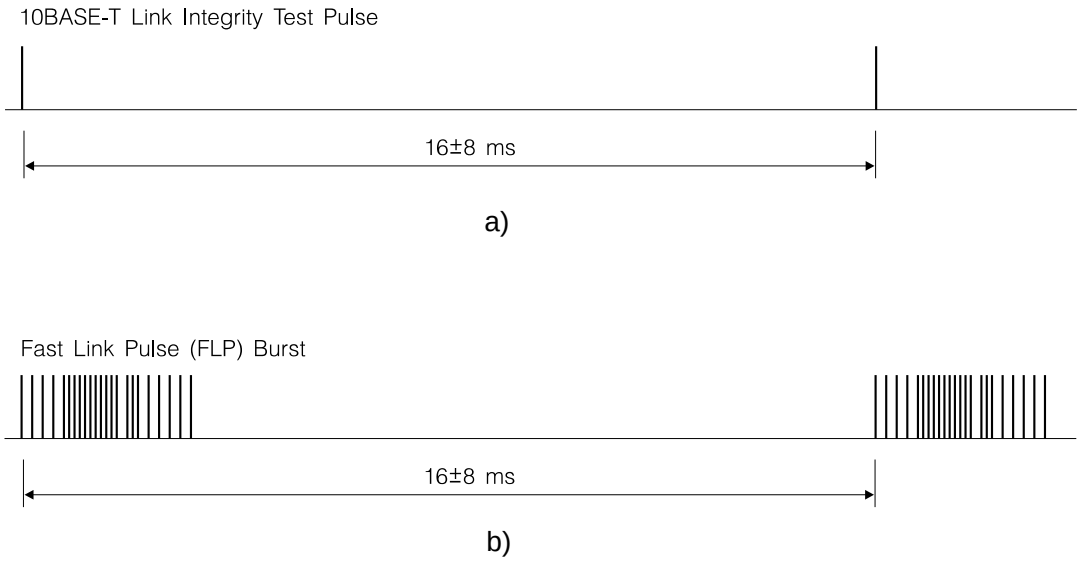
U přepojovaných sítí s rychlostí 100 Mb/s a rychlejších se silně projevuje problém známý z oblasti přepojovaných sítí - zahlcování přepínačů při absenci mechanismů *řízení toku*. Přepínač, jehož zdroje (paměti) jsou vyčerpány signalizuje tuto skutečnost sousedům, od nichž přebírá rámce. Koncovým stanicím může být simulována kolize, stanice je tak donucena snížit tok do sítě.

Nevýhodou rychlého Ethernetu zůstává stromová topologie sítě (se záložními kanály a výběrem kostry algoritmem Spanning Tree IEEE 802.1d) a z ní vyplývající omezení na přenosovou rychlost a pouze asynchronní režim práce s nepříjemným nedeterministickým řešením kolizí. Proti jiným moderním sítím chybí synchronní nebo isochronní režim výhodný pro multimediální aplikace. Při vhodném návrhu sítě (mikrosegmentaci) se však tento nedostatek nemusí vždy vážně projevit, a sítě opřené o standard rychlého Ethernetu mohou být ještě dlouho alternativou k přepojovaným sítím ATM.

8.3.8 Automatická konfigurace

Řada standardů dovolujících přenos signálu rychlého Ethernetu, spolu s možností konfigurovat jednotlivá rozhraní do různých režimů, by značně komplikovala konstrukci sítí. Podstatné zlepšení přináší automatická konfigurace parametrů, i když v určitých situacích i ta může selhat.

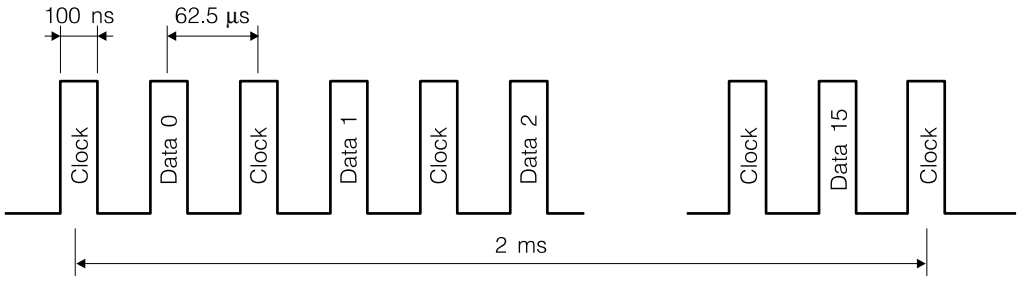
Automatická konfigurace zařízení propojených metalickým kabelem je založena na náhradě impulsů, které slouží u technologie 10BASE-T k testování správného propojení zařízení a případně k automatickému prohození vysílacího a přijímacího páru, posloupnostmi impulsů, které informují o schopnostech zařízení (obr. 8.22).



Obrázek 8.22: Testovací pulsy (a - 10BASE-T) a identifikační posloupnosti (b)

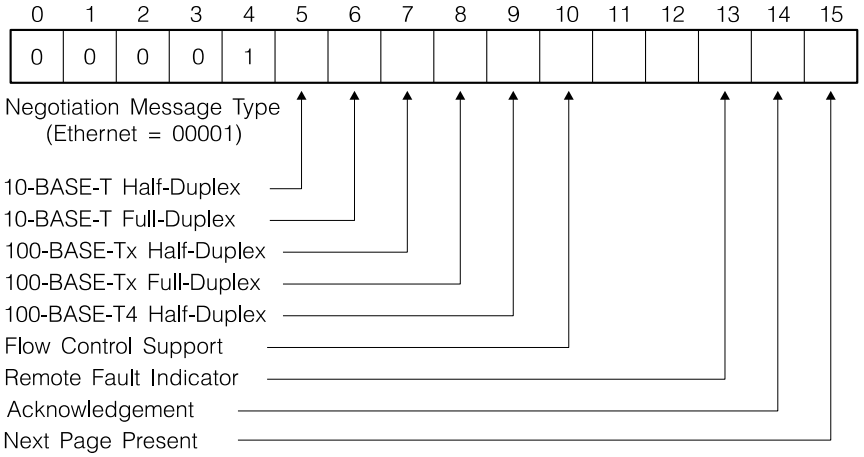
Posloupnosti identifikačních impulsů jsou přenášeny ve stejném odstupu jako původní testovací pulsy. Každá posloupnost přenáší šestnáct jednobitových parametrů zakódovaných jako přítomnost nebo nepřítomnost datových impulsů v posloupnosti, řešení předpokládá možnost prodloužení posloupnosti o další šestnáctibitová slova. Datové pulsy jsou v posloupnosti odděleny hodinovými pulsy, celkově je základní posloupnost tvořena až 33 pulsy (Obr. 8.23).

Jednotlivé identifikační pulsy vyjadřují schopnost zařízení pracovat s určitými standardy (10BASE-T, 100BASE-TX, 100BASE-T4) a režimy provozu (poloduplex, duplex) (Obr. 8.24.). Pro jednoznačný výběr je definována priorita standardů a režimů, současně je zajištěna



Obrázek 8.23: Identifikační pulsy Ethernetu

kompatibilita se staršími zařízeními 10BASE-T, která identifikační posloupnosti neznají.



Obrázek 8.24: Význam identifikačních bitů

Protože ne všechna zařízení rychlého Ethernetu musí být vybavena detekcí identifikačních posloupností, je celý mechanismus automatického nastavení doplněn o tzv. *paralelní detekci*. Zařízení vybavené identifikačním mechanismem musí být schopné rozpoznat typ signálu vysílaný protějškem, který nepoužívá identifikační posloupnosti, a přizpůsobit se mu.

8.3.9 Řízení toku

Přepínače v síti Ethernet zvyšují sumární průchodnost sítě, je s nimi však spojen jeden problém: kapacity přepínačů jsou konečné a při přetížení některého z rozhraní může dojít ke ztrátám rámců, které není kam uložit. Výrazné zvýšení kapacity pamětí přitom není řešením, oddálí riziko ztrácení paketů, ale za cenu zvýšeného zpoždění rámců čekáním ve frontách rozhraní.

U přepínačů s rozhraním v poloduplexním režimu se ztrátám rámců můžeme bránit odmítáním rámců, které není kam uložit. Lze toho dosáhnout dvěma metodami:

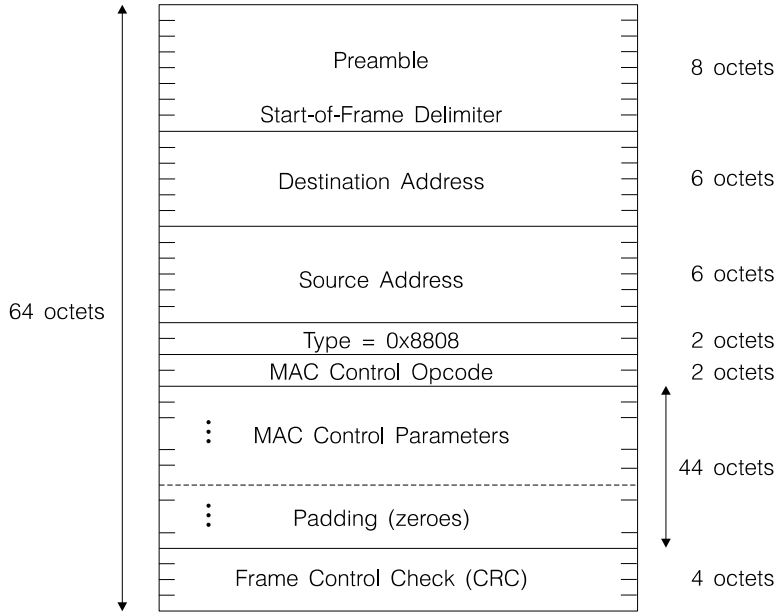
- vyvoláním kolize na vstupním rozhraní přepínače, z něhož nechceme přebírat rámce.
- vysíláním výplňových rámců do rozhraní, z něhož nechceme přebírat rámce.

Nevýhodou první metody je skutečnost, že opakovaná kolize vede na ustupování, nelze proto rychle reagovat na zlepšení situace, navíc po překročení limitu kolizí v sekvenci může dojít k indikaci výpadku linky a jejímu případnému vyjmutí z topologie sítě. Výhodou je pouze možnost rozlišit rámce, které mají být směrovány do zahlcených výstupů, od rámců, které problémy nevyvolávají.

Druhá metoda dovoluje sice rychlou reakci na zlepšení situace, protějšek může začít okamžitě po uvolnění média vysílat, v žádném případě však není možné diferencovat mezi rámci.

Podstatným problémem obou metod, označovaných jako *backpressure* metody, je skutečnost, že zahlcení jednoho přepínače je vede k přenesení problému na jeho okolí (přepínače v rozsáhlejší síti). Důsledkem se může stát zahlcení rozsáhlejších částí sítě a v důsledku i omezení datových toků, které přes přepínač, který zahlcení vyvolal nevedly.

Backpressure metody jsou použitelné pouze u poloduplexních spojů, u duplexu jsou z principu nepoužitelné. Proto byla pro řízení toku navržena podstatně pružnější metoda opírající se o přenos řídících MAC rámců - rámců PAUSE. Struktura rámce PAUSE odpovídá obr. 8.25.



Obrázek 8.25: Struktura řídícího MAC rámce

Rámce PAUSE se od datových rámců liší polem *Type*, ve kterém najdeme typ protokolu 8808, a které označuje skutečnost, že se jedná o řídící rámce MAC vrstvy. Rámce PAUSE jsou jedním konkrétním typem řídících rámců MAC, pole Opcode je u nich nastaveno na hodnotu 0x0001. Rámce PAUSE být směrovány všem zdrojům ve směru konkrétního rozhraní, pro tento účel je vyhrazena multicast adresa 01:80:C2:00:00:01. Alternativně lze rámce vysílat s unicast adresou konkrétního zdroje dat a tak selektivně omezit tok o sítě.

Nejdůležitější údaj přenášený v PAUSE rámci je informace o době, po kterou chceme pozastavit vysílání do spoje. Tento čas se udává jako násobek doby potřebné pro vyslání 512 bitů, tato volba vychází z alternativního využití obvodů u poloduplexu používaných pro mechanismus exponenciálního ustupování.

Pominou-li důvody pro pozastavení vysílání, lze rámcem PAUSE s nulovou hodnotou doby pozastavení vysílání okamžitě uvolnit. U vysokorychlostních spojů (mechanismus je navržen i pro gigabitový Ethernet a technologie ještě rychlejší) je nutné brát v úvahu zpoždění linek a množství dat, které do nich mohlo být vysláno (například kapacita dvou kilometrů gigabitového spoje je 20000 bitů).

U řízení toku v lokálních sítích odlišujeme dva typické scénáře. U prvního jsou špičky přenosu krátkodobé a nemají svůj zdroj převážně na jedné straně spoje. V takovém případě je rozumné dovolit *symetrické řízení toku*, tedy oba prvky na spoji si mohou v případě hrozícího zahlcení posílat rámce PAUSE.

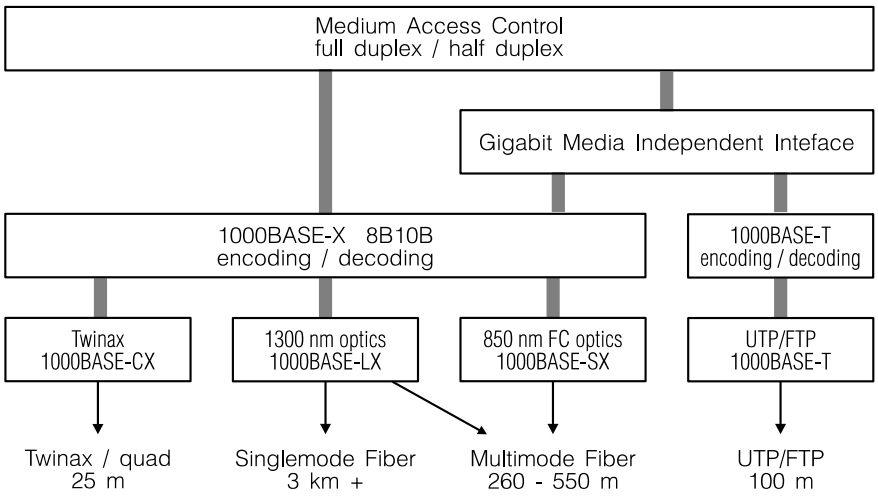
Alternativní *asymetrické řízení toku* je vhodné u koncových zařízení, hraniční přepínač sítě se omezením datového toku ze stanice může bránit přetížení sítě, stanice proti tomu nemůže ztěžovat práci zbytku sítě blokováním toku.

8.4 Gigabitový Ethernet

Přenosová rychlost 100 Mb/s nezůstala nadlouho limitem. Z iniciativy skupiny výrobců známé jako *GEA* (Gigabit Ethernet Alliance) byl vytvořen standard sítě založené na principech Ethernetu s přenosovou rychlostí 1 Gb/s - IEEE 803.z. Technologicky se gigabitový Ethernet opírá o ověřené technologie vyvinuté původně pro spoje Fiber Channel.

Podobně jako standard rychlého Ethernetu předpokládá gigabitový Ethernet více typů přenosového média. Základním médiem je vícevidové vlákno (62.5 μm, 50 μm) pracující na vlnové délce 780 nm (1000BASE-SX). Alternativní vlnovou délkou pro vícevidové vlákno je 1300 nm (1000BASE-LX), na této vlnové délce lze využívat i jednovidová vlákna a překlenout vzdálenosti i více než 3 km. Pro propojování zařízení na vzdálenost do 25 m lze využít kabel typu Twinax, dvoudrátové vedení s dobře definovanou impedancí proti vnějšímu plášti (1000BASE-CX).

Dodatečně byl standard gigabitové Ethernetu rozšířen i na typické přenosové médium pomalejších sítí, na kabely UTP/FTP (1000BASE-T) - IEEE 802.3ab. Přehled modifikací standardu a překlenutelné vzdálenosti při duplexním provozu uvádí obr. 8.26 a obr. 8.27.



Obrázek 8.26:

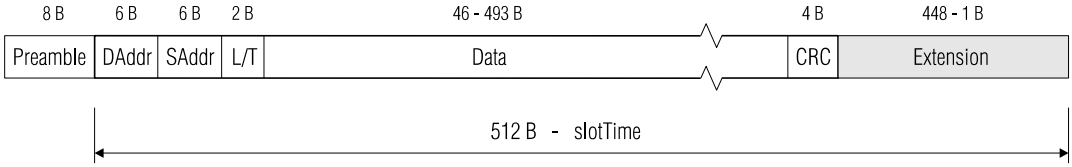
	Multimode 62.5/125 µm	Multimode 50/125 µm	Singlemode 9/125 µm	STP 150 Ω	UTP Cat.5+
1000BASE-SX	260 m	525 m			
1000BASE-LX	550 m	550 m	3000 m		
1000BASE-CX				25 m	
1000BASE-T					100 m

Obrázek 8.27:

Standard gigabitového Ethernetu zachovává ještě představu sdíleného kanálu, a i když je takové použití zcela výjimečné, vedlo k úpravě chování vysílačů média i k úpravě formátu rámců (prodloužení signálu, vysílání bloku rámců, definice Jumbo rámců).

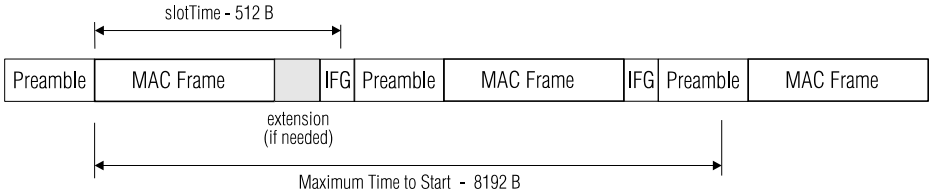
Pro správnou činnost detektoru kolize, který je využíván u poloduplexních spojů, je požadavek, aby doba vysílání nejkratšího rámce byla delší, než dvojnásobek doba potřebná k průchodu signálu mezi dvěma neodlehlejšími body spoje (včetně zpoždění aktivních prvků). To při 1 Gb/s omezuje průměr kolizní domény na cca 25 m, tedy hodnotu nižší, než jsou

vzdálenosti běžné ve strukturované kabeláži. Standard gigabitového Ethernetu se s tímto problémem vyrovnal změnou chování vysílače, který musí zůstat v provozu nejen po dobu potřebnou k odeslání rámce (nejméně 64 B a preambule), ale po dobu odpovídající odeslání 512 B a preambule (obr. 8.28). Mechanismus je označován jako *Carrier Extension*.



Obrázek 8.28:

Pouhé prodloužení doby vysílání u kratších rámců by pochopitelně vedlo ke snížení efektivity, jak výrazně se projeví u konkrétní sítě však pochopitelně závisí na poměru krátkých rámců v komunikaci. Zlepšení lze dosáhnout tím, že vysílači umožníme odeslat více sekvenci více rámců (obr. 8.29), mechanismus je označován jako *Frame Bursting*.



Obrázek 8.29:

Stanice smí zahájit vysílání dalšího rámce do vypršení časovače, který definuje nejkratší dobu vysílání (512 B po vyslání úvodní preambule). Jednotlivé rámce jsou přitom odděleny mezirámcovou mezerou *IFG/* (InterFrame Gap) o délce 96 bitů a každý rámec začíná svou vlastní preambulí. Efekt mechanismu *Frame Bursting* je pro krátké rámce velmi výrazný. Zatímco pouhé prodloužení práce vysílače vede ke snížení využití kanálu na 12 %, Při vysílání sekvencí rámců se můžeme vrátit k hodnotě 76 % dosažitelné na pomalejších sítích Ethernet (připomeňme, jde zde o vliv délky preambule a mezirámcové mezery).

I přes prodloužení doby, po kterou je vysílač aktivní, je použití poloduplexního režimu omezené na velice jednoduché sítě. Mezi stanicemi smí být nejvýše jeden opakovač, délky vedení, kterými lze připojit koncové zařízení uvádí obr. 8.30.

1000BASE-SX/LX	111 m
1000BASE-T	100 m
1000BASE-CX	25 m

Obrázek 8.30: Délky spojů pro sdílený spoj rychlého Ethernetu

Technologie gigabitového Ethernetu (kromě 1000BASE-T) kódují data pro přenos kódem 8B10B. Jde o kód převzatý, stejně jako další prvky řešení, ze standardu Fiber Channel, tento kód dovoluje úplnou eliminaci stejnosměrné složky a zaručuje dostatečné množství synchronizační informace.

1000BASE-SX

Základním přenosovým médiem gigabitového Ethernetu je vícevidové optické vlákno 50/125 μm nebo 62.5/125 μm a vlnová délka 850 nm.

1000BASE-LX

Alternativním optickým médiem gigabitového Ethernetu je optické vlákno využívané na vlnové délce 1310 nm, určitou nevýhodou je obvykle vyšší cena tohoto rozhraní.

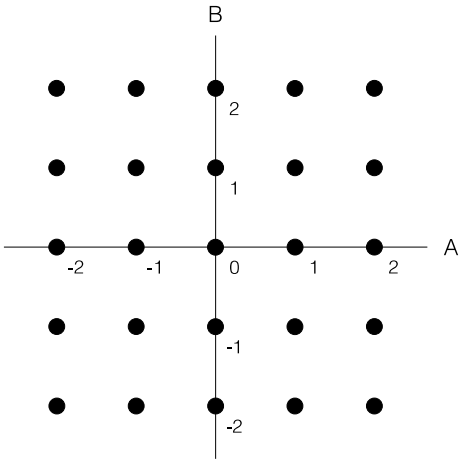
Standard 1000BASE-LX předpokládá využití vícevidových vláken 50/125 μm nebo 62.5/125 μm na vzdálenosti do 550 m. Při použití jednovidových vláken se lze bez větších problémů dostat až nad 3 km.

1000BASE-CX

Pro propojování zařízení gigabitového Ethernetu na velice krátkou vzdálenost (jednotky metrů) lze využit, ve srovnání s optikou levnějšího přenosového média, metalického vedení označovaného jako Twinax. Jde o stíněný kroucený dvoudrát obdobný kabelu STP, ale s přesněji definovanou impedancí. Stejně jako u optického signálu je signál vystupující z kódéru 8B10B vysílán kódováním NRZI (napěťová diference na straně vysílače je 1.1 - 2.0 V).

1000BASE-T

Technologie 1000BASE-T se od ostatních technologií gigabitového Ethernetu liší způsobem kódování datového signálu. Pro přenos jsou využívány všechny čtyři páry kabelu UTP/FTP v plném duplexu, data jsou kódována kódem PAM-5 (obr. 8.31) a přenášena jako pětiúrovňový napěťový signál.



Obrázek 8.31: Kódování PAM-5

Pro přenos jednoho oktetu dat potřebujeme jedinou změnu úrovně na kazdém ze čtyř párů, pro dosažení přenosové rychlosti 1000 Mb/s nám postačuje modulační rychlost 125 MBd. Dostatečné množství napěťových změn potřebné pro synchronizaci hodin přijímače a optimální detekci signálu zajišťuje scrambler a konvoluční kódér předcházející vlastnímu čtyřdimenzionálního PAM-5. Napětové úrovně signálu vysílače jsou 1 Vpp.

Šířku pásma, potřebnou pro přenos takového signálu, je schopen poskytnout běžný modernější kabel UTP/FTP. S ohledem na nutnost oddělit vlastní signál od signálu protějšku při duplexním provozu je však potřeba dodržet hodnoty doplňkových parametrů označovananých jako *Return Loss* (podíl signálu odraženého vlivem impedančních nerovnoměrností média a konektorů), *ELFEXT* (Equal Level Far-End Crosstalk - přeslech ze sousedního páru měřený na vzdáleném konci kabelu) a *PSELFEXT* (Power Sum ELFEXT - celkový přeslech z ostatních párů měřený na vzdáleném konci kabelu). Tyto parametry jsou zaručovány u moderních kabelů kategorie Cat.5 a lepších, které splňují doporučení ANSI/TIA/EIA-TSB 95 (Technical Service Bulletin). Kabeláže s takovými kabely, instalované v souladu s doporučením

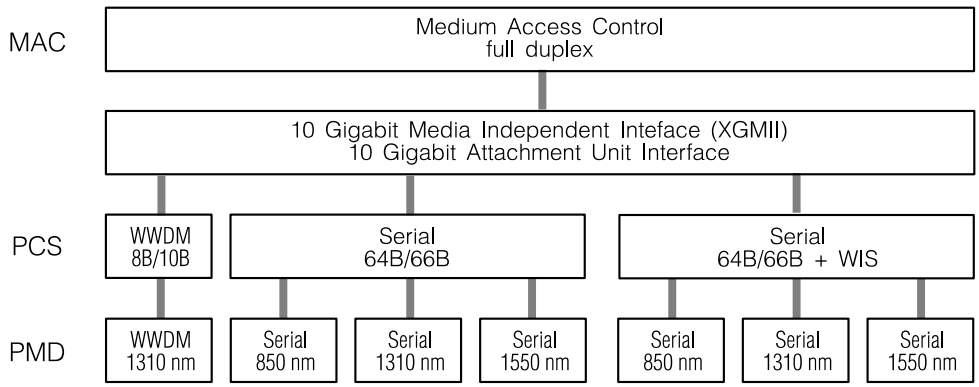
ANSI/TIA/EIA568-A nebo lépe ISO/IEC11801 (ten již s parametry Return Loss, ELFEXT a PSELFEXT pracuje) by měly provoz 1000BASE-T dovolit.

8.5 Ethernet 10 Gb/s

Modifikace technologie Ethernet na vyšší přenosové rychlosti mnohem častěji využívají plně duplexního provozu a přepojování. Jejich přenosová rychlost výrazně překračuje hodnoty potřebné většinou koncových zařízení, a spolu se schopností překlenout větší vzdálenosti (jednotky až desítky kilometrů) jsou chápány jako technologie metropolitních sítí, ale i sítí rozsáhlejších.

Typickým příkladem takového posunu je zvýšení přenosové rychlosti na 10 Gb/s, tyto sítě už jsou často využívány i jako alternativa k typickým WAN technologiím.

Standard desetigigabitového Ethernetu IEEE 802.3ae zahrnuje řadu variant využívajích různých přenosových kanálů. Na rozdíl od technologií pomalejších jde výlučně o optická vlákna a je podporován výlučně plně duplexní provoz.



Obrázek 8.32: Technologie desetigigabitového Ethernetu

Technologie gigabitového Ethernetu je použitelná jak pro velice malé sítě SAN (Storage Area Networks), tak pro klasické sítě lokální (LAN), metropolitní (MAN) a rozsáhlé (WAN). Této škále aplikací odpovídá i rozsah použitých technologií (obr. 8.32).

Desetigigabitový standard má dvě základní varianty, prvou je vlastní kódování signálu optického média, druhou je využití přenosových kanálů synchronního multiplexu SDH.

Nativní kódování pokrývá potřeby sítí SAN, LAN a MAN. Na krátké vzdálenosti sítí SAN (do 65 m) postačí použít vícevidová vlákna a vlnové pásmo 850 nm, ve vlnovém pásmu 1310 nm je dosažitelná vzdálenost 300 m. Druhou hranicí jsou vzdálenosti kolem 40 km dosažitelné s jednovidovými vlákny a vlnovou délkou 1550 nm (obr. 8.33).

	Encoding Method	Wawelength	PHY Type	Framing
10GBASE-SR	64B/66B	850 nm	serial	
10GBASE-LX4	8B/10B	1310 nm	WWDM	
10GBASE-LR	64B/66B	1310 nm	serial	
10GBASE-ER	64B/66B	1550 nm	serial	
10GBASE-SW	64B/66B	850 nm	serial	OC -192
10GBASE-LW	64B/66B	1310 nm	serial	OC -192
10GBASE-EW	64B/66B	1550 nm	serial	OC -192

Obrázek 8.33: Technologie desetigigabitového Ethernetu

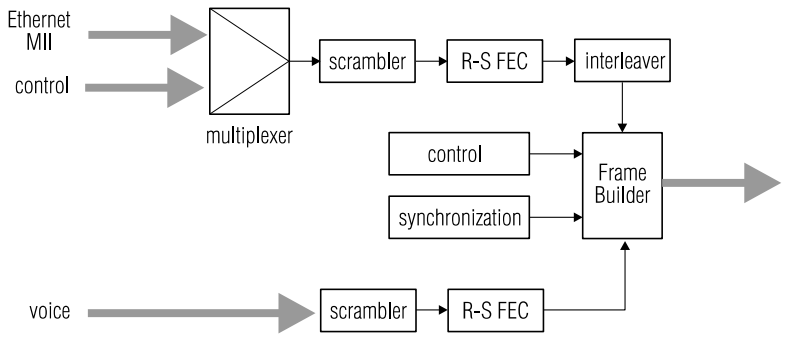
Slučitelnost technologie desetigigabitového Ethernetu s technologiemi telekomunikačních sítí SDH zajišťuje formátování rámců Ethernetu do rámců SDH. Přenosová rychlost kanálu OC-192, který může být použit pro přenos rámců desetigigabitového Ethernetu na libovolné vzdálenosti je cca 9.26 Gb/s, tedy postačující.

Spoje desetigigabitového Ethernetu dovolují budovat rozsáhlé sítě, ve spojení s technologií virtuální sítí a možností vytvářet stromy SPA algoritmu nezávisle pro jednotlivé virtuální sítě lze budovat výkonné, pružné a spolehlivé přenosové systémy schopné konkurovat přenosovým sítím SDH. Tato technologie je označována jako RPR (Resilient Packet Ring) a je vyvíjena pod označením IEEE 802.17.

8.6 Ethernet over VSDL - EFM

Zajímavou technologií, která je označována jako EFM (Ethernet fo the First Mile) nebo EoVDSL (Ethernet oer VDSL), je přenos datových rámců Ethernetu kanálem vybudovaným na běžné telefonní přípojce o délce stovek metrů, tedy na technologii VDSL. VDSL využívá kmitočtového pásma do 10 Mhz a je schopna modulací DMT (Discrete MultiTone) zajistit přenosovou rychlost až 51.84 Mb/s.

Technologie předpokládá kombinaci metalické přípojky, jejíž délka je přijatelná pro instalace v budovách, s optickým připojením aktivního rozvaděče signálu k telekomunikační ústředně optickým vláknem (podle vzdálenosti jednovidovým nebo vícevidovým).



Obrázek 8.34: Struktura vysílače systému EFM

Návrh EFM respektuje požadavek na upřednostnění real-time přenosů, například hovorových telefonních kanálů, před přenosy datovými. Přenosový kanál je proto rozdělen na dva podkanály, prvý prostřednictvím multiplexeru kombinuje přenos rámců Ethernetu a řídících

rámců, druhý zajišťuje přenos časové kritických dat. V obou kanálech jsou použity technické prvky obvyklé pro moderní vysokorychlostní sítě - scrambler "znáhodňující" přenášená dat, kódér Reed-Solomonova kódu dovolující detekovat a v určité míře (do počtu poškozených oktetů nižšího než je polovina počtu oktetů zabezpečení) i opravovat chyby při přenosu, a konečně prokládací obvod (interleaver) snižující jinak značnou citlivost korekčního kódu na shluky chyb (obr. 8.34).

Rozdělení pásma na dva podkanály se projevuje i v rozdělení prostoru v datových rámcích. Pro omezení vlivu délky rámců se v nich střídají pole určená pro přenos běžných a časově-kritických dat. Délka rámce je stanovena tak, aby odpovídala požadavku na přenos hovorových kanálů vzorkovaných frekvencí 8 kHz.

Obrázek 8.35: Využití rámce VDSL pro přenos datových a real-time dat

8.7 Pasivní optické sítě

Technologie EFM dovoluje dosáhnout přenosové rychlosti vyšší než 10 Mb/s, pro budoucí služby by však i tato rychlost mohla být nepříjemným omezením. Již i proto jsou v současné době připravovány standardy pro takzvané optické pasivní sítě.

Výhodou optických pasivních sítí (PON - Passive Optical Network) je, proti technologoii VDSL, že nepotřebují relativně náročný (a napájený) aktivní prvek na rozhraní optického vlákna a metalického vedení. Pochopitelným kritériem návrhu je minimalizace počtu vláken, kterými je propojen provozovatel připojení k telekomunikačním sítím s velkým množstvím koncových účastníků.

Z hlediska koncového účastníka výhodnější variantou je samostatné připojení. Jsou využívána jednovláknová připojení. Vlákno je využíváno v režimu širokopásmového vlnového multiplexu (vlnové délky 1300 nm a 1500 nm). Takové připojení jednovidovým optickým vláknem dovoluje be problémů dosáhnout přenosové rychlosti 100 Mb/s nebo 1 Gb/s.

I když je varianta samostatného připojení pro koncového účastníka zajímavější, její nevýhodou je vedení jednovidového vlákna ke každému zakončeni. Výhodnější možností je požití pasivního optického rozbočovače pro skupinu účastníků v malé lokalitě. Zakončení pak mohou být realizována vícevidovými vlákny, nevýhodou řešení je samozřejmě sdílení kanálu více účastníky.

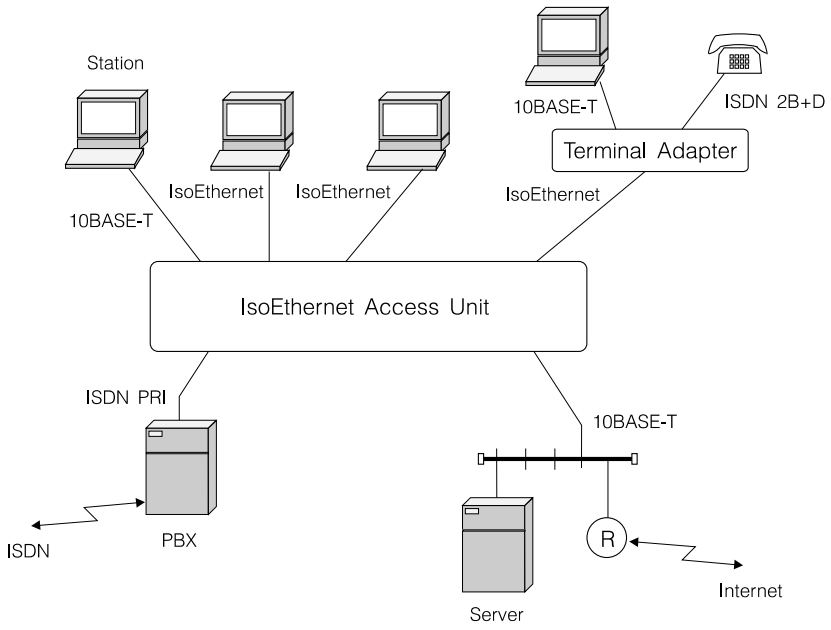
Poměrně zajímavou oblastí je způsob využití pásma poskytovaného pasivním optickým kanálem. Situace je složitější u sdílených kanálů, u kterých je potřebné zajistit řízení přístupu k dostřednému kanálu. Využívána je zde metoda obdobná technice používané u sítí využívajících distribučních sítí CATV. Jedno optické vlákno přivedené do objektu je pasivním rozbočovačem napojeno na vlákna vedoucí ke koncovým zařízením.

Pokud jde o základní formátování dat na optickém vedení, v současné době spolu soupeří tři přístupy - APON, EPON, GPON. Technologoie APON (ATM over PON) se opírá o buňky ATM, technologie EPON (Ethernet over PON) o rámce Ethernetu a konečně telekomunikační unií standardizovaná technologie GPON kombinuje synchronní přenos s přenosem dat.

8.8 Isochronní Ethernet

V mnoha případech je rychlost 10 Mb/s postačující pro připojení stanic, znesnadňuje však nebo zcela vylučuje realizaci zajímavých služeb opírajících se o přenos zvuku nebo pohyblivého obrazu. Důvodem je nemožnost definovat časový limit pro přenos a použít Ethernetu pro synchronní provoz (přidělení kapacity a vyhrazení pravidelného přístupu k médiu pro danou službu).

Zajímavou úpravou hvězdicových sítí Ethernet je způsob využití jejich kabeláže známý pod jménem *isochronní Ethernet* (Isochronous Ethernet Integrated Services – IEEE 802.9a). Opírá se o časový multiplex na médiu (podobný ISDN) na standardních kabelech UTP Cat.3. Vedle kanálu o rychlosti 10 Mb/s s přístupem odpovídajícím běžnému Ethernetu (*ISDN P Channel*) se vytváří synchronní kanál s rychlostí 6.144 Mb/s (*ISDN C Channel*). To dovolí vedle běžného provozu Ethernet (ISDN P Channel) propojit přes jednu stanici až 96 kanálů ISDN o rychlosti 64 kb/s (*ISDN B Channel*). Jeden další kanál s rychlostí 64 kb/s (*ISDN D Channel*) slouží ISDN signalizaci (podle ITU-T Q.931) a kanál o rychlosti 96 kb/s (*ISDN M Channel*) řízení a údržbě.



Obrázek 8.36: Struktura sítě postavené na isochronním Ethernetu

Isochronní Ethernet dovoluje vytvořit moderní ISDN systém (hlasová komunikace, videokonference) s využitím původní kabeláže Ethernetu (kabely UTP a optická vlákna, ne koaxiální kabely). Vyžaduje však pochopitelně náhradu původních opakovačů speciálními prvky, označovanými jako *jednotky AU* (Access Unit). Připojené stanice dovolující provoz isochronního ethernetu jsou označovány jako *stanice ISTE* (Integrated Services Terminal Equipment). K jednotkám AU lze připojit i běžné stanice a koncentrátory 10BASE-T, těm však jednotka AU zprostředkuje pouze provoz na kanálu Ethernet. Přítomnost stanic ISTE indikuje jednotka AU automaticky.

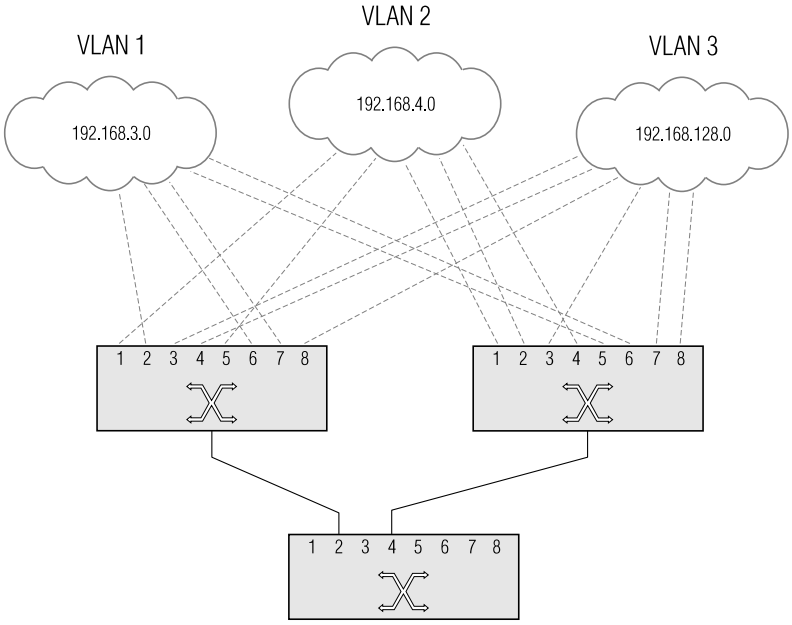
Potřebného zvýšení přenosové rychlosti je u isochronního Ethernetu dosaženo způsobem, který je běžný u moderních technologií lokálních sítí, překódováním datového signálu schématem 4B5B, náhradou čtyřbitových posloupností vybranými posloupnostmi pětibitovými, a kódováním NRZ na médiu. Takový postup kódování je podstatně úspornější než původní kód Manchester. Hodinový signál 20 MHz standardního Ethernetu je u isochronního Ethernetu zvýšen na pouhých 20.48 MHz.

9. Virtuální sítě

Princip virtuální lokální sítě (*VLAN - Virtual LAN*) je poměrně jednoduchý. Vychází z předpokladu mikrosegmentované LAN, u které jsou jednotlivá zařízení připojována přímo k přepínačům (obr. 9.1).

Virtuální síť je tvořena skupinou stanic, mezi kterými je zajištěna komunikace, mechanismus virtuální sítě zajišťuje, že data příslušející komunikaci stanic určité skupiny se nedostanou ke stanicím, které do skupiny nepatří.

Technické řešení virtuální sítě je velice jednoduché: rámce vyslané stanicí příslušející k určité skupině jsou ve vstupním přepínači označeny identifikátorem skupiny a přenášeny přepínanou sítí podobně, jako rámce neoznačené. Výstupní přepínače sítě před předáním rámce koncovému zařízení zkontrolují, zda toto zařízení přísluší ke skupině určené identifikátorem skupiny přenášeným v označeném rámci. Pokud zjistí shodu, jednoduše označení z rámce odstraní a rámec předá adresátovi. V opačném případě není rámec koncovému zařízení doručen a přepínač ho zlikviduje.

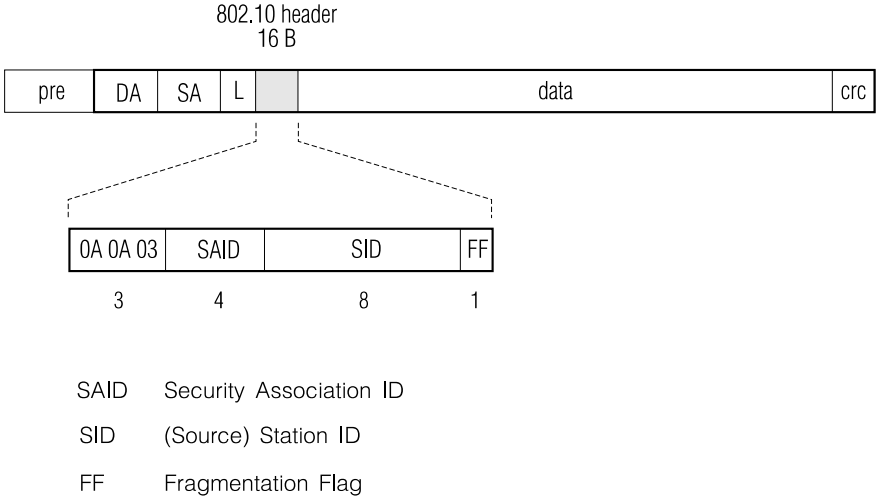


Obrázek 9.1: Struktura virtuální LAN

Mechanismus funguje jak pro dvoubodovou, tak pro vícebodovou komunikaci a broadcast. Jediným problémem, se kterým se muselo zavedení technologie virtuálních sítí vyrovnat bylo doplnění identifikátoru VLAN do struktury rámce.

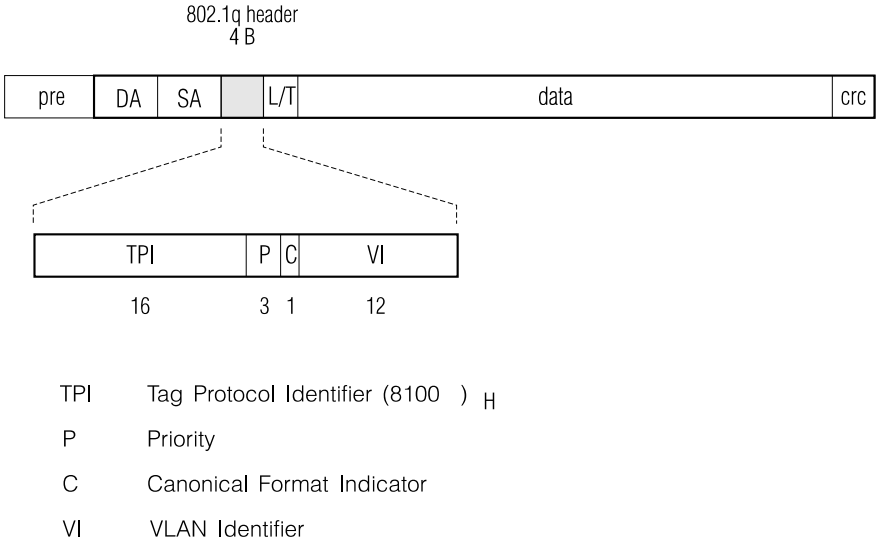
Předchůdcem v současnosti standardizované technologie virtuálních sítí, tedy technologie IEEE 802.1q, byla technologie virtuálních lokálních sítí navržená firmou Cisco pro Ethernet, Token Ring a FDDI. Tato technologie, v případě Ethernetu označovaná jako *ISL* (Inter Switch Link), se opírá o nevyužívaný standard IEEE 802.10 pro kryptografickou ochranu dat v rozsáhlých lokálních a metropolitních sítích. Formát rámce Ethernetu s identifikací virtuální sítě uvádí obr. 9.2.

Technologii IEEE 802.10 je vyhrazen identifikátor SAP (Service Access Point) 0x0A. Čtyřznakové pole SAID, původně určené pro identifikaci kryptovaného spojení, je využíváno jako identifikátor virtuální sítě. Implementace ISL v přepínačích a směrovačích firmy Cisco omezuje počet virtuálních sítí tohoto typu na 1024. Pole SID (Source Station ID) a FF (Fragmentation Flag) jsou rezervována pro funkce správy.



Obrázek 9.2: Formát rámců technologie Cisco ISL

Důležitým krokem v rozvoji virtuálních lokálních sítí bylo vytvoření standardů IEEE 802.1q a 802.1p. Oba využívají společný formát rámce, rozšíření rámce zahrnuje jednak identifikátor virtuální lokální sítě, jednak údaj o prioritě datového toku (obr. 9.3).



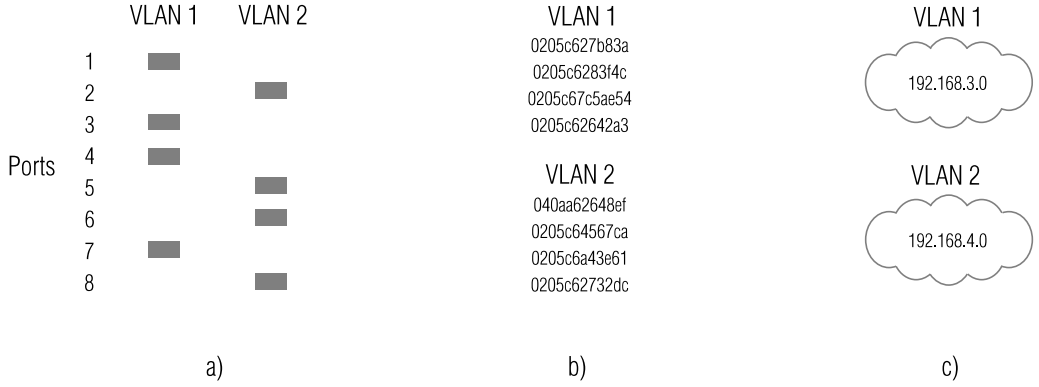
Obrázek 9.3: Formát rámců technologie IEEE 802.11p/q

Na rozdíl od ISL doporučení IEEE 802.1q vkládá doplněné pole *před* původní pole L/T. Pro identifikaci skutečnosti, že rámec je vybaven údajem podporujícím VLAN (*tag*) slouží šestnáctibitový identifikátor protokolu VLAN - TID (Tag Protocol Identifier) s hodnotou 0x8100.

Následující šestnáctibitové pole obsahuje tříbitový údaj o prioritě P, který dovoluje rozlišit osm úrovní priority. Přepínač podporující doporučení IEEE 802.1p pak upřednostňuje při zařazování do front portů rámce s vyšší prioritou, určitým druhům provozu (například hovorové služby, přenos videosignálu) tak lze zajistit potřebnou kvalitu provozu (doručení do časového limitu).

Virtuální lokální sítě jsou rozlišeny dvanáctibitovým identifikátorem VI, což dovoluje vytvořit na jedné fyzické LAN až 4096 LAN virtuálních. Příznak C (Canonical Format Identifier) je využíván u sítí Token Ring.

Rozdělení stanic do virtuálních sítí se může opírat o číslo portu, fyzickou (MAC) adresu koncové stanice, případně příslušnost koncové stanice k logické podsíti internetu (obr. 9.4).



Obrázek 9.4: Typy virtuálních sítí LAN

Prvá z metod je nejčastější, a pokud nevyžadujeme přiřazení jednoho portu do více lokálních sítí i nejjednodušší. Je vhodná v případech, kdy potřebujeme virtuální sítě oddělit i prostorově, například při vytváření komunikačního prostředí pro více společností v jedné budově.

Rozdělení stanic do virtuálních sítí podle fyzické adresy může být proti tomu užitečné pro sítě podporující mobilní koncová zařízení. Ta se pak mohou pohybovat v dosahu celé fyzické LAN, přiřazení do příslušné VLAN se však musí opírat o tabulku.

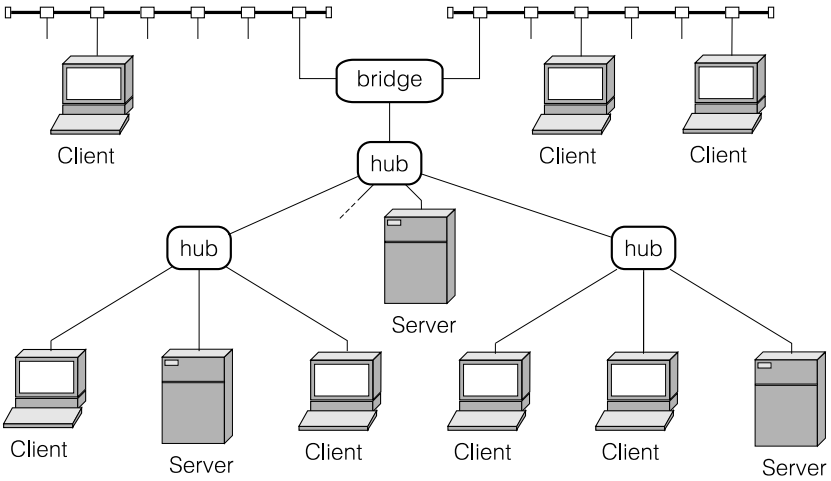
Využití informací o síťovém protokolu a informací z hlavičky paketu dovoluje například oddělit provoz pod protokoly IP a IPX nebo vytvořit na jedné fyzické LAN více logických podsítí internetu bez nutnosti definovat umístění zařízení jednotlivých podsítí.

Rozdělení jedné fyzické LAN na více lokálních sítí virtuálních dává, vedle administrativních důvodů, šanci efektivněji využívat spoje lokální sítě. Cestou k vyšší efektivitě je podpora nezávislé funkce algoritmu Spanning Tree pro každou z lokálních sítí. Takový přístup dovolí jednak využít všechny spoje fyzické sítě, jednak výpadek jednoho konkrétního spoje nemusí znamenat dočasný výpadek komunikace ve všech virtuálních LAN.

Určitým problémem je zajištění komunikace mezi virtuálními LAN. Směrovač propojující logické podsítě postavené na VLAN by bez vestavěné podpory IEEE 802.1q musel být připojen ke dvěma nebo více portům sítě. Podpora standardu IEEE 802.1q přímo ve směrovači dovoluje pracovat přímo s rámci VLAN, směrovač je pak do fyzické sítě připojen jediným rozhraním. Moderní směrovače takovou možnost podporují, častá je i kombinace přepínače se směrovačem (Layer 3 Switching).

10. VG-AnyLAN

Úspěšným pokusem o alternativní využití kabelového rozvodu UTP pro přenos dat přenosovou rychlostí 100 Mb/s je síť 100-VG AnyLAN firmy Hewlett-Packard podporovaná firmami IBM a Ungermann Bass. Přestože je často srovnávána s Ethernetem o rychlosti 100 Mb/s, nejedná se o technologii Ethernet (CSMA/CD). Jde o síť s *deterministickým přidělováním přístupu na žádost* a s podporou *prioritní komunikace*, metoda přístupu je označována jako *Demand Priority Protocol*. Je použitelná pro aplikace vyžadující dodržení časových limitů, jakými jsou aplikace v reálném čase, telekonference nebo multimédia, a pro výstavbu páteřních sítí.

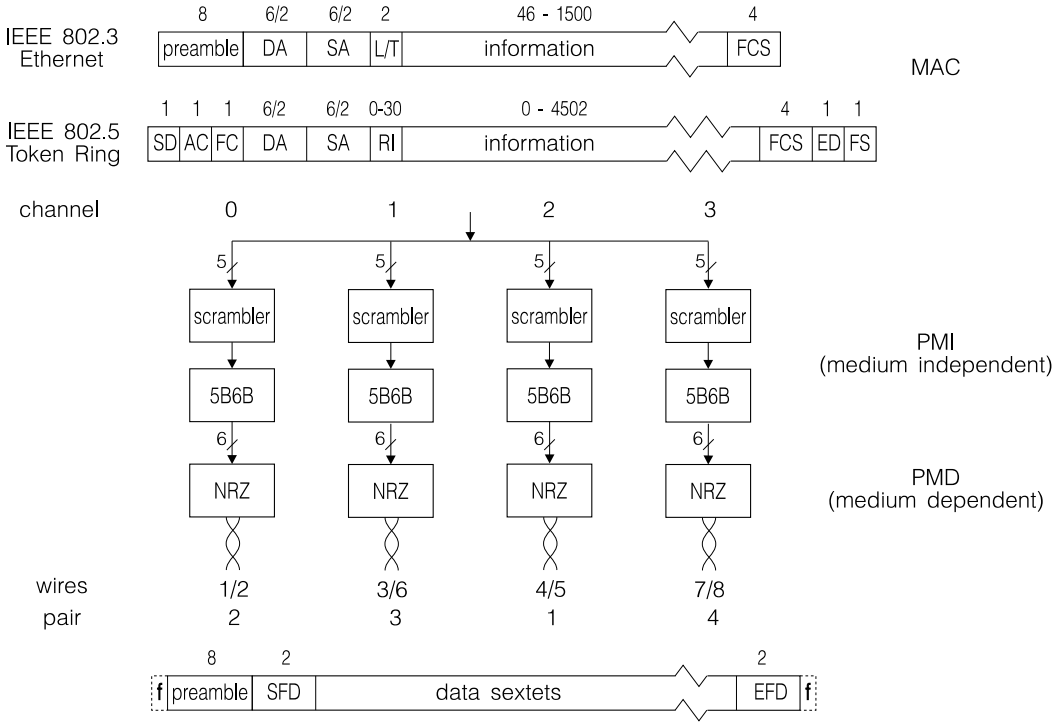


Obrázek 10.1: Struktura sítě 100VG-AnyLAN

Síť má hvězdicovou topologii (obr. 10.1), jejím základním prvkem je *víceportový řadič* (označovaný vzhledem k podobnosti síťové topologie se sítěmi 10BASE-T nebo Token Ring jako koncentrátor nebo rozbočovač, případně *Hub*). Na vstupy řadiče označené jako *Down-Link* jsou připojeny stanice, nebo další podřízené víceportové řadiče. Pro připojení k nadřízenému řadiči je víceportový řadič vybaven jedním vstupem označeným jako *Up-Link*. Řadiče lze spojovat pouze tak, že příslušný spoj propojuje vstup Up-Link jednoho řadiče se vstupem Down-Link řadiče jiného. V síti s více řadiči je tím definována hierarchie, jedinému řadiči nejvyšší, základní, úrovně jsou podřízeny řadiče nižší úrovně. Na nižších úrovních hierarchie jsou připojeny koncové stanice.

Základním přenosovým médiem je nestíněný čtyřnásobný dvoudrát o impedanci 100 Ω (kabel UTP), při použití kabelů UTP Cat.3 lze překlenout vzdálenosti do 100 m (písmena VG v názvu technologie jsou iniciálami slov Voice Grade, označujících kabel UTP Cat.3). Kvalitnější kabely UTP Cat.5 (Data Grade) dovolí prodloužit vzdálenosti mezi prvky sítě až na 150 m. Vysoké přenosové rychlosti na běžném médiu se dosahuje současným využitím všech čtyř dvoupárů pro přenos, na všech je přepínán směr přenosu. Alternativním médiem sítě 100VG-AnyLAN je dvojitý stíněný dvoudrát o impedanci 150 Ω (kabel STP), dvojitý nestíněný dvoudrát (UTP Cat.5) nebo vícevidové gradientní optické vlákno 62.5/125 μm; v těchto případech se využívají dvoudráty nebo vlákna jednosměrně.

Technologie 100VG-AnyLAN je definována specifikací IEEE 802.12. Ta popisuje metodu přístupu, tedy komunikaci stanice s víceportovým řadičem a komunikaci řadičů mezi sebou (vrstva MAC), formáty vyměňovaných datových a řídících rámců a signály na médiu (vrstva PHY). Fyzická vrstva je rozdělena na dvě podvrstvy: nezávislou na konkrétním médiu (*PMI – Physical Medium Independent Sublayer*) a závislou na konkrétním médiu (*PMD – Physical Medium Dependent Sublayer*).

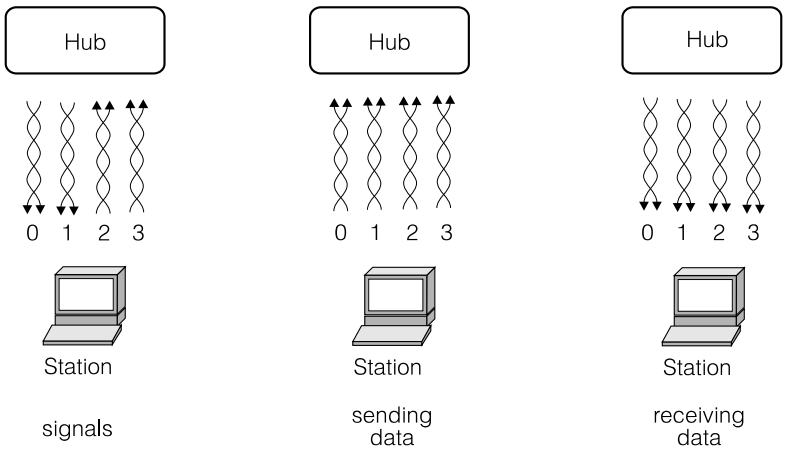


Obrázek 10.2: Kódování a struktura rámců sítě 100VG-AnyLAN

Technologie 100VG-AnyLAN se liší od jiných technologií v tom, že nedefinuje své vlastní *rámce linkové vrstvy* (adresace, zabezpečení proti chybám), ale plně přebírá buď definici rámců 802.3 (CSMA/CD) nebo 802.5 (Token Ring), pouze není možná práce s formáty obou technologií v jediné síti současně. Tyto rámce se pro přenos dělí na pětice bitů (kvintety), které se řadí do čtyř paralelních cest. V každé ze čtyř cest jsou pětice nejdříve překódovány, cílem je odstranit pravidelnosti v posloupnostech bitů (*scrambling*) a potom jsou převedeny na šestice (sextety) kódérem 5B6B a v kódu NRZ vyslány do příslušného dvoudrátu. Tento postup dovolí dosáhnout přenosové rychlosti 100 Mb/s při efektivní přenosové rychlosti 30 Mb/s v každé ze čtyř cest při zajištění dostatečného množství synchronizační informace (hran v signálu) a transparence dat (odlišení omezovačů a řídících signálů a rámců fyzické vrstvy). Je tedy podstatně efektivnější než kód Manchester běžných technologií Ethernet a Token Ring.

Vysílání posloupnosti sextetů každého *rámce linkové vrstvy* je v každém ze čtyř kanálů uvozeno 48-bitovou preambulí (osm sextetů) a 12-bitovým počátečním omezovačem *SFD* (Start Frame Delimiter), který odlišuje přenos se základní a zvýšenou prioritou. Rámec fyzické vrstvy je uzavřen 12-bitovým koncovým omezovačem *EFD* (End Frame Delimiter). Namísto koncového omezovače může být fyzický rámec ukončen příznakem neplatného rámce *IPM* (Invalid Packet Marker), ten je využíván při předčasném ukončení vysílání, nebo při zjištění chyby v přenášeném rámci. Tři výplňové bity f před preambulí fyzického rámce kanálů 2 a 3 a výplňové bity za koncovým omezovačem dovolují zlepšit zabezpečení proti chybám; samotné kódování 5B6B detekuje jednotlivé chyby v sextetech (Hammingova vzdálenost sextetů je rovna dvěma), cílem časového posunutí je omezit vliv interference do všech čtyř dvoudrátů současně. Detekci chyby

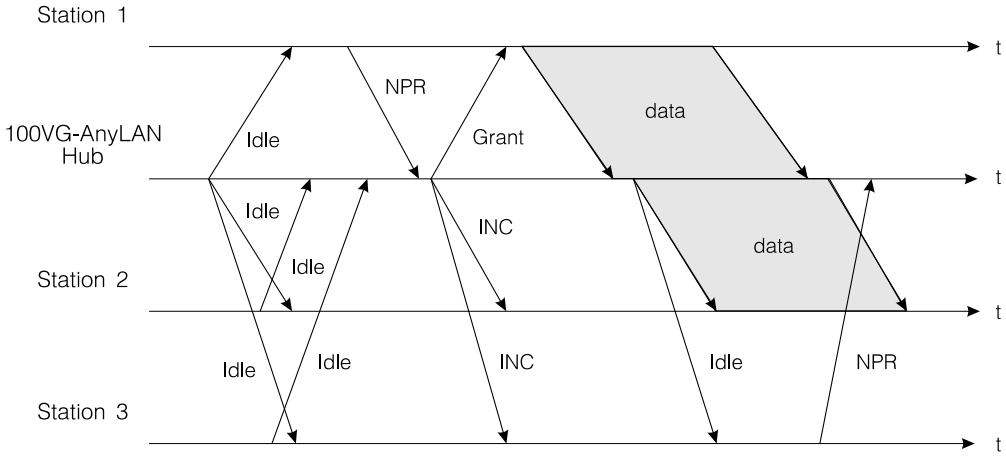
ve fyzické vrstvě pochopitelně doplňuje zabezpečení 32-bitovým cyklickým kódem v přenášených datových rámcích IEEE 802.3 nebo IEEE 802.5.



Obrázek 10.3: Využití párů kabelu UTP

Informace o stavu stanic a řadičů, žádosti stanic o přenos a souhlasy řadičů jsou předávány jako speciální signály na médiu, které se liší od přenášených dat. Jde o opakované posloupnosti šestnácti nul a šestnácti jedniček nebo osmi nul a osmi jedniček (s běžnou modulační rychlostí v kódu NRZ, standard je označuje jako *tóny*). Kanály 0 a 1 se používají pro signály vysílané nadřízeným řadičem stanici (nebo podřízenému řadiči), kanály 2 a 3 se používají pro signály ve směru opačném. Alternativní média nedávají možnost kódovat signály jako kombinace dvou základních posloupností (*tónů*) na dvou kanálech, protože takové kanály zde nemáme. Máme k dispozici jediný kanál v každém ze dvou směrů, je proto nutné použít více (pět) různých posloupností (tónů).

Stanice, která nemá rámce k odeslání (nebo řadič, který nepřijímá žádnou žádost na svých vstupech Down-Link) vysílá nadřízenému řadiči signál *Idle-Up*, nadřízený řadič naopak vysílá ke stanici (nebo k podřízenému řadiči) signál *Idle-Down*. Chce-li stanice vyslat rámec dat, požádá podle priority požadavku o přidělení média nadřízený řadič signálem *Normal Priority Request* nebo *High Priority Request*. Řadič tento požadavek zaregistruje a předá řadiči nadřízenému (pokud takový v síti existuje).



Obrázek 10.4: Předávání řízení v síti 100VG-AnyLAN

Algoritmus přidělování média je řízen řadičem v nejvyšší (základní) vrstvě. Ten, stejně jako řadiče v nižších vrstvách, vysílá v klidovém stavu stanicím a podřízeným řadičům signál

Idle-Down a v cyklu testuje požadavky na svých vstupech. Na zjištěnou žádost reaguje vysláním signálu *Grant* příslušné stanici nebo podřízenému řadiči. Při existenci více požadavků dává přednost požadavku s vyšší prioritou, požadavky se stejnou prioritou vyřizuje v cyklu (*Round-Robin*). Pro stanici je signál Grant souhlasem k odeslání rámce, smí odeslat jediný datový paket. Pro podřízený řadič je signál Grant výzvou k odstartování jednoho cyklu výběru, který je obdobou výběru na nejvyšší (základní) úrovni. Nadřízený řadič, který předal řízení řadiči podřízenému, může vyžádat omezení výběru na požadavky se zvýšenou prioritou signálem *Enable High Only*. Podřízený řadič po vyřízení požadavků (případně pouze po vyřízení požadavků se zvýšenou prioritou), včetně rekurentního předání řízení do nižších úrovní hierarchie, vrátí řízení nadřízenému řadiči. Stejně se zachová i stanice po odeslání jednoho rámce.

Prioritní vyřizování žádostí by při vysoké zátěži mohlo blokovat požadavky se základní prioritou. Pro zajištění přenosu i na základní prioritě se priorita běžných požadavků automaticky zvýšuje po uplynutí 200 až 300 ms.

Stanice, která dostane souhlas k odeslání rámce (signál Grant) začne vysílat po všech čtyřech párech. Řadič přebírá rámec, analyzuje adresu cílové stanice a rozhoduje se, na které výstupy rámec předá. Možnost filtrace toku dat zvyšuje bezpečnost sítě, požadavek stanice na předávání pouze jí adresovaných rámců, nebo informace o tom, že stanice je můstkem, si stanice vyměňuje s řadičem (a řadiče si je vyměňují mezi sebou) zvláštními *řídícími rámci* fyzické vrstvy při počáteční konfiguraci sítě. Před vysláním rámce stanicím (nebo podřízeným řadičům) nadřízený řadič požádá o uvolnění kanálů a přípravu k příjmu signálem *Incomming Data Packet*. Po odeslání rámce převede odesílající stanice kanály do stavu, kdy vysílá signál Idle-Up (případně žádost, má-li další rámec k odeslání); nadřízený řadič oznámí ukončení vysílání stanicím signálem Idle-Down.

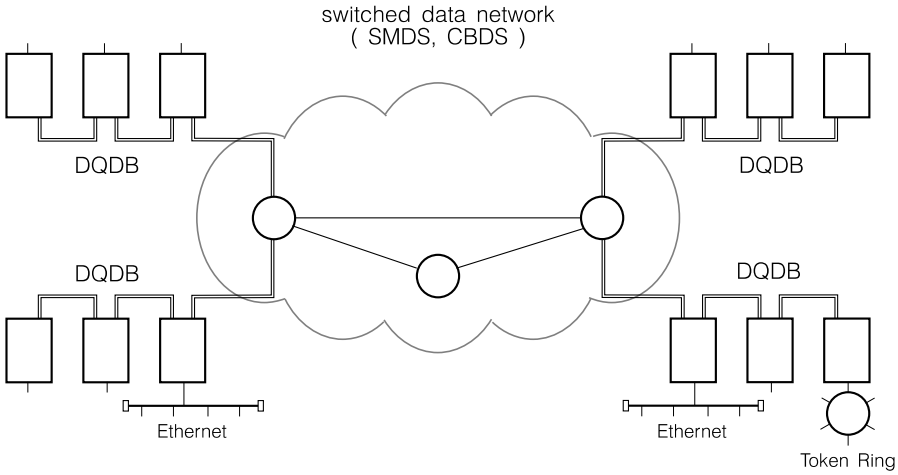
Technologie 100VG-AnyLAN se opírá o stromovou topologii kabeláže, která mohla být dříve vybudována pro síť 10BASE-T nebo pro Token Ring. Dovoluje využít původní kabely a výměna původních víceportových opakovačů nebo rozbočovačů za víceportové řadiče 100VG-AnyLAN může být proto cenově efektivní cestou k podstatnému zvýšení přenosové rychlosti sítí při zajištění podstatně vyšší kvality služby než poskytuje nedeterministický Ethernet (např. i 100BASE-TX, poznamenejme však, že v tomto okamžiku neuvažujeme přepojovaný Ethernet se schopností souběžné komunikace v několika kolizních doménách).

Síť 100VG-AnyLAN byla po krátkou dobu cenově výhodnou alternativou páteřní sítě k technologii FDDI; na rozdíl od FDDI však nedovolila zprostředkovat současný provoz IEEE 802.3 CSMA/CD i IEEE 802.5 Token Ring. Přechod od sdílení média k přepojování u Ethernetu, a s tím související zvýšení přenosové rychlosti a možnost škálovat rychlosti v topologii sítí, znamenal konec praktického využití technologie 100VG-AnyLAN.

11. Metropolitní sítě, rozhraní DQDB

Pro rozsáhlé sítě, schopné komunikačně podpořit i rozsáhlé městské aglomerace, sběrnicové a kruhové sítě nestačí. Jediným řešením je polygonální síť s vhodnou metodou sdílení vysoce rychlých synchronních dvoubodových kanálů standardizovaných v oblasti telekomunikací. Vážným problémem takových sítí je ale připojení koncových účastníků, náklady na samostatná dvoubodová připojení by byly neúnosné.

Jako vhodné řešení byly uvažovány rychlé sdílené kanály, pro připojení lokálních sítí k rozsáhlým sítím přenosovým bylo v rámci skupiny IEEE 802 navrženo velice zajímavé rozhraní označované jako DQDB (Double Queue – Double Bus). Jeho použití v metropolitní síti uvádí obr. 11.1.



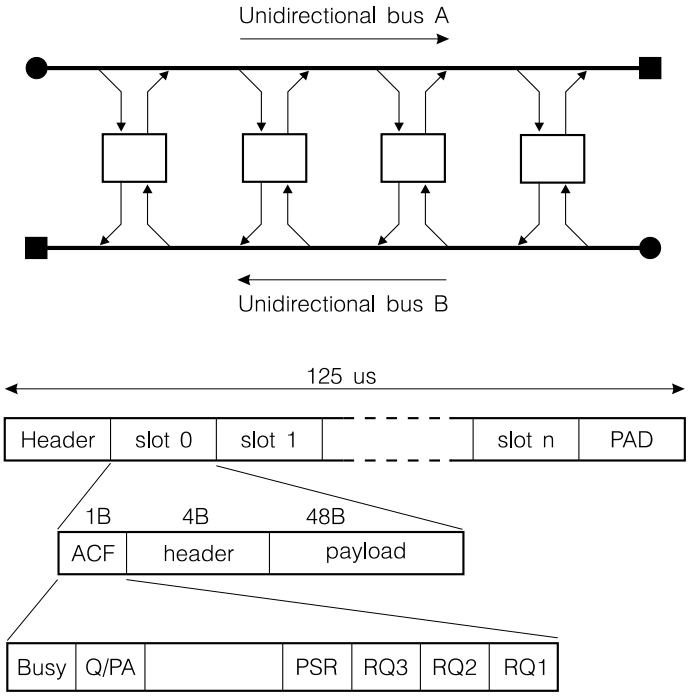
Obrázek 11.1: DQDB – Architektura metropolitní sítě s rohraním DQDB

Specifikace DQDB byla vytvořena pro australský Telecom a stala se základem standardu IEEE 802.6. Původní rozhraní DQDB bylo navrženo pro přenosovou rychlost 44.736 Mb/s (ANSI DS-3) a předpokládalo využití optických vláken. Specifikace IEEE 802.6 předpokládá použití přenosových rychlostí v rozmezí 1.544 Mb/s až 155.52 Mb/s (ale i výše) s využitím fyzických rozhraní ANSI DS-3 (44.736 Mb/s po optickém vlákně nebo koaxiálním kabelu), ANSI SONET a ITU-T SDH (155.52 Mb/s po optickém vlákně) a ITU-T G.703 (34.368 Mb a 139.264 Mb/s po metalickém vedení). Délka sběrnice může být i desítky kilometrů.

Rozhraní DQDB se opírá o dvě jednosměrné sběrnice, ke kterým jsou připojeny komunikační stanice, přenášející v opačných směrech v synchronním režimu velmi krátké datové bloky – *buňky*. Na obou koncích sběrnice jsou stanice, generující rámce časového multiplexu (obr.11.2).

Rámec časového multiplexu je odvozen od periody 125 μs. Je rozdělen na sloty (jejich počet záleží na přenosové rychlosti média, pro přenosovou rychlost 155.52 Mb/s odpovídající optickým kanálům OC-3 je počet slotů v rámci roven 44). V každém slotu je přenášena jedna buňka, která má délku 53B (což je stejná délka jako u buněk ATM). První slabika buňky je využita pro řízení přístupu stanice k rozhraní (pole ACF – Access Control Field), čtyři další slabiky tvoří hlavičku, pro přenos dat zbývá pole o délce 48B (označované jako *payload*).

Jednotlivé sloty časového rámce lze pevně vyhradit komunikaci vybraných stanic a vytvořit mezi nimi isochronní spoje (o rychlosti 3.077 Mb/s). Takové spoje lze využít např. pro propojení telefonních ústředen, distribuci TV signálu (při sdružení více slotů), apod.. Druhým, pro nás



Obrázek 11.2: DQDB – Struktura sítě DQDB a formát buňky

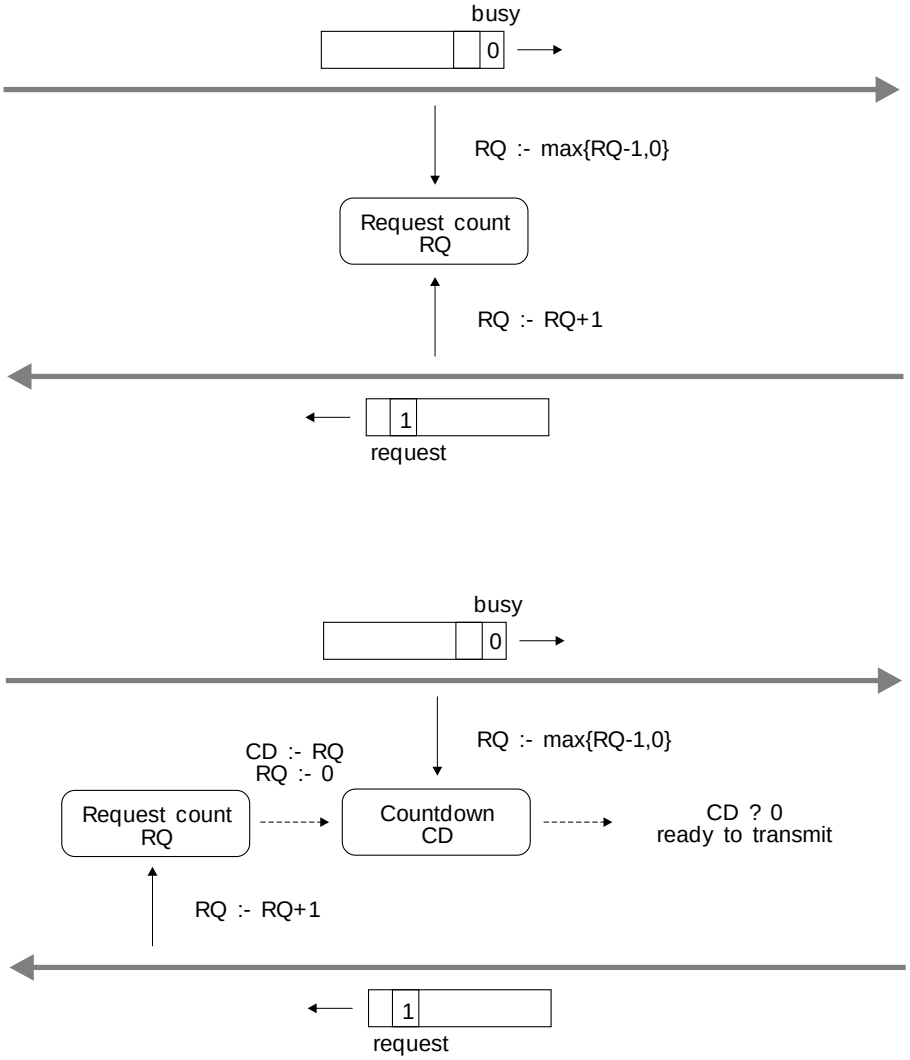
zajímavějším, režimem činnosti je přidělování jednotlivých slotů stanicím na jejich žádost. Tyto sloty jsou tedy využívány v režimu adaptivního časového multiplexu. Rozhraní DQDB poskytuje služby označované jako isochronní služba, datagram (Connectionless Data Transfer) a virtuální kanál (Connection-Oriented Data Transfer).

Pole ACF obsahuje informaci o obsazení buňky (bit Busy), o způsobu rezervace (PA/QA – Pre-Arbitrated/Queue-Arbitrated), možnosti využít již nepotřebný slot (PSR – Previous Slot Reserved) a tříbitové pole pro rezervaci slotu s jednou ze tří úrovní priority. Zbytek hlavičky dovoluje identifikovat odesílatele (prostřednictím dvacetibitové identifikace virtuálního kanálu VCI – Virtual Circuit Identifier) a zajišťuje hlavičku osmibitovým cyklickým kódem, který používá i ATM a který je schopný opravit jednobitovou chybu.

Řízení přístupu stanice k médiu je plně distribuované. Stanice, která chce vyslat buňku po vedení v jednom ze směrů, musí nejprve požádat o rezervaci volné buňky na vedení ve druhém směru. Použije k tomu libovolnou (volnou nebo obsazenou) buňku, která nemá obsazené pole požadavku s danou prioritou, a toto pole vyplní. Mechanismus uvedený dále zajistí, že po odeslání požadavku stanice získá na prvém z vedení neobsazený slot.

Algoritmus, který přidělování slotů zajišťuje, se opírá o dvojici čítačů pro každý ze dvou směrů a pro každou úroveň priority (obr.11.3). Prvý z čítačů – Request Counter (RQ) je inkrementován vždy, když stanice indikuje průchod slotu s vyplněným rezervačním polem, a dekrementován vždy, když stanice indikuje průchod neobsazeného slotu v opačném směru. Druhý čítač – Down Counter (DC) je používán při vlastní žádosti stanice o přístup ke sběrnici. Tehdy stanice vloží svůj požadavek na přenos do prvého rámce s nepoužitým rezervačním bitem a zkopíruje obsah čítače RQ do čítače DC. Od tohoto okamžiku stanice pouze inkrementuje čítač RQ (při průchodu požadavků jiných stanic) a dekrementuje čítač DC (při průchodu volných rámců pro jiné stanice) a to až do okamžiku, kdy hodnota čítače DC klesne na nulu. To je stav, ve kterém stanice může obsadit procházející volný slot svými daty. Současně se vrací do klidového režimu, kdy je dekremenentován přímo čítač RQ.

Funkce algoritmu je celkem průhledná, stanice počítá počet procházejících žádostí a dá jim přednost před žádostí vlastní. Vytváří si tedy jakousi *distribuovanou frontu*, ve které má určenu svou pozici. Tato fronta dala také rozhraní jméno.



Obrázek 11.3: DQDB – Přístupová metoda

Sběrnici DQDB je rozumné realizovat tak, že koncové stanice jsou vzájemně sdruženy a sběrnice DQDB vytváří kruh. Takové řešení dovolí rekonfigurovat sběrnici DQDB při přerušení některého spoje nebo při výpadku některé stanice, kdy stanice sousedící s přerušením sběrnice přebírají funkci stanic koncových a dvojice původních stanic koncových degeneruje ve stanici běžnou.

Struktura buňky rozhraní DQDB odpovídá struktuře buňky ATM (délka datového pole, identifikace virtuálních kanálů) a sítě DQDB lze se sítěmi ATM navzájem kombinovat, např. tak, že síť ATM vytváří komunikační infrastrukturu pro účastníky připojené na rozhraní DQDB.

12. ATM

Úzkým místem klasických lokálních sítí je limitovaná kapacita sdíleného přenosového kanálu (ať už sběrnicového nebo kruhového). Rozsáhlejší sítě jsou běžně vybavovány víceportovými mosty, přepínači a směrovači. Lokální sítě se tak stále více přibližují svou architekturou klasickým sítím s přepojováním paketů, dvoubodové spoje přepojovacích sítí jsou "pouze" nahrazovány spoji vícebodovými (segmenty, kruhy), které často degradujeme na dvoubodové spoje (jako je tomu v případě duplexního Ethernetu).

Vážným problémem lokálních sítí zůstává jejich propojování na větší vzdálenosti. Zde nezbývá, než využít co nejrychlejších analogových kanálů (pevné linky vybavené GDN modemy dovolily přenos rychlostí stovek kilobitů na kilometrové vzdálenosti, dnešní technologie, ADSL a VDSL, dovolují dosáhnout rychlostí jednotek až desítek Mb/s na stovky metrů až jednotky kilometrů telefonních přípojek) nebo lépe digitálních kanálů (základní a primární ISDN, digitální spoje E1 nebo E3). S rozvojem překryvné digitální sítě se objevila perspektiva využití přídavného asynchronního přenosu datových buněk o délce 48B dat po synchronních optických spojích telefonních systémů na prakticky neomezené vzdálenosti.

Přenosová metoda označovaná jako *asynchronní přenosový mód – ATM* (*Asynchronous Transfer Mode*) však rozhodně nebyla chápána pouze jako metoda dovolující velmi efektivní propojování lokálních sítí moderní digitální překryvnou sítí. Setkáváme se s ní i jako s metodou pro vytváření vlastních rychlých lokálních sítí s přirozeně polygonální topologií (přenosová rychlost jednotlivých linek je běžně 155 Mb/s). Příslušné specifikace definující využití buňkové technologie pro budování lokálních a privátních sítí vytvořila skupina výrobců ATM zařízení – *ATM Forum*. Základním přenosovým médiem sítí definovaných ATM Forem je optické vlákno, na malé vzdálenosti lze využít i kabeláž UTP Cat.5. Přepojovací prvky (*ATM Switches*) zajišťují směrování buněk (to je silně podporováno obvodově), datové buňky jsou předávány po virtuálních kanálech sdružovaných do virtuálních cest, vlastní přepojování je řízeno pětiznakovou hlavičkou buňky.

Lokální sítě ATM vytlačily kruhové sítě FDDI a vzhledem k jejich vlastnostem se očekávalo jejich široké využití jako páteřních sítí a sítí podporujících multimediální aplikace. V polovině devadesátých let jejich rychlost překonávaly pouze sítě *HIPPI* (High Performance Parralel Interface) a sítě *Fiber Channel*. Ty však byly vyhrazeny převážně pro propojování počítačů v multipočítačových sestavách. Pozdější rozvoj vysokorychlostních duplexních spojů Ethernetu znamenal konec představy technologie ATM jako jednotného komunikačního prostředí pro lokální i dálkové komunikace.

12.1 Synchronní provoz – STM

Technologie ATM vznikla v oblasti telekomunikací jako doplňková služba moderních rychlých synchronních přenosových systémů (*STM – Synchronous Transfer Mode*). Ty mají svůj původ v systémech PCM, ze kterých se později vyvinuly systémy ISDN.

Systémy časového multiplexu

Systémy časového multiplexu jsou založeny na využití časového multiplexu pro přenos digitalizovaného hovorového signálu. Hovorový signál je pro přenos vzorkován s periodou 125 μs, je tak získáno 8000 vzorků za sekundu. Digitalizovaný signál je doplněn o řídící informace a sdružen do rychlých kanálů časovým multiplexem. Systémy používané v Evropě se od systémů používaných v Severní Americe a Japonsku poněkud liší. V Americe a Japonsku jsou řídící

informace přenášeny jako osmý bit v jednotlivých kanálech a těch je sdruženo 24 v první úrovni multiplexu. Vzniká tak digitální signál o přenosové rychlosti 1.544 Mb/s označovaný jako T1 (nebo J1). V Evropě jsou řídící informace přenášeny v samostatných kanálech, v první úrovni multiplexu jsou k třiceti hovorovým kanálům přidány dva kanály řídící. Vzniká digitální signál o přenosové rychlosti 2.048 Mb/s označovaný jako E1. Digitální signály T1 a E1 jsou pak sdružovány ve vyšších úrovních multiplexu, přenosové rychlosti uvádí obr. 12.1.

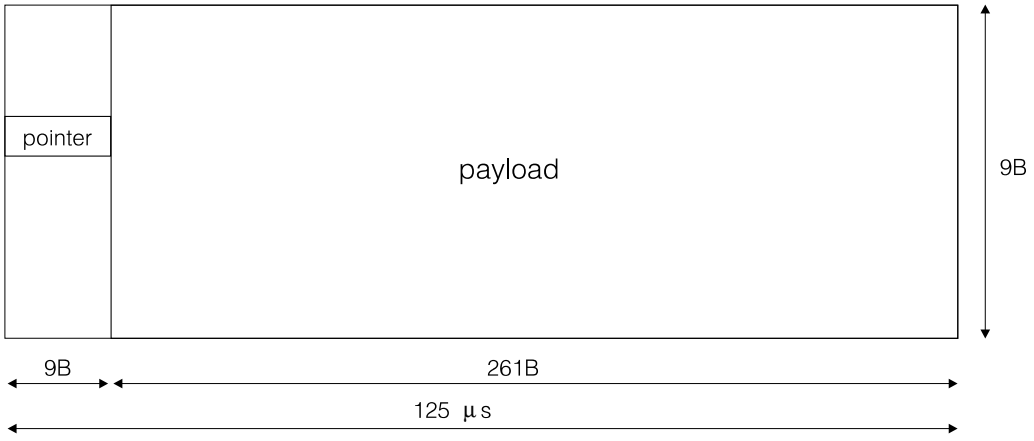
Europe	America	Japan	Number of 64 kb/s circuits	Digital Rate [Mb/s]
	T1	J1	24	1.544
E1			30	2.048
	T2	J2	96	6.312
E2			120	8.448
		J3	480	33.064
E3			480	34.368
	T3		672	44.736

Obrázek 12.1: Systémy časového multiplexu

Digitální kanály časového multiplexu byly používány po dlouhou dobu pouze uvnitř telekomunikačních systémů. Jako zvláštní telekomunikační služba byl k dispozici pronájem kanálů T1 a E1, využívaný pro propojování lokálních sítí na větší vzdálenosti. Zpřístupnění digitálních kanálů koncovému uživateli v *síti integrovaných digitálních služeb ISDN* (Integrated Service Digital Network) znamenalo důležitý mezník. Koncový účastník ISDN získává základní připojení (*Basic Rate ISDN*) dvěma duplexními kanály o rychlosti 64 kb/s (B) a jedním kanálem řídícím o rychlosti 16 kb/s (D), připojení je označováno jako 2B+D. Pro rychlejší komunikace lze využít primární připojení (*Primary Rate ISDN*) odpovídající kanálu E1 s rychlostí 2.048 Mb/s, připojení je označováno jako 30B+D (celkem 31 kanálů s rychlostí 64 kb/s, chybějících 64 kb/s spotřebovává synchronizace a správa).

Synchronní hierarchie

Data jednotlivých digitálních kanálů (a bloků nižších úrovní hierarchie – kontejnerů) jsou vkládána do rámců, které jsou konstruovány tak, aby bylo možné korigovat nutná časová posunutí mezi sousedními uzly sítě.



Obrázek 12.2: Rámec synchronní hierarchie

Přenosové rychlosti synchronních systémů (v Severní Americe *SONET – Synchronous Optical Network*, v Evropě *SDH – Synchronous Digital Hierarchy*) leží podstatně výše než u sítí časového multiplexu. Využívají převážně optických vláken (elektrických vedení pouze na krátké vzdálenosti), přehled jejich přenosových rychlostí uvádí obr. 12.3.

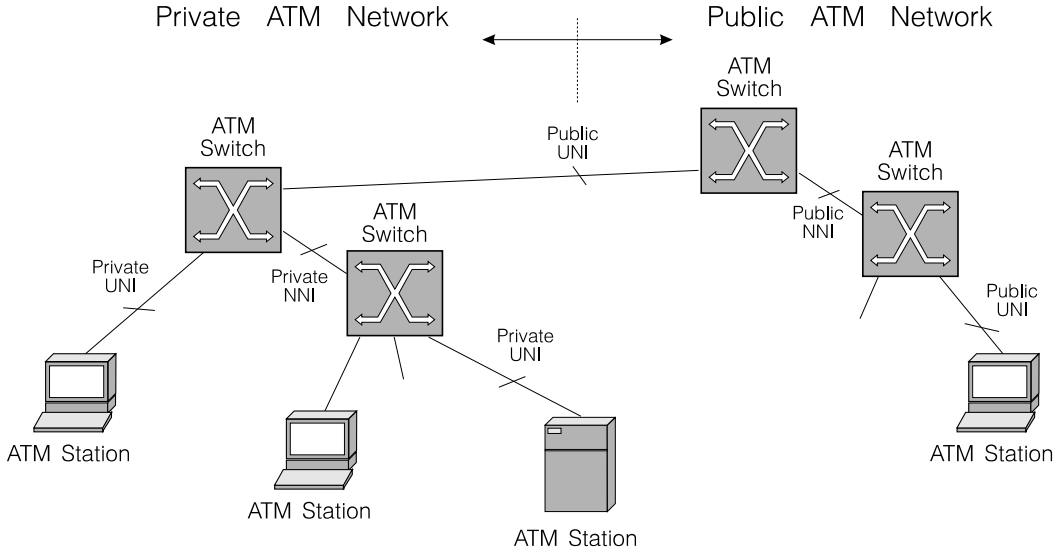
SDH STM-n	SONET STS-n	Digital Rate [Mb/s]
	STS-1	51.84
STM-1	STS-3	155.52
	STS-9	466.56
STM-4	STS-12	622.08
	STS-18	933.12
	STS-24	1244.16
	STS-36	1866.24
STM-16	STS-48	2488.32

Obrázek 12.3: Synchronní přenosové systémy

12.2 Asynchronní provoz – ATM

Rámce a kontejnery synchronních systémů jsou obsazovány přenosy synchronních hovorových kanálů. Prostor zbývající v rámcích mimo tyto staticky vyčleněné oblasti lze užitečně využít pro přenos dat – *asynchronní přenosový mód* (ATM – Asynchronous Transfer Mode).

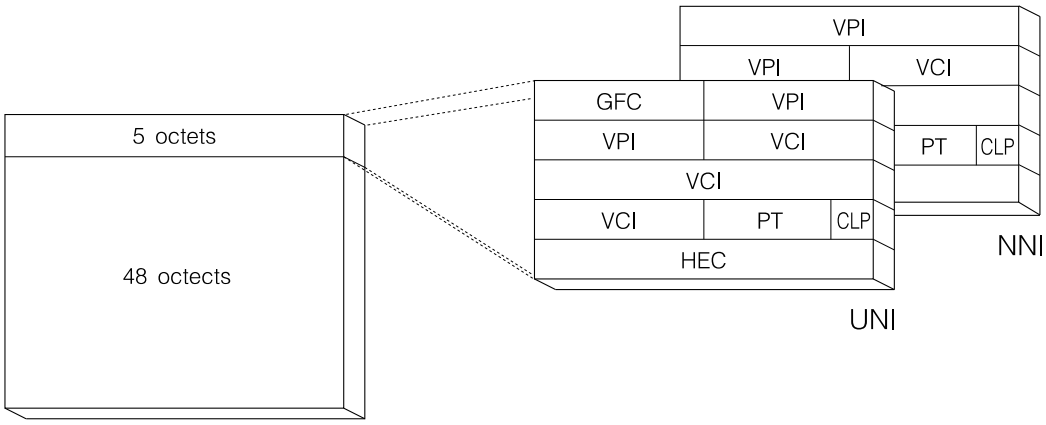
Síť ATM je tvořena přepínači ATM, mezi kterými jsou vedeny rychlé dvoubodové spoje, a na které jsou připojena koncová zařízení ATM (obr. 12.4). Struktura, funkce a chování rozsáhlých veřejných sítí je definováno materiály ITU-T, pro malé sítě privátní se o rychlé vytvoření podkladů stará skupina výrobců ATM technologie označovaná jako ATM Forum.



Obrázek 12.4: Struktura sitě ATM

Data jsou mezi koncovými zařízeními ATM předávána v krátkých *ATM buňkách* (obr. 12.5) přenášených po předem otevřených *virtuálních kanálech*. Dvoubodové virtuální kanály, které specifikují materiály ITU-T, doplňuje specifikace ATM Fora UNI 3.1 o kanály typu Point-to-Multipoint.

Každá buňka ATM má délku 53 oktetů a přenáší 48 oktetů dat. Standardizovaná délka buňky je kompromisem mezi původními návrhy, které předpokládaly délku 32 oktetů a 64 oktetů.



Obrázek 12.5: Buňka ATM

V hlavičce buňky, která má délku pět oktetů, najdeme identifikákor virtuálního spoje *VPI/VCI* (VPI – Virtual Path Identifier, VCI – Virtual Circuit Identifier), tříbitovou informaci o typu buňky *PT* (Payload Type), ta odlišuje buňky řídící od buněk datových a dovolí rozlišit i mezi různými typy řídících buněk, a jednobitový příznak *CLP* (Cell Loss Priority), který dovolí při přetížení ATM přepínačů (vyčerpání vyrovnávacích pamětí) selektivně likvidovat buňky s nižší prioritou. Hlavička buňky je chráněna osmibitovým cyklickým kódem *HEC* (Header Error Control) opírajícím se o generující polynom

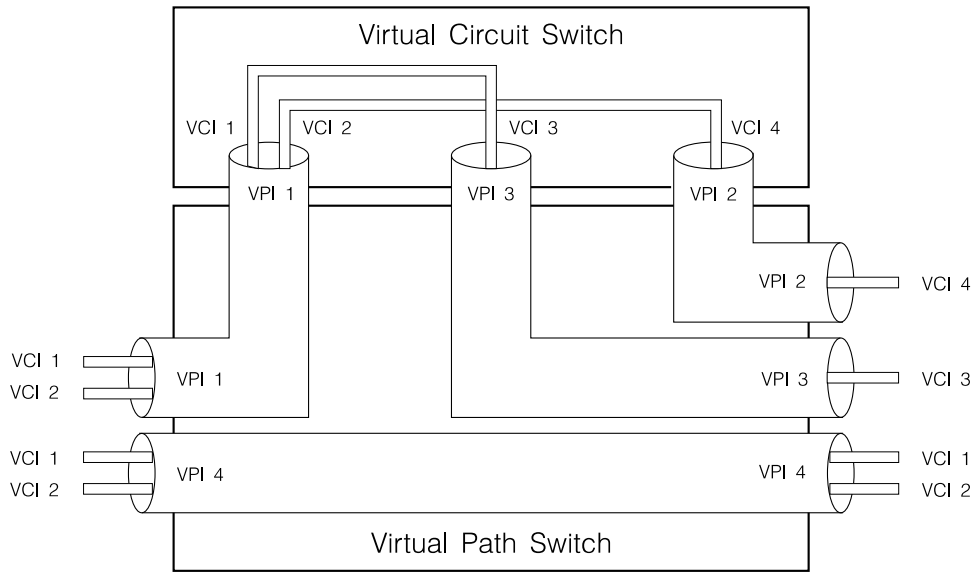
$$x^8 + x^2 + x + 1$$

a dovolujícím opravit jednobitové chyby. Respektuje se tak skutečnost, že pro optické spoje jsou typické izolované jednobitové chyby nebo relativně dlouhá narušení přenosu.

Rozhraní mezi koncovým zařízením a přepínačem ATM (*UNI – User Network Interface*) se od rozhraní mezi přepínači ATM (*NNI – Network Node Interface*) liší celkem nepodstatně – formátem záhlaví buněk. Na rozhraní UNI se objevuje pole *GFC* (Generic Flow Control) sloužící řízení toku.

Chování ATM přepínače při směrování buněk ATM definuje přepojovací tabulka. Každá položka tabulky váže identifikátor VPI/VCI na konkrétním vstupu s identifikátorem VPI/VCI na konkrétním výstupu. ATM přepínač analyzuje pole VPI/VCI přijaté buňky, přepojovací tabulka určuje po kterém rozhraní bude buňka odeslána k dalšímu ATM přepínači a jaká bude nová hodnota jejího identifikátoru VPI/VCI. Rozdělení dvanáctibitového (pro UNI), resp. šestnáctibitového identifikátoru (pro NNI), na pole VPI a VCI dovoluje zjednodušit činnost ATM přepínačů. Rozlišujeme složitější *přepojování virtuálních kanálů* (Virtual Circuit Switching), kdy je možné vystupujícím buňkám přiřadit libovolný identifikátor VPI/VCI a zjednodušené (a rychlejší) *přepojování virtuálních cest* (Virtual Path Switching), které zachovává hodnotu v poli VCI (obr. 12.6). Delší pole VPI na rozhraní mezi ATM přepínači (rozhraní NNI) prakticky odstraňuje riziko problémů spojených s využitím přepojování virtuálních cest. Na rozhraní UNI je pole VPI téměř vždy nulové.

Z hlediska způsobu vytváření virtuálních kanálů (zápisu položek do přepojovacích tabulek uzlů) rozlišujeme dva typy virtuálních kanálů – permanentní *PVC* (Permanent Virtual Circuit) a dočasně otevírané *SVC* (Switched Virtual Circuit).



Obrázek 12.6: Přepojování virtuálních kanálů a cest

Permanentní kanály PVC – Permanent Virtual Circuits

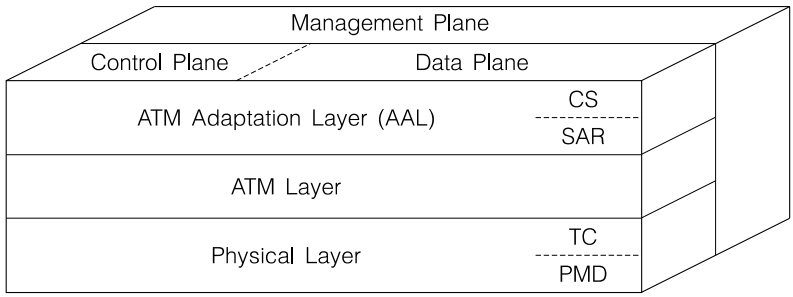
V přepojovacích tabulkách jsou položky definující virtuální kanál předdefinovány nebo nastavovány externě, typicky prostředky správy (například SNMP) a často manuálně. Permanentní spojení mají statický charakter, jejich použití se omezuje na některé vnitřní funkce sítě (signalizace, správa, virtuální spoje k serverům LANE) a na malé sítě se statickou topologií.

Dočasné kanály SVC – Switched Virtual Circuits

K nastavení položek v přepojovacích tabulkách dochází na základě žádosti koncových stanic o vybudování virtuálního kanálu. Žádost o otevření virtuálního kanálu je předávána po služebním kanále PVC s vyhrazeným identifikátorem (VPI=0,VCI=5).

12.2.1 Architektura ATM

Architektura vrstev sítí ATM se poněkud liší od architektury sítí lokálních. Pokrývá nejnižší vrstvy, ale dále je jemněji dělí. Standardy ATM vyjadřují architekturu funkcí ATM formou obrázku 12.6. Vertikální členění na vrstvy je zde doplněno o zdůraznění faktu, že každá z vrstev kromě zajištění funkce pro předávaná data má svou vlastní řídící komunikaci a funkce správy.



Obrázek 12.7: Architektura ATM

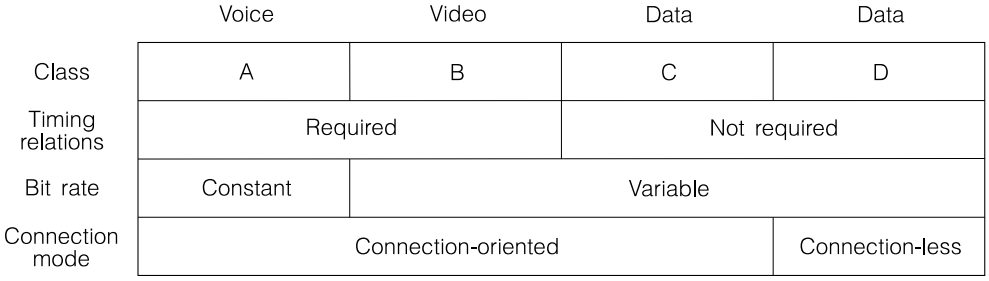
Architektura ATM dělí *fyzickou vrstvu* na část nezávislou na médiu (*Transmition Convergence Sublayer*), ta definuje strukturu buněk a využití informací v hlavičce, a na část závislou na použitém médiu (*Physical Medium Dependent Sublayer*), ta popisuje přenosové médium,

konektory, signály a kódování. Jako rozhraní mezi nimi je definován *UTOPIA Bus* (Universal Test & Operation Physical Interface).

V současných sítích ATM lze pro přenos buněk využít rychlých spojů E1 (2.048 Mb/s), E3 (34.368 Mb/s), T1 (1.544 Mb/s) a T3 (44.736 Mb/s), synchronních spojů SDH nebo SONET STM-1, OC-3, STS-3 (155.52 Mb/s), ale i spojů rychlejších. Přenos buněk ATM lze zajistit i kruhy s technologií FDDI, nebo dvoubodovými spoji optickými a metalickými.

Linkové vrstvě klasických sítí odpovídají vrstva ATM, ta definuje činnost ATM přepínače a využití pole VPI/VCI, a adaptační vrstva *AAL* (ATM Adaptation Layer). Ta se dále dělí na vrstvu *SAR* (Segmentation and Reassembly), která rozkládá rámce vyšších vrstev na buňky a opačně skládá buňky do rámců, a na vrstvu *CS* (Convergence Sublayer) zodpovědnou za zabezpečení přenosu rámců pro danou třídu provozu.

Sítě ATM byly navrženy jako podpora pro přenos zvukové, obrazové a datové komunikace. Požadavky, které klade přenos zvuku a obrazu, se od požadavků kladených na přenos dat podstatně liší, technologie ATM proto rozlišuje čtyři třídy přenosů A, B, C a D (obr. 12.8) a jednotlivé třídy charakterizuje nutností dodržet přenosovou rychlost, časové relace (rozptyl zpoždění buněk) a zajistit potvrzování.



Obrázek 12.8: Třídy provozu ATM

Požadavky na kvalitu služeb *QoS* (Quality of Service), které odpovídají jedné ze tříd přenosu, zadávají koncová zařízení při otevírání spojení. Třídám přenosu odpovídají o něco přesněji definované kategorie, pro každou kategorii je definován určitý soubor parametrů zadávaných při otevírání virtuálního kanálu.

CBR – Constant Bit Rate

Je požadována konstantní přenosová rychlost, limitované zpoždění buněk a rozptyl zpoždění a případně i limit buněk ztracených při přenosu. Kategorie CBR definuje nejpřísnější požadavky na virtuální kanál ATM, vyžaduje zcela pravidelné doručování ATM buněk a je využívána pro přenos hovorového signálu, videosignálu a pro emulaci digitálních kanálů jako jsou T1 a E1.

VBR – Variable Bit Rate

Je požadována přenosová rychlost v určitém rozmezí, limitované střední zpoždění buněk a případně i limit buněk ztracených při přenosu. Kategorie VBR je vhodná pro přenos komprimovaného hlasového a obrazového signálu. Podle tolerance na překročení limitního zpoždění rozlišujeme mezi kategorií *VBR/RT* (Real Time) (používá se například pro přenos komprimovaného videosignálu) a *VBR/NRT* (Non Real Time) (používá se například pro vytvoření kanálu pro přenos rámců Frame Relay).

ABR – Available Bit Rate

Je požadováno maximální možné využití přenosové rychlosti v daném rozmezí při omezeném počtu ztracených buněk, ale bez požadavku na dodání do nějakého časového limitu. Tento režim provozu je závislý na spolehlivém řízení toku a je považován za ideální pro propojování a výstavbu lokálních sítí.

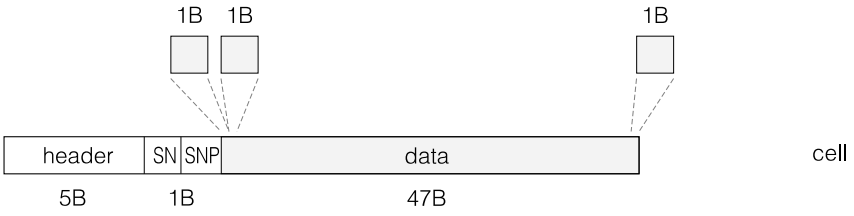
UBR – Unspecified Bit Rate

Jde o obdobu ABR, ale nezaručuje dodání přenášených dat, která mohou být v přetížených uzlech sítě likvidována. Dnes se jedná o provoz běžně podporující propojování a budování lokálních sítí.

Součástí specifikace ATM je definování zobrazení datových bloků sloužících aplikaci na buňky ATM. Takovou transformaci zajišťuje vrstva označovaná jako vrstva adaptační, různé třídy a kategorie provozu podporují odlišné adaptační vrstvy označované jako AAL1 až AAL5.

Adaptační vrstva AAL1

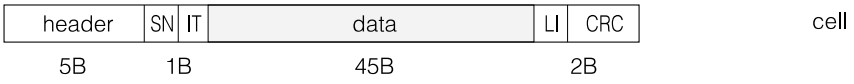
Slouží k uložení toku oktetů provozu CBR (produkovaných např. převodníkem hlasového signálu) do buněk ATM. Adaptační vrstva AAL1 nepodporuje ochranu proti chybám, pouze dovoluje detekovat ztracené buňky. Buňky jsou číslovány čtyřbitovým polem SN (Sequence Number), zabezpečeným proti chybám čtyřbitovým polem SNP (Sequence Number Protection). Pro data je v buňce k dispozici 47 oktetů.



Obrázek 12.9: Adaptační vrstva AAL1

Adaptační vrstva AAL2

Slouží k přenosu bloků dat odpovídajících provozu VBR (např. komprimovaný videosignál). Buňky jsou číslované ve čtyřbitovém poli SN (Sequence Number), počáteční a koncová buňka aplikačního rámce je identifikována ve čtyřbitovém poli IT (Information Type). Každá buňka obsahuje šestibitovou informaci o délce přenášených dat LI (Length Indicator) a je zajištěna desetibitovým cyklickým kódem CRC. Pro data je v buňce k dispozici 45 oktetů.

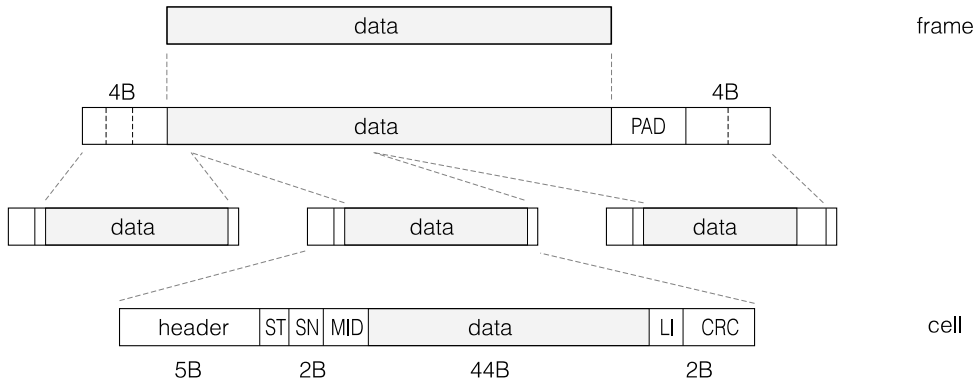


Obrázek 12.10: Buňka AAL2

Adaptační vrstva AAL3/4

Adaptační vrstva AAL3 podporuje přenos dat (provoz ABR a UBR) virtuálním kanálem vyšší vrstvy, vrstva AAL4 podporuje přenos datagramů. Dvoubitové pole ST (Segment Type) dovoluje rozlišit úvodní a koncové buňky aplikačního rámce od buněk vnitřních a od buněk, které pojmou rámec celý. Buňky jsou číslovány čtyřbitovým polem SN (Sequence Number).

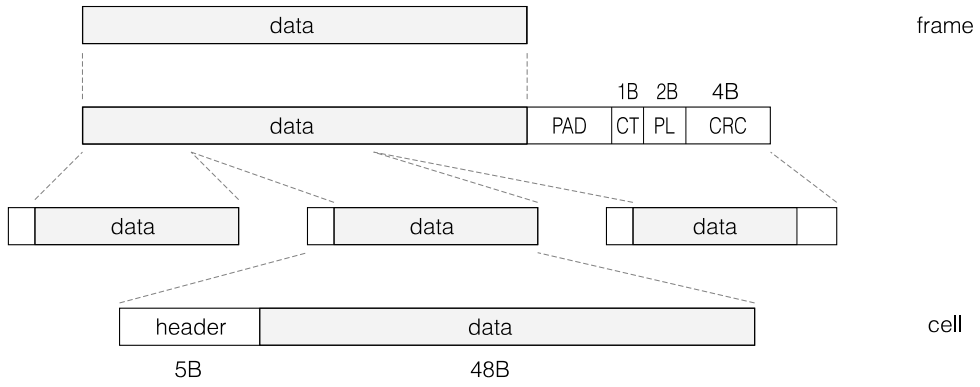
Každá buňka obsahuje šestibitovou informaci o délce přenášených dat LI (Length Indicator) a je zajištěna desetibitovým cyklickým kódem CRC. Desetibitové pole MID (Multiplexing Identification) dovoluje současný přenos více aplikačních rámců po jediném virtuálním kanále ATM. Pro data je v buňce k dispozici 44 oktetů, rámce vyšší vrstvy jsou před rozkladem na buňky doplněny o čtyřznakové záhlaví, čtyřznakové zakončení a výplň, která je doplní na celistvý počet buněk.



Obrázek 12.11: Adaptační vrstva AAL3/4

Adaptační vrstva AAL5

Adaptační vrstva AAL5 byla navržena jako efektivnější varianta k vrstvě AAL3/4 a je využívána pro přenos dat lokálních sítí. Nedovoluje však multiplex podobný provozu AAL3/4. Uživatelské rámce dat jsou doplněny o výplňové znaky tak, aby po doplnění o řídící pole, o údaj o délce bloku dat a o cyklický kód zajišťující data proti chybám vzniklým poškozením nebo ztrátou buněk, byly rozdělitelné do celistvého počtu buněk (využita je plná délka datového pole 48B). Informace potřebná pro zpětné skládání buňek je uložena v posledním bitu pole PTI hlavičky buňky.



Obrázek 12.12: Adaptační vrstva AAL5

12.2.2 Adresace a signalizace (navazování spojení)

Asynchronní provoz byl navržen v rámci telekomunikačních standardů ITU-T jako doplnění synchronních hierarchií a podpora sítí ISDN. Je proto přirozené, že se navazování spojení, otevírání kanálů pro asynchronní provoz, opírá o adresaci koncových zařízení telekomunikačních systémů. Vychází z protokolů ITU-T Q.2931 (signalizace ve veřejných sítích) a ITU-T Q.931 (signalizace v sítích ISDN) a opírá se o adresaci definovanou doporučením ITU-T E.164 pro veřejné telefonní sítě a veřejné širokopásmové sítě ISDN. Koncové zařízení žádá o vytvoření

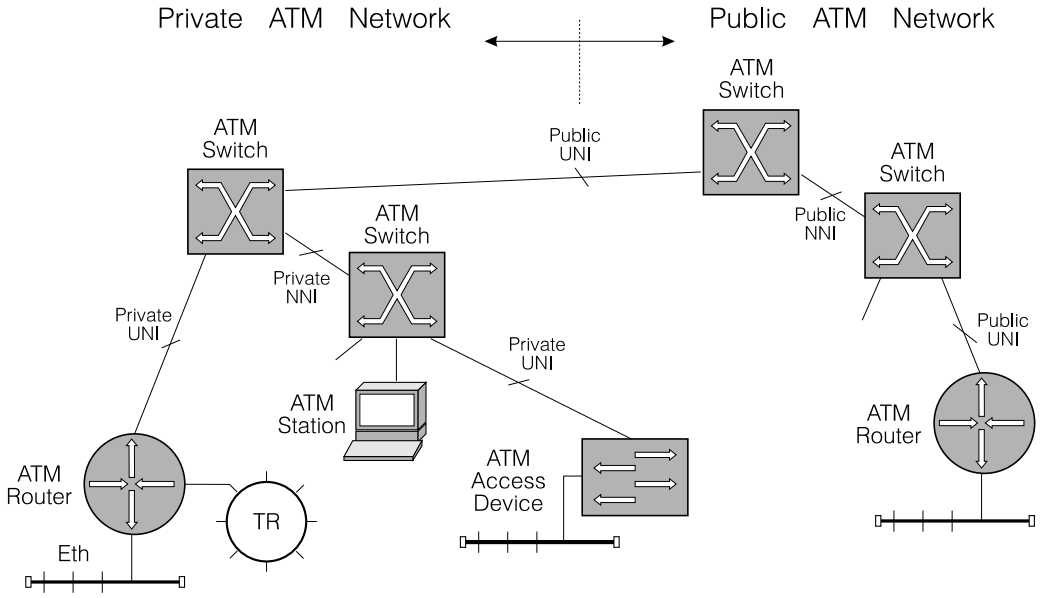
virtuálního kanálu odesláním žádosti Setup (obsahuje adresu cílové stanice a požadavky na parametry kanálu) po služebním kanálu (VPI=0,VCI=5) a obdrží od prvého ATM přepínače potvrzení Call Proceeding. Žádost Setup je mezitím předávána ATM přepínači sítě k cílové stanici a současně je budován virtuální kanál.

Cílová stanice může žádost přijmout nebo odmítnout. Odmítnutí signalizuje paketem Release, který při cestě ke stanici, která o navázání spojení požádala, uvolňuje přidělené zdroje (VPI/VCI identifikátory a případně paměti). O rozpojení virtuálního kanálu může požádat v průběhu navazování spojení i později nejen koncová stanice, ale i kterýkoliv ATM přepínač.

12.3 Lokální sítě ATM

Standardní technologie ATM poskytuje dvoubodové permanentní (PVC) nebo přepojované (SVC) virtuální kanály. Běžně se opírá o velmi rychlé komunikační kanály (OC3 – 155 Mbps) a díky polygonální topologii není tato rychlost limitem průchodnosti sítě jako celku. (Klasický i přepojovaný Ethernet se proti tomu musí omezit na stromové topologie, Token Ring používá poměrně komplikované zdrojové MAC směrování při propojování sítí mosty). Je tedy celkem přirozené, že byly hledány cesty k využití ATM v lokálních sítích. Přenos buněk ATM je navíc podporován rozsáhlými synchronními sítěmi (STM, SONET), technologie ATM dovoluje transparentní propojení lokálních sítí ATM i na velké vzdálenosti.

Přirozeným využitím sítě ATM je její přímé využití jako síťové vrstvy s tím, že jsou nad ní přímo vystavěny aplikace, nebo že je překryta vrstvou internetu. V prvém případě jsou přímo k dispozici možnosti, které poskytuje volba parametrů QoS, ve druhém případě je přístup k parametrům QoS zprostředkován moderními protokoly internetu jako jsou *RSVP* (Resource Reservation Protocol) a *RTP* (Real-Time Transport Protocol). Takové využití většinou označujeme jako *lokální síť ATM* (Native Mode ATM LAN) a stanice sítě musí být vybaveny rozhraními ATM.

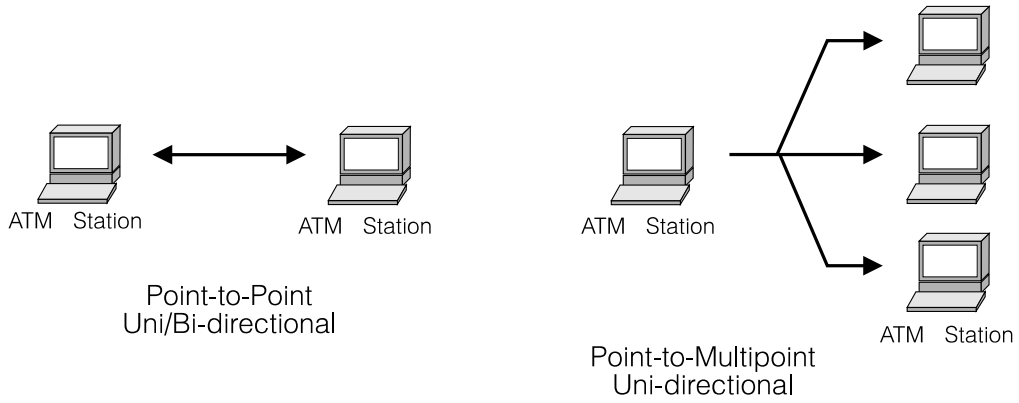


Obrázek 12.13: Struktura sítě ATM s emulací LAN

Podstatně častěji než s lokálními sítěmi ATM (v čisté formě) se setkáme se sítěmi, které kombinují ATM s klasickými technologiemi Ethernetu nebo Token Ringu. Takovou síť tvoří ATM přepínače propojené dvoubodovými spoji do polygonální sítě. K síti jsou připojeny koncové stanice (obr. 12.13), těmi mohou být buď počítače vybavené rozhraním ATM nebo

prvky označované jako *ATM mosty* (LAN Access Devices). Ty dovolují připojovat celé klasické lokální sítě (Ethernet, Token Ring), svou funkcí připomínají mosty lokální sítě a jsou využívány tam, kde potřebujeme propojit lokální sítě páteří s vysokou průchodností a/nebo překonat větší vzdálenost. Pro přímo připojené stanice může technologie ATM vytvářet lokální síť založenou přímo na přenosu buněk ATM, častěji však modeluje spoje, přenášející rámce Ethernetu nebo Token Ringu, mluvíme *o emulaci sítě LAN* (LANE – LAN Emulation).

Síť ATM podporuje dvě základní komunikační schémata: dvoubodové (*Point-to-Point*) a vícebodové (*Point-to-Multipoint*) kanály (obr. 12.14). Zatímco dvoubodové kanály mohou být jednosměrné i obousměrné, vícebodové kanály jsou pouze jednosměrné a anglický termín vyjadřuje fakt, že se jedná o kanály schopné distribuovat buňky jediného vysílače k více přijímačům. Potřebnou replikaci ATM buněk zajišťují ATM přepínače (ale mohou ji provádět i koncové stanice). Obousměrné vícebodové kanály (anglicky označované jako *Multipoint-to-Multipoint*) lze sice na ATM síti také v principu vytvářet, museli bychom se však omezit na provoz AAL3/4, u kterého by bylo možné identifikovat odesílatele buňky (buňky různých odesílatelů je nutné na straně příjemce roztřídit). Standardně využívaný provoz AAL5 podobnou identifikaci neumožňuje, odesílatelem může být jediná stanice na spoji.



Obrázek 12.14: Typy ATM kanálů

Vícebodová komunikace odpovídající schématu Multipoint-to-Multipoint je však potřebná pro realizaci řady funkcí v lokálních sítích, v síti ATM je realizovatelná následujícími způsoby (obr. 12.15):

Virtual Path Multicasting

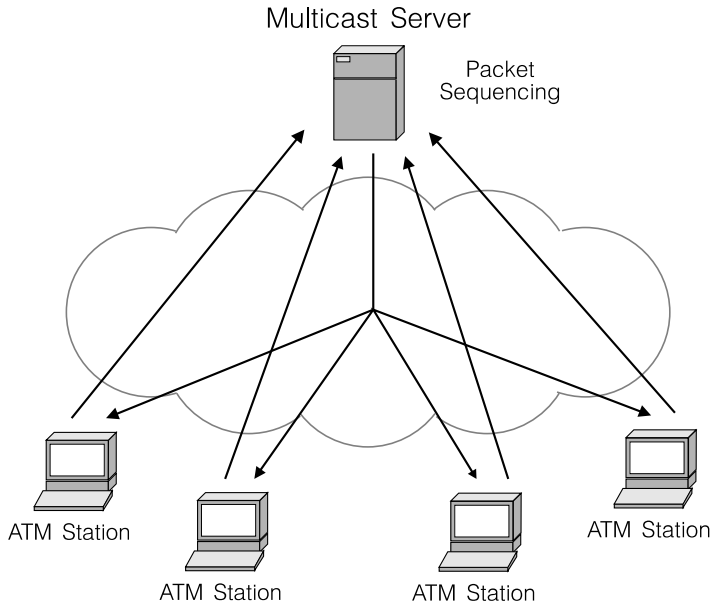
Vícebodový kanál používá vyhrazený identifikátor VPI, identifikátor VCI identifikuje stanice. Jedná se o teoretickou možnost s ještě většími omezeními než má Multipoint-to-Multipoint komunikace u provozů AAL3/4, technika není podporována.

Multicast Server

Koncová stanice odesílá datový rámec vyhrazenému serveru (Multicast Server – obr. 12.15) po dvoubodovém kanále. Ten jednotlivé rámce, po jejich složení z ATM buněk, rozešle po vícebodovém kanále (typu Point-to-Multipoint) případně po samostatných dvoubodových kanálech.

Overlaid Point-to-Multipoint Connections

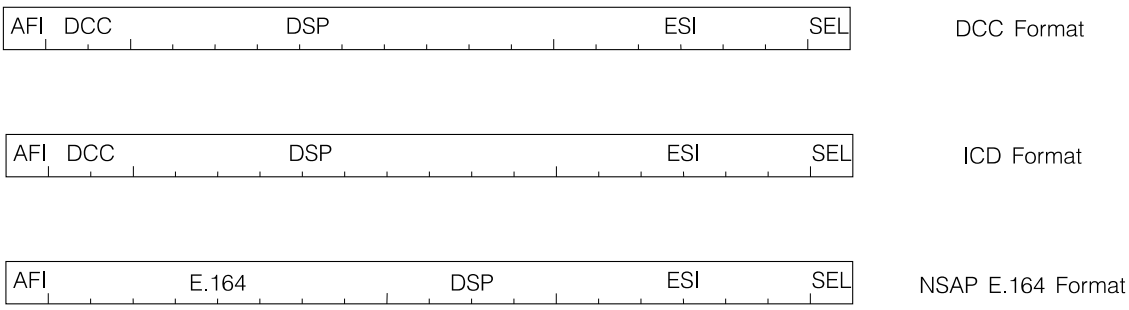
Vícebodový kanál typu Multipoint-to-Multipoint je modelován skupinou kanálů typu Point-to-Multipoint. Každá z koncových stanic modelovaného kanálu si vytváří vlastní vícebodový kanál pro distribuci, přidání stanice vede na složitý proces rekonfigurace distribučních kanálů ostatních stanic.



Obrázek 12.15: Realizace vícebodového kanálu Multipoint-to-Multipoint

12.3.1 Adresace a směrování

Adresace v privátních sítích ATM vychází z materiálů ITU-T (E.164 pro veřejné sítě) a ISO (ISO 3166 a ISO 6523). Pole adresy je dvacetislabičné, strukturu adresy uvádí obr. 12.16.



Obrázek 12.16: Adresy v privátních sítích

Za zmínku stojí struktura všech tří formátů adresy ATM přepínačů, ATM mostů (LAN Access Device) a koncových stanic. Jsou složené z identifikace formátu, identifikace domény nejvyšší úrovně (DCC – Data Country Code, ICD – International Code Designator, adresa E.164) následované adresou ATM stanice (ATM mostu). Koncové stanice lokální sítě připojené k ATM mostu jsou rozlišené 48-bitovou MAC adresou (podle IEEE 802.2), jednoznakové pole SEL slouží k multiplexu v rámci koncové stanice (více ATM rozhraní pro ATM zařízení). Uvedený formát adresy dovoluje registraci stanic lokální sítě protokolem ILMI (Interim Local Management Interface), pro který je vyhrazen permanentní virtuální kanál (VPI=0, VCI=16).

Směrování ve veřejných sítích ATM se opírá o signalizaci ITU-T B-ISUP a směrovací protokol ITU-T MTP Level 3. Pro privátní sítě byl ATM Forem definován směrovací protokol P-NNI (Private Network-to-Network Interface).

P-NNI Phase 1

Směrovací protokol ATM Fora *P-NNI Phase 1* si klade za úkol respektovat řadu parametrů QoS a přizpůsobit budování virtuálních spojů požadavkům na parametry spojení a stavu ATM sítě. Správa potřebných informací je proto nutně složitější než u protokolů opírajících se o optimalizaci jediného parametru (zpoždění, počet kroků) jako jsou RIP nebo OSPF.

Trasu virtuálního spoje navrhuje hraniční ATM přepínač po příjmu požadavku na navázání spojení na základě známé topologie (podobně jako u protokolu OSPF) a parametrů jednotlivých spojů. Možné kolize, ke kterým může při vlastním otevírání spoje dojít, jsou řešeny lokálně v rámci skupin sousedících ATM přepínačů.

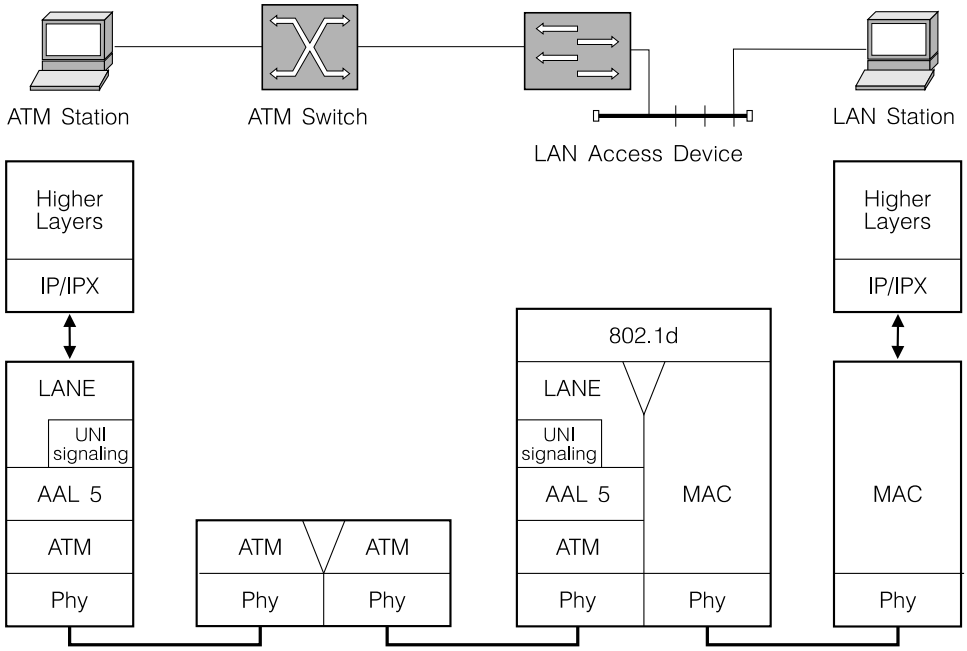
P-NNI Phase 0 (IISP – Interim Inter-Switch Signaling Protocol)

Neboť definice směrovacího protokolu P-NNI Phase 1 byla velmi zdlouhavá, byl pro malé privátní ATM sítě vytvořen zjednodušený směrovací protokol označovaný jako *P-NNI Phase 0* nebo *IISP* (Interim Inter-Switch Signaling Protocol), který vychází ze statického popisu ATM sítě.

Činnost ATM přepínače definovaná protokolem IISP je velmi jednoduchá a vychází z hierarchického rozdělení adresního prostoru. Adresa v žádosti o otevření virtuálního kanálu je porovnávána s tabulkou prefixů, která je pro ATM přepínač ručně nakonfigurována. Je vybrán nejdelší prefix, který se shoduje s nejvyššími bity cílové adresy. Virtuální spoj je pak protažen k prefixu odpovídajícímu sousedovi. Tomu je odeslána žádost Setup, a pokud nedojdeme k cílové stanici, postup se opakuje.

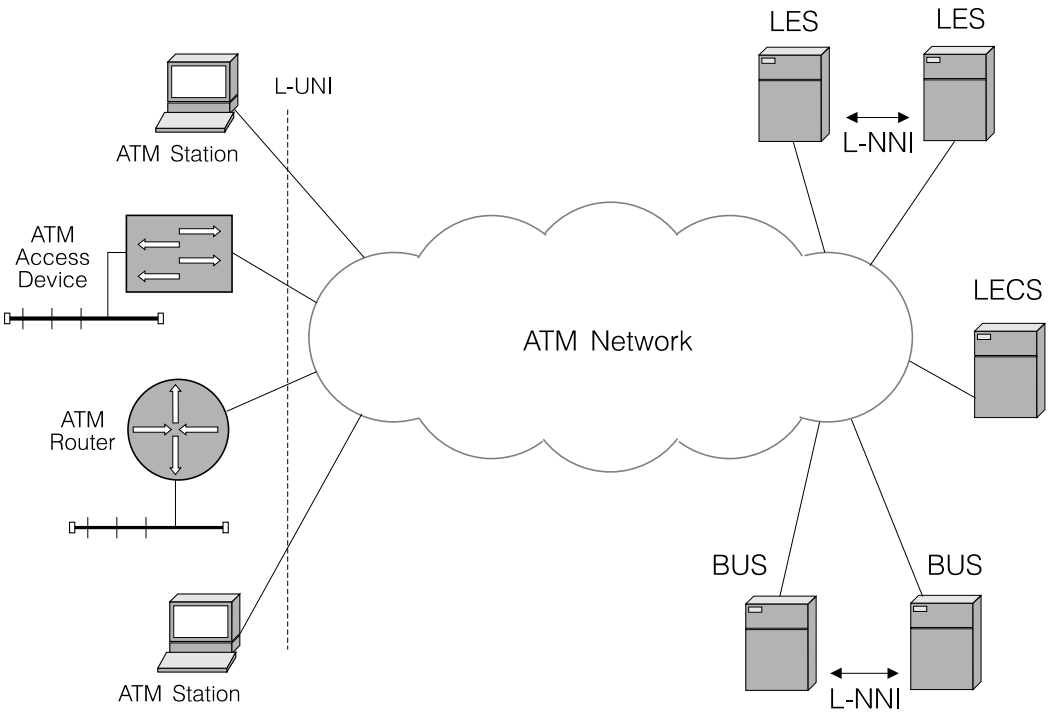
12.4 Emulace LAN

Plná náhrada technologií sdíleného kanálu pro lokální komunikaci plně přepojovanou sítí ATM nebyla reálná. Zajímavé je ale využití sítě ATM pro přenos rámců odpovídajících standardům běžných lokálních sítí (tedy Ethernetu).



Obrázek 12.17: Architektura lokální sítě s emulací LAN

Použití ATM jako přenosového prostředí pro rámce jiných lokálních sítí vyžaduje doplnit podporu komunikačních technik, které sítě LAN využívají. Jde o skupinovou komunikaci a broadcast, které nejsou technologií ATM přímo podporovány, a o adresaci stanic, která je vlastní každé technologii LAN a odlišná od adresace ATM (např. síť Ethernet používá adresaci podle IEEE 802.3 o délce 48 bitů, adresa ATM podle ISI NSAP (Network Service Access Point) má délku 20 slabik). Využít síť ATM pro výstavbu lokálních sítí vyžaduje namodelování odpovídajících mechanismů. Lokální síť modelovanou technologií ATM označujeme jako *virtuální síť LAN*, na jedné síti ATM lze vytvořit více zcela nezávislých virtuálních sítí. Tyto virtuální sítě mohou být i různých typů (Ethernet společně s Token Ringem). Technologie modelování, kterou si dále popíšeme, je označována jako *LAN emulace* (LANE – LAN Emulation).



Obrázek 12.18: Podpora emulace LAN

Stanice je k virtuální síti LAN emulované sítí ATM připojena prostřednictvím klientského rozhraní *LEC* (LAN Emulation Client), které zastupuje vrstvu MAC skutečné LAN. Základní funkcí klientského rozhraní je rozklad běžných rámců LAN (Ethernet nebo Token Ring) do buněk ATM a jejich vyslání po otevřeném virtuálním spoji, buňky přijaté z virtuálního spoje klientské rozhraní naopak skládá do rámců LAN. Protějškem klientského rozhraní LEC v síti ATM je skupina služeb, které dovolují transformovat komunikační schémata využívaná sítěmi LAN se sdílením média pro přepojovanou síť ATM. K těmto službám patří *konfigurační server LECS* (LAN Emulation Configuration Server), *server pro skupinovou komunikace BUS* (Broadcast and Unknown Server), *server emulované sítě LES* (LAN Emulation Server).

Postup, který stanice používá pro komunikaci ve virtuální LAN je následující: Po připojení stanice k síti ATM se stanice spojí s konfiguračním serverem LECS a od něho obdrží seznam emulovaných sítí LAN, ke kterým má přístup. Pro vytvoření vlastního spojení se serverem LECS (Configuration Direct VCC) stanice využívá ILMI proceduru, která vrací adresu serveru, pevně stanovené ATM adresy serveru nebo pevného služebního kanálu (VPI=0, VCI=17).

Dalšími dotazy směrovanými na konfigurační server může stanice získat adresy serverů LES (ale i další parametry) jednotlivých emulovaných sítí. Pro každou emulovanou síť stanice vytváří samostatné klientské rozhraní LEC, toto rozhraní propojuje s příslušným serverem LES (virtuálním spojením označovaným jako Control Direct VCC) a registruje zde své adresy MAC a ATM. Server LES tuto informaci využívá pro vytváření datových spojení mezi klientskými rozhraními LEC (přesněji pro zodpovídání dotazů na korespondenci MAC a ATM adres, tuto funkci označujeme podobně jako u sítí TCP/IP jako ARP – Address Resolution Protocol). Speciální stanice, jakými jsou například transparentní mosty (LANE standard o nich mluví jako o *proxy* prvcích), mohou předávat serveru LES informace ze svých směrovacích tabulek (na speciální žádost LES serveru), vlastní přenos dat pak může transparentní most obejít.

Kromě obousměrného kanálu mezi LEC a LES je vytvářen další jednosměrný kanál orientovaný od LES k LEC (Control Distribute VCC). Kanál využívá LES pro distribuci dotazů na vazbu adres MAC a ARP (podpora ARP protokolu). Adresu serveru pro skupinovou komunikaci BUS v dané emulované síti stanice získá ARP dotazem (Address Resolution Message) u odpovídajícího serveru LES.

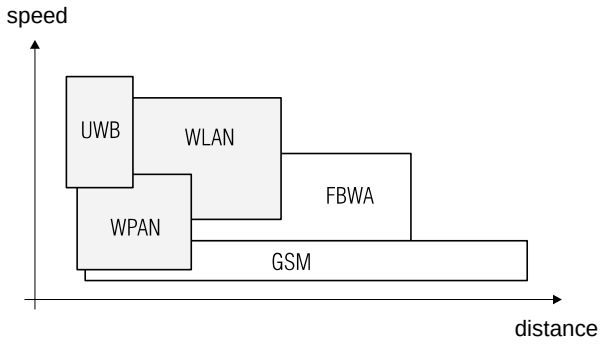
Současná řešení LAN emulace (LUNI – LAN Emulation User to Network Interface) nepodporují redundanci serveru LECS, zálohování serverů LES a BUS se však již objevuje. Standardizované rozhraní serverů LECS, LEC a BUS (*NNNI – LAN Emulation Node to Network Interface*) dovolí replikaci a zálohování služeb. Vlastní komunikace dvou stanic ve virtuální síti probíhá po virtuálním spojení (PVC nebo SVC). Stanice požádaná o přenos dat (konkrétního paketu) k určité protistanici musí nejprve získat ATM adresu protějšku (služby MAC stanice stanice pracují s MAC adresou, ne přímo s ATM adresou). Pokud tuto ATM adresu nemá klientské rozhraní LEC k dispozici z dřívějška (v oblasti cache), požádá server LES o převod adresy ARP dotazem. Je možné, že LES server nebude schopen ARP dotaz zodpovědět buď vůbec (protistanice není registrována u LES a ani není uvedena ve směrovacích tabulkách proxy uzlů) nebo včas, proto je o rozeslání paketu požádán server BUS. Výsledkem postupu je konečně získání ATM adresy protějšku a pokud virtuální spoj k protějšku se získanou ATM adresou dosud neexistuje (PVC nebo SVC), je otevřen nový virtuální spoj SVC (označovaný jako Data Direct VCC) s využitím standardní ATM signalizace (doporučení ITU-T Q.2931). Po získání virtuálního spoje stanice převede datový provoz dosud zprostředkovaný serverem BUS do tohoto kanálu.

Skupinová a broadcast komunikace je ve virtuální síti zprostředkována serverem BUS, který přijímá požadavky na rozeslání a rozesílá kopie všem stanicím virtuální sítě (včetně odesílatele). Tato skutečnost vyžaduje přidání identifikátoru odesílatele k rozesílanému paketu, paket vrácený serverem BUS odesílateli pak může být likvidován.

13. Bezdrátové sítě

Bezdrátové sítě se staly během posledních deseti let běžným prostředníkem naší komunikace. Zvykli jsme si nahradit Bellův analogový telefon (mám teď na mysli účastnický přístroj, na jehož principu se, až na signalizaci ovšem, tak moc nezměnilo) bezdrátovou digitální technologií GSM. Tato technologie nám dovolila získat, samozřejmě v oblastech s příslušnou infrastrukturou většinou buněčné sítě, neomezenou dosažitelnost hovorové telefonní služby. Satelitní implementace stejného principu, tedy sítě LEO (Low Earth Orbit), například Iridium známé i pro své problémy s financováním, dovolila rozšířit tuto dosažitelnost na celý povrch Země.

Přestože bezdrátové sítě určené digitální telefonii dovolují zajistit i přenosy dat, potřebné pro přístup k informačním službám (přenášejí přeci hovorový signál jako synchronní data), je jejich využitelnost v této oblasti přeci jen omezená, a ani očekávaný přechod k technologii UMTS na této skutečnosti asi příliš rychle mnoho nezmění. Podstatně vyšší přenosové rychlosti potřebné pro moderní služby (bohužel často maximalizující obrazový/multimediální balast a minimalizující užitečnou informaci) dovolují dnes dosáhnout bezdrátové sítě označované jako bezdrátové lokální sítě WLAN (Wireless Local Area Network), bezdrátové personální sítě WPAN (Wireless Personal Area Networks), bezdrátové směrové spoje FBWA (Fixed Broadband Wireless Access). Jednotlivé technologie lze charakterizovat poskytovanou rychlostí přenosu a úrovní dosažitelné mobility (obr. 13.1).

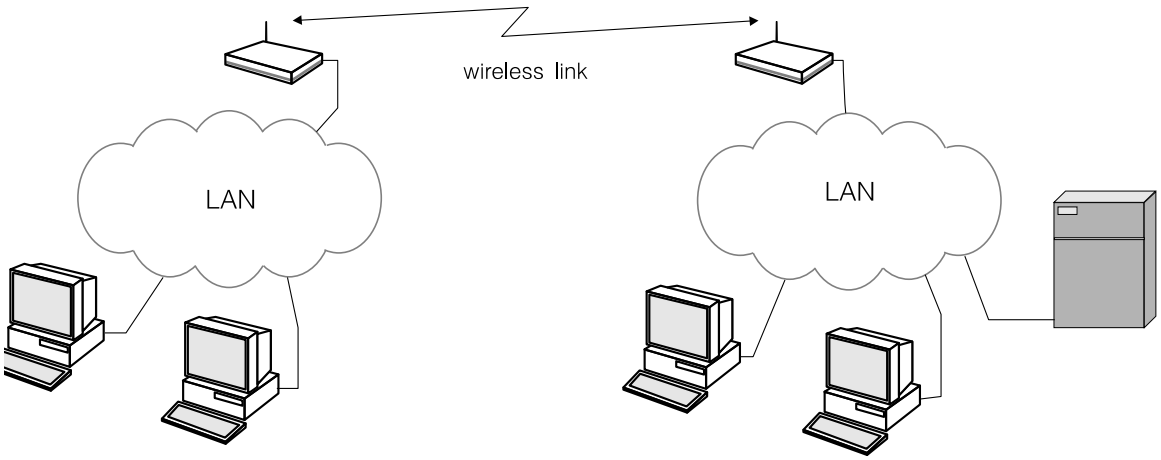


Obrázek 13.1: Bezdrátové technologie

Zatímco přenosová rychlost je měřitelná veličina (a účastník využívající přetížený sdílený kanál může mít značně osobní názor na její dostatečnost), pojem mobilita má přeci jenom poněkud vágní charakter - vyjadřuje v uvedeném grafu jednak možnost pohybu po oblasti pokryté infrastrukturou rádiové sítě, jednak schopnost vytvářet komunikace schopné skupiny mobilních zařízení nacházejících se v geografické blízkosti.

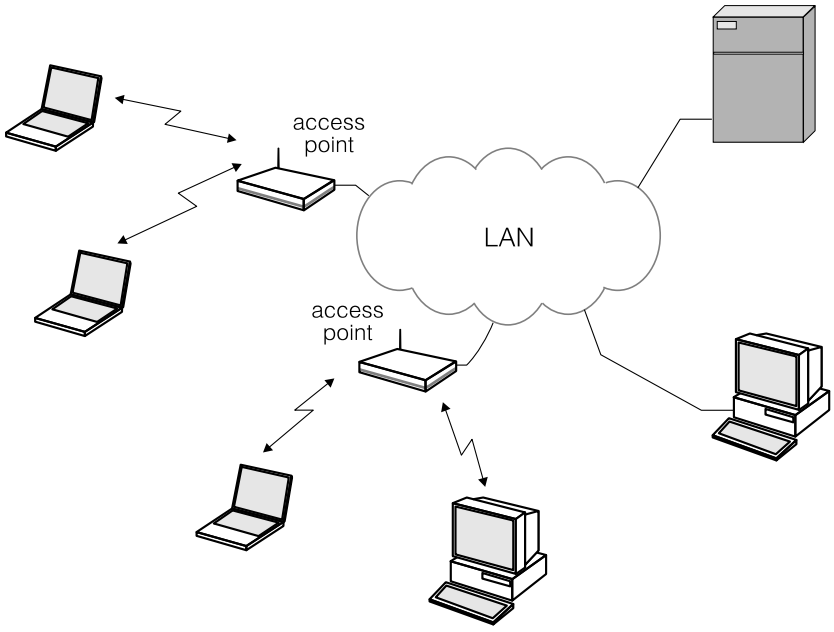
Nejstarší široce využívanou formou bezdrátového přenosu v počítačové komunikaci jsou směrové spoje. Dovolují rychle realizovat propojení nepříliš geograficky oddělených lokálních sítí, zajistit jednotlivým účastníkům přístup k Internetu (obr. 13.2), a jistě by se daly uvést i aplikace podobné.

Pro směrové spoje lze využít jak rádiové kanály v pásmech od zhruba 2 GHz do 60 GHz, tak vzdušné optické spoje. Rádiové směrové spoje využívají jak licensovaná pásma, v nichž se poskytovatel služby postará o nerušený provoz (a ten pak může být úzkopásmový), tak volně použitelná pásma, kde musíme počítat s rušením a interferencí jiných služeb a uživatelů (a nelze se obejít bez širokopásmových technologií, kterým se v našem článku budeme věnovat). Pevné spoje poskytují vysokou přenosovou rychlost a díky prostorovému multiplexu i efektivní využití přenosových kanálů. Optické spoje jsou většinou omezené na vzdálenost stovek metrů, a při vyšších výkonech musíme respektovat hygienická/bezpečnostní omezení.



Obrázek 13.2: Pevné bezdrátové spoje

Technologie bezdrátových lokálních sítí WLAN lze, samozřejmě s vhodnými směrovými anténami, využít jako pevné bezdrátové spoje, jejich základní aplikační oblastí je však zajištění přístupu mobilních účastníků ke službám dostupným v pevných počítačových sítích, tedy v podnikových lokálních sítích nebo v Internetu. Bezdrátové přístupové sítě se opírají o infrastrukturu tvořenou základnovými stanicemi připojenými pevnými spoji (i bezdrátovými) k síti, do které potřebujeme zajistit přístup. Každá základnová stanice kolem sebe vytváří oblast, ve které se mohou pohybovat stanice mobilní. Potřebujeme-li pokrýt větší oblast nebo komplikovanější prostředí (budovy) vytváříme zčásti se překrývající buňky kolem více základnových stanic, mobilní stanice se pak mohou pohybovat po celém signálem pokrytém území a technologie WLAN zajistí jejich transparentní předávání mezi základnovými stanicemi(obr. 13.3).

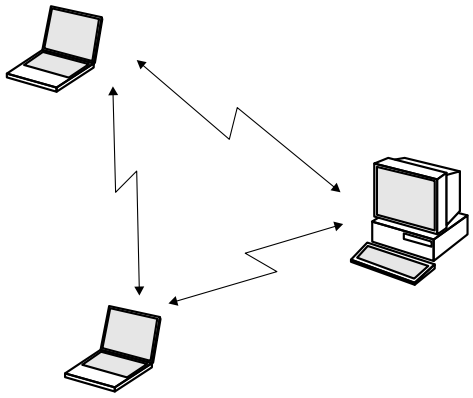


Obrázek 13.3: Bezdrátové sítě s infrastrukturou

Bezdrátové lokální sítě se dostaly do našeho povědomí jako technologie IEEE 802.11, a její dnes nejběžněji používaná modifikace 802.11b, známá podle iniciativy pracovní skupiny WECA (Wireless Ethernet Compatibility Alliance) pod označením WiFi. Rozhraními bezdrátové sítě IEEE 802.11b jsou dnes vybavovány notebooky, což podstatně zvyšuje snadnost jejich používání v sítích. Přestože technologie IEEE 802.11 je primárně určena pro privátní sítě (podnikové, ale příjemné jsou i bezdrátové základnové stanice v domácnostech), lze se v řadě míst setkat s

veřejným poskytováním této služby (letiště, hotely, konferenční centra, školy, ...).

Budování infrastruktury je poměrně náročné a pro určité aplikace je postačující umožnit přenos dat mezi stanicemi, které se dostanou do geografické blízkosti. Patří sem takové aplikace jako je synchronizace dat mezi osobním počítačem/notebookem a PDA, zajištění spojení mezi notebookem/PDA a mobilním telefonem pro přenos dat sítí GSM, zajištění komunikace mezi mobilním telefonem a bezdrátovým hands-free, zajištění bezdrátového přenosu EKG signálu z těla pacienta do vyhodnocovacího/záznamového zařízení, sběr dat z bezdrátově komunikujících senzorů, a jisté by bylo možné uvést i další.



Obrázek 13.4: Bezdrátové ad-hoc sítě

Sítě, které podporují takovéto funkce a nevyžadují infrastrukturu (obr. 13.4) označujeme jako ad-hoc sítě, nebo s ohledem na jejich časté osobní využívání jako sítě personální - WPAN (Wireless Personal Area Networks). V tomto režimu mohou pracovat i sítě WLAN IEEE 802.11, spíše však máme ad-hoc sítě spojené s technologií Bluetoooth vyvinutou fy Ericsson. Tyto sítě jsou zajímavé tím, že infrastruktura může být vytvářena dynamicky, komunikace se tedy neomezuje na přímo se slyšící stanice.

Následující text bude věnován technologiím WLAN a WPAN, v závěru si všimneme i v současnosti standardizovaných technologií bezdrátových metropolitních sítí WirelessMAN (IEEE 802.16) a technologie UWB (Ultra Wide Band).

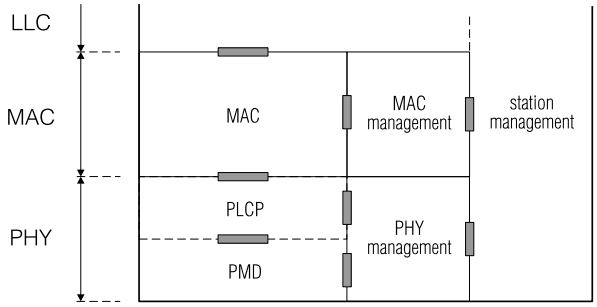
13.1 IEEE 802.11

Základem pro výstavbu lokálních bezdrátových sítí se stal standard IEEE 802.11 vytvořený v polovině devadesátých let pro přenos v pásmu ISM 2.400-2.4835 GHz a v pásmu infračerveného světla. Prvá verze vyšla v roce 1997, standard vycházel ze zkušeností s využíváním technologie frekvenčně rozprostřeného pásma v sítích pracujících na kmitočtech pásma ISM 902-928 MHz. Pásma ISM (Industry, Science, Medicine) jsou primárně určena pro technologické aplikace v průmyslu, vědě a medicíně, přenos dat je zde umožněn jako sekundární služba. Musíme tedy počítat s i poměrně výrazným úzkopásmovým rušením (jako příklad, v pásmu 2.4 GHz pracují mikrovlnné trouby).

Nevýhodou pásma 902-928 MHz byla skutečnost, že je pro tuto službu vyhrazeno pouze v regionu 2 (kam patří Spojené státy); v regionu 1, kam patří Evropa je podstatná část těchto frekvencí využívána mobilními telefony GSM. Pásmo 2.400-2.4835 GHz je s určitými omezeními v některých zemích (pokud jde o jeho šířku nebo nejvyšší povolený výkon) použitelné celosvětově. Další z ISM pásem, 5.725 - 5.850 GHz, je opět problematické, v Evropě je jeho použití vyhrazeno technologii rádiových sítí HiperLAN; o ní se později také určitě zmíníme.

Standard 802.11 byl vytvořen normalizačními skupinami IEEE věnujícími se standardizaci

lokálních sítí a pokrývá proto, stejně jako ostatní standardy lokálních sítí, hlavně nižší vrstvy síťové architektury - vrstvu fyzickou a linkovou (obr. 13.5).



Obrázek 13.5: Architektura IEEE 802.11

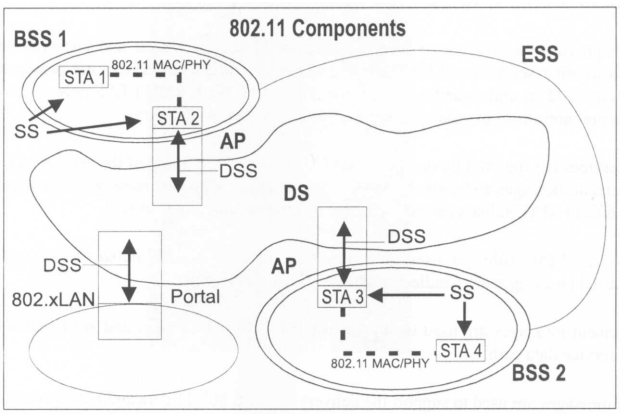
Fyzická vrstva se přitom dělí na vrstvu PLCP (Physical Layer Convergence Protocol), která je do určité míry nezávislá na použitém přenosovém médiu (rádiový kanál, optický kanál, metoda rozprostření pásma, modulace) a vrstvu PMD (Physical Media Dependent) specifikující vlastní přenosový kanál.

Linková vrstva zahrnuje přístupovou metodu MAC (Medium Access Control), s ohledem na podstatně vyšší chybovost jsou na rozdíl od klasických lokálních sítí využívána i potvrzovací schémata, obvykle zahrnovaná do LLC (Logical Link Control).

Protože použité přenosové médium, rádiový nebo optický kanál, je volně přístupné, nelze si představit prakticky využitelnou technologii nedovolující rozumnou kryptografickou ochranu přenášených dat a zajištění autenticity komunikujících účastníků, součástí standardů je tedy i definice bezpečnostních mechanismů. Konečně, standard specifikuje mechanismus správy jednotlivých vrstev.

Struktura sítě IEEE 802.11

Technologie IEEE 802.11 je určena primárně pro výstavbu lokálních rádiových sítí s infrastrukturou, dovoluje však i výstavbu ad-hoc sítí a propojování lokálních sítí nebo připojování jednotlivých stanic pevnými, typicky směrovými spoji. (Poslední možnosti využívá řada malých poskytovatelů připojení k Internetu, samozřejmě je výhodnější, jsou-li pro takovou službu použita jiná, licensovaná, pásma a ne pásmo ISM.) Prvky, kterými technologie IEEE 802.11 podporuje budování uvedených sítí a spojů uvádí (obr. 13.6).



Obrázek 13.6: Struktura sítě IEEE 802.11

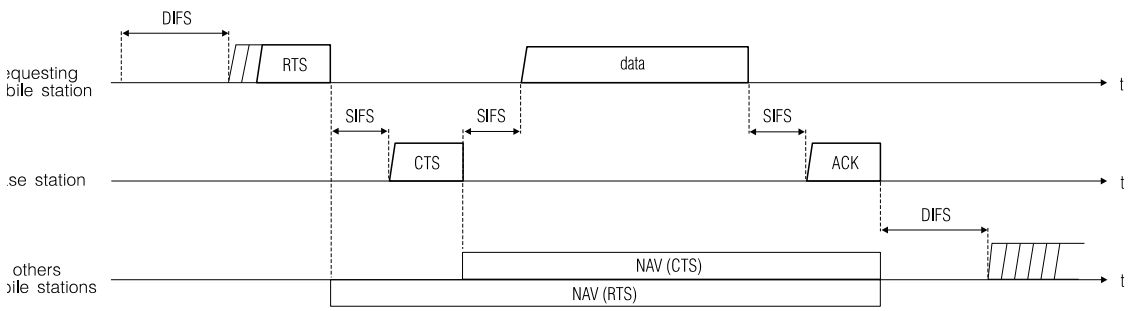
Koncové stanice STA (Station) mohou vytvářet skupiny (na území omezeném dosahem

stanic) označované jako BSS (Basic Service Set), komunikace mezi stanicemi je označována jako SS (Station Service). U ad-hoc sítí je taková skupina označována jako nezávislá BSS (IBSS - Independent BSS); u sítí s infrastrukturou slouží některá ze stanic jako základnová a může připojit skupinu BSS k distribuční síti DS (Distribution System); je pak označována jako přístupový bod AP (Access Point). Služba přístupového bodu je označována jako DSS (Distribution Systém Service), služba zprostředkovaná mobilním účastníkům v různých BSS distribuční sítí je označována ESS (Extended Service Set). Distribuční síť může být založena na libovolné technologii schopné zajistit přenos dat s požadovanými parametry (kapacita, zpoždění, ztráty), případné připojení jiných lokálních sítí k síti distribuční označuje obrázek jako portál.

Řízení přístupu - MAC

Stanice sdílející bezdrátový komunikační kanál musí být vybaveny efektivním mechanismem dovolujícím pokud možno bezkolizní přístup k přenosovému médiu. Takový mechanismus je u všech technologií lokálních sítí označován jako MAC (Medium Access Control) a musí zajistit, že na sdíleném přenosovém kanále vysílá v daném časovém okamžiku jediná stanice. S nejrůznějšími formami přístupové metody se setkáme ve všech, dnes již často historických, technologiích lokálních sítí se sdíleným médiem. U bezdrátových sítí řízení přístupu komplikuje jeden podstatný fakt: stanice, které se potřebují rozhodnout zda mohou zahájit vysílání totiž nemají plnou informaci o provozu na kanále. Důvodem je skutečnost, že se některé stanice pro překážky neslyší (sítě pracují v mikrovlnném nebo optickém pásmu), u některých technologií s infrastrukturou tomu brání už samotná specifikace přenosových kanálů (jako příklad si uveďme technologii mobilních telefonů GSM, které mají vysílací a přijímací kanál na různých kmitočtech, nebo technologii bezdrátových telefonů DECT, které využívají pro vysílání a příjem odlišné sloty časového duplexu).

Technologie 802.11 používá pro řízení přístupu metodu, označovanou jako CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), MACA (Multiple Access Collision Avoidance), případně RTS/CTS. Opírá se o skutečnost, že v síti s infrastrukturou slyší základnová stanice všechny stanice mobilní a všechny mobilní stanice slyší stanici základnovou . Metoda přístupu se opírá o požadavek na přidělení kanálu, který stanice vyšle k základnové stanici, a který musí být potvrzen před zahájením vlastního vyslání dat. Kolize požadavků vyslaných současně více stanicemi vyvolá interferenci a pravděpodobně zabrání bezchybnému přijetí libovolného z nich. Výsledkem je, že základnová stanice neodpoví, a každá z kolidujících žádostí musí být po uplynutí náhodně určené prodlevy zopakována. Mechanismus je poměrně jednoduchý, jeho základní funkci si popíšeme pro předání rámce mobilním účastníkem základnové stanici na (obr. 13.7).

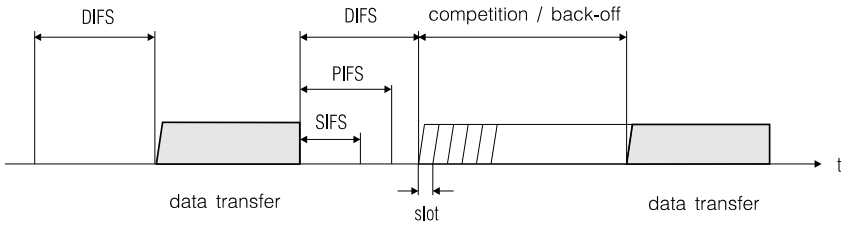


Obrázek 13.7: Přístupová metoda IEEE 802.11

Stanice, která předpokládá volný přenosový kanál (na základě poslechu předchozího provozu) vyšle k základnové stanici krátký rámec - požadavek RTS (Request To Send); v něm je uvedena požadovaná doba rezervace kanálu. Základnová stanice příjem požadavku potvrdí

rámcem CTS (Clear To Send), ve kterém sdělí dobu, po kterou bude kanál vyhrazen. Odpověď využije přímo žádající účastník, on i ostatní jsou informováni o době obsazení kanálu hodnotou NAV (Network Allocation Vector).

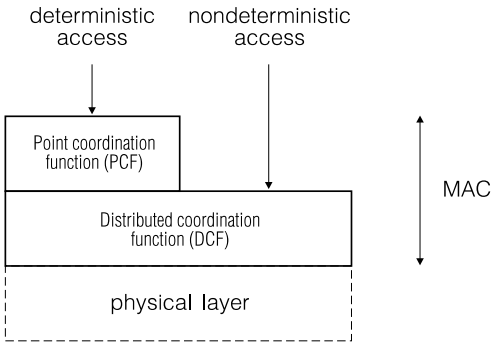
Uvedený popis mechanismu předpokládá existenci základnové stanice, která koordinuje provoz skupiny stanic. Tato funkce je označována jako PCF (Point Coordination Function), základnová stanice má určitou prioritu vyjádřenou schopností obsadit komunikační kanál po jeho uvolnění dříve, po prodlevě PIFS (PCF InterFrame Space), než stanice ostatní (obr. 13.8). Funkce PCF je využívána pro vytvoření synchronních kanálů, pro vysílání rámců předávaných přes základnovou stanici a pochopitelně pro správu BSS.



Obrázek 13.8: Modifikace přístupové metody IEEE 802.11

Kratší prodleva SIFS (Short InterFrame Space) dává staníci možnost potvrdit přijatý rámec bez další žádosti na přidělení kanálu (potvrzování je bezkolizní), naopak delší DIFS (DCF InterFrame Space) dovoluje spolupráci stanic bez základnové stanice. U distribuovaného řízení přístupu DCF (Distributed Coordination Function) (ale i u výše popsaného PCF mechanismu) se mohou vyskytnout kolize, snížení jejich pravděpodobnosti zajišťuje mechanismus přidávající náhodnou prodlevu při odesílání požadavku RTS, doplněný o exponenciální ustupování (Back-Off) po kolizích. Exponenciální ustupování chrání před zablokováním sítě při vysokém provozu, je obdobou mechanismu, jak ho známe u klasického Ethernetu.

Technologie IEEE 802.11 tak podporuje deterministický přístup CF (Contention Free) i přístup založený na soupeření stanic, označovaný obvykle jako nedeterministický nebo náhodný (obr. 13.9).



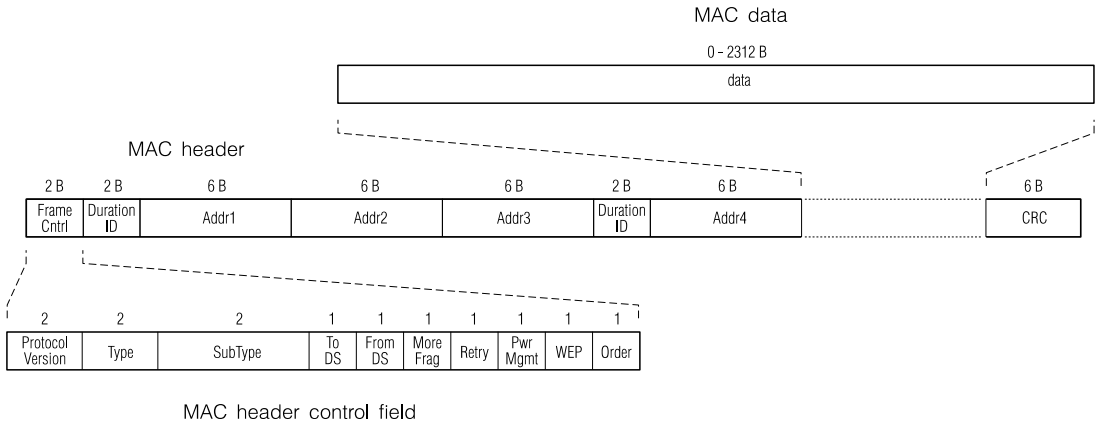
Obrázek 13.9: Přístupové mechanismy IEEE 802.11

Oba přístupové mechanismy, tedy PCF a DCF, je možné ve skupině stanic s infrastrukturou kombinovat, ad-hoc sítě se opírají pouze o DCF.

Rámce MAC a jejich formát

Rámce MAC bezdrátových sítí IEEE 802.11, které jsou předávané fyzické vrstvě (často je označujeme jako MPDU - MAC Protocol Data Unit) mají složitější strukturu než rámce jiných lokálních sítí, například Ethernetu. Nejvýraznějším rozdílem jsou až čtyři adresní pole, dovolující

popsat přímou komunikaci koncových stanic, komunikaci zprostředkovanou základnovou stanicí a komunikaci zprostředkovanou dvojicí základnových stanic propojených distribuční sítí. Využití adresních polí určují bity ToDS a FromDS řídícího pole hlavičky. Základní strukturu MAC rámce IEEE 802.11 si můžeme popsat na obr. 13.10.



Obrázek 13.10: Formát rámců MAC

Uvedenou strukturu mají všechny MAC rámce. Kromě datových rámců. přenášejících užitečná data (například IP pakety) si stanice předávají řídící rámce, které podporují řízení přístupu k přenosovému kanálu a potvrzování, a rámce pro správu podporující mechanismy autentizace, kryptografické ochrany, registrace stanic v BSS, časové synchronizace a řízení spotřeby vypínáním stanice. V poli Frame Control najdeme příznaky podporující fragmentaci a řízení výkonu. Formát MAC rámců je společný pro všechna fyzická média, tedy pro rádiové i optické kanály.

Definice přenosových kanálů

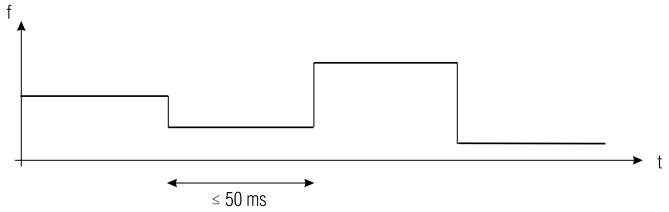
Standard IEEE 802.11 definuje tři odlišné kanály, zajišťující komunikaci ve skupině stanic. Přenos na rádiových kmitočtech využívá technologií rozprostřeného pásma, za 2. světové války vyvinuté pro "utajenou" komunikaci. V rádiových lokálních sítích je jejím smyslem potlačit vliv úzkopásmového rušení tím, že pro přenos využíváme širšího frekvenčního rozsahu. Jsou využívány dvě základní metody označované jako FHSS (Frequency Hopping Spread Spectrum), a DSSS (Direct Sequence Spread Spectrum) nebo častěji CDMA (Code Multiplex Multiple Access).

FHSS - frekvenční rozprostření pásma

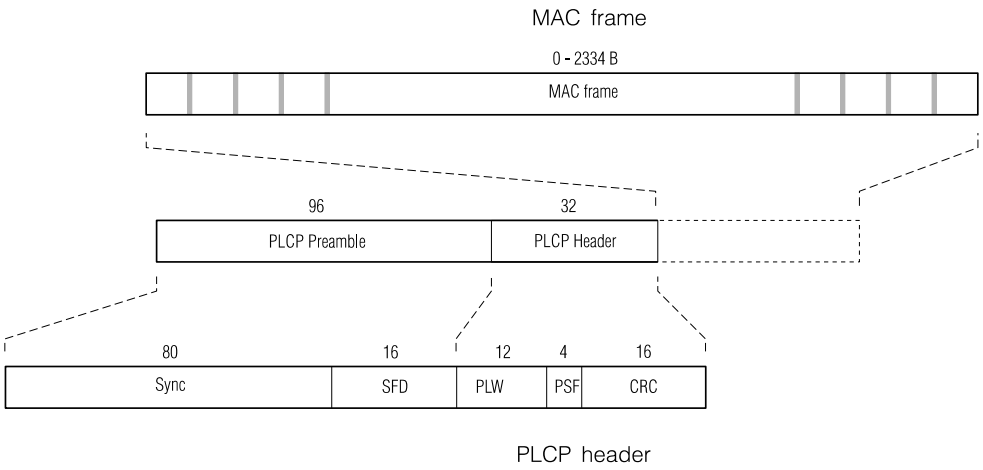
Principem mechanismu rozprostření pásma FHSS (Frequency Hopping Spread Spectrum) je změna používaného kmitočtu po ukončení určité fáze přenosu. Je respektován požadavek americké FCC na rovnoměrné využití 79 z 85 možných kanálů o šířce 1 MHz, které jsou k dispozici v pásmu 2.4 GHz a maximální setrvání na jednom z nich po dobu 50 ms (obr. 13.11).

Standard současně stanovuje konkrétní posloupnosti, a to nejen pro státy, které dávají pásmo 2.400 - 2.4835 GHz k dispozici v plné šíři, ale i pro státy, které šířku využitelného pásma omezují.

Pro vlastní přenos na rádiovém kanále je nutné rámce předávané vrstvou MAC doplnit o synchronizaci, informaci o délce rámce a informaci o přenosové rychlosti použité pro odvysílání vlastních dat MAC rámce. Takto doplněný rámec je označován jako rámec PLCP (Physical Layer Convergence Protocol) nebo, s ohledem na ISO OSI, také PPDU (Physical Layer Protocol Data Unit).



Obrázek 13.11: Rozprostření pásma FHSS



Obrázek 13.12: Struktura rámce PLCP FHSS

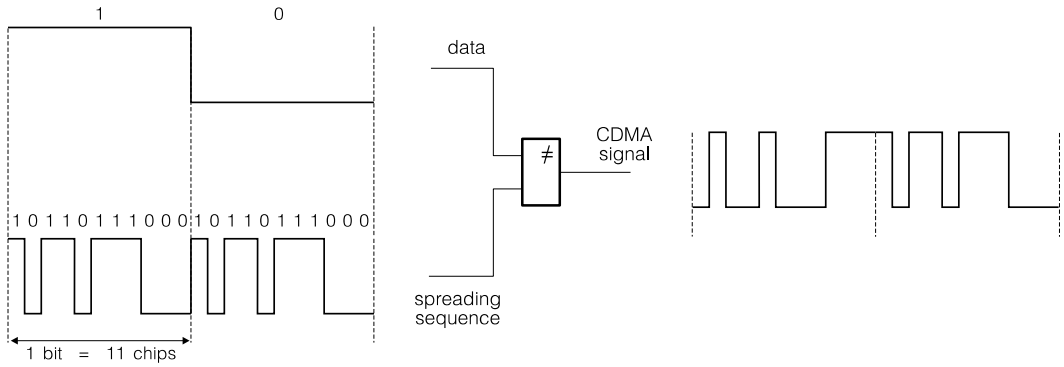
Rámec PLCP pro přenos FHSS (obr. 13.12) začíná preambulí - posloupností střídajících se nul a jedniček, která přijímači dovolí doladění se na frekvenci vysílače, případně výběr antény; základní funkcí preambule je však podpořit bitovou synchronizaci a rozhodnout, zda přijímaný signál je dostatečně silný. Šestnáctibitová posloupnost SFD (Start Frame Delimiter) označuje začátek rámce PLCP. Údaj PLW (PSDU Length Word) v hlavičce rámce informuje o délce přenášeného bloku dat, pole PSF určuje přenosovou rychlost, se kterou budou vysílána data, hlavička je chráněna detekčním CRC kódem v poli HEC (Header Error Check) proti chybám při přenosu. Přenášená data randomizuje scrambler, každý blok 32 oktetů je doplněn o oktet, který kompenzuje stejnosměrnou složku (nulová stejnosměrná složka je důležitá pro správnou funkci automatického dolaďování přijímače).

Modulační metoda použitá pro přenos dat závisí na cílové přenosové rychlosti. Pro přenosovou rychlost 1 Mb/s je využívána dvoustavová frekvenční modulace 2GFSK, pro 2 Mb/s je využívána čtyřstavová 4GFSK. Hlavička PLCP je vždy vysílána rychlostí 1 Mb/s.

Rozprostření pásma FHSS se do standardu IEEE 802.11 dostalo ze starších bezdrátových sítí v pásmu 902-928 MHz, naprostá většina výrobců se časem přiklonila k rozprostření pásma DSSS. Technologie FHSS je však dnes využívána v jiných rádiových sítích jako jsou personální sítě Bluetooth nebo sítě SWAP (Shared Wireless Access Protocol), které definovala pracovní skupina HomeRF pro sítě v domácnostech. Obě tyto technologie dovolují vytvářet rádiové sítě v pásmu 2.4 GHz, a podporují vedle přenosu běžných dat i přenos plně duplexních synchronních kanálů digitální telefonie.

DSSS - kódové rozprostření pásma

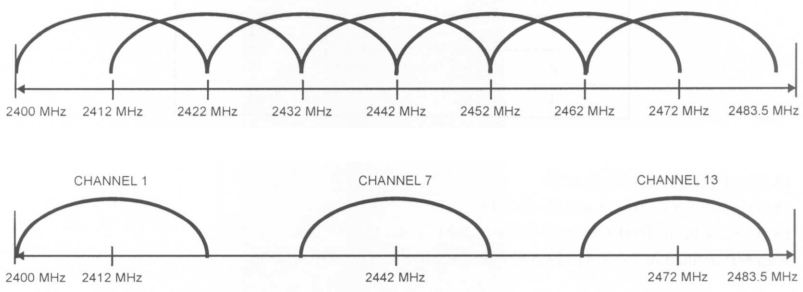
Alternativní metodou přenosu v sítích IEEE 802.11 je rozprostření pásma dosažené tak, že bity dat přenášíme jako sekvence řezů (chips). Sekvence pro nulu a jedničku jsou navzájem inverzní, získání modulačního signálu uvádí obr. 13.13.



Obrázek 13.13: Kódové rozprostření pásma

Rozprostření pásma je označováno jako DSSS (Direct Sequence Spread Spectrum) nebo častěji jako CDMA (Code Division Multiple Access) - kódový multiplex. Rozprostírající posloupnost je pseudonáhodná, bez znalosti této posloupnosti signál připomíná náhodný šum a po modulaci pokrývá široké pásmo kmitočtů. Při dostatečně dlouhých rozprostírajících posloupnostech metoda dovoluje současný přenos více kanálů s ortogonálně volenými rozprostírajícími posloupnostmi na tomtéž pásmu. Praxe však diktuje co nejvyšší přenosovou rychlost, důsledkem je délka rozprostírající posloupnosti na hranici připuštěné americkou FCC, tedy v normě určených jedenáct řezů.

Pásmo 2.4 GHz poskytuje sedm, částečně se překrývajících kanálů, nebo tři dostatečně oddělené kanály (obr.13.14).



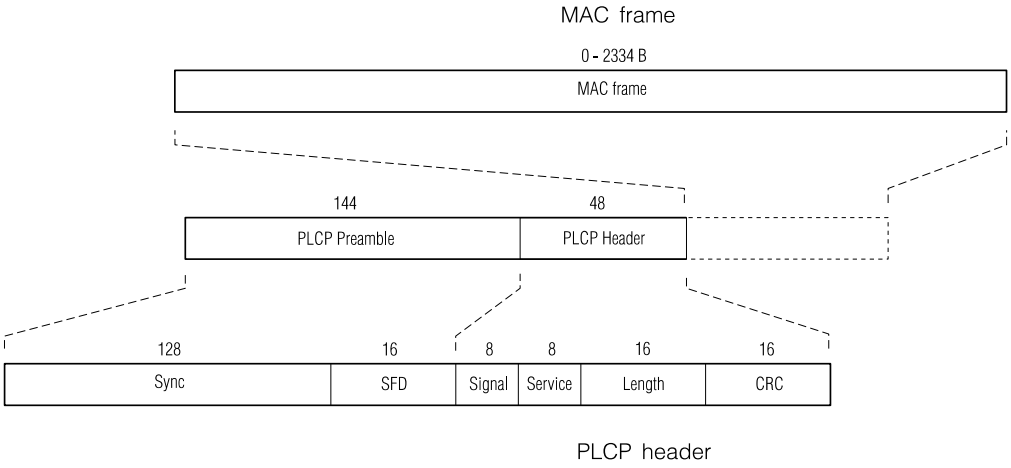
Obrázek 13.14: Frekvenční kanály PHY DSSS

Použitý rozprostírající kód, Barker Code, není schopen zajistit násobné využití kanálu, konvoluční detektor na straně přijímače však dovoluje snadno detekovat začátky jednotlivých bitů a opravit určitá poškození způsobená nekorelovaným rušením nebo interferencí.

Struktura rámce PLCP pro DSSS (obr. 13.15) se poněkud liší od rámce, který jsme si uvedli pro FHSS.

Podobně jako u frekvenčního rozprostření pásma FHSS zajišťuje i u kódového rozprostření DSSS preambule, zde tvořená posloupností samých jedniček zpracovanou scramblerem a ukončená šestnáctibitovou posloupností SFD (Start Frame Delimiter), bitovou synchronizaci a rozpoznání začátku rámce PLCP. Struktura hlavičky rámce PLCP je však poněkud odlišná, osmibitové pole Signal určuje přenosovou rychlost (1 Mb/s nebo 2 Mb/s), pole Service identifikuje soulad se standardem IEEE 802.11 a pole Length udává délku přenášených dat. Hlavička je chráněna šestnáctibitovým detekčním kódem CRC. Přenášená data randomizuje scrambler.

Modulační metoda použitá pro přenos dat závisí na cílové přenosové rychlosti. Pro přenosovou rychlost 1 Mb/s je využívána dvoustavová fázová modulace DBPSK, pro 2 Mb/s je využívána čtyřstavová DQPSK. Hlavička PLCP je vždy vysílána rychlostí 1 Mb/s.

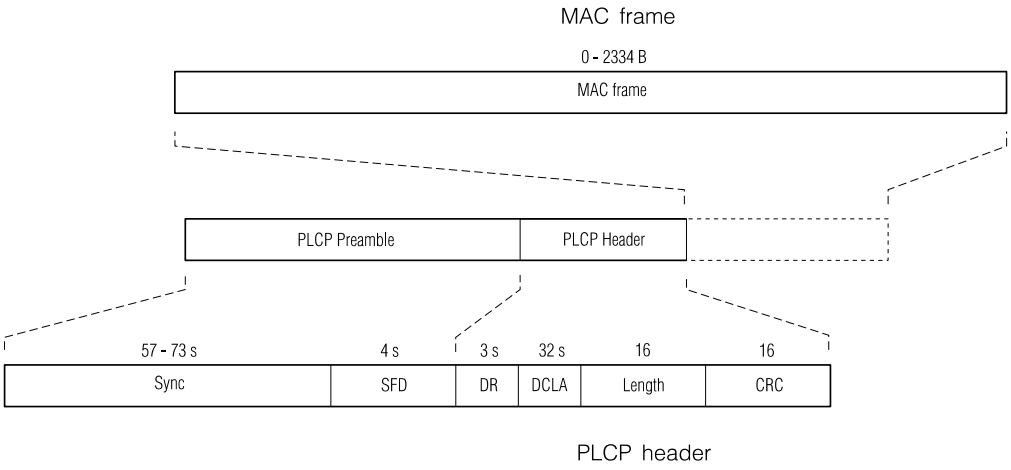


Obrázek 13.15: Struktura rámce PLCP DSSS

IR - optická rozhraní

Vedle rádiového přenosu specifikuje standard IEEE 802.11 použití optického rozhraní, využíváno je infračervené světlo (IR - Infra-Red) s vlnovou délkou v rozsahu 850 - 950 nm. Přenos je možný na vzdálenost do deseti metrů, počítá se s přenosem v místnostech a s využitím odraženého/difuzního světla.

Rámce PLCP pro optické rozhraní mají strukturu podle obr. 13.16.



Obrázek 13.16: Struktura rámce PLCP IR

Hlavička dovoluje definovat přenosovou rychlost pro data DR (Data Rate) a korekci stejnosměrné složky DCLA (DC Level Adjustment). Pro přenos je využívána modulace PPM (Puls Position Modulation), pro přenosovou rychlost 1 Mb/s jde o 16-PPM (kóduje čtyři bity jako pozici světelného impulsu v jednom ze šestnácti časových slotů o délce 250 ns), pro 2 Mb/s se používá 4-PPM (kóduje dva bity jako jednu ze čtyř možných pozic impulsu). Preambule je tvořena posloupností pulsů s periodou 500 ns, SFD, DR a DCLA jsou standardem definované posloupnosti impulsů.

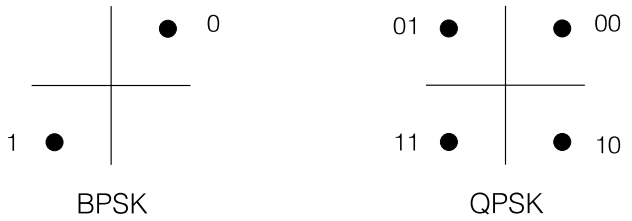
Standard IEEE 802.11 se stal základem pro rychlejší bezdrátové sítě, dnes využívané hlavně pro komunikaci přenosných počítačů, notebooků, v infrastrukturních sítích. Tyto sítě, označované jako WiFi, využívají efektivnější metody kódování přenášených dat a/nebo efektivnější metody modulace. Sítě IEEE 802.11b (normalizované v roce 1999 a s prvky podle základní normy plně spolupracující) dovolují vedle rychlosti 1 Mb/s a 2 Mb/s přenos vyššími rychlostmi 5.5 a 11 Mb/s, technologie IEEE 802.11b+ dosahuje přenosové rychlosti 22 Mb/s. Zcela odliš-

nou metodu modulace používají sítě podle IEEE 802.11a normalizované v roce 1999. Modulace OFDM (Orthogonal Frequency Division Multiplex) dovoluje přenosovou rychlost až 54 Mb/s v pásmu 5.7 Ghz, které není tak silně využívané jako pásmo 2.4 Ghz, a je zde tedy mnohem menší úroveň rušení. Ve fázi dokončování je v současnosti standard IEEE 802.11g poskytující, s využitím modulace OFDM, přenosovou rychlost 54 Mb/s i v pásmu 2.4 GHz.

13.1.1 IEEE 802.11b

Standard IEEE 802.11 ve formě, v jaké byl definován v roce 1997 předpokládal přenosové rychlosti 1 Mb/s a 2 Mb/s a využití tří alternativních přenosových prostředí: frekvenčně rozprostřeného spektra (FHSS) v pásmu ISM 2.4 GHz, kódově rozprostřeného spektra (DSSS) v pásmu ISM 2.4 GHz a pulsně-kódové modulace v krátkovlnném infračerveném pásmu. Z uvedených tří možností se v praxi prosadila technologie DSSS, dosažitelná přenosová rychlost však byla, ve srovnání s tím co poskytovaly běžné lokální sítě s metalickou nebo optickou kabeláží, poněkud nízká.

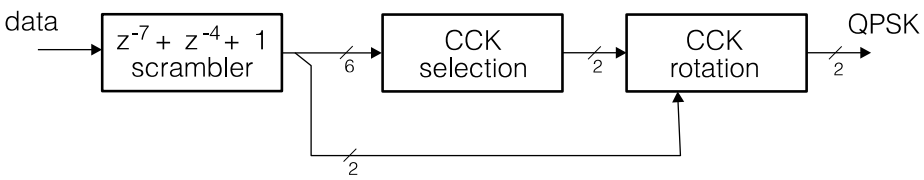
Technologie kódově rozprostřeného spektra DSSS podle IEEE 802.11 se opírá o použití jedenáctibitové rozprostírající sekvence - Barkerova kódu. Tato posloupnost (10110111000) generovaná s frekvencí 11 Mhz je modulárně sečtena (modulo 2) s přenášeným datovým signálem o rychlosti 1 Mb/s a výsledek označovaný jako posloupnost bitových řezů) je použit jako modulační signál pro dvoustavovou fázovou modulaci BPSK (Binary Phase Shift Keying). Zvýšené přenosové rychlosti 2 Mb/s se dosahuje, při frekvenci bitových řezů 22 MHz a stejné modulační rychlosti 11 MBd, čtyřstavovou fázovou modulací QPSK (Quaternary Phase Shift Keying) (obr. 13.17).



Obrázek 13.17: Dvoustavová BPSK a čtyřstavová QPSK modulace

Jediná využívaná rozprostírací sekvence dovoluje dosáhnout vysoké citlivosti, pochopitelně však mizí možnost současných přenosů v jedné lokalitě na jednom kmitočtu. Výhodou, podstatnou z hlediska složitosti implementace v době vzniku standardu, je potřeba jediného korelátoru v přijímači.

Poměr mezi rychlostí přenosu dat a frekvencí rozprostírající sekvence byl vzhledem k potřebě zajistit přenosové rychlosti srovnatelné s lokálním sítěmi neúnosně vysoký a vedl k náhradě Barkerovy sekvence podstatně efektivnějším mechanismem opírajícím se o komplementární kódy. Metoda, označovaná jako CCK (Complementary Code Keying), kterou vyvinuly Lucent Technologies a Harris Semiconductor, se stala základem modifikace původního standardu - IEEE 802.11b.

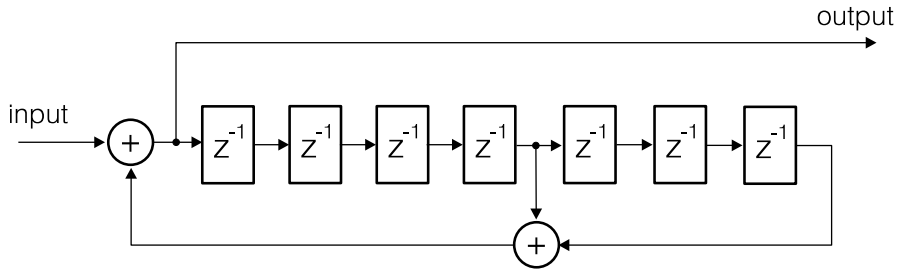


Obrázek 13.18: Struktura modulátoru CCK IEEE 802.11b

Osmibitová slabika přenášených dat je rozdělena na šestici a dvojici bitů (obr. 13.18). Šestice

bitů vybírá jednu ze 64 sekvencí o délce osmi čtyřhodnotových symbolů, tyto sekvence si můžeme představit jako posloupnosti komplexních čísel (i+1, i-1, -i-1 a -i+1). Zbývající dvojice bitů vybírá jedno ze čtyř pootočení základní sekvence, výsledný signál je přímo využit pro řízení modulátoru QPSK. Pro dosažení bitové rychlosti 11 Mb/s nám tak při modulaci QPSK postačí modulační rychlost 11 MBd. Při použití modulace BPSK je potřeba jeden výstupní symbol modulátoru přenést dvěma změnami fáze, přenosová rychlost je tak při modulační rychlosti 11 MBd snížena na 5.5 Mb/s.

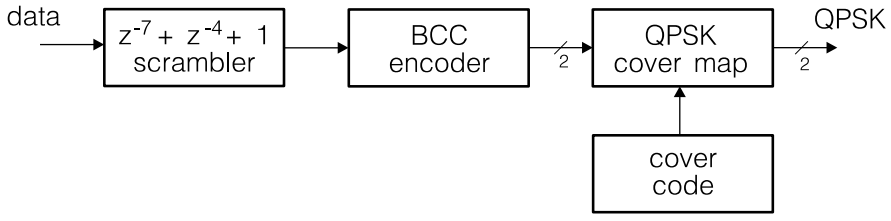
Vysoká efektivita využití přenosového kanálu je podmíněna tím, že přenášený signál je blízký náhodné posloupnosti bitů. Takový požadavek však reálné datové signály nesplňují. Cestou, jak převést datový signál s dlouhými posloupnostmi nul a jedniček na signál blízký náhodnému, je použití scrambleru. Jde o poměrně jednoduchý obvod, založený na polynomiální transformaci. Scrambler používaný v modulátorech IEEE 802.11b má strukturu odpovídající obr. 13.19.



Obrázek 13.19: Scrambler $z^{-7} + z^{-4} + 1$

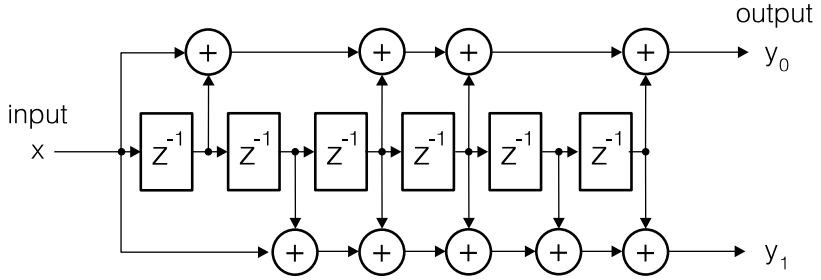
Kódování CCK není jedinou cestou jak dosáhnout přenosových rychlostí 5.5 a 11 Mb/s. Standard IEEE 802.11b nabízí alternativně kódování PBCC (Packet Binary Convolutional Coding), které poskytuje, za cenu složitějšího dekódéru, poněkud lepší výsledky.

Strukturu modulátoru PBCC uvádí (obr. 13.20). Datový signál, překódovaný scramblerem je veden do kódéru BCC, který vytváří dvoubitový signál pro řízení QPSK modulátoru. Ten je ještě modifikován binárním pseudonáhodným signálem (Cover code), který posouvá fázi modulačního signálu o 90^o.



Obrázek 13.20: Struktura modulátoru PBCC IEEE 802.11b

Vlastní kódér BCC se opírá o dvojici polynomů s binárními koeficienty a je poměrně jednoduchý (obr. 13.21)

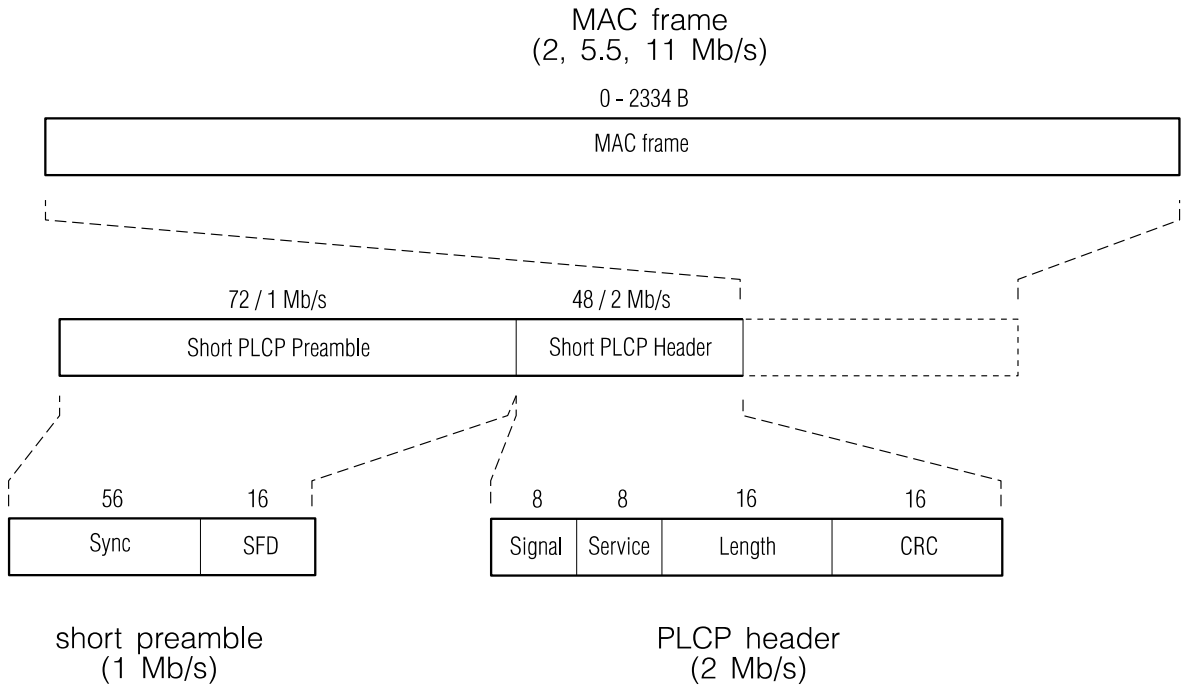


Obrázek 13.21: Struktura kódéru BCC IEEE 802.11b

Jeden bit scramblerem překódovaného datového signálu vstupující do kódéru BCC vyprodukuje dvoubitový signál pro řízení QPSK modulátoru. Při modulační rychlosti 11 MBd tak dosahujeme přenosové rychlosti 11 Mb/s. Při použití modulace BPSK je pro přenos každého bitu dvou změn fáze, výsledkem je přenosová rychlost 5.5 Mb/s.

O kódování PBCC se opírá i nejnovější modifikace IEEE 802.11b, u které byla přenosová rychlost zvýšena na 22 Mb/s. Využívá se zde osmistavová modulace 8PSK, každý symbol generovaný rychlostí 11 MBd přenáší dvojici bitů scramblovaného datového signálu.

Podstatně zvýšená přenosová rychlost (ve srovnání s rychlostmi 1 a 2 Mb/s standardu IEEE 802.11) si vyžádala úpravu rámců. Vedle standardní synchronizační preambule o délce 144 bitů a hlavičky rámce PLCP o délce 48 bitů vysílaných rychlostí 1 Mb/s (BPSK) je u technologie IEEE 802.11b možné využít zkrácenou synchronizační preambuli o délce 72 bitů (pro kompatibilitu se standardem IEEE 802.11 je vysílána rychlostí 1 Mb/s). Hlavička rámce PLCP je pak vysílána rychlostí 2 Mb/s (QPSK), vlastní data jsou vysílána s kódováním (CCK, PBCC) a rychlostí určenou v poli Signal (tedy 5.5, 11 nebo 22 Mb/s).



Obrázek 13.22: Struktura rámců IEEE 802.11b

13.1.2 IEEE 802.11a

Nevýhodou pásma ISM 2.4 GHz je skutečnost, že jednak není pro datovou komunikaci primárně určeno a musíme proto počítat s rušením z IMS zdrojů, a že jeho struktura nijak nevymezuje jeho využívání pro odlišné přenosové služby. Poměrně vysoký povolený výkon (1 W pro USA, 0.1 W pro Evropu) v celém pásmu a malý počet nepřekrývajících se pásem může omezit použitelnost této technologie v konkrétním místě.

Podstatnou výhodou je, pokud je kmitočtové pásmo vyhrazeno pro datové přenosy, a jeho struktura nutí k umístění různých typů přenosů (směrové spoje na větší vzdálenosti, rozsáhlejší buňky, malé buňky) do odlišných kmitočtových intervalů. Takovým pásmem je pásmo 5.7 GHz, pro toto pásmo byla navržena technologie lokálních sítí známá pod označením IEEE 802.11a.

Určitou nevýhodou pásma 5.7 GHz je na druhou stranu fakt, že jeho využití není definováno jednotně pro všechny oblasti ITU-R. Navíc, v Evropě bylo toto pásmo již dříve vyhrazeno pro

technologie lokálních sítí vyvíjené evropským ETSI - tyto technologie jsou známé pod jménem HiperLAN.

Pásmo [GHz]	5.15 - 5.25	5.25 - 5.35	5.47 - 5.725	5.725 - 5.825
Evropa	200 mW	200 mW	1 W	25 mW
USA	200 mW	1 W	-	4 W
Japonsko	200 mW	-	-	-

Využitelnost pásma 5.7 GHz

Větší využitelná šířka pásma 5.7 GHz bohužel nedovoluje zvýšit přenosovou rychlost přímo, zvýšením modulační rychlosti. Důvodem je skutečnost, že rádiový signál se nešíří přímo, ale musíme počítat s vlivem odrazů o objekty blízké přímé cestě, a s vlivem ohybů. Řešením, které standard IEEE 802.11a volí, je použití více pomalejších kanálů frekvenčního multiplexu. Metoda je označována jako ortogonální frekvenční multiplex OFDM (Ortogonal Frequency Division Multiplexing).

Technologie OFDM využívá nepřekrývající se kanály o šířce 20 MHz, do každé ze tří částí pásma (jak je definováno pro USA) se vejdou čtyři takové kanály. Každý z těchto kanálů poskytuje prostor pro 52 nosných, pro každou z nich je vyhrazeno zhruba 300 kHz.

Pro vlastní přenos dat je využíváno 48 nosných, data jsou, na rozdíl od IEEE 802.11b, chráněna proti chybám kódováním, dovolujícím opravu chyb (tento postup je obvykle označován jako FEC - Forward Error Correction). Základní přenosovou rychlostí IEEE 802.11a při FEC kódování, které zvyšuje počet přenášených bitů na dvojnásobek (r=1/1) a modulaci BPSK je 6 Mb/s. Použití alternativního (a nepovinného) FEC kódování s vyšší efektivitou (r=3/4) a modulace BPSK poskytuje 9 Mb/s. Vyšších rychlostí dosahují režimy, opírající se o čtyřstavovou QPSK (12 a 18 Mb/s), o šestnáctistavovou 16-QAM (24 a 36 Mb/s) a o čtyřiašedesátistavovou 64-QAM (48 a 54 Mb/s).

Odlišnost technologie IEEE 802.11a opírající se o přenos OFDM symbolů, které přenášejí od 36 bitů dat (pro 6 Mb/s) pro 324 bitů dat (pro 54 Mb/s), se projevila ve struktuře rámce. Preambule, hlavička, i data rámce jsou přenášeny jako OFDM symboly, preambule a hlavička jsou vysílány rychlostí 6 Mb/s.

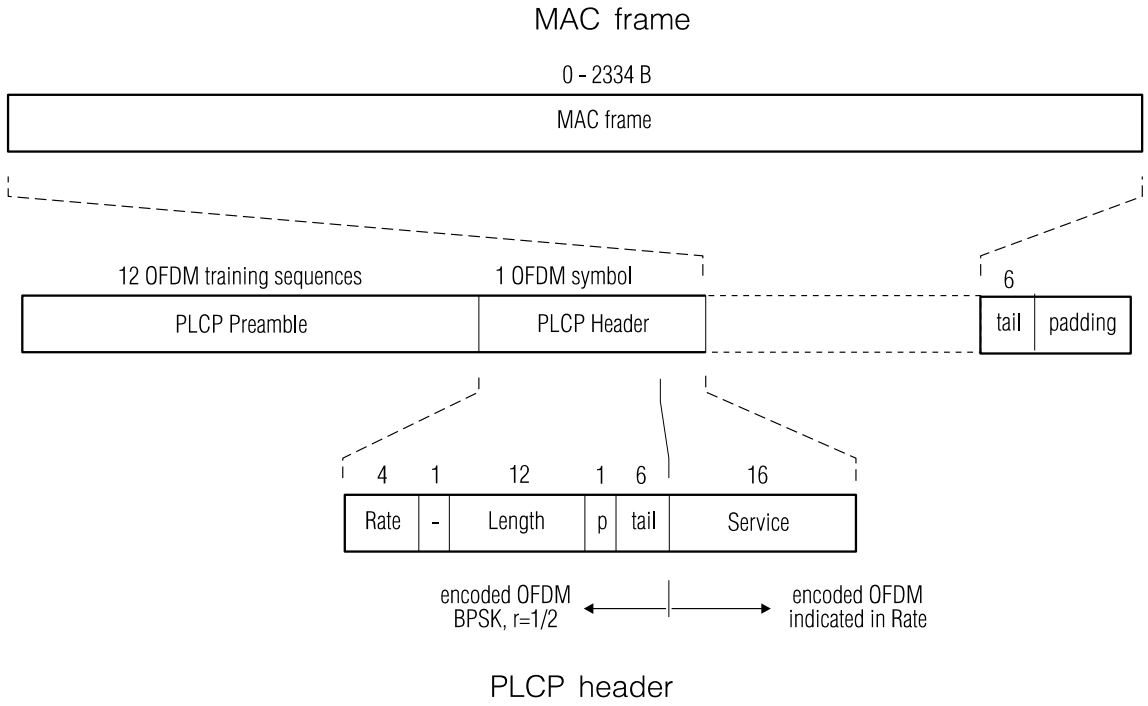
Větší šířka pásma a použití technologie OFDM dovoluje vytvářet rychlé bezdrátové lokální sítě ve složitějším prostředí budov. Větší počet nepřekrývajících se kanálů IEEE 802.11a usnadňuje návrh takových sítí a dovoluje dosáhnout mnohem vyšší přenosové kapacity.

	802.11a	802.11b	802.11
Pásmo [GHz]	2.4 - 2.4835	2.4 - 2.4835	5.15 - 5.35 5.725 - 5.825
Šířka pásma [MHz]	83.5	83.5	300
Počet nepřekrývajících se kanálů	3	3	12
Rychlost [Mb/s]	1, 2	1, 2, 5.5, 11	6, 9, 12, 18, 24, 36, 48, 54
Přenosová metoda	FHSS	DSSS	OFDM

Porovnání technologií IEEE 802.11, 802.11b a 802.11a

13.1.3 IEEE 802.11g

Snížení modulační rychlosti u OFDM, které usnadňuje budování bezdrátových sítí v kancelářském prostředí se ukázalo jako přínos. O využití výhod OFDM v původním pásmu 2.4 GHz se pokouší standard IEEE 802.11g.



Obrázek 13.23: Struktura rámce IEEE 802.11g

Klíčovým problémem standardu je zajištění kompatibility se staršími mechanismy IEEE 802.11 a IEEE 802.11b. Rámce IEEE 802.11g proto mají hlavičku (případně zkrácenou) podle IEEE 802.11b, pole Signal pak určuje, že pro vlastní přenos dat je použita technika OFDM.

Technologie IEEE 802.11g je blízko konečnému schválení, řada firem ji již ve svých zařízeních implementovala na základě předběžných verzí standardu.

Bezpečnost bezdrátových lokálních sítí

Nepříjemnou vlastností rádiových lokálních sítí, ve srovnání se sítěmi, které používají metalickou nebo optickou kabeláž, je skutečnost, že veškerou komunikaci lze v oblasti pokryté rádiovým signálem monitorovat. Probíhá-li veškerá komunikace v nechráněné formě (bez autentifikace a šifrování), můžeme v blízkosti bezdrátové lokální sítě provoz odposlechnout a/nebo do něj neoprávněně vstupovat.

Vzhledem k přístupnosti komunikačního kanálu pro odposlech a neoprávněný přístup je nutné využívat prostředků ochrany, které standardy bezdrátových sítí definují. Tyto mechanismy jsou označované jako WEP - Wireless Equivalent Privacy a jsou součástí standardu.

Ochrana WEP se opírá o použití kryptografického mechanismu RC-4. Jde o proudovou šifru, vysílací strana na základě klíče vygeneruje pomocnou bitovou posloupnost, kterou potom použije pro zakódování přenášených dat (kódérem je obvod XOR). Ve své základní podobě, dané dřívějšími omezeními na export technologií kryptografické ochrany z USA, je klíč 40-bitový, doplněný pro generování pomocné posloupnosti o 24-bitový počáteční vektor. Tento klíč (případně malý počet klíčů) je obvykle sdílem všemi stanicemi bezdrátové sítě, standardy bezdrátových lokálních sítí distribuci klíčů neřeší. Čtyřiadvacetibitový počáteční vektor má zkomplikovat dekódování, prostor hodnot je však natolik malý, že mechanismus neposkytuje dostatečnou kryptografickou ochranu. Navíc v řadě implementací není mechanismus implementován dostatečně korektně (počáteční vektory by měly být generovány náhodně), obsah přenášených dat lze často předpokládat (opakovaná pole v IP hlavičkách), mechanismus

XOR použitý pro skrytí dat nechrání proti modifikaci a odeslání odposlechnutých rámců, ... Těchto problémů se nezbavíme ani, pokud konkrétní použitá zařízení dovolují použít delší klíč.

Celkově, mechanismy zabudované ochrany WEP je nutné chápat jako ochranu před náhodným a neúmyslným odposlechem, a spolu s mechanismy autentifikace (ty nejsou součástí standardu) jako ochranu proti neoprávněnému využívání prostředků bezdrátové sítě. Proti cílenému pokusu o dekódování dat a průnik do sítě se musíme bránit jinými, podstatně účinnějšími, a hlavně korektně implementovanými, prostředky (mechanismy virtuálních privátních sítí, protokoly jako jsou IPSec, L2TP).

13.2 HiperLAN

V předcházející části přehledu technologií pro lokální bezdrátové sítě jsme se v souvislosti s technologií IEEE 802.11a, jež dovoluje v pásmu 5 GHz dosáhnout přenosové rychlosti 54 Mb/s, zmínili o technologii HiperLAN (HIgh Performance Radio LAN). Tato technologie byla vyvinuta z iniciativy evropského standardizačního institutu ETSI jako alternativa k technologii IEEE 802.11. Vývojové práce na technologii HiperLAN byly zahájeny v roce 1990, tedy zhruba ve stejné době, kdy se IEEE rozhodla vytvořit sjednocující normu pro bezdrátové technologie LAN pracující v té době v americkém pásmu ISM 900 Mhz.

Filosofie návrhu prvotní technologie HiperLAN, dnes označované jako HiperLAN/1, byla podstatně odlišná od filosofie přístupu, který zvolila IEEE. S ohledem na omezení vlivu rušení (připomeňme si, že pásmo ISM 2.4 GHz, ve kterém pracují dnes používané sítě IEEE 802.11, 802.11b a nejnověji 802.11g, je primárně určeno pro technologické aplikace v průmyslu, vědě a lékařství - ale také v našich kuchyních) se ETSI rozhodla pro rezervaci pásma v oblasti 5 GHz speciálně pro tuto službu. Technologie HiperLAN/1 byla navrhována pro použití jak v ad-hoc sítích (bez základnových stanic), tak v sítích s infrastrukturou (se základnovými stanicemi, které zprostředkují komunikaci mobilních stanic a jejich přístup k pevným sítím). Byl předpokládán klasický přenos dat, bez specifických požadavků na kvalitu přenosové služby (QoS - Quality of Service).

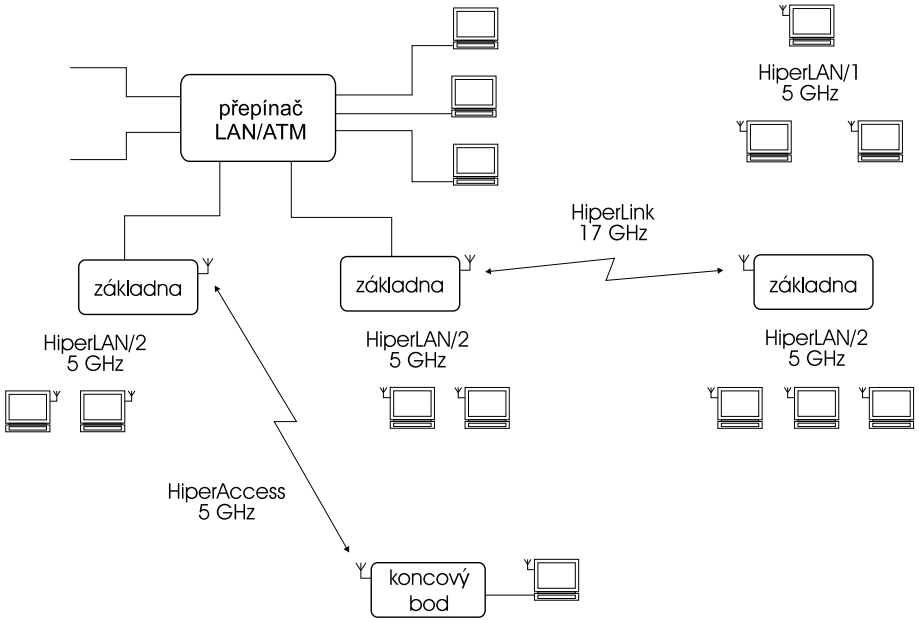
Vývoj technologie HiperLAN trval poměrně dlouho, a byl ukončen až v roce 1995, kdy se již výrazně prosazovala technologie IEEE 802.11 v pásmu 2.4 GHz. Navíc bylo zřejmé, že zadání projektu již neodpovídá požadavkům doby, tehdy se totiž bouřlivě rozvíjela technologie ATM a důraz byl kladen na zajištění kvality přenosové služby dostatečné pro přenos hovorových kanálů a případně i obrazového signálu. ETSI se proto rozhodla modifikovat zadání a přizpůsobit technologii HiperLAN tak, aby bylo možné zajistit přenos synchronních dat, ale realizovat i službu rádiového připojení pevných stanic a službu dvoubodových rádiových spojů. Jedná se ve skutečnosti o představu rodiny technologií HiperLAN (obr. 13.24). Technologie HiperLAN/2 je určena pro sítě se základnovou stanicí a její centralizovaný rozvrhovací mechanismus dovoluje zajistit diferencovanou kvalitu přenosu požadovanou různými službami. Technologie HiperLAN/3 (HiperAccess) je určena pro připojení pevných stanic k základnové stanici a je obdobou technologií FWA (Fixed Wireless Access), které dnes využívají pásma 26 a 28 GHz. Konečně, HiperLAN/4 (HiperLink) dovoluje vytvářet v pásmu 17 GHz dvoubodové spoje.

Charakter lokální komunikace mají technologie HiperLAN/1 až HiperLAN/3, které využívají pásmo 5 GHz. Pro pevné spoje HiperLAN/3 je předurčen úsek pásma 5.4 - 5.725 GHz, kde je povolen anténou vyzářený výkon 1W, úsek pásma 5.15 - 5.35 je vyhrazen pro mobilní komunikaci (HiperLAN/1 a HiperLAN/2) s výkonem do 200 mW. S ohledem na potřeby mobilních účastníků jsou pro nás zajímavé technologie HiperLAN/1 a HiperLAN/2, obě si v následujícím textu popíšeme. Globální představu využití všech technologií HiperLAN v kontextu technologií ATM

HiperLAN Type 1	HiperLAN Type 2	HiperAccess (Type 3)	HiperLink (Type 4)
Wireless LAN	Wireless ATM	Wireless Local Loop	Wireless Point-to-Point
5 GHz	5 GHz	5 GHz	17 GHz
23.5 Mbps	~ 20 Mbps	~ 20 Mbps	~ 155 Mbps

Obrázek 13.24: Rodina standardů HiperLAN

uvádí obr. 13.25.



Obrázek 13.25: Příklad použití technologií HiperLAN

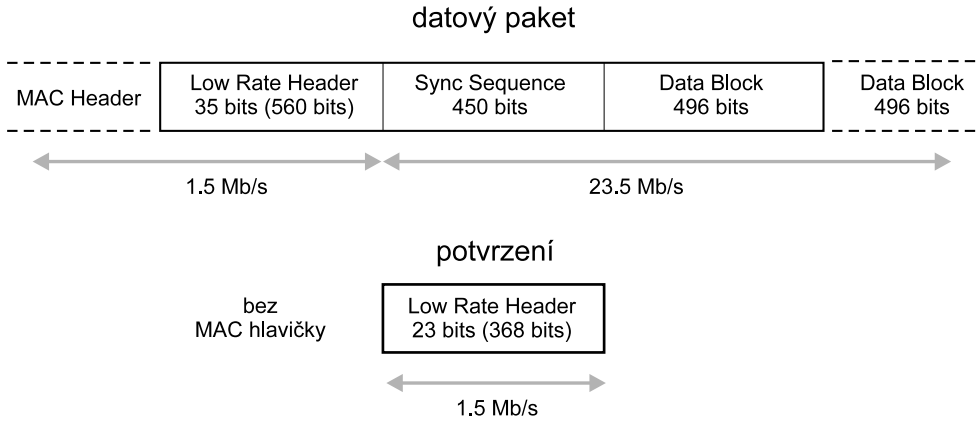
Uvědomuji si, že technologie HiperLAN mohou mnohému připadat jako papírová norma, která není schopna konkurovat dnes rozšířené IEEE 802.11b. Jde však o velice hezké metody, které zajišťují parametry technologii IEEE 802.11 nedostupné. Situace, kterou jsme viděli u technologie GSM vyvinuté ETSI, tedy souběh moderního technologického řešení a jeho širokého komerčního využití, se v případě HiperLAN bohužel neopakovala

13.2.1 HiperLAN/1

Technologie HiperLAN/1 byla navrhována s cílem zajistit přenos hovorového signálu rychlostí 32 kb/s, videosignálu rychlostí 2 Mb/s a dat rychlostí až 10 Mb/s.

HiperLAN/1 využívá pěti kanálů v úseku pásma 5.15 - 5.3 GHz. Vlastní data jsou přenášena rychlostí 23.5 Mb/s, pakety jsou pro přenos rozdělené do bloků o délce 496 bitů chráněných proti poškození kódem s možností korekce chyb BCH(31,26). Přenos dat (a řídících bloků, například potvrzení) je zahajován hlavičkou přenášenou nižší rychlostí 1.5 Mb/s. Příklad přenosu datového paketu rozděleného na bloky uvádí obr. 13.26.

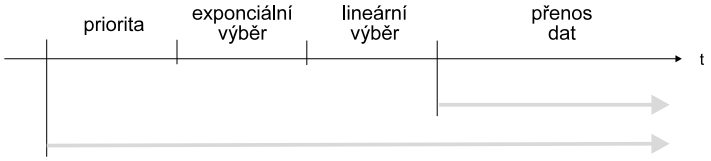
Zajímavý je plně distribuovaný mechanismus, který řídí přístup stanice ke sdílenému kanálu. Je označován jako CAC (Channel Access Control), přístupová metoda označovaná jako NPMA



Obrázek 13.26: Přenos datového paketu

(Non-preemptive Priority Multiple Access) je sice komplikovanější než metoda RTS/CTS používaná u IEEE 802.11, dává však podstatně lepší výsledky.

Stanice musí pro získání přístupu ke komunikačnímu kanálu projít úspěšně třemi fázemi soupeření. V první fázi je vyřizována priorita požadavku, k dispozici je pět úrovní priority vázaných na časový limit vyřízení požadavku. Stanice, která zjistí obsazení kanálu před tím, než jí úroveň priority dovolí vysílat, ustupuje stanicím, které kanál obsadily dříve (díky vyšší prioritě). Stanice s nejvyšší prioritou si pro další fázi generují náhodně číslo i z intervalu $< 0,11 >$, přičemž pravděpodobnost hodnoty toho, že bude vybrána hodnota i, je 0.5^i. Mechanismus minimalizuje počet stanic, které postupují do posledního kola, a to bez ohledu na počet soupeřících stanic. Poslední krok se opírá o náhodně generované číslo z intervalu $< 0,9 >$.



Obrázek 13.27: Řízení přístupu ke sdílenému kanálu - NPMA

Mechanismus přístupu je poměrně efektivní a dovoluje ve skupině stanic zajistit současný přenos 25 hovorových kanálů 32 kb/s s časovým limitem 10 ms, 25 hovorových kanálů 16 kb/s s časovým limitem 20 ms, jednoho videokanálu s časovým limitem 100 ms a asynchronního datového přenosu do 13 Mb/s. Pětiúrovňová priorita dovoluje podstatně jemnější rozlišení požadavků než je pouhé dvouúrovňové řešení dovolující u IEEE 802.11 práci základnových stanic.

Podobně jako IEEE 802.11 zahrnuje technologie HiperLAN možnost uvádět do pasivního stavu přijímač a šetřit tak baterie.

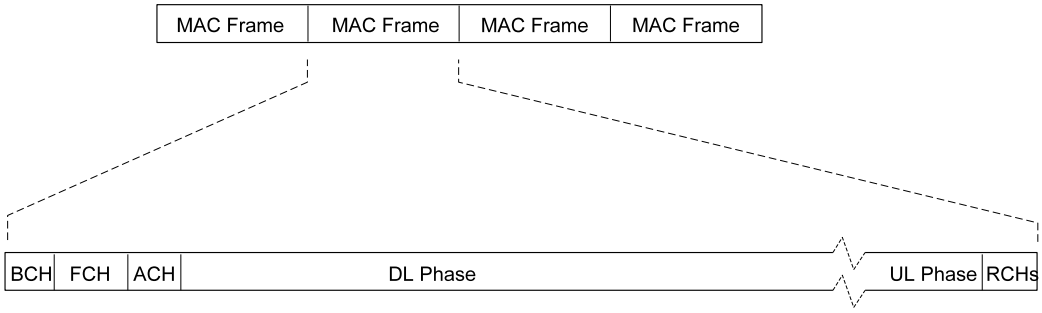
13.2.2 HiperLAN/2

Technologie HiperLAN/2 byla vyvíjena v době, kdy potřeba přenášet data s definovanými požadavky na dobu doručení se stávala nutností (i jako důsledek nasazování technologie ATM v optických sítích). Technologie používá, stejně jako IEEE 802.11a, mnohem modernější přenos technologií OFDM (Orthogonal Frequency Division Multiplex) a dovoluje po nepřekrývajících se kanálech o šířce 20 Mhz přenášet data rychlostmi od 6 Mb/s do 54 Mb/s (modulace a kódování odpovídají technologii IEEE 802.11a).

Tím ale podobnost s technologiemi IEEE 802.11 končí. Technologie HiperLAN/2 je určena

pro sítě s infrastrukturou, to má vliv na použitou metodu řízení přístupu ke komunikačnímu kanálu: přístup ke kanálu plně řídí základnová stanice.

Základnová stanice se při využívání kanálu střídá se stanicemi klientskými/mobilními, takový režim využívání jediného kanálu (ovšem, protože se jedná o OFDM, rozděleného do více subkanálů) je označován jako časový duplex - TDD (Time Division Duplex). Na kanále můžeme pozorovat posloupnost MAC rámců o délce 2ms, jejichž vnitřní členění určuje základnová stanice (obr. 13.28).



Obrázek 13.28: Rámce MAC sítě HiperLAN/2

Struktura MAC rámce zahrnuje kanál BCH (Broacast Channel) pro některé řídící informace (například informace o začátku polí FCH a RCH, informace o vysílacích úrovních, informace podporující hospodaření energií v mobilních stanicích) vysílané broadcastem všem mobilním stanicím, vysílačem je základnová stanice.

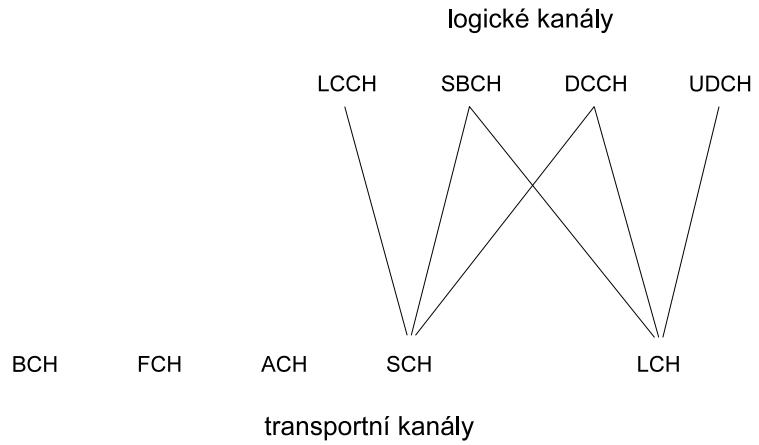
Kanál FCH (Frame control CHannel) doplňuje informace o rozdělení kapacity rámce na prostor, který využívá základnová stanice (DL - DownLink), a prostor, o který se dělí stanice mobilní (UL - UpLink).

V kanále ACH (Access feedback CHannel) potvrzuje základnová stanice příjem požadavků mobilních stanic, kanál RCH je posloupností kolizních slotů, ve kterých si mobilní stanice mohou vyžádat pozornost základnové stanice.

Přenos dat po kanálech DL a UL je zajišťován posloupností buněk o délce 53 oktetů s místem pro 48 oktetů přenášených dat (zde HiperLAN/2 zřetelně vychází z technologie ATM), tyto buňky jsou označovány jako U-PDU (User Protocol Data Unit) a kanál tvořený těmito buňkami je označován jako LCH (Long transport CHannel). Pro přenos řídících informací, kde by buňka o délce 53 oktetů nebyla efektivně využita, jsou k dispozici devítioktetové buňky C-PDU (Control Protocol Data Unit). Kanál tvořený buňkami C-PDU je označován jako SCH (Short transport CHannel).

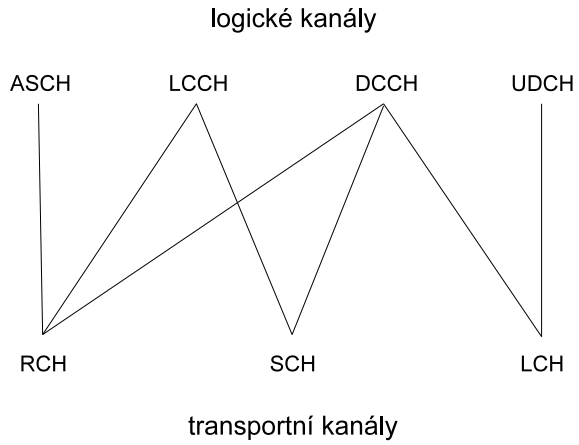
Přístup k přenosovému kanálu je téměř deterministický, základnová stanice se stanicemi mobilními soupeřit nemusí, mobilní stanice soupeří pouze ve slotech, které pro soupeření vyhradí základnová stanice (RCH). Počet těchto slotů základnová stanice upravuje podle okamžité aktivity mobilních stanic, předpokládána je snaha základnové stanice o omezení kolizí a z toho vyplývajících přídavných zpoždění.

Kanály prostoru DownLink jsou využívány pro vlastní přenos dat (UDCH - User Data CHannel), potvrzovací informace linkové vrstvy (LCCH - Link Control CHannel), řízení komunikace mobilní stanice se stanicí základnovou (DCCH - Dedicated Control Channel) a pro distribuci informací využívaných více mobilními stanicemi (SBCH - Slow Broadcast CHannel). Využívání standardních buněk U-PDU a krátkých buněk C-PDU těmito *logickými kanály* uvádí obr. 13.29.



Obrázek 13.29: Využití DownLink prostoru

Kanály prostoru UpLink nezahrnují logické kanály SBCH, navíc zde najdeme kanály dovolující předávat požadavky mobilních zařízení na nová spojení (ASCH - Association control CHannel) - například na vytvoření nového hovorového kanálu. Obr. 13.24 uvádí využití buněk U-PDU a C-PDU v logických kanálech prostoru UpLink.



Obrázek 13.30: Využití UpLink prostoru

Poměrně složité mechanismy dovolují rozdělit celkovou kapacitu přenosového kanálu buňky mezi logická spojení charakterizovaná odlišnými požadavky na přenos, základnová stanice si udržuje podrobný přehled o okamžitých požadavcích všech přihlášených stanic na přenos dat. Mechanismem lze podpořit technologie QoS vyšších vrstev síťové architektury (ATM Q.2931,IEEE 802.1p, RSVP, DiffServ).

Vedle zajímavého (a dokonalého) mechanismu rozdělování kapacity kanálu disponuje technologie HiperLAN/2 mechanismem pro automatickou volbu kmitočtu, na kterém základnová stanice pracuje, mechanismem předávání mobilních stanic mezi stanicemi základnovými (handover), mechanismem řízení spotřeby a podporou kryptografické ochrany. HiperLAN předpokládá podporu autentizačních mechanismů dalšími prostředky standardizovanými v rozsáhlých sítích (RADIUS).

Porovnání technologií IEEE 802.11 a HiperLAN

Na závěr této základní informace o systému HiperLAN/2 si můžeme uvést porovnání jeho vlastností s technologiemi sítí IEEE 802.11.

	802.11	802.11b	802.11a
Pásmo	2.4 GHz	2.4 GHz	5 GHz
Fyzická rychlost	2 Mb/s	11 Mb/s	54 Mb/s
Efektivní rychlost	1.2 Mb/s	5 Mb/s	32 Mb/s
Řízení přístupu	CSMA/CA	CSMA/CA	CSMA/CA
Linková spojení	-	-	-
Multicasting	ano	ano	ano
QoS	PCF	PCF	PCF
Volba kmitočtu	FHSS/pevný CDMA	pevný CDMA	pevný OFDM
Autentizace	-	-	-
Šifrování	RC-4	RC-4	RC-4
Podpora LAN	Ethernet	Ethernet	Ethernet
Správa	802.11 MIB	802.11 MIB	802.11 MIB
Adaptace na kvalitu	-	-	-

	HiperLAN/2
Pásmo	5 GHz
Fyzická rychlost	54 Mb/s
Efektivní rychlost	32 Mb/s
Řízení přístupu	centralizované
Linková spojení	ano
Multicasting	ano
QoS	ano
Volba kmitočtu	aut. volba OFDM
Autentizace	ano
Šifrování	DES,3DES
Podpora LAN	Ethernet/IP/ATM/UMTS
Správa	HiperLAN/2 MIB
Adaptace na kvalitu	ano

Přestože technologie HiperLAN vypadá v současné době poněkud exoticky, její význam se může projevit ve spojení s technologiemi poskytujícími pomalejší datové kanály na rozsáhlejších územích, tedy například pro lokální posílení přenosových kapacit sítí UMTS. Centralizovaná správa přenosové kapacity není specialitou technologie HiperLAN/2, obdobná řešení najdeme u technologií poskytující rádiové připojení pevným účastníkům v kmitočtových pásmech 26 a 28 GHz a vyšších (FWA - Fixed Wireless Access).

13.3 Bluetooth

Zajímavou oblastí lokálních komunikací jsou technologie dovolující propojení zařízení na krátké vzdálenosti bez nutnosti vytvářet infrastrukturu. Nejznámější takovou technologií je Bluetooth, standard vytvořený skupinou firem (Bluetooth SIG) vytvořené fy. Ericson, obecněji technologie těchto sítí, označovaných jako bezdrátové lokální sítě (WPAN - Wireless Personal Area Network) pokrývá standard IEEE 802.15.

Bluetooth pracuje v ISM pásmu 2.4 -2.4835 GHz ve kterém vytváří 79 kanálů s odstupem 1 Mhz (využívaná šířka pásma je 220 kHz) v režimu frekvenčního rozprostření pásma (FHSS), ke změně frekvence podle zvolené posloupnosti dochází po odvysílání každého rámce, při délce rámce 625 μs je to 1600 přechodů za vteřinu. Technologie tak dovoluje současnou práci více sítí na omezeném prostoru, k interferenci mezi sítěmi dochází pouze tehdy, pokud zařízení sítí používající různé a navíc i fázově se posouvající sekvence kmitočtů použijí stejný kanál.

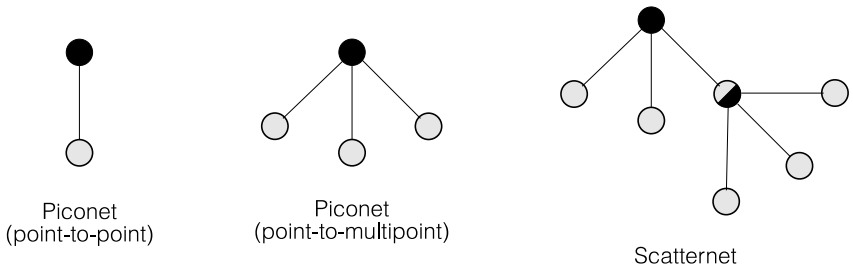
Bluetooth byl navržen pro propojení zařízení na malou vzdálenost (jednotky metrů až desítky metrů), tomu odpovídají i limity vyzářeného výkonu pro tři výkonové třídy:

1 - 100 mW,
2 - 2.5 mW,
3 - 1 mW.

Bluetooth je obvykle využíván pro výstavbu dvoubodových spojů, je však vybaven konfiguračními mechanismy dovolujícími vytvářet sítě typu Master/Slave, označované jako *piconet*.

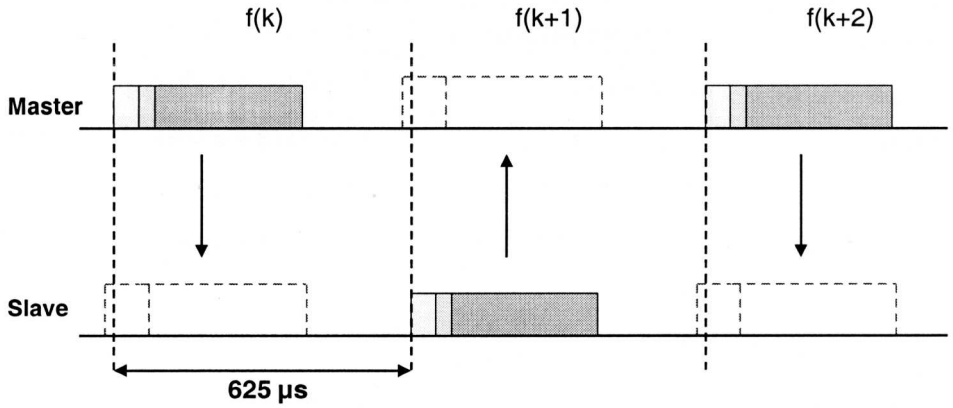
V jedné síti piconet může pracovat vedle řídící stanice nejvýše sedm stanic podřízených, pro jejich adresaci stačí tříbitová adresa. Vedle takových aktivních stanic může řídící stanice registrovat až 256 stanic, které nejsou aktivní (jsou označovány jako zaparkované), adresovaných osmi bity. Přechod zaparkované stanice do aktivního režimu může být velmi rychlý, v řádu milisekund. Stanice systému Bluetooth jsou, vedle krátkých pracovních adres, jednoznačně identifikovány 48-bitovou adresou.

V případě potřeby je možné malé sítě piconet propojovat mosty, ty kombinují funkci typu Master s funkcí typu Slave, nebo mosty, které jsou ve více sítích ve funkci Slave. Složitější sítě takto budované je označováno jako *scatternet* (obr. 13.31).

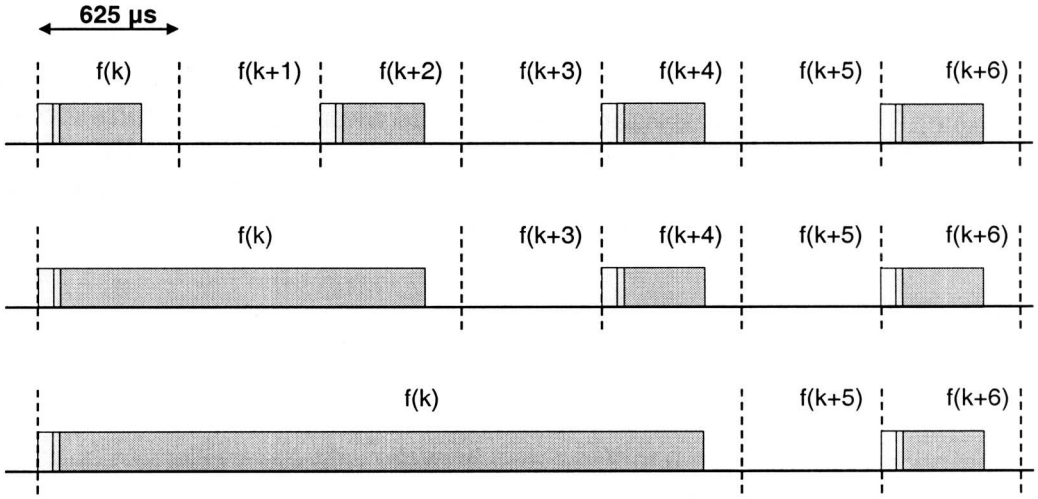


Obrázek 13.31: Konfigurace sítí Bluetooth

Přístup ke komunikačnímu kanálu je označován jako časový duplex (TDD - Time Division Duplex), řídící stanice se ve vysílání střídá vždy s jednou ze stanic podřízených na principu výzvy. Řídící stanice smí zahajovat vysílání v lichých rámcích o délce 625 μs, podřízené stanice v rámcich sudých (obr. 13.33).



Obrázek 13.32: Časový multiplex



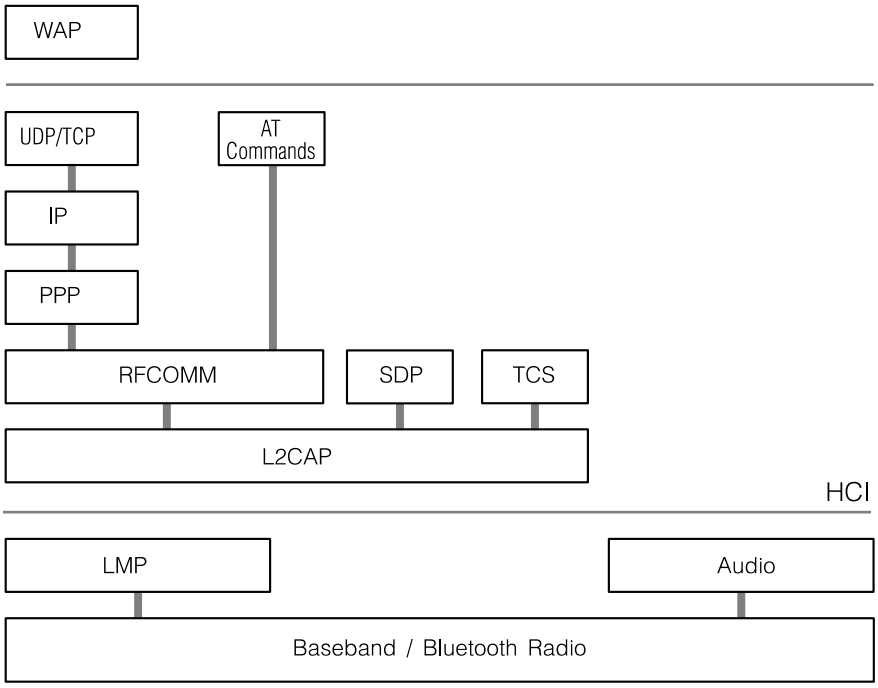
Obrázek 13.33: Časový multiplex - prodloužení rámce

Pokud stanice potřebuje delší čas pro odvysílání dat, může své vysílání prodloužit o dva nebo čtyři časové sloty 625 μs.

Komunikační kanál sítě Bluetooth má přenosovou rychlost 1 Mb/s (včetně režie), lze ho využít pro vytvoření až tří obousměrných synchronních kanálů o rychlosti 64 kb/s, zbylou kapacitu lze využít pro asynchronní přenos dat. U symetrického dvoubodového kanálu lze dosáhnout přenosové rychlosti 433.9 kb/s, při nesymetrickém využívání kanálu se lze dostat na 723.2/57.6 kb/s. Při práci více stanic v síti piconet se pochopitelně o kapacitu kanálu stanice dělí.

Detekci a korekci chyb podporují mechanismy opírající se o trojí opakování bitů v hlavičce a rámcích hovorových kanálů (1/3 rate FEC), Hammingův kód (15,10) s generačním polynomem $g(x) = (x+1)(x^4+x+1)$ (2/3 rate FEC), osmibitové zajištění dat CRC kódem a o negativní potvrzování (ACK/NAK).

Součástí technologie Bluetoooth je i programové vybavení, které zahrnuje vytváření kanálů pro přenos hovoru a dat, mechanismy kryptografické ochrany a rozhraní klienta (obr. 13.34).



Obrázek 13.34: Architektura komunikačních protokolů a rozhraní

Funkce rádiového transceiveru, kódování dat při přenosu, formátování dat pro přenos a ochrana proti chybám jsou součástí vrstvy označované jako *Baseband/Bluetooth Radio*. Vyhledávání prvků v ad-hoc architektuře, navazování spojení, autentizace a přístup ke komunikačnímu kanálu jsou funkce správy linkové vrstvy *LMP*. Tyto funkce jsou obvykle realizovány v obvodech Bluetooth, funkce nad rozhraním *HCI* (Host Controller Interface) jsou obvykle implementovány na procesoru, k němuž je Bluetooth připojen.

Vyšší vrstvy technologie, zahrnují protokoly linkové vrstvy pro přenos dat a vyšší protokoly (pro TCP/IP). Architektura je doplněna o kryptografické zabezpečení a poskytuje podporu pro protokol přístupu k webovým službám WAP (Wireless Access Protocol).

14. Komunikační protokoly

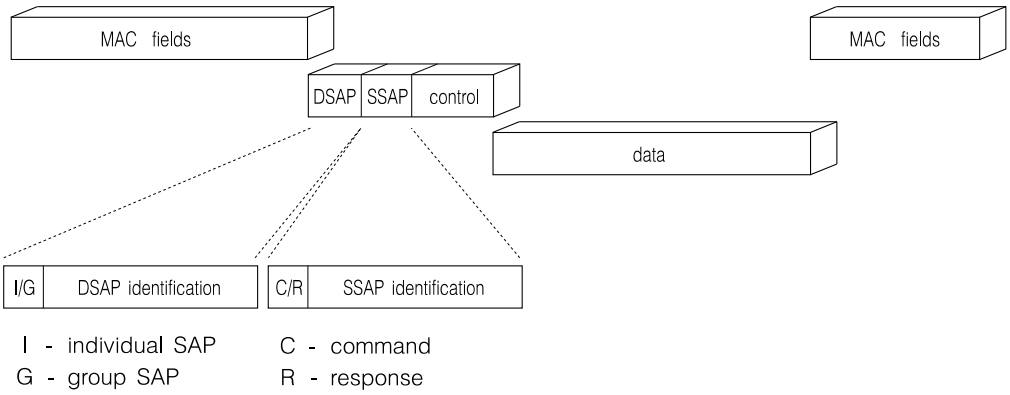
Síťová podpora aplikací musí být opřena o systém komunikačních protokolů, které zajistí předání dat v prostředí lokální sítě. Patří sem protokoly, které zajišťují *potvrzování* předávaných dat (na úrovni linkové nebo síťové vrstvy) a *směrování* (na úrovni síťové vrstvy). Jako příklad *protokolu linkové vrstvy* si uvedeme protokol IEEE 802.2. Protokolů *síťové vrstvy* je dnes používáno vedle sebe několik, v tomto textu si uvedeme základní principy protokolů NetBIOS, IPX/SPX a TCP/IP. Nepůjdeme do podrobností jejich popisu, všimneme si spíše jejich začlenění do programového vybavení lokálních sítí.

14.1 Linkové protokoly – rozhraní IEEE 802.2

Standardy lokálních sítí definují sdílení média, jednotlivé techniky jsme si popsali v předchozích kapitolách. Kromě toho definují protokol, který jednak podporuje potvrzovací schémata, jednak umožňuje současný provoz více různých vyšších protokolů (NetBIOS, IPX/SPX, TCP/IP). Protokol jednotný pro všechny technologie uvádí specifikace *IEEE 802.2 – Logical Link Control* (LLC), později modifikovaná jako standard ISO 8802/2. Vrstva logického řízení spoje zajišťuje tři úrovně služeb:

- datagramovou službu bez potvrzování (*Unacknowledged Connection-less Service*),
- logické spojení (*Connection-Mode Service*) a
- datagramovou službu s potvrzováním (*Acknowledged Connection-less Service*).

Funkce protokolů LLC je podporována služebními informacemi v rámcích *PDU* (Protocol Data Unit), jejich formát a příklad uložení v rámci Ethernetu uvádí obr. 14.1, seznam typů rámců uvádí obr. 14.2.



Obrázek 14.1: Formát rámců PDU protokolů LLC

Protokoly LLC (konkrétně u logického spojení) vycházejí z principů, používaných protokoly s modulárním potvrzováním jako jsou X.25 LAPB nebo ISDN LAPD. Pole *DSAP* (Destination Service Access Point) a *SSAP* (Source Service Access Point) dovolují multiplexovat na jednom linkovém spojení provoz pod různými síťovými protokoly. Příklady konkrétních protokolů a jim příslušející hodnoty polí DSAP a SSAP jsou:

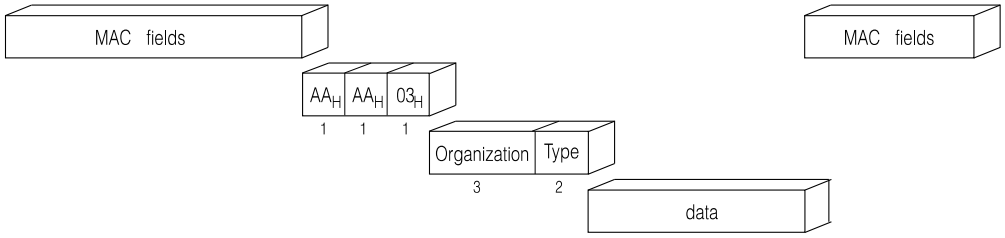
04	- SNA Path Control (individual)
AA	- SNAP
E0	- Novell Netware
F0	- IBM NetBIOS
FE	- ISO Network Layer

LLC1	Unnumbered			
	UI	unnumbered information	C	data exchange
	XID	exchange identification	C/R	operation type, window size
	TEST	test	C/R	loopback test
LLC2	Information			
	I	information	C/R	data exchange
	Supervisory			
	RR	receive ready	C/R	positive acknowledgement
	RNR	receive not ready	C/R	positive acknowledgement
	REJ	reject	C/R	negative acknowledgement
	Unnumbered			
	SABME	set ABM extended	C	connection request
	DISC	disconnect	C	terminate connection
	UA	unnumbered acknowledgement	R	acknowledgement
	DM	disconnect mode	R	connection rejection
	FRMR	frame reject	R	frame rejection
LLC3	Unnumbered			
	AC	acknowledged information	C/R	data exchange

Obrázek 14.2: Typy PDU protokolů LLC

Pole Control o délce jednoho nebo dvou oktetů (pro číslování modulo 128) určuje typ rámce a případně obsahuje číslo vysílaného a očekávaného rámce.

Určitou zajímavostí je přístupové místo SAP AA_H , označované jako SNAP (Subnetwork Service Access Point). To dovoluje uložit v poli dat strukturu, odpovídající libovolnému protokolu identifikovatelnému v poli Type formátu DIX Ethernet, přenášené bloky nejsou samozřejmě potvrzovány (jsou přenášeny v rámcích UI – Unnumbered Information). Hlavičku SNAP, která kromě dvouznakového pole Type zahrnuje i tříznakový kód organizace, uvádí obr. 14.3.

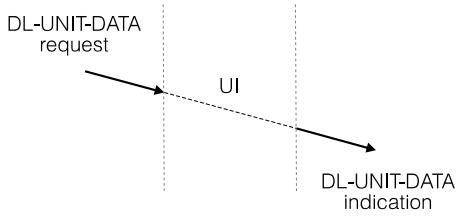


Obrázek 14.3: Rámce protokolu SNAP

LLC1 – Datagramová služba bez potvrzování (Unacknowledge Connection-less Service)

Datagramová služba bez potvrzování je velmi jednoduchá. Nezajisťuje bezpečné dodání paketu příjemci ani neinformuje odesílatele o nedodání paketu (např. proto, že příjemce paketu nebyl aktivní). Jednotlivé odesílané pakety nejsou vzájemně svázány, síť nezajišťuje jejich dodání v pořadí, ve kterém byly vyslány. Jeden paket lze odeslat jedinému určenému příjemci (*Point-to-Point*), skupině příjemců (*Multicast*) nebo všem aktivním uživatelům (*Broadcast*).

Datagramová služba se opírá o pouhá dvě primitiva, jejich použití při výměně jednoho paketu mezi odesílatelem a příjemcem ilustruje obr. 14.4.



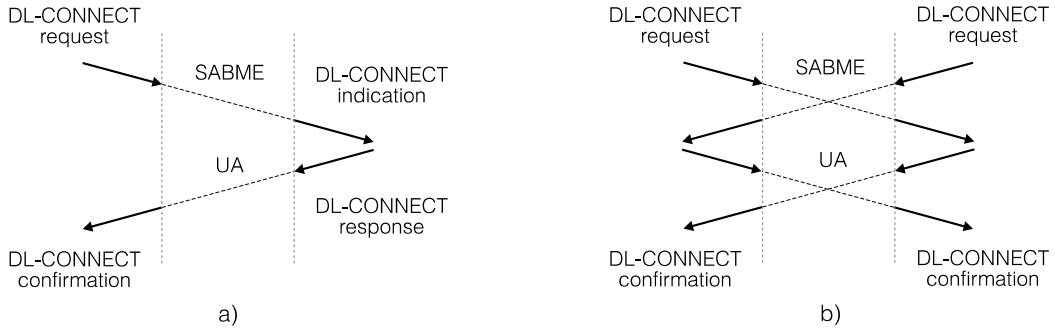
Obrázek 14.4: Nepotvrzovaný datagram

Odeslání dat zajišťuje primitiva DL-DATA.request, jejím protějškem na straně příjemce je DL-DATA.indication. Data jsou předávána mezi přístupovými místy obou účastníků nečíslovaným informačním rámcem UI. U technologií, které to dovolují, lze využít prioritní mechanismus.

Nepotvrzovaná datagramová služba je nejjednodušší službou zajišťovanou sítí a je postačující, jestliže aplikace nevyžadují spolehlivé doručení veškerých dat, nebo jestliže je potřebné potvrzování realizováno na vyšší protokolové úrovni (v transportní nebo aplikační vrstvě). Přes minimální zabezpečení přenášených dat má nepotvrzovaná datagramová služba široké užití. Je vhodná pro sběr dat v měřících a řídících systémech, kde je typická periodická distribuce dat a výpadek jednoho údaje je brzy nahrazen údajem novým. Podobná je situace u rozesílání všeobecných informací a informací o čase. Pro řadu aplikací je zpoždění způsobené potvrzováním nepřijatelné a nepotvrzovaná datagramová služba je jedinou možnou. Mezi takové aplikace patří přenos hovorového signálu a rychlá telemetrie.

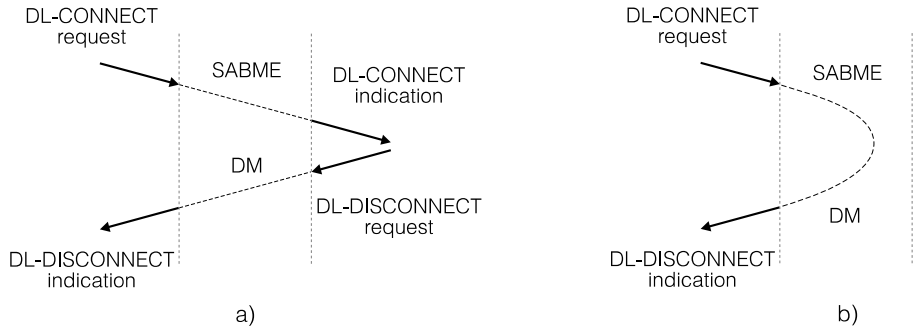
LLC2 – Logické spojení (Connection-Mode Service)

Služba dovoluje vytvářet, využívat a rušit logická spojení mezi dvěma komunikujícími účastníky. Při navazování spojení se oba komunikující účastníci dohodnou na přenosu dat a na obou stranách je inicializován mechanismus sledující spojení. Ten během vlastního přenosu zajišťuje, že všechna odeslaná data budou předána protějšku, a že budou předána v pořadí, ve kterém byla odeslána. V případě poruchy je odesílateli indikována neschopnost sítě předat data příjemci. Pro *navázání spojení* slouží primitivy DL-CONNECT, navázání spojení podporují rámce SABME a UA. Typické situace, ke kterým může při navazování spojení dojít, uvádí obr. 14.5 a obr. 14.6.



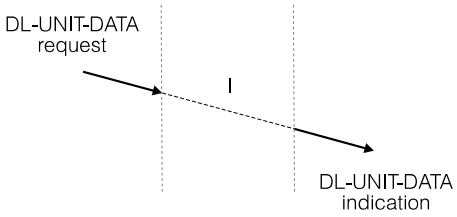
Obrázek 14.5: úspěšné navázání logického spoje

Spojení je navazováno mezi přístupovými místy obou účastníků. Pokud to technologie dovoluje, mohou si účastníci při otevírání spojení dohodnout využívanou prioritu. Tou je hodnota v odpovědi, která může být nejvýše rovna hodnotě v požadavku. Při současné žádosti o navázání spojení je spojení navázáno s nižší z obou požadovaných priorit.



Obrázek 14.6: Neúspěšné navázání logického spoje

Protějšek může žádost odmítnout primitivou DL-DISCONNECT. K odmítnutí spojení může dojít i pro neschopnost sítě navázat spojení se zadaným protějškem (například proto, že protistanice není aktivní). Další důvody odmítnutí mohou mít lokální charakter (nedostatek prostoru v tabulkách, porucha síťového adaptéru). O důvodu odmítnutí je účastník navazující spojení informován.



Obrázek 14.7: Přenos dat

Po navázání spojení mohou oba účastníci zahájit *přenos dat* (obr. 14.7). Přenos dat zajišťují primitivy DL-DATA rámci typu I. Potvrzování nutné pro zajištění bezpečného sekvenčního předání dat se opírá o modulární číslování rámců. Je-li třeba, lze přenos dat doplnit o *řízení toku* podporované primitivami DL-CONNECTION-FLOWCONTROL. Během přenosu dat může dojít k situacím, kdy je třeba už běžící spojení uvést do *počátečního stavu* (Reset), aniž bychom ho rozpojili. Tuto funkci zajišťují primitivy DL-RESET. O reset může požádat kterýkoliv z partnerů, ale také síť, například při ztrátě synchronizace v potvrzovacím schématu.

O *rozpojení fungujícího spojení* může požádat kterýkoliv z komunikujících partnerů nebo síť. Aplikace o rozpojení žádá, chce-li komunikaci ukončit normálně nebo při nějaké výjimečné situaci. Síť o ukončení spojení žádá při zjištění závady adaptéru nebo média. Při neočekávaném rozpojení může dojít ke ztrátě přenášených dat. Možné situace odpovídající zrušení spojení z iniciativy aplikace a z iniciativy sítě uvádí obr. 14.8.

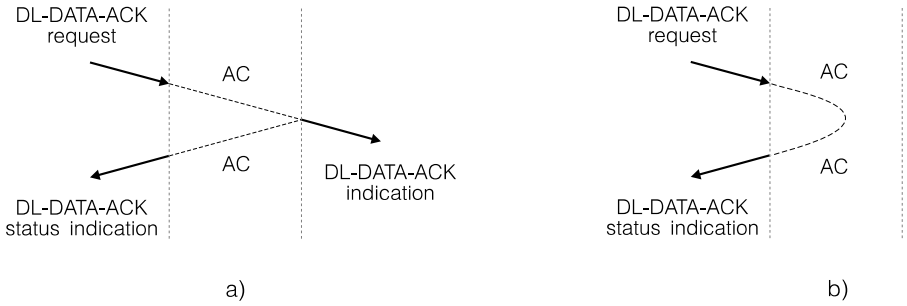
Obrázek 14.8: Rozpojení logického spoje

LLC3 – Potvrzovaná datagramová služba (Acknowledged Connection-less Service)

Potvrzovaná datagramová služba zahrnuje dvě obdobné, ale vzájemně nezávislé služby. Prvá ze služeb, DL-DATA-ACK, zabezpečuje potvrzovaný přenos dat. Druhá služba, DL-REPLY, dovoluje požádat vzdálenou aplikaci o předem připravená data.

DL-DATA-ACK

Jeden z komunikujících partnerů odesílá primitivou DL-DATA-ACK.request datagram, který je protistanici předán primitivou DL-DATA-ACK.indication. Správné předání datagramu AC vzdálené aplikaci je potvrzeno primitivou DL-DATA-ACK-STATUS.indication. Možné situace při předávání datagramu uvádí obr. 14.9.

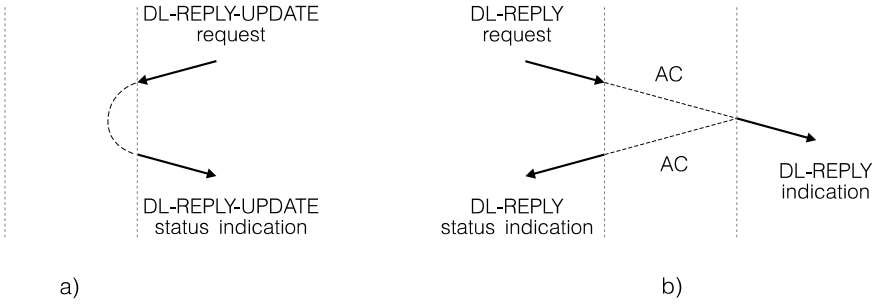


Obrázek 14.9: Služba DL-DATA-ACK

Služba DL-DATA-ACK dovoluje vyslat další datagram až po potvrzení datagramu předchozího a má tedy menší efektivitu než logické spojení.

DL-REPLY

Služba předává data mezi dvěma aplikacemi, z nichž jedna nejdříve data pro přenos připraví primitivou DL-REPLY-UPDATE a druhá si je později převezme primitivou DL-REPLY. Obě fáze komunikace uvádí obr. 14.10.



Obrázek 14.10: Služba DL-REPLY

14.2 Síťové protokoly

Bloky dat předávané mezi koncovými účastníky obvykle označujeme jako pakety. V jejich formátech najdeme síťové adresy obou koncových účastníků a informace potřebné pro potvrzování a případně i řízení toku. Pakety mohou být předávány jako zcela nezávislé *datagramy*, nebo jako součást souvislejší komunikace po *virtuálním kanále*. V následujícím textu si uvedeme nejdůležitější vlastnosti síťových protokolů, se kterými se můžeme setkat v lokálních sítích – NetBIOS, IPX/SPX a TCP/IP.

14.2.1 NetBIOS, NetBEUI

Nejstarším síťovým protokolem určeným specificky pro prostředí lokální sítě (kde existuje možnost, aby rámec odeslaný jednou ze stanic sítě byl přijat všemi ostatními stanicemi) je *NetBIOS* navržený firmou IBM. Rozšíření doznal hlavně díky svému začlenění jako základní komunikační protokol do struktury sítě MS-Net. Aplikace se pro NetBIOS identifikuje jménem a protokol pro správu jmen NetBIOSu se stará o jedinečnost tohoto jména v síti. Adresace nezávisle předávaných datagramů i adresace nutná pro otevření virtuálních kanálů se o jména opírá. NetBIOS byl u sítí IBM přímo vázán na ovladač komunikačního řadiče, stejným způsobem je implementován např. v LAN Manageru, kde je rozšířen, doplněn uživatelsky příjemnějším rozhraním a pojmenován *NetBEUI* (NetBIOS Extended User Interface). U sítí, které nejsou na NetBIOSu životně závislé (Novell Netware, Banyan VINES, UNIX), bývají jeho funkce zpřístupněny jako nadstavba protokolů jiných (IPX/SPX, VIP/VTP nebo TCP/IP) – mluvíme obvykle o *emulátorech NetBIOSu*.

Rozhraní NetBIOSu, které mají aplikace k dispozici, tvoří čtyři skupiny funkcí – správa tabulek jmen, datagramová služba, služba virtuálních kanálů a pomocné funkce.

Aplikace musí pro vyžádání funkce NetBIOSu připravit požadavkový blok *NCB* (Network Control Block), ve kterém zadává parametry volání – jména, číslo logického kanálu, adresu a délku předávaných dat, časové limity pro vyslání a příjem. Požadavek předá aplikace NetBIOSu voláním systému (voláním programového přerušení $5C_H$). Po předání požadavku může být aplikace pokračovat ve výpočtu. Ukončení požadavku může aplikace aktivně testovat nebo lze ukončením požadavku aktivovat dokončovací rutinu.

Jak jsme již uvedli, komunikující aplikace (nebo jejich komunikační kanály) jsou identifikovány jmény, která mají délku šestnáct znaků. Jméno může být buď individuální (a jedinečné v síti) nebo skupinové. Stanice si udržují tabulky jmen, pro jejich pro jejich údržbu mají k dispozici primitiva:

ADD NAME	- přidání jména
ADD GROUP NAME	- přidání skupinového jména
DELETE NAME	- vymazání jména
FIND NAME	- vyhledání jména

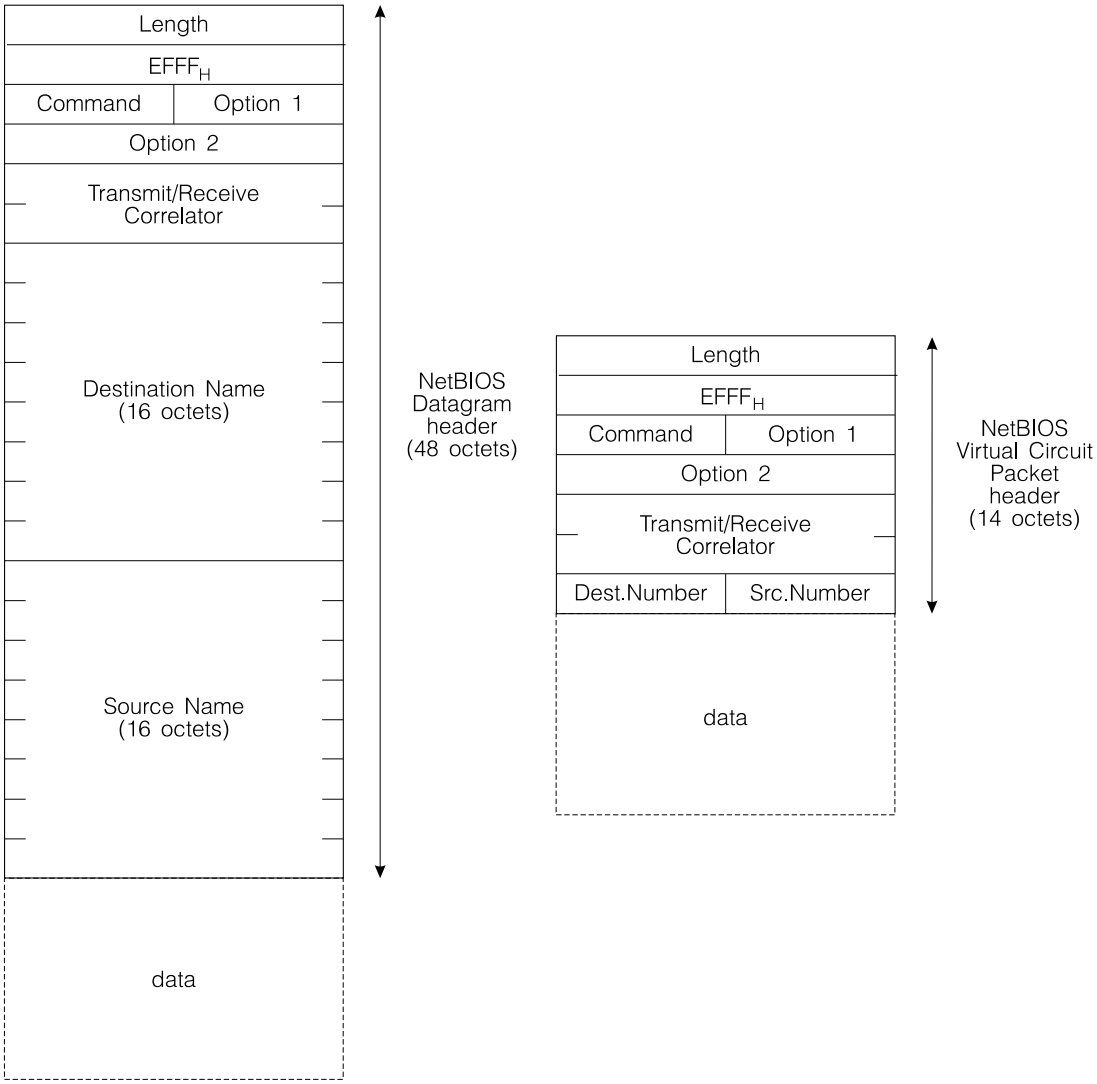
Základní služba, kterou NetBIOS podporuje, je *datagramová služba* (u protokolu NetBEUI jí odpovídá služba *MailSlot*) dovolující předání zprávy o délce do 512 B jednomu adresátovi nebo libovolné stanici na síti, která takovou zprávu očekává (*Broadcast*). Pro práci s datagramy slouží primitiva:

SEND DATAGRAM	- odeslání datagramu
SEND BROADCAST DATAGRAM	- odeslání datagramu broadcastem
RECEIVE DATAGRAM	- příjem datagramu
RECEIVE BROADCAST DATAGRAM	- příjem datagramu broadcastem

Virtuální kanály (v terminologii NetBIOSu je používán termín *relace*, u NetBEUI jim odpovídá služba *Named Pipes*) dovolují přenášet zprávy o délce 131071 znaků, které jsou při přenosu děleny do paketů. Komunikace je podporována primitivami:

CALL	- aktivní otevření relace (na straně klienta)
LISTEN	- pasivní otevření relace (na straně serveru)
SEND (NO ACK)	- odeslání zprávy (bez vyžádaného potvrzení)
RECEIVE (ANY)	- příjem zprávy (příslušející libovolné relaci)
HANGUP	- ukončení relace
SESSION STATUS	- zjištění stavu kanálu

Pomocné funkce dovolují inicializovat NetBIOS (RESET), zjistit stav komunikačního rozhraní (ADAPTER STATUS) a zrušit dřívější požadavek (CANCEL).



Obrázek 14.11: Pakety protokolu NetBIOS

Funkce NetBIOSu jsou podporovány dvaadvaceti typy předávaných paketů, formát uvádí obr. 14.11. Ty jsou identifikovány v poli Command, pole Transmit/Receive Correlator umožňuje svázat příkazy s odpověďmi. Pole Option1 a Option2 jsou využívána různě u různých typů paketů. Hlavičky paketů podporujících správu tabulek jmen a datagramovou službu obsahují šestnáctiznaková jména, hlavičky paketů virtuálních kanálů obsahují logická čísla kanálů.

14.2.2 IPX/SPX

U nás nejrozšířenější operační systém pro lokální sítě Novell Netware se opírá o protokoly *IPX/SPX* (Internet Packet eXchange/Sequential Packet eXchange). Protokoly vycházejí ze systému *XNS* (Xerox Network System), který byl alternativou firmy Xerox k protokolům TCP/IP. Protokol IPX zajišťuje přenos paketů bez potvrzování mezi aplikacemi připojenými na zvolená připojovací místa (*Socket*). Protokol SPX je nadstavbou IPX, zajišťuje potvrzování přenesených paketů a umožňuje práci více aplikačních procesů na jednom portu.

Výhodou protokolů IPX/SPX je adresace, která vychází z adresace stanic v lokální síti (Ethernet byl vyvinut v laboratořích firmy Xerox). Adresa je v IPX definována jako dvojice (32-bitová adresa sítě, 48-bitová adresa stanice), to zjednodušuje práci směrovačů ale i stanic v síti. Podstatnou nevýhodou IPX/SPX je skutečnost, že adresu sítě definuje správce konkrétní sítě. Chybějící kooperace v přidělování adres v principu znemožňuje vzájemné propojení sítí pod protokoly IPX/SPX mezi sebou.

Rozhraní protokolů IPX/SPX tvoří funkce, dovolující otevřít a uzavřít přístupová místa, zjistit nejvýhodnější směrovač na cestě k adresátovi, odeslat a přijmout IPX paket. Funkce související s protokolem SPX dovolují pasivně a aktivně otevřít virtuální kanál, vyslat a přijmout SPX paket (na rozdíl od NetBIOSu se o rozdělení delší zprávy do paketů stará aplikace) a po ukončení komunikace virtuální kanál uzavřít. Vedle funkcí, které slouží vlastnímu přenosu dat, je součástí rozhraní i řada funkcí pomocných.

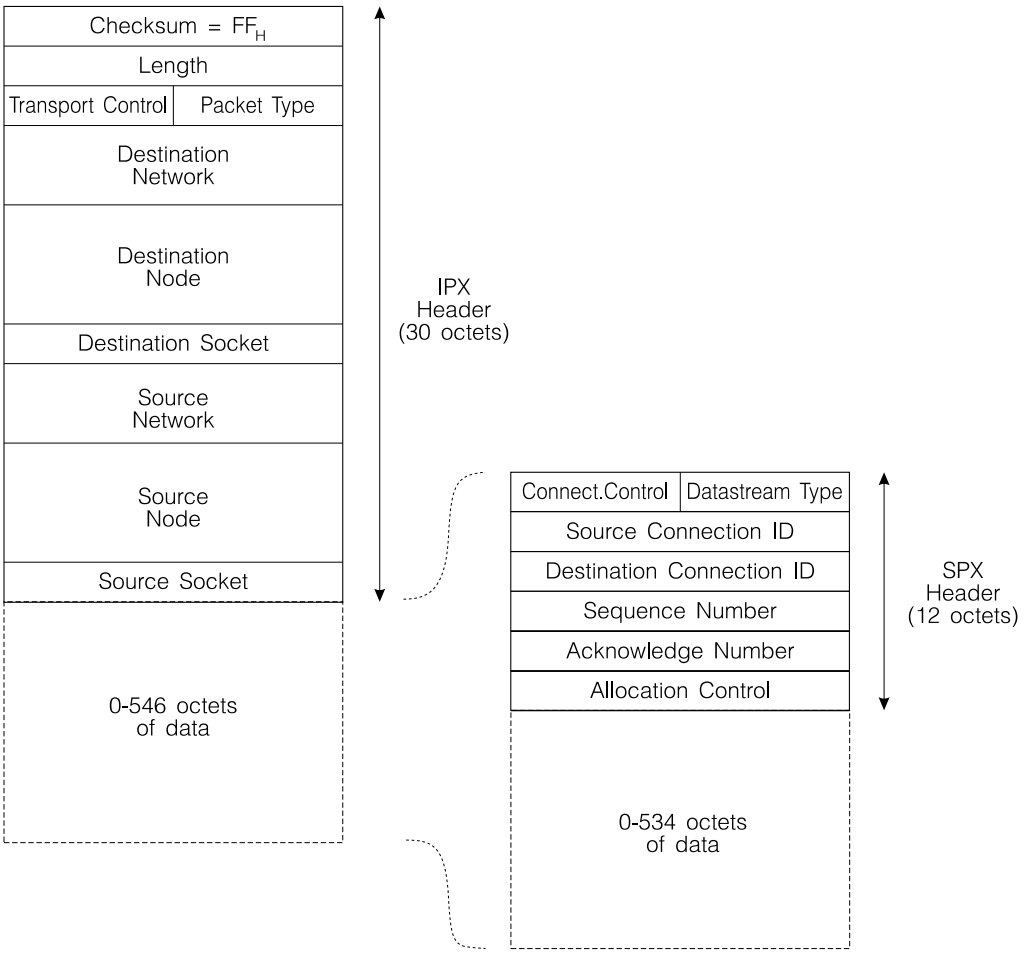
Komunikační funkce IPX/SPX vyžadují, aby aplikace uložila potřebné parametry do požadavkového bloku *ECB* (Event Control Block), obsluha požadavků může být asynchronní k dalšímu běhu aplikace. Aplikace může na ukončení požadované funkce aktivně čekat nebo může být přerušena dokončovací rutinou.

Formát paketů odpovídá obr. 14.12. Pole Checksum má historický význam a není u lokálních sítí, které mají efektivní detekci chyb při přenosu, využíváno, pole Length udává délku paketu. Nižší čtyři bity pole Transport Control jsou využívány k počítání směrovačů, kterými paket prošel. Překročení limitu šestnácti směrovačů je důvodem k likvidaci paketu. Pole Packet Type odlišuje pakety přenášející data od paketů služebních, kódy pro nejběžnější druhy provozu uvádí následující tabulka:

00_H	- Unspecified Packet
01_H	- Routing Information (RIP)
02_H	- Echo Packet
03_H	- Error Indication
04_H	- IPX Packet
05_H	- SPX Packet
11_H	- NCP Packet

Adresy odesílatele a adresáta jsou složeny z čísla sítě, z adresy stanice a šestnáctibitového čísla přípojného místa (socketu). Rozdělení adresního prostoru socketů, které uvádí tabulka, dovoluje souběžnou práce více aplikacím:

451_H	- Netware Control Protocol (NCP)
452_H	- Service Advertisement Protocol (SAP)
453_H	- Routing Information Protocol (RIP)
455_H	- NetBIOS
456_H	- diagnostics
4000_H -$7FFF_H$	- dynamically assigned
8000_H -$FFFF_H$	- well-known



Obrázek 14.12: Pakety protokolů IPX a SPX

Protokol SPX je nadstavbou protokolu IPX. čtyři významnější bity pole Connection Control slouží řízení toku po virtuálním kanále:

10_H - End of Message
20_H - Attention
40_H - Acknowledgement Required
80_H - System Packet

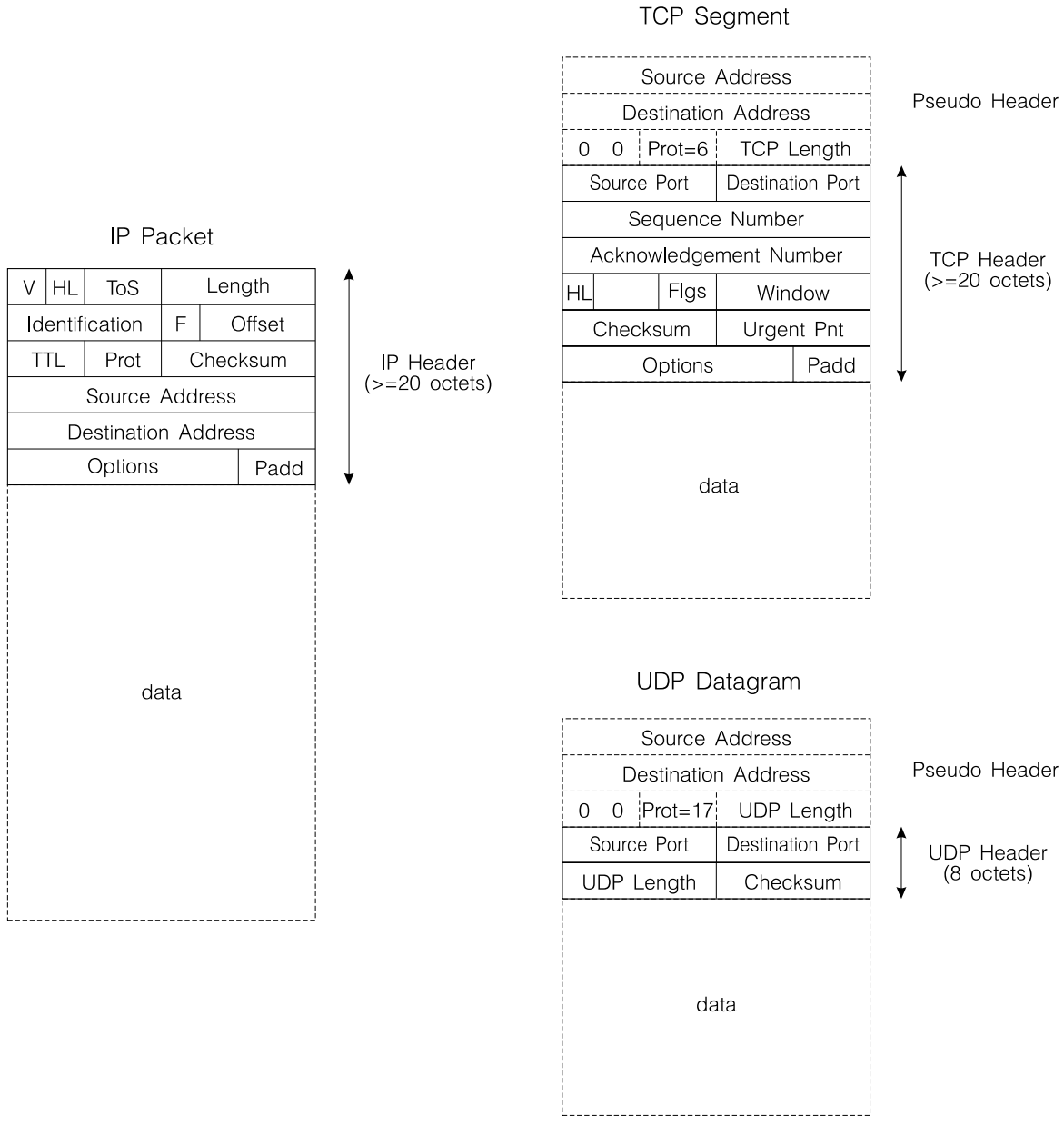
Pole Datastream Type je využíváno k indikaci ukončení práce na virtuálním kanále:

FE_H - End of Connection
FF_H - End of Connection Acknowledgement,

ostatní kombinace mohou využít aplikace. Pole Source Connection ID a Destination Connection ID umožnují multiplex v rámci protokolu SPX (více kanálů na jedno přípojné místo), pole Sequence Number a Acknowledge Number podporují potvrzování, a konečně pole Allocation Control slouží k řízení toku.

14.2.3 TCP/IP

Protokoly TCP/IP jsou v současnosti akceptovány jako *de-facto standard* pro komunikaci v rozsáhlých počítačových sítích. Jejich pozice se s využíváním systému UNIX, s implementací jejich podpory pod Windows a s příchodem Windows for Worgroups, Windows 95 a Windows NT dále posiluje. Architektura TCP/IP zahrnuje vlastní *přenos paketů IP* (Internet Protocol), jednoduché *datagramové rozhraní UDP* (User Datagram Protocol) a dobře navržený protokol *logického kanálu TCP* (Transmission Control Protocol). Protokol TCP zajištuje potvrzování v prostředí propojených sítí, ve kterých mohou být pakety dodávány v nezaručeném pořadí, mohou být při přenosu štěpeny na fragmenty a mohou se ztrácet. Je vybaven důmyslným řízením toku a ochranou proti chybám vyvolaným opakovaným navazováním spojení. Aplikacím viditelné protokoly IP, UDP a TCP jsou podporovány služebními protokoly, které zajišťují transformace adres TCP/IP na adresy lokální sítě (ARP, RARP), řízení sítě (ICMP) a podporu směrování (RIP, OSPF).



Obrázek 14.13: Formáty paketů IP, TCP a UDP

Dá se říct, že protokoly TCP/IP jsou v současné době k dispozici v libovolné lokální síti, minimálně proto, aby zajistily spolupráci s počítači pod operačním systémem UNIX a propojení s Internetem. Aplikační rozhraní protokolů IP, UDP a TCP jsou poměrně přesně definována v operačních systémech UNIX jako *BSD sockety* (BSD Sockets) nebo jako *rozhraní TLI* (Transport Layer Interface). Rozhraní v systémech Windows je obdobou BSD socketů doplněné o podporu asynchronního provádění funkcí.

Funkce rozhraní zahrnují vytváření (Socket) a rušení (Close) datových struktur řídících komunikaci na daném přípojném místě (portu) nebo po virtuálním kanále, jejich vazbu na logický kanál a vazbu na adresační informaci (Bind) a limit počtu neobsloužených požadavků na vstupu (Listen). Součástí rozhraní TCP jsou funkce pro pasivní a aktivní otevření kanálu (Accept a Connect) a pro jeho uzavření (Close). Přenos paketů a zpráv zajišťují volání funkcí Write a Read, spolu s několika formami funkcí Send a Receive. Formát IP paketů, UDP datagramů a TCP segmentů uvádí obr. 14.13.

Hlavička *IP paketu* obsahuje údaj o verzi protokolu (prozatím stále používáme verzi 4) a o délce hlavičky ve slovech. Následující pole ToS definuje typ provozu (interaktivní, přenos dat) nebo požadavky na dobu odezvy, kapacitu kanálu a spolehlivost nebo bezpečnost přenosu. Pole Length uvádí délku paketu (nebo fragmentu) včetně hlavičky, pole Identification dovoluje identifikovat fragmenty paketu, na které se může paket při průchodu sítí rozpadnout. Tříbitové pole příznaků F dovoluje zakázat dělení paketu na fragmenty a rozpoznat poslední fragment v paketu, pole Offset definuje umístění fragmentu v paketu. V poli TTL najdeme počet "sekund" , které zbývají paketu pro jeho cestu k adresátovi, hodnota je snižována nejméně o jedničku při průchodu každým směrovačem. Pole Prot identifikuje vyšší protokol, hodnota Prot=6 odpovídá protokolu TCP, hodnota Prot=17 protokolu UDP. Následují adresy příjemce a odesílatele a případně pole Option pro služební informace.

Hlavičce *TCP segmentu* na obr. 14.13 předřazujeme "pseudohlavičku IP" , která obsahuje podstatné údaje z IP hlavičky zahrnované do kontrolního součtu. Adresy portů jsou šestnáctibitové a jsou následovány údaji Sequence Number a Acknowledgement Number pro potvrzování. Pole HL uvádí délku hlavičky, příznaky Flgs slouží pro předávní služebních údajů při otevírání a rušení spojení, informují o platném potvrzení a prioritní informaci v segmentu. Pole Window dovoluje příjemci uvést velikost paměti alokované pro očekávaná data, slouží pro řízení toku. V poli Checksum najdeme kontrolní součet segmentu včetně "pseudohlavičky" (v "inverzním" kódu). Pole Urgent Pnt uvádí pozici prioritní informace v přenášených datech.

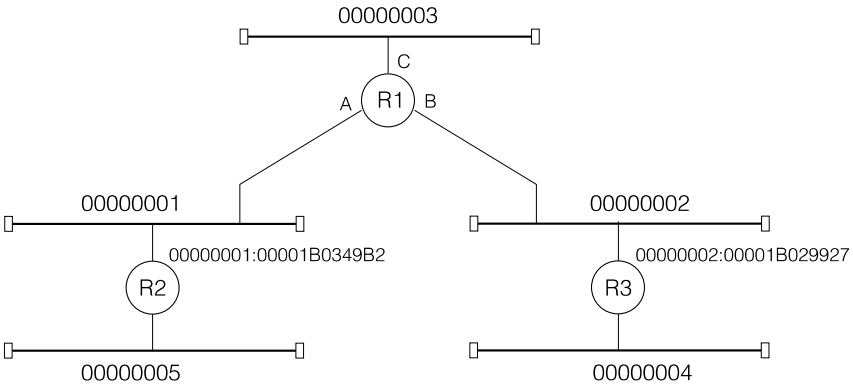
Konečně, hlavička *UDP datagramu* nese pouze čísla portů, délku UDP datagramu a kontrolní součet.

Protokoly OSI a Banyan VINES

Náš přehled si neklade za cíl kompletní výčet protokolů používaných v lokálních sítích. Patří sem jistě protokoly odpovídající standardům ISO, které vytvářejí konzistentní základnu pro síťové aplikace. V oblasti rozsáhlých sítí se opírají o služby veřejných datových sítí X.25, v oblasti lokálních sítí vycházejí z norem IEEE 802 a ISO 8882). Definují vlastní transportní rozhraní TP4, které je obdobou TCP protokolu. S použitím protokolů ISO se setká uživatel sítí DECNET. Zcela záměrně např. zůstaly stranou protokoly sítě Banyan VINES, které jsou obdobou protokolů TCP/IP.

14.3 Směrování

Prvotním úkolem síťové vrstvy je podpora výstavby přepojovacích sítí z dvoubodových a vícebodových spojů (v tomto případě většinou lokálních sítí). Propojovacími prvky jsou *směrovače* (*Router*), ty směrují pakety od odesílatele k adresátovi a opírají se přitom o síťové adresy. Síťové adresy mohou být do určité míry svázány s adresami linkovými (MAC adresami), jako je tomu u protokolů XNS a IPX/SPX. Tato vazba usnadňuje zjištění linkové adresy z adresy síťové, což je operace při komunikaci potřebná. Adresami jsou dvojice (32-bitové číslo sítě, 48-bitová MAC adresa). Vzniká tak dvouúrovňová *hierearchie* síť:linka, ta dovoluje směrovačům omezit se při své činnosti (směrování IPX paketů) na číslo sítě. Příklad sítě s adresami sítí a adresami rozhraní směrovačů uvádí obr. 14.14.



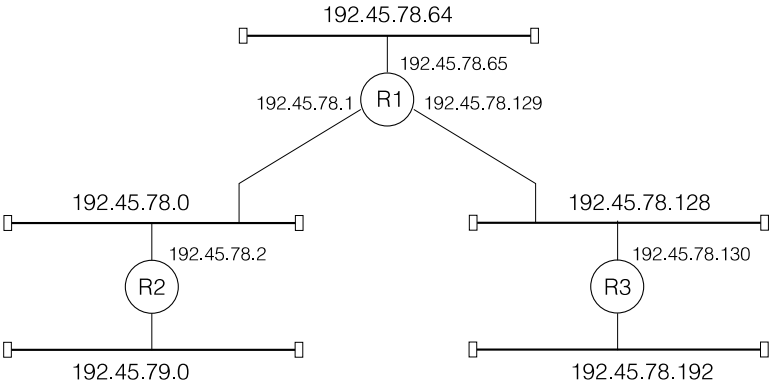
Obrázek 14.14: Propojení lokálních sítí směrovači IPX

Jiné protokoly se opírají o síťové adresy na linkových adresách zcela nezávislé, tak je tomu u protokolů NetBIOS a TCP/IP. Tyto dva příklady se však podstatně liší.

U protokolu NetBIOS nemá struktura síťových adres (nebo, přesněji jmen, která jsou navíc vázána na aplikaci a ne na počítač nebo komunikační rozhraní) s topologií sítě nic společného. Důvodem je historie tohoto protokolu, který byl vytvořen v době, kdy propojování lokálních sítí a jejich začleňování do rozsáhlých systémů bylo vzdálenou budoucností a kdy zvolené řešení využívalo do té doby nepředstavitelně vysoké přenosové rychlosti sítě. Překlad síťových adres nezávislých na topologii je náročný na rozsah a strukturu tabulek směrovacího systému, ale i na počet vyměňovaných paketů a na čas. V případě NetBIOSu není překlad v rozsáhlých sítích ani možný a není tedy možné ani směrování opírající se o ně. Standardním řešením je zprostředkování komunikace aplikací využívajících NetBIOS vkládáním paketů NetBIOSu do paketů jiných protokolů (IPX, IP) – mluvíme o *emulátorech NetBIOSu*.

U adresace TCP/IP můžeme do určité úrovně mluvit o *hierarchické adresaci*. Adresa o délce 32 bitů je složena ze dvou částí, adresy sítě a adresy počítače v síti. Rozhraní těchto dvou částí adresy je určeno *třídou adresy* (A,B nebo C), ale lze ho dále zjemnit vytvářením podsítí. Adresy všech počítačů v síti (nebo v podsíti jedné sítě) mají společnou část odpovídající adrese sítě (podsítě), lze je rozdělit do sítí (podsítí) porovnáním pod *maskou*. Maska tak dovolí odlišit komunikaci, která probíhá v rámci jednoho spoje (jedné lokální sítě), od komunikace, která má být směrovačem (směrovači) předána do jiného spoje. Příklad sítě s adresami sítí a adresami rozhraní směrovačů uvádí obr. 14.15.

Směrovače se při své práci opírají o informaci o "délkách" spojů. Tato informace jim dovoluje vybrat nejvýhodnější cestu pro datagram nebo virtuální kanál. Uvedenou informaci nejčastěji získávají jednou ze dvou metod distribuovaného výpočtu. Prvním postupem je algorit-



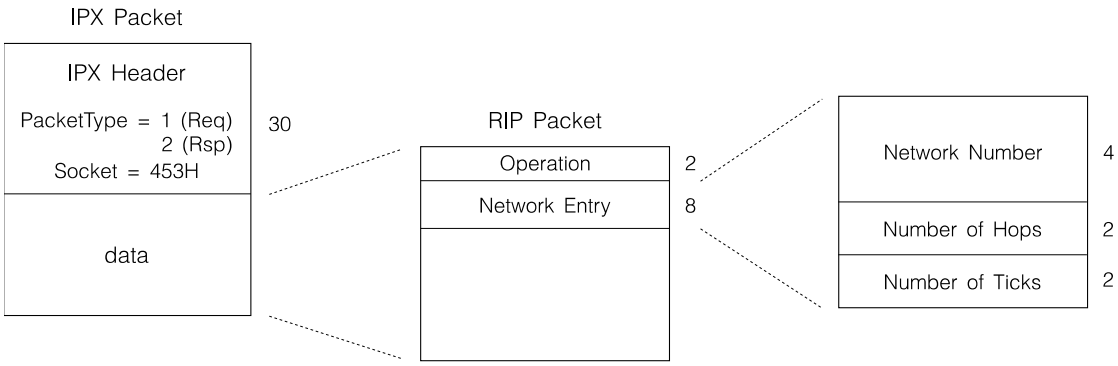
Obrázek 14.15: Propojení lokálních sítí směrovači IP

mus známý jako Ford-Fulkersonův a využívaný v technice *RIP* (Routing Information Protocol), který dovoluje každému směrovači modifikovat své směrovací tabulky na základě směrovacích tabulek získaných od jeho sousedů. Druhým postupem je vlastní výpočet směrovacích tabulek na základě úplné informace o topologii sítě a o délkách jednotlivých linek, které jsou distribuovány periodicky nebo při podstatných změnách. Tento postup je označován jako *OSPF* (Open Shortest Path First), je stabilnější než RIP a dovoluje i respektovat určité požadavky na kvalitu služeb.

14.3.1 RIP

Algoritmus distribuovaného výpočtu směrovacích tabulek *RIP* (Routing Information Protocol) se opírá o výměnu údajů ze směrovacích tabulek mezi sousedními uzly sítě. Algoritmus byl využíván v počátečních fázích vývoje sítě ARPANet ("předchůdce" Internetu), je používán v současných jednodušších autonomních systémech Internetu ale i v lokálních sítích s protokoly IPX/SPX a AppleTalk. Zde si uvedeme modifikaci algoritmu RIP používanou v sítích Novell Netware.

Pro předávání směrovacích informací slouží pakety RIP se strukturou odpovídající obr. 14.16.



Obrázek 14.16: Struktura RIP paketu

Těmito pakety může směrovač požádat (PacketType=1 – Request) o sdělení informací o všech nebo jen některých sítích z tabulky souseda, stejné pakety (PacketType=2 – Response) slouží i jako odpovědi nebo jako informace o změnách, které směrovač zaznamenal. Periodicky rozesílané pakety obnovují informace v tabulkách sousedů, neobnovovaná informace stárne (proces označujeme jako *Aging*) a síť může reagovat i na nenahlášené změny. Jednotlivé položky

RIP paketu obsahují informaci o adrese sítě, o počtu směrovačů na cestě k této síti a jako přídavnou informaci i údaj o zpoždění na této cestě (měřený v počtu "tiků" – 1/18 sec). Směrovače si informace získané algoritmem RIP ukládají ve směrovacích tabulkách, směrovací tabulky mohou mít například formu odpovídající obr. 14.17.

Network number	Hops	Ticks	NIC	Address of Forwarding Router	Aging Time
00000001	1	1	A		0
00000002	1	1	B		0
00000003	1	5	C		0
00000004	2	2	B	00000002:00001B029927	1
00000005	2	4	A	00000001:00001B0349B2	2

Obrázek 14.17: Směrovací tabulka získaná algoritmem RIP

Funkce směrovače je poměrně jednoduchá. Po zapnutí rozešle (broadcastem) žádosti o směrovací informace do všech připojených sítí. Na základě odpovědí si vytvoří svojí směrovací tabulku (přičte jedničku k počtu kroků a o změřené zpoždění zvýší počet tiků) a rozešle tuto tabulku v RIP paketech do připojených sítí. Dále již rozesílá RIP pakety pravidelně s periodou 60 sec, nebo při změnách v tabulce. Do RIP paketů není zahrnována informace, týkající se sítí, do kterých směrovač RIP pakety posílá. V našem příkladě například směrovač R1 nevysílá do sítě 00000002 informace týkající se rozhraní B, tedy sítí 00000002 a 00000004, a do sítě 00000001 nevysílá informace týklající se rozhraní A, tedy sítí 00000001 a 00000005. Tato modifikace je označována jako *Split Horizon*, její použití snižuje zátěž sítě a zvyšuje stabilitu směrování při změnách v síti.

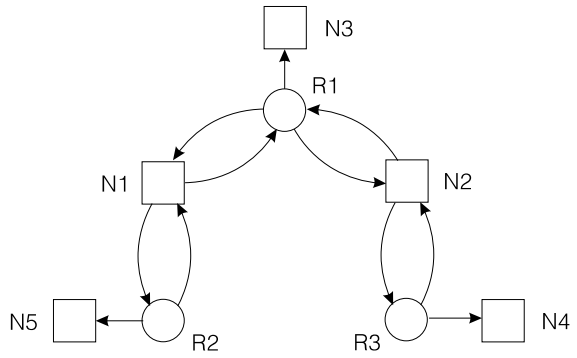
Výpadky rozhraní (nebo připojené sítě) směrovač oznamuje rozesláním RIP paketů s údajem Hops=16 v příslušné položce, tato hodnota má pro algoritmus RIP význam "nekonečna" . Paket RIP s údajem Hops=16 pro všechny připojené sítě směrovač rozesílá při regulárním ukončení své činnosti, výpadek směrovače zjistí sousední směrovače jako výpadek rozesílání RIP paketů. Pokud směrovač nepřijme RIP paket obnovující údaj v jeho tabulce po dobu delší než 3 minuty, je odpovídající cesta k dané síti považována za nepoužitelnou. Nemá-li směrovač možnost najít náhradní cestu, je síť považována za nedostupnou a směrovač to oznámí sousedům hodnotou Hops=16 v příslušné položce. Uvedený postup je označován jako *Aging*.

Protokolu RIP využívají vedle směrovačů sítě (v případě sítě Novell Netware mohou plnit a typicky i plní funkci směrovačů servery sítě) i připojené stanice. Jim pakety RIP dovolují zjistit MAC adresu nejbližšího směrovače na cestě k adresátovi (nahrazují tak protokoly ARP, BOOTP nebo DHCP, jak je známe ze sítí TCP/IP), tuto adresu pak stanice používá při přenosu dat.

14.3.2 OSPF

Algoritmus distribuovaného výpočtu směrovacích tabulek *OSPF* (Open Shortest Path First) se od algoritmu RIP liší tím, že si každý směrovač v síti udržuje kompletní informaci o topologii sítě a o zpožděních na jednotlivých linkách (pochopitelně vztažených k výstupu odpovídajícího rozhraní).

Aktuální informaci o topologii sítě si směrovače udržují ve formě orientovaného grafu, jehož uzly tvoří vícebodové spoje (lokální sítě) a směrovače, a hrany reprezentují možný tok dat od směrovačů k adresátům. Příklad grafu udržovaného při práci algoritmu OSPF pro síť z obr. 14.15 najdeme na obr. 14.18. Aktuální informace o stavu linek je uložena jako ohodnocení



Obrázek 14.18: Topologická informace pro protokol OSPF

orientovaných hran a využívána pro lokální výpočet směrovacích tabulek (příklad směrovací tabulky pro směrovač R1 z obr. 14.15 uvádí obr. 14.19). Algoritmus OSPF dovoluje použít více metrik pro ohodnocení spojů, je tedy využitelný pro sítě poskytující více typů služeb *TOS* (Type of Service – interaktivní práce, přenos souborů), nebo pro sítě dovolující aplikacím definovat požadavky na kvalitu služby *QoS* (Quality of Service).

Network	Network Address	Mask	Next Hop	Cost
N1	192.45.78.0	255.255.255.192	192.45.78.1	1
N2	192.45.78.128	255.255.255.128	192.45.78.129	1
N3	192.45.78.64	255.255.255.192	192.45.78.65	1
N4	192.45.78.192	255.255.255.128	192.45.78.129	2
N5	192.45.79.0	255.255.255.0	192.45.78.1	5

Obrázek 14.19: Směrovací tabulka směrovače R1

Získání informací potřebných pro výstavbu topologické databáze a její údržbu podporují pakety OSPF protokolu. Svou činnost zahajuje směrovač OSPF dotazem na své sousedy na připojených linkách a lokálních sítích. Příslušný paket je označován jako *Hello Packet*, výsledkem výměny Hello paketů je seznam sousedů. U vícebodových spojů hraje výraznou roli jeden ze směrovačů – *vyhrazený směrovač* (Designated Router). Topologickou databázi (*Topology Database*) si směrovač buduje na základě informací vyměňovaných se sousedy v paketech *Database Description*. Výsledkem je jednak získání vlastního OSPF grafu, jednak zprostředkování topologických informací směrovačům v nově propojené síti. Dynamicky se měnící údaje o stavu jednotlivých spojů (lokálních sítí) jsou po zasynchronizování topologických databází rozesílány záplavovým směrováním. Jejich výměně slouží pakety *Link State Request*, *Link State Update* a *Link State Ack*.

Algoritmus má svůj původ v pozdějším směrovacím algoritmu ARPANetu, pro TCP/IP je jeho v současné době používaná verze 2 specifikována materiálem RFC 1583. Obdobný mechanismus je používán i v rozsáhlejších sítích IPX/SPX pod označením *NLSP* (Netware Link State Protocol) a v sítích ISO pod označením *IS-IS* (Intermediate System – Intermediate System).

15. Správa lokálních sítí

Lokální sítě, a zvláště ty složitější, tvořené více částmi propojenými mosty, přepojovači a směrovači je nutné udržovat v provozu a to v co nejefektivnějším. Je potřeba zjišťovat stavové informace týkající se aktivních prvků (opakovačů, rozbočovačů, mostů, přepojovačů a směrovačů), oznamovat jejich výpadky a chyby na médiu, měřit zatížení sítí a segmentů a následně soustředit tyto údaje pro potřebu správce sítě v jediném místě. Podle získaných údajů se pak správce rozhoduje o řídících zásazích do struktury sítě a do parametrů jednotlivých aktivních prvků. Je výhodné, pokud lze takové zásahy do sítě provést na dálku, přímo z pracoviště správce.

Pro podporu uvedených funkcí jsou aktivní prvky sítě a koncová zařízení (servery a pracoviště), doplňovány o programové moduly a často i o doplňkový HW. Tyto moduly sbírají informace o stavu a provozu aktivních prvků a koncových zařízení a dovolují nastavovat jejich parametry.

Na systém správy sítě je kladen velice důležitý požadavek, a tím je schopnost ovládat zařízení různých výrobců, z nichž může být síť složena. Tento požadavek vedl na vytvoření standardů, které spolupráci programů správy a různých síťových prvků (technických i programových) dovolují. Byly vytvořeny standardy *ISO CMIS/CMIP* (Common Management Information Service/Common Management Information Protocol) v rámci norem ISO OSI a jednodušší standard *SNMP* (Simple Network Management Protocol) v rámci internetových RFC. Ten se také stal všeobecně používaným.

15.1 Síťové analyzátory

Jako první položku jsme do této kapitoly zařadili zmínku o *síťových analyzátorech*. Nejedná se sice v pravém smyslu slova o prostředky pro správu sítě, ale tato zařízení, schopná sledovat a analyzovat tok dat v jednotlivých spojích sítě, mohou poskytnout neocenitelné údaje, které mnohdy ani nelze jinak získat.

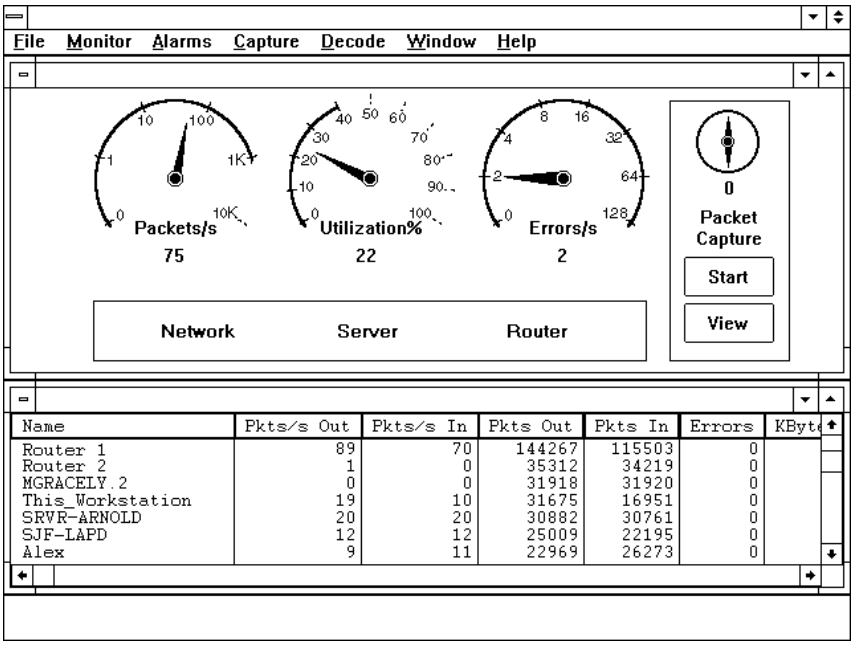
Struktura síťového analyzátoru je velice jednoduchá. Většinou dnes jde o přenosný osobní počítač, vybavený potřebným síťovým rozhraním. Vedle rozhraní pro lokální sítě, které nás v tomto textu zajímají, je obvykle pevně vestavěno sériové rozhraní schopné analyzovat dvoubodové spoje rozsáhlých sítí (patří sem asynchronní kanály a synchronní kanály, rozhraní X.25, Frame Relay, ISDN a další).

Na rozhraní lokální sítě analyzátoru jsou kladeny poněkud vyšší požadavky, než na rozhraní běžného počítače sítě. Musí být schopné převzít a předat ke zpracování veškeré rámce, které procházejí příslušným segmentem sítě. Zatímco rozhraní běžných počítačů z tohoto toku filtrují pouze tu část, jejíž jsou adresátem, rozhraní analyzátoru musí přijmout vše (mluvíme o *promiskuitním módu* práce). Navíc, zajímají nás nejen rámce přijaté bez chyb, ale i rámce neúplné, rámce poškozené kolizí a rámce, ve kterých byla indikována chyba.

Klíčovou roli hraje u síťového analyzátoru specializované programové vybavení. To dovoluje analyzovat i údaje o poškozených rámcích a určit tak zdroj problémů na spoji. V této funkci ho ocení zvláště technici. Dovoluje však také roztřídit tok podle protokolů a komunikujících účastníků a poskytnout správci sítě reálné údaje o zatížení sítě – o nejzatíženějších serverech, jejichž posílení může zkrátit odezvy, o nejzatíženějších segmentech u sítí s mosty nebo směrovači, kde dává podklady pro jemnější segmentaci a/nebo nasazení rychlejší technologie (například 100BASE-TX Ethernet na místě 10BASE-T, dnes již přichází v úvahu i technologie gigabitové). Velice důležité jsou informace o aplikacích, které v reálném provozu nejvíce zatěžují síť a

jejichž náhrada, konfigurace nebo modifikace může komunikačnímu systému podstatně odlehčit. Typickým příkladem aplikace neúměrně zatěžující síť je databázový stroj běžící na pracovišti uživatele opírající se o soubory na serveru. Skutečný vliv takové aplikace na chování sítě však obvykle nelze prokázat bez reálně naměřených dat. Existence podobných aplikací v síti může, pokud nezjistíme, jak vypadá skutečný provoz na médiu, po dlouhou dobu (třeba než je nahradíme za velkých vynaložených nákladů efektivnějšími) maskovat skutečný zdroj problémů.

Pouze jako příklad si na závěr uvedeme obrázek obrazovky analyzátoru Novell LanAnalyser poskytující údaje o celkovém zatížení segmentu a o rozdělení toků podle komunikujících účastníků (obr. 15.1).



Obrázek 15.1: Obrazovka síťového analyzátoru

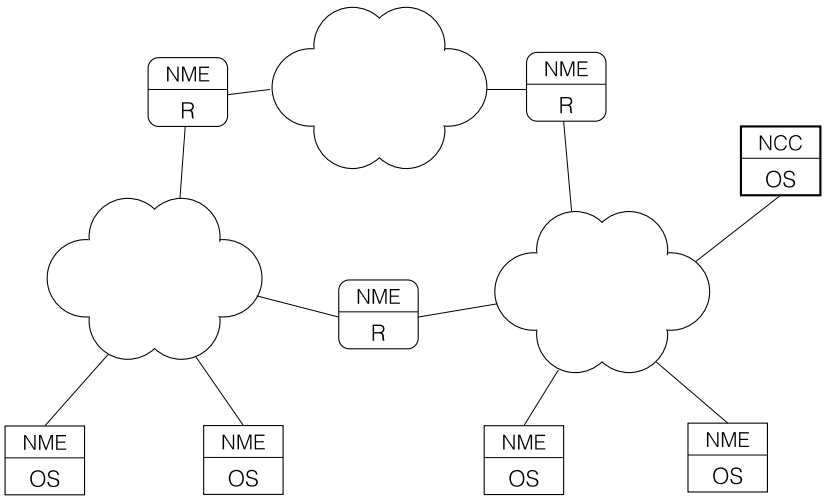
Podmínky, podle kterých vybíráme z toku dat rámce (nebo spíše jejich začátky), jejichž příspěvek k celkovému toku chceme indikovat v reálném čase, a které ukládáme do paměti počítače pro následnou statistiku a/nebo detailní analýzu, zahrnují výběr linkových a síťových protokolů (např. IP, ICMP, ARP pro TCP/IP a obdobně i pro další protokolové sady), ale i vyšších protokolů transportních (např. UDP, TCP) nebo aplikačních (např. Telnet, FTP nebo NFS).

Detailní analýza na úrovni síťové vrstvy může odhalit problémy způsobené např. nesprávným statickým směrováním. Detailní analýza na úrovni transportního protokolu může být dobrým podkladem i pro programátory – při detekci závad, které jsou důsledkem nekorektního chování programu.

15.2 CMIS/CMIP

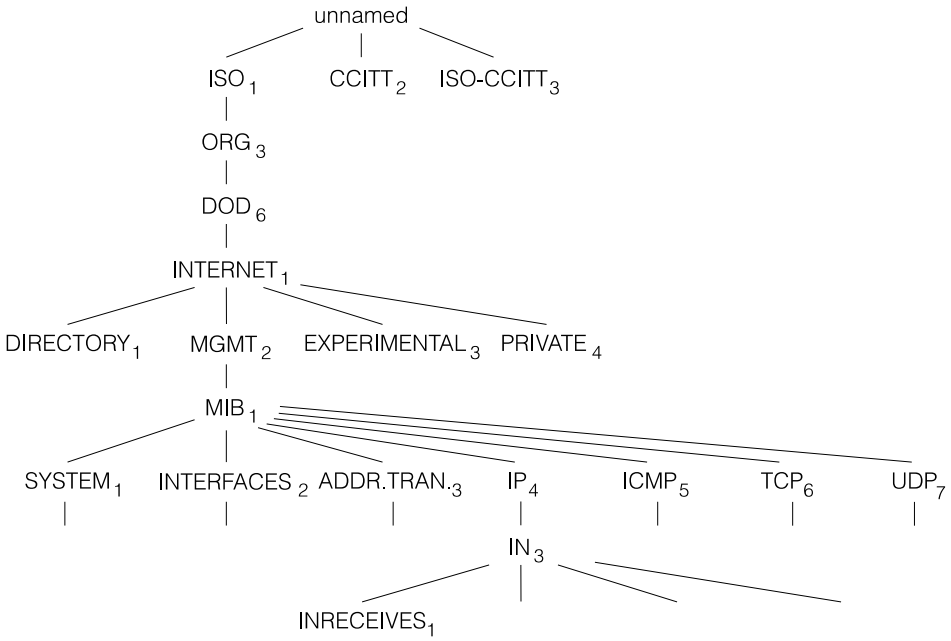
Podívejme se nejprve na obecné principy v kontextu systému správy ISO CMIS/CMIP. Systém správy je tvořen ovládanými prvky a pracovištěm pro správu sítě (obr. 15.2).

Ovládanými prvky (*Managed Objects*) jsou aktivní prvky sítě – směrovače, mosty, opakovače a rozbočovače. Lze spravovat i koncová zařízení – servery a pracoviště uživatelů. Každý z ovládaných prvků je vybaven programovým modulem, který správu podporuje (*NME* – Network Management Entity). Tento modul má za úkol sbírat statistické údaje o provozu



Obrázek 15.2: Architektura ISO CMIS/CMIP

ovládaného zařízení, lokálně je ukládat a na příkaz z pracoviště správy tyto údaje předat. Kromě toho musí modul dovolit předat informace o stavu (např. o nastavených parametrech, o délkách front, o provozuschopnosti komunikačních rozhraní a spojů). Na příkaz z pracoviště správy musí umět změnit parametry aktivního prvku (např. časové limity, směrovací tabulky, ale také restartovat ovládaný prvek).



iso.org.dod.internet.mgmt.mib.ip.in.InReceives - 1.3.6.1.2.1.4.3.0

Obrázek 15.3: Struktura databáze MIB

Systém správy se opírá o standardizovaný, objektově orientovaný, pohled na spravované informace. Vychází ze struktury označované jako *databáze MIB* (Management Information Base). Databáze MIB dovoluje jednoznačně identifikovat informace využívané systémem správy a společné prvkům všech výrobců. Jednoznačná identifikace dovoluje spolupráci ovládaných zařízení s programy správy různých výrobců. Kromě standardních společných informací MIB dovoluje přidávat informace experimentálního charakteru a informace týkající se konkrétních zařízení konkrétního výrobce – tyto části databáze MIB jsou označované jako *experimentální* a

privátní (Experimental MIB, Private MIB).

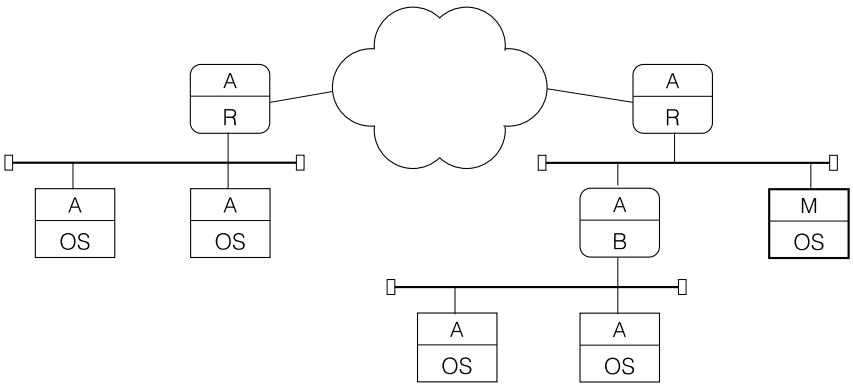
Pracoviště pro správu sítě (*NCC* – Network Control Center) je vybaveno programem, který komunikuje s moduly NME ovládaných prvků, získává od nich stavové a statistické informace, výsledky presentuje správci sítě a příkazy správce (nebo příkazy automaticky generované) modulům MME rozesílá. Kromě této formy komunikace je modulům NME umožněno oznamovat výjimečné stavy (výpadky komunikačních rozhraní a spojů) samostatně.

V rozsáhlém síťovém systému je vhodné rozdělit správu na více pracovišť správy, jejichž kompetence se mohou překrývat. Systém správy ISO přístup k ovládaným prvkům z více pracovišť správy dovoluje, zahrnuta je pochopitelně ochrana proti neoprávněnému získání informací z ovládaných prvků a proti neoprávněným řídícím zásahům.

Systém správy ISO je kompletně vystavěn nad protokoly ISO OSI. Ty zajišťují jednotný formát předávaných dat (použití presentačního formátu *ASN.1* – Abstract Syntax Notation) a jednotný způsob komunikace mezi ovládanými prvky a pracovišti správy.

15.3 SNMP

Standardy ISO vznikaly pomalu a byly značně složité. Potřeba mít k dispozici základní funkce správy vedla k návrhu alternativního systému *SNMP* (Simple Network Management Protocol). Jeho struktura se systému ISO CMIS/CMIP velice blíží (obr. 15.4).

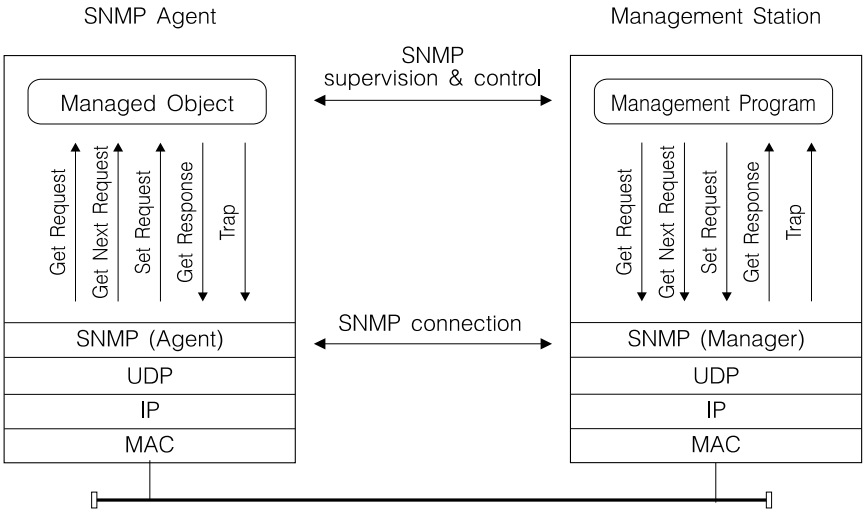


Obrázek 15.4: Architektura SNMP

Moduly správy na ovládaných zařízeních jsou označovány jako *agenti SNMP* (SNMP Agents), program pro správu sítě je označován jako *správce SNMP* (SNMP Manager). Moduly správy SNMP jsou běžnou součástí složitějších síťových prvků, ale najdeme je i u dražších opakovačů.

Základem pro komunikaci SNMP správce se SNMP agenty je, stejně jako v případě ISO CMIS/CMIP, databáze MIB. Ta je definována v textové formě a lze ji snadno rozšiřovat. Pracoviště správy získává informace od ovládaných zařízení tak, že jim zasílá požadavky *Get Request* nebo *Get Next Request* s identifikací MIB prvku a dostává odpovědi *Get Response* obsahující příslušnou hodnotu. Pro změnu hodnoty ovládaného prvku používá žádost *Set Request*. Kromě toto může ovládané zařízení asynchronně hlásit na pracoviště správy výjimečné situace zprávou *Trap*.

Komunikace mezi pracovištěm správy a ovládanými zařízeními se opírá o protokolovou sadu TCP/IP a presentační formát *ASN.1* (Abstract Syntax Notation). Úlohu správce SNMP plní většinou univerzální programy správy SNMP (např. HP OpenView, IBM NetView nebo Cabletron Spectrum), někdy se setkáme i se specializovanými programy dodávanými výrobci síťových prvků (např. Synoptics Optivity). Tyto programy dovolují správci získat informaci

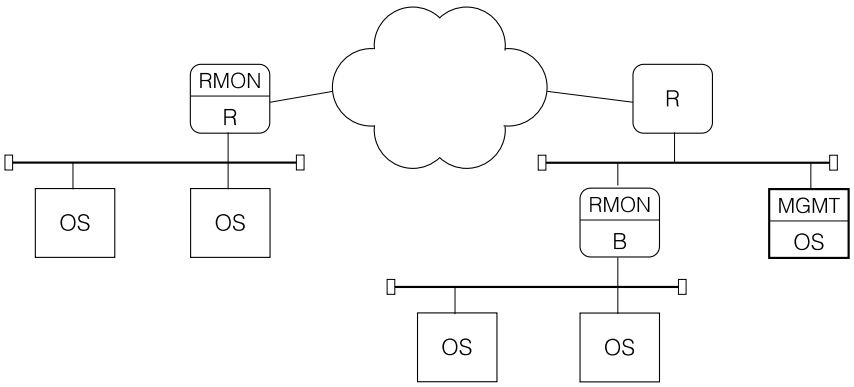


Obrázek 15.5: Komunikace SNMP

o okamžitém stavu sítě a upravovat její konfiguraci nebo parametry, a to často ve velice přehledné grafické formě a s možností intuitivního ovládání.

15.4 RMON

U malých lokálních sítí je možné získat informace o provozu na síti komunikačním analyzátorem připojeným k segmentu sítě (nebo do vedení kruhu). Komunikační analyzátor, určený původně pro řešení problémů v komunikaci stanic, je často využíván ve funkci monitoru sítě, pro měření zátěže, pro hlášení chybových situací. S rostoucím nasazováním přepojovacích prvků – mostů, přepojovačů a směrovačů do rozsáhlých lokálních sítí není však již jejich monitorování v jediném místě možné. Vhodnou alternativou k analyzátoru je sledování provozu v jednotlivých kolizních doménách samostatnými zařízeními, která plní funkci komunikačního analyzátoru, ale předávají analyzované údaje na pracoviště správy jako agenti SNMP. Ještě výhodnější je, pokud tuto funkci mohou plnit přímo aktivní prvky sítě (resp. jejich komunikační rozhraní), které mají ke sledovaným kolizním doménám přístup.



Obrázek 15.6: Architektura RMON

Odpovídající technologie, která rozšiřuje možnosti správy lokální sítě o sledování provozu na médiu, filtraci dat podle nadefinovaných kritérií pro jednotlivé komunikační protokoly a jejich vyhodnocování na pracovišti správy, dostala název *RMON* (Remote MONitor). O objekty sloužící funkci RMON byla rozšířena standardní databáze MIB a moduly RMON jsou dnes častou součástí aktivních zařízení sítě a programů správy.

16. Síťové operační systémy

Technické prvky lokálních sítí, kterým jsme se dosud věnovali, tvoří sice podstatnou, ale pouze část systému, který označujeme jako lokální síť. Další jeho součástí je programové vybavení počítačů připojených ke komunikační struktuře lokální sítě.

Funkce základního programového vybavení lokální sítě jsou pochopitelně ovlivněny výběrem aplikace, kterou chceme nad lokální sítí provozovat. Rozhodně nejčastějším využitím lokální sítě dnešních osobních počítačů je zpřístupnění systémových zdrojů některých počítačů – *serverů*, jiným počítačům – *klientským pracovištím*. Systémovými zdroji, které se vyplatí nebo které je nutné spravovat vybranými servery nebo jejich skupinami, jsou nejčastěji specializovaná zařízení (např. výkonné nebo specializované tiskárny), sdílené nebo rozsáhlé soubory dat a některé aplikační programy, jako jsou databáze nebo elektronická pošta. Servery, jejichž funkce se omezují na správu souborových systémů a obsluhu tiskáren, obvykle označujeme jako *souborové servery* (*File Server*), servery na kterých běží aplikace nebo jejich významné části označujeme jako *aplikační servery*. Programovou podporu dovolující zpřístupnění a sdílení prostředků lokální sítě označujeme (zjednodušeně a často nepřesně) jako *síťový operační systém*.

Právě uvedená definice serverů a klientských pracovišť odpovídá vnějšímu pohledu na lokální síť, kdy ji vidíme jako skupinu počítačů. Odráží však rozdělení programů na programy, které realizují rozhraní uživatele a lokální výpočetní funkce, a na programy, které udržují sdílené souborové systémy, fronty požadavků na sdílená zařízení a realizují společné výpočetní funkce (databáze, elektronická pošta). První označujeme jako *klienty*, druhé jako *servery*; výpočetní model, který rozkládá aplikaci na takové dvě části označujeme jako *Client-Server* model. Rozdělení aplikace na části, které pak běží na různě vybavených počítačích se promítá do označování těchto počítačů, jak jsme si je uvedli v předcházejícím odstavci.

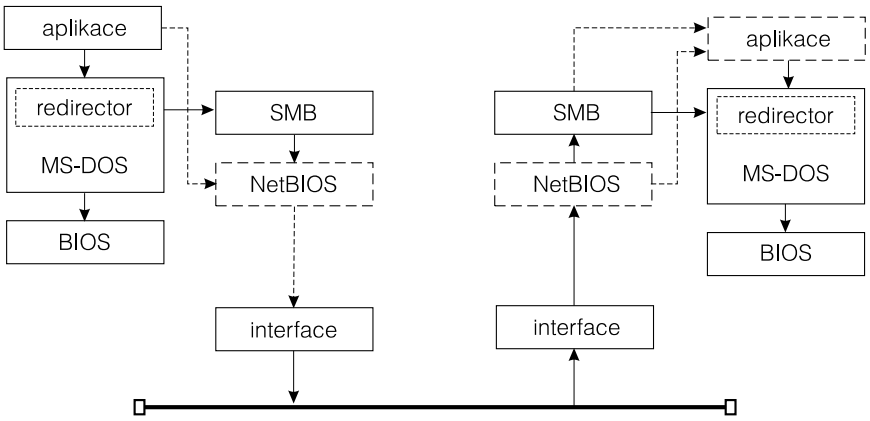
Ponechme stranou historické systémy, z nichž se dnešní síťové systémy vyvinuly, a jejichž cílem bylo poskytnout primitivně vybaveným mikropočítačům podporu jednoduchého řídícího programu se systémem souborů, se standardizovaným ovládáním periférií a primitivním řízením úloh. U takového řídícího programu bylo snadné náhradou ovladače převést žadost aplikace o periferní operaci na zprávu, a tu předat běžným sériovým rozhraním na lépe vybavený počítač. Ten pak, vybaven specializovaným programem, přijímal takové zprávy, přebíral požadavky a řídil podle nich reálné periférie k němu připojené. Naši studenti znali v polovině osmdesátých let podobný systém vyvinutý a provozovaný na katedře pod jménem FELNET.

Rozšíření vzájemně kompatibilních osobních počítačů (standardně vybavených jednotným řídícím programem MS-DOS) přináší potřebu podpořit jednoduše konfigurované počítače jednotně spravovaným systémem souborů a zpřístupnit jim prostředky, které by byly pro levné konfigurace nedostupné (hlavně tiskárny, ale i diskový prostor). Objevuje se u lokálních sítí s označením IBM PC-LAN, Microsoft MS-Net a Novell Netware a s ním i řešení do dnešní doby používaná.

Síťové rozšíření operačního systému

Zpřístupnění systémových zdrojů serverů v lokální síti musí respektovat přístup aplikačního programu ke službám systému osobního počítače, který je o služby vzdálených serverů doplňován. V uvedených sítích podporujících MS-DOS je takové rozšíření realizováno způsobem, který si popíšeme na příkladě historického produktu MS-Net firmy Microsoft.

MS-Net vkládá mezi aplikaci a systémové služby programový prvek, označovaný jako *redirector*. Ten u každého systémového požadavku aplikace, který přes něj prochází, rozhodne, zda příslušná funkce bude realizována lokálně (např. otevření lokálního souboru nebo čtení z něj) nebo zda o její realizaci bude požádán vzdálený server (např. otevření souboru na vzdáleném



Obrázek 16.1: Struktura síťového rozšíření operačního systému MS-DOS MS-Net

serveru nebo čtení z něj). V prvním případě redirector aktivuje lokální systémovou funkci, ve druhém, pro nás zajímavějším, případě vytvoří požadavek *SMB – Server Message Block*, který prostřednictvím sítě zašle serveru. Server přijímá požadavky SMB od více svých klientů, analyzuje je a aktivuje lokální systémové funkce, které požadavek aplikace splní. Náš obrázek respektuje i fakt, že aplikace může vyžadovat sítí podporované funkce, které mezi lokálními funkcemi neexistují (např. rozšíření adresářů o přístupová práva k souborům, ale i o evidenci uživatelů, počítačů, obslužných programů, rozšíření o časové funkce), že žádosti o některé lokální systémové funkce mohou redirector obcházet, že se aplikace může obracet přímo na komunikační funkce a že na serveru může běžet samostatná aplikace. Obrázek respektuje i skutečnost, že MS-Net se opírá o komunikační funkce definované firmou IBM pro její první síť PC LAN označované jako *NetBIOS* a firmou Microsoft později rozšířené na *NetBEUI*.

Tento základní princip je realizován v řadě produktů. U některých (Microsoft LAN Manager, IBM OS/2 LAN Server) jsou implementovány funkce odpovídající SMB, jiné (Novell Netware) mají svůj vlastní soubor síťových funkcí (NCP u Novell Netware, NFS a lpr u UNIXu). Jednotlivé produkty, které na trhu existují, se od sebe liší ve dvou důležitých bodech:

- ve způsobu, jakým je realizována systémová podpora serveru a
- v důslednosti, s jakou jsou odděleny funkce serveru od funkcí aplikačního počítače.

Pokud jde o prvý z bodů, systémovou podporu funkcí serveru, nezbývá než konstatovat, že MS-DOS (ale i jeho rozšíření Windows) byl pro podporu serveru extrémně nevhodný. Řešení, která podporují běh aplikací na souborovém serveru, musí zajistit, aby nedošlo ke kolizi asynchronně realizovaných funkcí serveru se systémovými požadavky lokální aplikace (použití operačního systému MS-DOS nebo Windows bylo nutností, pokud jsme chtěli dovolit, aby osobní počítač – klientské pracoviště, sloužil současně i jako server pro ostatní pracoviště v síti). Bezpečnějším prostředím pro klientská pracoviště se staly až operační systémy Windows for Workgroups a Windows 95.

Uvedené řešení lze charakterizovat jako *síťové rozšíření operačního systému* nebo možná ještě lépe jako *síťové rozšíření systému souborů a periferního systému*. Aplikace využívá originálních funkcí původního operačního systému, řešení je pro ni transparentní z hlediska základní funkce, ne nutně z hlediska výkonu.

Peer-to-Peer

Základna, na které je server vystavěn, omezuje možnosti využít jeden počítač současně jako pracoviště i jako server. Sítě, které server opírají o univerzální operační systém, tak činí i se záměrem koexistenci rozhraní a aplikačních programů uživatele a funkcí serveru na jednom počítači povolit. Sítě jsou označovány jako *Peer-to-Peer* sítě. Rozhodnutí o případném rozdělení počítačů v síti *Peer-to-Peer* na klientská pracoviště a servery je víceméně administrativní záležitostí (vedle technického vybavení počítačů).

Výhodou současného využití počítačů jako klientských pracovišť i serverů jsou nižší náklady: pro funkci serveru nemusíme vyhradit samostatný počítač a vybavit ho poměrně drahým programovým vybavením. Jde o řešení pro malé sítě, má však větší požadavky na disciplinu uživatelů, jeho správa může být u větších sítí pracnější a poskytuje nižší spolehlivost a bezpečnost. Realizaci funkcí serveru na klientském počítači najdeme již u jednoduchých sítí osobních počítačů typu Peer-to-Peer, jakými byly např. PC-LAN, LANTASTIC nebo Netware Lite. Dnes lze sítě Peer-to-Peer budovat s použitím prvků téměř všech síťových operačních systémů (Windows NT, OS/2, UNIX).

Client-Server

Pokud má souborový server pracovat spolehlivě a s rozumnou efektivitou, je výhodnější ho opřít o operační systém, který podporuje souběžnou práci procesů. Takovým základem může být univerzální operační systém OS/2 využívaný servery sítí LAN Manager (Microsoft) a OS/2 LAN Server (IBM), operační systém Windows NT využívaný servery Windows NT Server, operační systém UNIX využívaný servery sítě VINES (Banyan), nebo zcela optimálně pro podporu funkcí serveru navržený operační systém, jako je tomu u sítě Novell Netware.

Sítě, které z důvodu bezpečnější správy nebo s ohledem na vybavení počítačů (požadavky na vybavení počítačů pracujících pod operačními systémy OS/2, Windows NT nebo UNIX jsou vyšší než u počítačů pracujících pod MS-DOS nebo Windows) rozdělují počítače na servery a pracoviště, označujeme jako sítě typu *Client-Server*.

Důsledkem konfigurace Client-Server jsou sice vyšší náklady na samostatný počítač (počítače) a specializované programové vybavení, získáme však vyšší spolehlivost a bezpečnost a jednodušší správu i v rozsáhlejších sítích.

V průběhu času se střídavě zvýrazňovaly výhody jednoho nebo druhého přístupu (Client-Server nebo Peer-to-Peer). Současné síťové operační systémy podporují spíše filosofii Client-Server, ale zahrnují i možnost využití některých zdrojů klientských počítačů (tiskáren, lokálně spravovaných dat) a snaží se o smazání rozdílu mezi oběma přístupy.

Aplikační servery

Vedle podpory aplikací běžících na klientských pracovištích často vyžadujeme schopnost serveru provozovat aplikace, které slouží více klientům. Jde o například o situaci, kdy klientská pracoviště vytvářejí uživatelská rozhraní ke *společné databázi* na serveru. Dalšími příklady jsou *transakční systémy* (transakcí zde budeme rozumět nedělitelnou posloupnost operací nad databází), systémy *elektronické pošty* (které musí být nezávislé na zapnutí konkrétního klientského počítače v konkrétním okamžiku), systémy *MHS* (Message-Handling System) a systémy označované jako *groupware* podporující spolupráci v pracovních skupinách. Konečně, moderní řešení rozkládají i běžné aplikace na části běžící na více počítačích, tuto technologii obvykle označujeme již definovaným termínem *Client-Server*.

Sítě opírající se o výkonný operační systém, jakým je např. OS/2 nebo Windows NT, koexistenci aplikačních programů s funkcemi souborového serveru principiálně neomezují, jeden počítač může bez omezení pracovat jako server i pracoviště uživatele. Takové řešení je optimální i z hlediska snadnosti rozšiřování funkcí serveru, pro rozšíření funkce stačí doplnit aplikační program (programy).

Konečně, servery opírající se o specializovaný operační systém (Novell Netware) práci uživatele na serveru vylučují, rozšiřování funkcí serveru není možné prostřednictvím běžných aplikačních programů, ale pouze prostřednictvím speciálních rozšíření (*NLM modulů*), pro jejichž vývoj je potřeba použít speciální technologii a dodržet řadu zvláštních omezení.

Současné trendy

Pro starší síťová rozšíření operačních systémů je typická poměrně úzká vazba na podporovaný operační systém klientských pracovišť, vyžadovaný operační systém serveru a využívanou sadu komunikačních protokolů. Požadavky na vzájemnou spolupráci různě vybavených počítačů vedly postupně k současné situaci, kdy se síťové operační systémy snaží o nezávislost na konkrétních operačních systémech. Přesněji o podporu více operačních systémů u klientských pracovišť a o schopnost serverů pracovat v prostředí různých operačních systémů a zpřístupnit jejich prostředky. Příkladem síťových operačních systémů, které podporují určitý výběr klientských pracovišť, jsou prakticky všechna moderní řešení. Příkladem schopnosti práce pod více operačními systémy může být LAN Server dostupný pro OS/2, ale i pro AIX (operační systém typu UNIX) a velké systémy IBM VM a MVS, nebo Pathworks dostupný pro OS/2, Windows NT, Digital UNIX (OSF.1) a DEC VMS. Objevuje se i snaha o nezávislost na konkrétní sadě komunikačních protokolů, příkladem řešení může být nezávislé transportní rozhraní MPTS dovolující volný výběr sady protokolů.

Klíčovou vlastností současných operačních systémů je schopnost dosažení co nejvyšší *bezpečnosti*. Jedná se o možnost co nejpřesnějšího definování *přístupových práv* pro jednotlivé uživatele, a to jak pro systém souborů, tak pro sdílené aplikace, a o splnění požadavků na *autentizaci* klientů a *autorizaci* jejich přístupu k prostředkům definovaných mezinárodními standardy.

Velký rozvoj prožívají technologie *vzdáleného dohledu a správy*, které se již neomezují na správu technických prvků lokálních sítí (směrovačů, mostů, přepínačů, opakovačů a rozbočovačů, ale i jednotlivých rozhraní stanic), ale začínají zasahovat i oblast programového vybavení.

Současnou "módou" je vybavování serverů lokálních systémů prostředky dovolující spolupráci s moderními technologiemi globálního přístupu k informacím. Jde o podporu *"pavučiny"* – systému pro přístup k informacím *WWW* (World-Wide Web) a o doplnění jeho klientů, ale i serverů, o aktivní komponenty programované v jazyce Java.

Rozšíření *mobilních* klientských pracovišť, ale i serverů, vyžaduje modifikovat techniky zpřístupnění sdílených prostředků. Nutností se stává replikace datových zdrojů, ale i aplikací, a potřeba nasazení synchronizačních prostředků, které zajistí konzistenci replikovaných dat.

17. Novell Netware

NetWare je představitelem jednoho z možných komplexních řešení služeb lokální sítě. NetWare je synonymem pro několik pojmů. Jednak jde o specializovaný operační systém, který dovoluje na jednom počítači poskytovat služby souborového serveru, tiskového serveru či aplikačního serveru. Dále může být směrovačem v rozlehlých sítích. V neposlední řadě může být i aplikačním serverem těžícím z dostupných moderních programátorských technologií. Pojmem NetWare zároveň bývají označovány i komunikační protokoly firmy Novell. V širším významu je tak označována celá lokální síť budovaná s využitím serveru NetWare.

Lokální síť se servery Novell NetWare umožňuje uživatelům několika typů počítačů a jejich operačních systémů využívat služeb serverů. Kromě obvyklých klientských pracovišť s operačním systémem typu Windows mohou být v síti začleněny i unixové počítače nebo například systémy Macintosh.

Serverem sítě je nejčastěji počítač typu PC. Na něm běží operační systém NetWare, který je optimalizovaný pro funkci souborového serveru. Existence serveru se specializovaným "operačním systémem" je sice cestou k jeho maximální efektivitě, podstatně však v minulosti komplikovala rozšiřování serveru o aplikačně orientované procesy.

17.1 Komunikační protokoly v sítích Novell

V novellské síti lze používat všechny běžně používané technologie pro výstavbu lokálních sítí. Nejčastěji některý typ Ethernetu, ale i Token Ring, ATM nebo například FDDI.

Pro vlastní komunikaci mezi serverem NetWare a jeho klienty je použit protokol NCP (*NetWare Core Protocol*). Služby operačního systému klientské stanice se v případě práce s adresáři a soubory uloženými na serveru převádějí na komunikaci protokolem NCP.

Samotný protokol NCP může být zapouzdřen buď do IP protokolu nebo do protokolu IPX/SPX.

Protokol IPX (Internetwork Packet Exchange) byl používán v minulosti. Představoval firemní řešení protokolu pro nespojovanou a nepotvrzovanou komunikaci, tedy klasickou datagramovou službu. Pro identifikaci jednotlivých stanic je použita hierarchická adresa. Ta se skládá z adresy sítě (4 byty) a adresy počítače v rámci sítě (6 bytů). Adresa počítače je odvozena od adresy komunikačního adaptéru, v případě ethernetovských sítí je s ní totožná. Komunikační vrstva SPX (Sequenced Packet Exchange) je vybudována nad IPX. Jde vlastně o službu virtuálního spoje. Informace o existujících serverech a jimi poskytovaných službách byly mezi servery šířeny protokolem SAP (*Service Advertising Protocol*). Informace o topologii sítě potřebné pro správné směrování jsou zveřejňovány protokolem RIP (*Routing Information Protocol*), který je funkční obdobou RIPu v rodině protokolů IP.

Soudobé sítě s NetWare jsou již budovány nad IP protokolem. Svoji existenci servery oznamují protokolem SLP (*Service Location Protocol*) a stejný protokol používají klienti i při vyhledávání serveru.

Ať už NCP používáme nad IP nebo IPX protokolem, musí být na straně klienta instalováno programové vybavení obvykle nazývané NetWare klient. NetWare server ale kromě NCP dnes umožňuje klientům komunikovat i jejich nativním protokolem. Pro windowsovské počítače je tedy k dispozici CIFS (*Common Internet File System*), sdílení souborů přes NFS (*Network File System*) využijí unixy a konečně pro počítače Macintosh lze použít AFP (*Apple Filing Protocol*). Při používání nativních protokolů uživatelé ani nemusejí poznat, že pracují v síti NetWare. Pro

plné využití vlastností serveru a administraci sítě je však nutné používat klasického NetWare klienta.

17.2 eDirectory

Ve starých verzích NetWare řady měl každý server svůj vlastní katalog oprávněných uživatelů serveru. Tento katalog byl označován termínem *bindery*. Pokud uživatel potřeboval přistupovat k datům uloženým na několika serverech, musel mít na těchto serverech vytvořeny účty a jednotlivě se k nim přihlašoval. To komplikovalo správu i užívání rozsáhlejší sítě.

Proto je nyní v NetWare zavedena společná databáze objektů eDirectory. Lze se setkat i se starším termínem NDS (*NetWare Directory Services*). Databáze soustřeďuje informace o jednotlivých objektech sítě — uživatelích, tiskárnách apod. Díky této databázi se celá síť s větším počtem serverů jeví jako jeden homogenní celek.

eDirectory je distribuovanou databází. Je hierarchicky organizována do podoby stromu. Rozeznáváme objekty typu kontejner, které v sobě obsahují další objekty. Koncovými objekty, listy stromu, jsou například uživatelé, servery, diskové svazky nebo tiskárny. Struktura stromu může odpovídat organizačnímu uspořádání podniku. V případě velkých firem lze zohlednit i geografická hlediska.

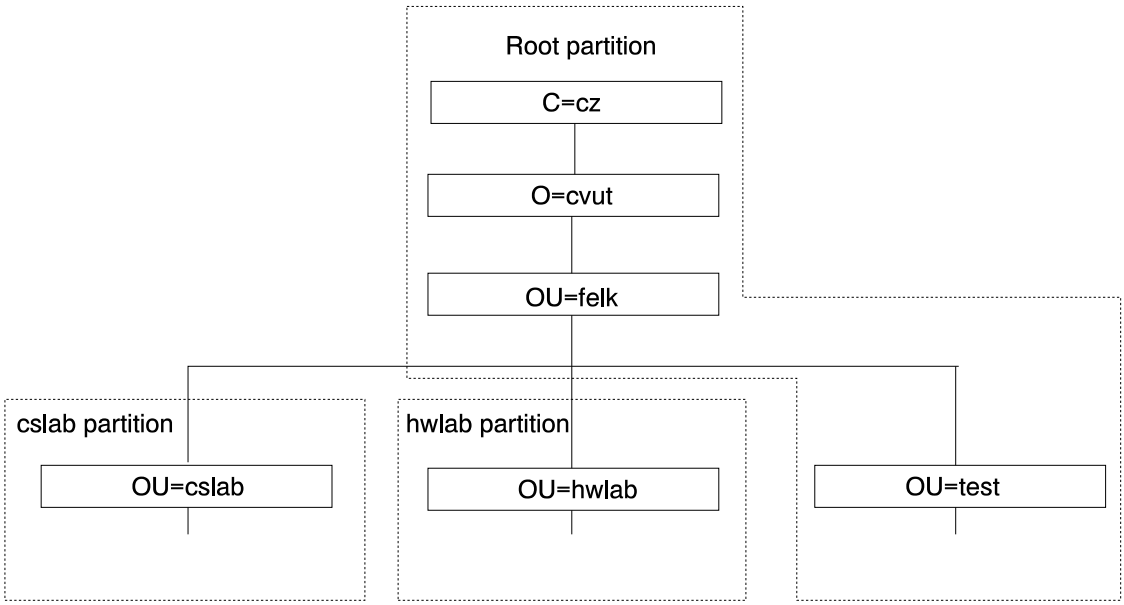
Existence databáze, na kterou můžeme zjednodušeně pohlížet jako na společný centrální katalog uživatelů (a dalších objektů), podstatně zjednodušuje a zefektivňuje správu rozlehlých sítí s více servery. Tuto výhodu dokládá například postup při zřizování uživatelského účtu. Administrátor sítě nejprve vytvoří v eDirectory nový objekt typu uživatel a následně tomuto objektu poskytuje přístupová práva k adresářům a souborům na libovolných serverech sítě. Odtud vychází tvrzení, že uživatel se nepřihlašuje na server, ale do sítě.

Databáze se vytvoří při instalaci prvého serveru sítě, je na tomto serveru fyzicky uložena. V rozlehlé síti mohou být na dalších serverech k dispozici její kopie (repliky). Informace z eDirectory lze získávat a změny zapisovat prostřednictvím nejbližší, nejrychleji přístupné repliky. To má význam zejména ve velkých sítích, kde jednotlivé geograficky vzdálené lokality jsou propojeny linkami s nižší přenosovou rychlostí. Zavedení replik je významné i z hlediska zajištění stálé dostupnosti eDirectory při výpadku serveru obsluhujícího některou repliku. Informace v takovém případě jsou dostupné prostřednictvím repliky z jiného serveru. Rozlišujeme originál (též označovaný jako master replika), repliku určenou pouze pro čtení (read only) a repliku s povoleným čtením i zápisem (read write). Master replika je právě jedna, ostatních typů replik může administrátor sítě vytvořit více.

Údaje uložené v objektech (vlastnosti objektů) se poměrně často mění. Ke změně dochází např. i při každém přihlášení a odhlášení uživatele ze sítě. Po jakékoliv změně některého z objektů dojde k samočinné synchronizaci obsahu jednotlivých replik. Pokud nelze z důvodu výpadku serveru nebo komunikační trasy některou repliku synchronizovat, informace v ní uložené budou aktualizovány později, po obnovení její dosažitelnosti. Při synchronizaci se mezi servery nepřenáší celá replika, ale jen potřebné změny.

V případě členitého stromu eDirectory s více kontejnerovými objekty lze informace ukládat do několika samostatných částí (partition) a pro každou z nich vytvořit vlastní repliky. Toto rozdělení probíhá na úrovni kontejnerových objektů. Zvolený objekt a všechny jeho podobjekty (podstrom) pak budou patřit do jiné oblasti, viz obr. 17.1. Z pohledu správy jednotlivých objektů je rozdělení databáze na několik částí zcela transparentní.

Správnou volbou struktury eDirectory, replik a jejich jejich uložením na vhodné servery lze jak snížit objem dat přenášených při synchronizaci replik po pomalejších komunikačních linkách,



Obrázek 17.1: Rozdělení eDirectory na oblasti

tak i zvýšit odolnost a dostupnost databáze při výpadcích serverů a komunikačních kanálů.

17.2.1 Objekty eDirectory

Mezi kontejnerové objekty patří samotný kořen stromu [Root], dále objekty Country, Organization a Organizational Unit.

[Root]. Kořen stromu [Root] vzniká při instalaci prvého serveru a vytváření eDirectory.

Country. Objekt Country (zkratka C) je nepovinným objektem vytvářeným bezprostředně pod objektem [Root].

Organization. Objekt typu Organization (O) musí být vždy alespoň jeden vytvořen. Tyto objekty se zakládají na nejbližší možné úrovni pod kořenem stromu [Root] s přihlédnutím k tomu, že mezi [Root] a Organization může být objekt Country.

Organizational Unit. Nepovinné objekty Organization Unit (OU) se vytvářejí pod úrovní Organization. Tyto kontejnerové objekty v sobě mohou obsahovat další objekty typu OU.

Koncové objekty, listy stromu, lze vytvářet v kontejnerových objektech O a OU. Na rozdíl od kontejnerových objektů představují skutečné objekty sítě. Některými pro nás zajímavými typy objektů jsou:

Alias. Alias lze používat jako odkaz na jiný objekt. Použitím alias objektu lze uživatelům sítě usnadnit práci s objekty v jiné části stromu.

Directory Map. Jde vlastně o odkaz na určitý adresář diskového svazku některého ze serverů. Uživatelé sítě si adresář mohou zpřístupnit (namapovat jej) na základě znalosti jména serveru, svazku a adresáře. Pro případ přesunu adresáře na jiný disk či server je ale vhodnější se na adresář v těchto případech odkazovat prostřednictvím objektu Directory Map.

Group. Skupina uživatelů. Tomuto objektu lze poskytovat přístupová práva k adresářům a souborům. Začleněním uživatele do jedné nebo více skupin získává uživatel navíc práva přidělená těmto skupinám.

NetWare Server. Tento objekt vzniká při instalaci serveru.

Organizational Role. Skupina uživatelů, kteří například v podniku zastávají stejnou funkci. Tomuto objektu lze poskytovat práva pro manipulaci s objekty eDirectory. Nezaměňovat s objektem Group, se kterým lze spojit přístupová práva k souborům a adresářům.

Print Server. Tiskový server sítě.

Printer. Fyzická tiskárna.

Profile. Profile script obsahuje příkazy, které se provádějí při přihlašování určité skupiny uživatelů do sítě.

Print Queue. Tisková fronta.

User.Uživatel sítě.

Volume. Diskový svazek některého serveru.

eDirectory lze pro potřeby jednotlivých aplikací rozšiřovat o další typy objektů. Též lze zavádět další atributy stávajícím objektům. Implementace eDirectory existují i pro celou řadu unixových operačních systémů včetně Linuxu. Kromě klasického programátorského rozhraní pro práci s eDirectory může být nad databází spuštěn LDAP server. Údaje z eDirectory tak mohou být dostupné celé řadě aplikací. eDirectory tak nemusí být jen seznamem uživatelů lokální sítě, ale je i plnohodnotným adresářovým a autentizačním serverem, který poskytuje údaje o stovkách tisíc objektů.

17.2.2 Přístupová práva k objektům v eDirectory

Každý objekt obsahuje několik různých informací, které jsou v terminologii eDirectory označovány jako *properties* (vlastnosti objektu či atributy). Například objekt typu uživatel nese údaje o uživatelově jménu a příjmení, jeho uživatelském jménu, době platnosti účtu nebo o členství ve skupinách uživatelů. Vůči ostatním objektům lze stanovit přístupová práva pro práci s tímto objektem jako s celkem (*object rights*) nebo s jeho jednotlivými atributy (*property rights*). Práva přiřazená pro přístup ke kontejnerovému objektu se vztahují i na jemu podřízené objekty. Toto dědění přístupových práv lze potlačit maskou přístupových práv IRF (Inherited Rights Filter). Přístupová práva k objektům eDirectory jsou shrnuta v tabulkách 17.1 a 17.2.

Název	Význam
Supervisor	Všechna práva k objektu i ke všem jeho vlastnostem
Browse	Právo číst (vidět) objekt a vyhledávat jej
Create	Možnost vytvořit nový objekt uvnitř kontejnerového objektu
Delete	Právo objekt zrušit
Rename	Právo změnit název objektu

Tabulka 17.1: Přístupová práva k objektům eDirectory

Přístupová práva k objektům a jejich vlastnostem se typicky přidělují jednotlivým uživatelům nebo skupinám uživatelů. Například administrátor na úrovni organizační jednotky má plná práva k objektu představujícímu tuto jednotku. Jeho práva se pak dědí i k objektům uloženým v organizační jednotce. Ať už jde o uživatele nebo další podřízené organizační jednotky. Administrátor sám může být reprezentován objektem ve zcela jiné organizační jednotce. Dědění přístupových práv lze eventuelně potlačit maskou IRF.

Název	Význam
Supervisor	Všechna práva k dotyčnému atributu objektu
Compare	Možnost porovnání konkrétní hodnoty s hodnotou dotyčného atributu, přičemž atribut nelze z objektu přímo přečíst; výsledkem porovnání je ano/ne
Read	Možnost zjistit hodnotu dotyčného atributu
Write	Právo zapsat nebo změnit hodnotu atributu
Add or Delete Itself	Možnost přidat nebo vyřadit sám sebe z objektu typu seznam; nejčastěji jako právo začlenit se sám do určité skupiny uživatelů (do objektu typu group)

Tabulka 17.2: Přístupová práva k atributům objektů eDirectory

17.2.3 Identifikace objektů eDirectory

Nejprve si zaveďme pojem *kontext*. Jeho význam je podobný tomu, k čemu slouží aktuální adresář při práci se soubory. Jde o odkaz na určitý kontejnerový objekt. Jednotliví uživatelé sítě si na svém počítači mohou kontext měnit a tím si zjednodušit práci s objekty. Při práci s objekty uloženými v dotyčném kontejneru totožném s nastaveným kontextem stačí totiž uvádět jen vlastní jména objektů (Common Names, CN).

Pro práci s objekty v jiném kontejneru (kontextu) je nutno vyjít ze znalosti plné identifikace objektu. Vyjadřuje vlastně cestu od kořene stromu přes jednotlivé kontejnery až k vlastnímu objektu. Příkladem identifikace je

```
CN=bily.OU=cslab.OU=felk.O=cvut.C=CZ
```

Jde o objekt se jménem `bily` spadající do organizační jednotky `cslab`, která je podřízena organizační jednotce `felk` organizace `cvut` v České republice. Z tohoto zápisu nelze zjistit, o jaký typ objektu se jedná. Z toho vyplývá, že v jednom kontejneru nemohou existovat dva objekty stejného jména lišící se pouze typem. Pro identifikaci objektu lze používat i stručný zápis ve tvaru `bily.felk.cvut.cz`.

Lze používat také relativní odkazy na objekty v jiných kontejnerech (kontextech). Aby nemohlo dojít k případné nejednoznačnosti mezi relativním odkazem a stručným zápisem identifikace objektu, platí jednoduché pravidlo. Zápis začínající tečkou je považován za stručný zápis identifikace objektu. V ostatních případech je doplněn o aktuální kontext.

Odkazem na nadřízený objekt je tečka, dvě tečky odkazují o dvě úrovně výše ve stromu objektů. Zápis `cerny.hwlab.` představuje objekt se jménem `cerny` v sousedním kontejnerovém objektu `hwlab`.

17.3 Synchronizace času

Operace s objekty eDirectory by měly být prováděny v tom pořadí, v jakém byly vznášeny požadavky na jejich provedení. Každá žádost o práci s objekty proto obsahuje časové razítko doby svého vzniku. V rozsáhlé síti s více servery je třeba zajistit, aby všechny servery byly navzájem časově synchronizovány. Teprve po vytvoření jednotného "síťového času" je možné pracovat s eDirectory.

Dle počtu serverů, topologie sítě, rychlosti přenosových cest a přesnosti lokálních hodin serverů lze volit různé strategie pro vzájemnou synchronizaci času. Jednotlivé souborové servery

se tak stávají i časovými servery, přičemž rozpoznáváme několik typů časových serverů.

Single Reference.Časový server typu Single Reference je jediným zdrojem přesného času v síti. Přesný lokální čas tohoto serveru je nastavován operátorským zásahem. Je-li v síti používán Single Reference server, nesmějí být použity servery typu Primary ani Reference. Jde o schema vhodné pro menší lokální sítě.

Primary. Server Primary synchronizuje svůj čas nejméně s jedním dalším serverem Primary nebo Reference serverem. Jimi stanovený síťový čas je poskytován serverům typu Secondary. V případě sítí propojených pomalejšími dálkovými linkami by v každé geografické zóně měl být alespoň jeden server tohoto typu.

Reference. Je-li použit tento typ serveru, stává se jediným místem distribujícím přesný čas ostatním serverům. Interní hodiny Reference serveru bývají řízeny přesným externím zdrojem.

Secondary. Sekundární servery přebírají přesný čas z výše uvedených serverů a navzájem jej synchronizují s ostatními Secondary servery.

V novějších verzích NetWare je možné společný síťový čas serverů odvozovat i od světového času UTC prostřednictvím standarního internetovského protokolu NTP.

17.4 Operační systém NetWare

Operační systém NetWare je optimalizován pro efektivní poskytování služeb souborového serveru. Jde o systém s nepreemptivním plánováním. Jednotlivé procesy se musejí dobrovolně vzdávat procesoru. Pokud se proces z tohoto hlediska nechová korektně, může na delší dobu přerušit až zcela zastavit funkci serveru. To je poněkud nepříjemné při případné tvorbě vlastních aplikačních modulů a jejich odlaďování. Předností tohoto způsobu plánování naopak je, že nedochází k nadbytečnému přepínání kontextu a zvyšování režie operačního systému.

Z pohledu programátora jde o opravdový operační systém, který je vybaven správou operační paměti, plánovačem pro spouštění a synchronizaci jednotlivých procesů a vláken.

Server (jádro serveru) je spouštěn z prostředí MS DOS jako program `server.exe`. Jeho vlastnosti lze dále rozšiřovat zaváděním programových modulů zvaných *NetWare Loadable Module*, NLM. Typicky mezi ně patří ovladače diskových jednotek, komunikačních adaptérů, podpora pro další poskytované služby (např. tiskový server), administraci serveru a též aplikační moduly (např. databázový server).

17.5 Aplikační server

Server NetWare se postupně stal i aplikačním serverem. K dispozici je www server Apache s možností tvorby skriptů v PHP či Perlu. K dispozici je celá řada databází od MySQL až po Oracle. Přeportovány jsou nástroje a knihovny pro zabezpečenou komunikaci SSL. Lze provozovat vlastní certifikační autoritu, která pro ukládání dat využívá služeb eDirectory.

V poslední době je velký důraz kladen i na javovské prostředí, což se projevuje existencí Jakarta Tomcat serveru pro provozování servletů. V javě jsou psány i některé administrační nástroje, které pak lze provozovat jak přímo v prostředí operačního systému serveru, tak i na klientských stanicích.

17.6 Souborový systém

Server má svůj vlastní souborový systém. V novellských oblastech fyzických disků se vytvářejí logické svazky (volumes). Každý svazek má vlastní označení (`SYS:`, `DATA:` apod.). Na klientských pracovištích si uživatelé sítě tyto svazky mohou připojit (namapovat), přiřadit jim označení MS DOSových diskových jednotek (`F:` apod.) a dále se soubory na nich uloženými pracovat běžným způsobem.

Diskový svazek serveru může být ve skutečnosti složen z několika segmentů umístěných na různých fyzických discích serveru. Při zaplnění svazku jej lze za chodu serveru rozšířit o další segment z dosud nezaplněné novellské oblasti některého disku.

Protože alokační blok může mít velikost až 64 kB, ztráta diskové kapacity při práci s malými soubory může být citelná. Proto lze používat tzv. subalokaci, kdy je samostatně sledován nevyužitý prostor v posledních alokačních blocích souborů. Jednotlivé neobsazené sektory o velikosti 512 B lze přidělovat jiným souborům a tím ztrátu kapacity podstatně snížit.

Další úsporu diskové kapacity lze dosáhnout kompresí souborů. Pokud se s nějakým souborem delší čas nepracuje, může jej server v době nižšího zatížení zkomprimovat. Z pohledu uživatele sítě není rozdíl v práci s běžnými a komprimovanými soubory. Při příjmu prvého (nebo dalšího) požadavku na práci s komprimovaným souborem jej server dekomprimuje do původní podoby. Znamená to ale, že na svazku musí být dostatek volného prostoru pro dekomprimaci souborů. Pokud není, pracuje server trvale nad komprimovanými soubory a ztrácí tím část svého výkonu.

Jména souborů a adresářů vytvářejí tzv. jmenný prostor (name space). Klienti s operačním systémem MS DOS pracují se soubory o délce jména 8+3 znaky bez rozlišení malých a velkých písmen. Jiné představy o jménu souboru mají uživatelů různých verzí Windows, jiné představy mají uživatelé Unixu nebo Apple Macintosh. Na jednom novellském svazku proto může být zavedeno několik jmenných prostorů. Každý soubor pak má několik jmen.

Pro podporu databázových aplikací je k dispozici transakční systém. V pomocném souboru si poznamenává průběh rozpracovaných transakcí. Pokud transakci nelze úspěšně dokončit, dosud změněné záznamy v databázových souborech obnoví do původního stavu.

17.6.1 Atributy souborů a adresářů

Každý soubor i adresář může mít nastaveny stejné atributy jako v jsou MS DOSu. NetWare zavádí atributy další. Význam atributů je shrnut v tabulkách 17.3 a 17.4.

Pro jednotlivé adresáře nebo celé svazky lze stanovit limity (kvóty) na čerpání diskové kapacity jednotlivými uživateli.

17.6.2 Přístupová práva k souborům a adresářům

Efektivní přístupová práva uživatele k nějakému souboru či celému adresáři jsou dána sjednocením přístupových práv, která jsou poskytnuta v tomto adresáři (souboru) právě tomuto uživateli a dále též všem skupinám, do kterých je uživatel zařazen. Přístupová práva k souborům a adresářům lze též stanovit pro celé kontejnerové objekty. Pak se vztahují na všechny jim podřízené objekty. Seznam možných typů přístupových práv je stručně shrnut v tabulce 17.5.

Nejsou-li přístupová práva k souboru nastavena, aplikují se práva nastavená pro celý adresář. Podobně, nejsou-li nastavena práva pro adresář, dědí se z nadřízeného adresáře. V případě potřeby lze dědění potlačit maskou přístupových práv IRF.

Název	Zkratka	Význam
Archive needed	A	význam totožný s MS DOSem
Copy inhibit	Ci	soubor nelze kopírovat; má význam jen pro Mac
Delete inhibit	Di	soubor nelze zrušit nebo přepsat
Don't compress	Dc	soubor nebude komprimován
Don't migrate	Dm	soubor nelze odklidit na sekundární paměťové zařízení
Don't subalocate	Ds	zákaz subalokace bloků pro často rozšiřované soubory
Execute only	X	soubor nelze kopírovat ani archivovat, pouze provést jako program; NetWare neposkytuje prostředky ke zrušení tohoto atributu
Hidden	H	význam totožný s MS DOSem
Immediate compression	Ic	po ukončení práce se souborem bude soubor vzápětí komprimován
Purge	P	zrušený soubor není možno programem Filer obnovit
Read only	Ro	význam totožný s MS DOSem; s nastavením tohoto atributu se nastaví i Di a Ri
Rename inhibit	Ri	soubor je chráněn proti přejmenování
Shareable	Sh	se soubor může pracovat více uživatelů současně
System	Sy	význam totožný s MS DOSem
Transactional	T	transakční operace jsou podporovány systémem pro sledování transakcí (TTS)

Tabulka 17.3: Atributy souborů

Název	Zkratka	Význam
Delete inhibit	Di	adresář nelze zrušit
Don't Compress	Dc	soubory v adresáři nebudou komprimovány
Don't migrate	Dm	soubory v adresáři nebudou migrovat na sekundární paměťové zařízení
Hidden	H	význam jako v MS DOSu
Immediate Compression	Ic	soubory v adresáři budou po použití komprimovány
Purge	P	soubory zrušené z adresáře nelze obnovit
Rename inhibit	Ri	adresář nelze přejmenovat
System	Sy	význam jako v MS DOSu

Tabulka 17.4: Atributy adresářů

Název	Zkratka	Význam
Supervisor	S	právo supervisor v sobě zahrnuje všechna práva k souboru či adresáři; toto právo nelze potlačit maskou přístupových práv
Read	R	možnost číst obsah souboru
Write	W	právo měnit obsah existujícího souboru
Create	C	možnost vytvořit nový podadresář nebo soubor; do nového souboru lze bezprostředně po jeho vytvoření zapisovat, aniž by k tomu bylo nutné mít právo Write
Erase	E	možnost rušit soubory a adresáře (pokud to jejich atributy dovolují)
Modify	M	právo měnit atributy souborů a adresářů
File scan	F	právo zjišťovat jména souborů a adresářů; soubor lze utajit před příkazem DIR
Access control	A	poskytnutí možnosti definovat přístupová práva a jejich masku k dotyčnému souboru či adresáři

Tabulka 17.5: Přístupová práva k adresářům a souborům

17.7 Audit

Důvěryhodný uživatel může vykonávat funkci auditora. Nepotřebuje k ní žádná zvláštní přístupová práva ani se nepředpokládá znalost administrace serveru. Auditor jen vyhodnocuje, kdo a jak pracuje se soubory nebo objekty eDirectory. V tom je auditor zcela nezávislý na administrátorovi sítě a v konečném důsledku tak kontroluje i jeho činnost.

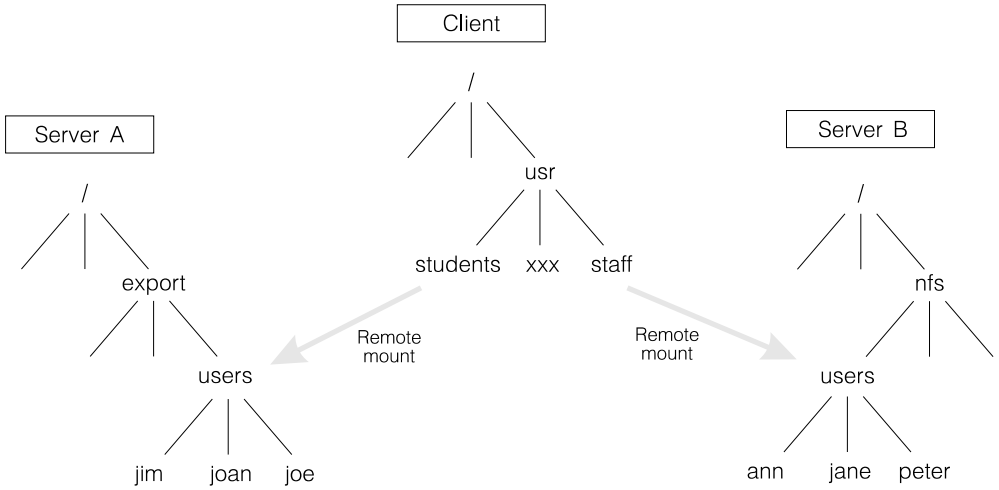
Auditor stanoví, jaké typy operací budou sledovány a zaznamenávány. Lze sledovat prakticky všechny typy operací s objekty eDirectory, tedy jejich vytváření, rušení, změny objektů a přístupových práv k nim. V souborovém systému lze sledovat změny určitých souborů a jejich původce, nebo naopak lze zaznamenávat souborové aktivity konkrétního uživatele sítě. Záznamy lze následně vyhodnocovat podle různých kritérií, jakými jsou čas, typ události nebo její původce.

18. UNIX: NFS, AFS, DCE

Mezi systémy podporující práci v lokálních sítích je nutné počítat i ty, ve kterých se servery i klientská pracoviště opírají o operační systém UNIX. Vzhledem k možnostem hostitelského systému jde ve srovnání se systémy opírajícími se o NCP nebo SMB o mnohem pružnější řešení. Technologickým standardem se v této oblasti stal systém *NFS* (Network File System) firmy Sun Microsystem (ponecháme-li stranou jednoduché služby jako *FTP* nebo *lpr*).

NFS

Systém NFS má podobnou vnitřní strukturu jako systémy, které jsme si uvedli dříve (obr. 18.1). Aplikace využívá transparentní rozhraní *VFS* (Virtual File System), které rozděluje požadavky na lokální a vzdálené. Vzdálené požadavky jsou podpořeny mechanismem volání vzdálených procedur *SunRPC* (Remote Procedure Call) doplněným o knihovnu funkcí pro překlad dat *XDR* (External Data Representation).

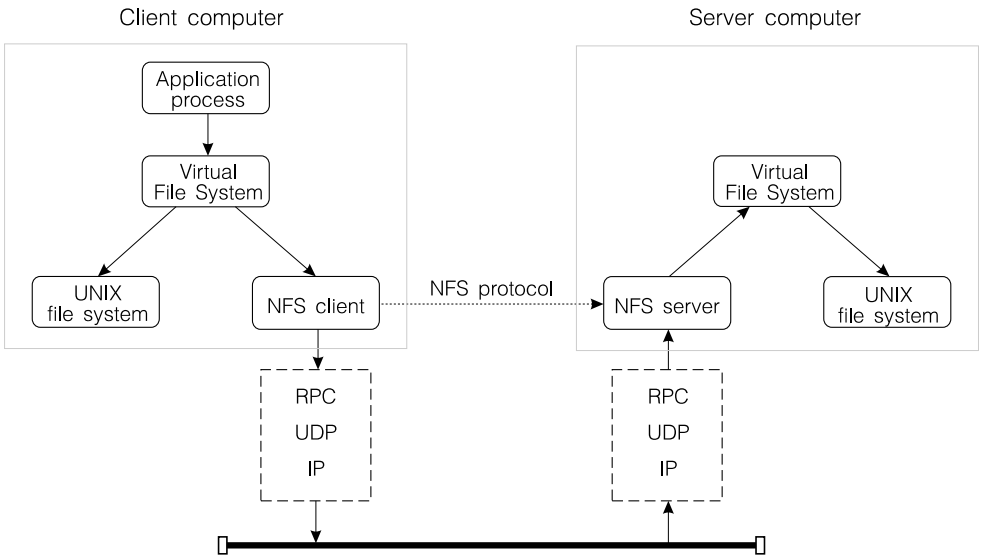


Obrázek 18.1: Adresářové vazby v systému NFS

Přístup k lokálním i vzdáleným souborům se opírá o logické spoje mezi stromovými adresáři fyzicky oddělených počítačů (obr. 18.2). Počítač, dovolující zpřístupnění svých adresářů, uvádí přístupová místa, na která se lze připojit, v souboru /etc/exports. Počítač, který si vzdálené adresáře připojuje, tak může učinit příkazem *mount* (např. při spoustění). Dočasné vazby na vzdálený adresář lze realizovat procesem Automounter.

Pro zajištění shodné sémantiky vzdáleného a lokálního přístupu i při výpadku serveru je server NFS koncipován jako *bezestavový*. Veškeré informace spojené s přístupem k souborům jsou udržovány na straně klienta, vzdálené operace jsou *idempotentní* a lze je opakovat (po výpadku komunikace nebo po restartu serveru).

Použití *paměti cache* na straně serveru je samozřejmostí, na rozdíl od dříve uvedených systémů NFS využívá paměť cache i na *straně klienta*. Bloky spravovaných dat, *stránky* mají typicky délku 8 kB. Mechanismus zajišťující konzistenci lokální kopie s daty na serveru se opírá o ověřování, zda na serveru nedošlo ke změně v souboru, ke kterému se lokální kopie vztahuje. Takové ověření má platnost po dobu 3 vteřin pro data souboru a 30 vteřin pro data adresářů.



Obrázek 18.2: Struktura systému NFS

AFS

Na základě zkušeností se systémem NFS v lokálních i rozsáhlých sítích byly vytvářeny systémy další. Poměrně úspěšným byl systém *AFS – Andrew File System*. Základní rysy systému AFS jsou shodné s NFS. Podstatnou odlišností je však to, že AFS pracuje se souborem jako s celkem. Při požadavku na přístup ke vzdálenému souboru je tento soubor přenesem do lokální oblasti cache (samozřejmě realizované na disku) jako celek. Modifikovaný soubor je předáván zpět serveru až po uzavření souboru. Udržení konzistence dat mezi kopiemi a originálem je podporováno seznamem kopií na straně serveru a mechanismem *call-back*, kterým server předchozí kopie modifikovaného souboru zneplatňuje. Filosofie systému AFS se opírá o data, získaná statistickými analýzami práce v systémech UNIX. Z nich vyplývá převaha práce s malými soubory (do 10 kB), s mnohem častějším čtením než zápisem, a typicky se sekvenčním zpracováním. Malé soubory jsou sdíleny pouze výjimečně, a pokud tomu tak je, tak většinou pro čtení.

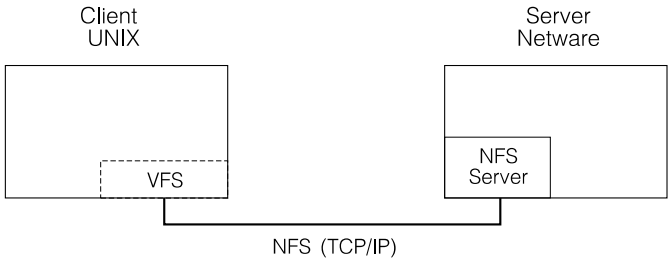
Interoperabilita s jinými sítěmi

Abychom se vrátili zpět k běžnějším technologiím, uvedeme si, že firemní systémy UNIX bývají pro komunikaci v lokálních sítích doplňovány o podporu klientských pracovišť využívajících protokoly IPX/SPX, NetBIOS nebo AppleTalk, jako příklad můžeme uvést AIX Connections pro systém AIX (str. **??**). Jindy je server konkrétní lokální sítě realizován jako proces spustitelný pod operačním systémem UNIX, jako přiklad může sloužit implementaci Pathworks pro UNIX (str. **??**). Běžné systémy UNIX, které podporu jiných protokolů než jsou protokoly TCP/IP neposkytují, lze doplnit o *portabilní rozšíření*. Příkladem může být systém Samba, který tvoří klíčové moduly:

smbd - SMB server běžící na "souborovém serveru" a dovolující klientským pracovištím DOS, Windows, WindowsNT a OS/2 přístup k souborům a tiskárnám protokolem SMB,

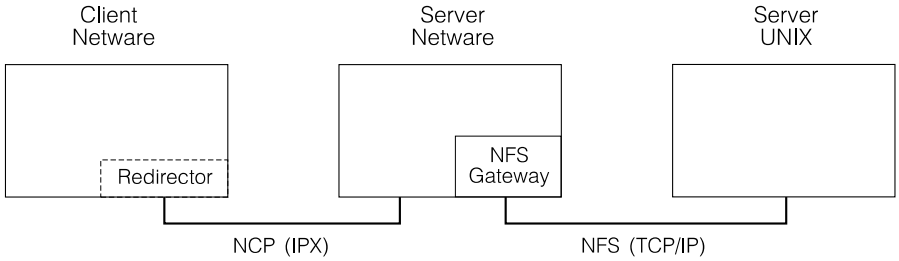
nmbd - name server podporující emulaci NetBIOSu nad TCP/IP a

smbclient - klientské pracoviště běžící pod systémem UNIX.



Obrázek 18.3: Modul NFS serveru lokální sítě

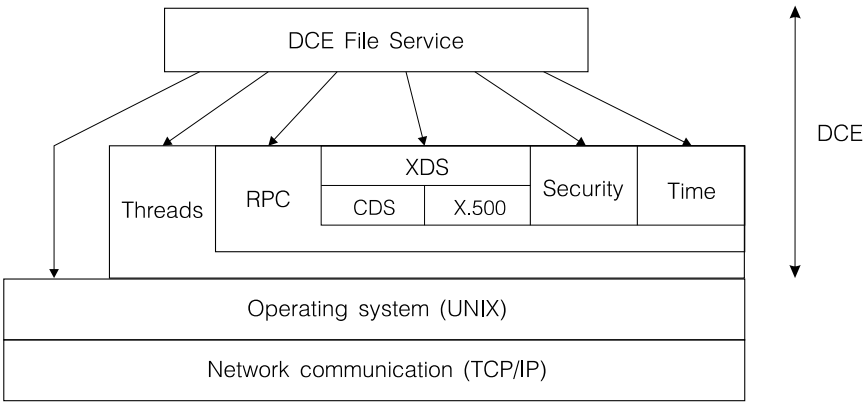
Často se setkáme i s opačným postupem, zpřístupněním souborů a tiskových front serverů lokální sítě (Netware, Windows NT) "klientským pracovištím" pod systémem UNIX využívajícím protokoly TCP/IP. Takové moduly označujeme, podobně jako pod UNIXem, jako *FTP servery*, *NFS servery* (obr. 18.3 pro přístup k souborům) a *lpr servery* (pro přístup k tiskovým frontám). Setkáme se i s moduly, které dovolují serverům lokální sítě přístup k systému NFS a tiskárnám počítačů pod UNIXem. Zde jsou používány termíny *NFS gateway* (obr. 18.4) a *lpr gateway*.



Obrázek 18.4: Modul NFS gateway v lokální síti

DCE

Na závěr této kapitoly (a vlastně i celé části věnované programové podpoře lokálních sítí) si uvedeme technologii, která se stala průmyslovým standardem v oblasti technologických lokálních sítí pod systémem UNIX. Sice se poněkud vymyká zaměření tohoto textu, ale může sloužit jako příklad optimálního řešení "operačního systému" pro lokální síť, jak ji známe v oblasti administrativy. Jedná se o technologii *DCE* (Distributed Computing Environment), její architekturu uvádí (obr. 18.5).



Obrázek 18.5: Architektura systému DCE

Prostředí DCE bylo navrženo pro rozsáhlé systémy rozdělené do samostatně spravovaných skupin počítačů – *buněk* (Cells). Je vystavěno nad operačním systémem UNIX s komunikačními protokoly TCP/IP a je poměrně portabilní a široce rozšířené. Základní služby UNIXu doplňuje DCE o podporu *vláken výpočtu* (Threads), ta odpovídá standardu POSIX 1003.4d. Vlákna jsou nutná pro efektivní realizaci procedurální komunikace *RPC* (Remote Procedure Call). Procedurální komunikace je využívána pro další služby, ale pochopitelně i pro aplikace. Aplikace jsou budovány na principu rozkladu aplikace na klientskou část a na server (*Client-Server* model). Pro jejich vývoj DCE poskytuje prostředky dovolující vytvářet rozhraní Client-Server ve speciálním jazyce *IDL* (Interface Definition Language).

Mezi standardní služby DCE patří adresářové služby *DCE Directory Service*. Ty se opírají o vlastní replikovatelné adresáře samostatně spravovaných buněk *Cell Directory Service* (CDS), a/nebo mohou být navázány na globálně používaný systém ITU-T X.500. Využít lze i systém DNS (Domain Name Service). Autentizaci a autorizaci přístupu k serverům služeb podporují bezpečnostní prostředky *DCE Security Service* opírající se o činnost procesu Security Server v buňce. Ten klientským částem aplikací zprostředkuje přístup k serverům, opírá se přitom o přidělování jednorázových přístupových práv (*Tickets*) a o seznamy oprávněných klientů (*ACL – Access Control List*). Podporuje současně ochranu datových přenosů mezi klientskými a serverovými částmi aplikací symetrickou šifrou *DES* (Data Encryption Standard). Řada aplikací vyžaduje koordinaci systémového času mezi počítači, na nichž běží. Koordinaci mezi počítači buňky a více časovými servery podporuje *DCE Distributed Time Service* (DTS).

Konečně, *DCE Distributed File Service* (DFS) dovoluje rozložit soubory do skupin, označovaných jako *filesets*. Ty mohou být umístěny na libovolném serveru buňky, přístup aplikací k nim zprostředkují adresářové služby CDS. Podporována je možnost přemístit soubory skupiny na nejvýhodnější počítač v buňce. Skupiny souborů mohou být pro zvýšení spolehlivosti a rychlosti přístupu replikovány. Přístup k datům je zprostředkován technologií Client-Server a využívá možností zpřístupnění přes *DCE Security Server*. Možnosti ochrany dat tak jsou mnohem širší, než u běžných souborových serverů. Podobně jako u dříve uváděných souborových systémů NFS a AFS i systém DFS podporuje oblast paměti chache na straně klienta i serveru.

Literatura

[1] Boisseau M., Demange M., Munier J-M.: *High Speed Networks.* John Wiley & Sons, 1994. ISBN 0-471-95109-9

[2] Black U.: *Computer Networks – Protocol, Standards and Interface.* Prentice Hall, 1993. ISBN 0-13-090861-4

[3] Stallings W.: *Networking Standards – A Guide to OSI, LAN, and MAN Standards.* Addison-Wesley, 1993. ISBN 0-201-56357-6

[4] Sloman M.: *Network and Distributed Systems Management.* Addison-Wesley, 1994. ISBN 0-201-62745-0

[5] Přichystal O.: *Novell Netware 3.x a 4.x.* Computer Press, 1996. ISBN 80-85896-21-4

[6] Best K., Burnham K.: *Novell Netware 4.0.* Novell Press/Grada, 1993. ISBN 80-7169-024-4

[7] Rosenberry W., Kenney D., Fisher G.: *Understanding DCE.* O'Reilly & Associates, 1993. ISBN 1-56592-005-8

[8] Tanenbaum A.: *Computer Networks – 2nd ed.* Prentice-Hall, 1988. ISBN 0-13-162959-X

[9] Miller M.A.: *LAN Protocol Handbook.* M&T Publishing, 1990. ISBN 1-55851-099-0

[10] Zenk A.: *Lokale Netze – Kommunikationsplatform der 90er Jahre.* Addison-Wesley 1994. ISBN 3-89319-741-9

Text vychází z informací v literatuře uvedené v tomto přehledu, z norem a specifikací síťových technologií a z řady technických materiálů a publikací firem Digital, IBM, Microsoft, Novell. Pro čtenáře, který se chce seznámit podrobněji s řadou zde popsaných technologií autoři odkazují na již zmíněný přehled doporučené četby.

Index