Lokální sítě

Jan Janeček, Martin Bílý

Říjen 1996

Předmluva

Tento text je učební pomůckou pro studenty denního studia Elektrotechnické fakulty ČVUT, kteří si zapsali volitelný 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.

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, 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 16 napsal Ing. Martin Bílý, ostatní kapitoly Ing. Jan Janeček, CSc. Chceme poděkovat všem, kteří nám s přípravou textu pomohli, poskytli potřebné materiály a firemní informace. Chceme poděkovat Ing. Martinovi Červenému, jehož připomínky přispěly k přehlednosti a užitečnosti předkládaného materiálu.

Text vychází v této formě poprvé a autoři uvítají poznámky pečlivého čtenáře k jeho formě a obsahu.

Praha, říjen 1996 autoři

Obsah

1 Úvod **4**

2 Architektura, topologie a média **5**

2.1 Topologie 5

2.2 Přenosová média 7

2.3 Architektura komunikačních funkcí 13

3 Širokopásmové sítě **18**

4 Náhodný přístup ke sdílenému médiu **22**

4.1 Aloha 22

4.2 Metody CSMA 25

4.3 Metody CSMA/CD 28

4.3.1 Ethernet 29

4.3.2 Appletalk 30

4.4 Deterministické řešení kolize – CSMA/DCR 30

4.5 Metody CSMA/CA 32

5 Deterministický přístup ke sdílenému médiu **33**

5.1 Centralizované řízení 33

5.2 Distribuované řízení 35

5.3 ARCNet 38

5.4 IEEE 802.4 39

6 Kruhové sítě **42**

6.1 Newhallův kruh 43

6.2 Pierceův kruh 44

6.3 Vkládání rámců 45

6.4 IBM Token Ring (IEEE 802.5) 45

6.5 FDDI 48

6.6 FDDI II 51

7 Propojování lokálních sítí **53**

7.1 Most – Bridge 54

7.2 Směrovač – Router 59

8 Ethernet (IEEE 802.3) 61

8.1 Technologie 10BASE5 63
8.2 Technologie 10BASE2 64
8.3 Technologie 10BROAD36 65
8.4 StarLAN 66
8.5 Technologie 10BASE-T 67
8.6 Optické spoje FOIRL a 10BASE-FX 68
8.7 Přepojovaný Ethernet 69
8.8 Technologie 100BASE-TX a 100BASE-FX 72
8.9 Isochronní Ethernet 73

9 VG-AnyLAN 75

10 Metropolitní síť, rozhraní DQDB 79

11 ATM 82

11.1 Synchronní provoz – STM 82
11.2 Asynchronní provoz – ATM 84
11.2.1 Architektura ATM 86
11.2.2 Adresace a signalizace (navazování spojení) 89
11.3 Lokální sítě ATM 90
11.3.1 Adresace a směrování 92
11.4 Virtuální sítě, emulace LAN 93

12 Bezdrátové sítě 96

12.1 Rádiové spoje 96
12.1.1 Rozprostřené pásmo 97
12.1.2 Směrové spoje 99
12.1.3 Rádiové sítě LAN 100
12.2 Optické spoje 103

13 Komunikační protokoly 104

13.1 Linkové protokoly – rozhraní IEEE 802.2 104
13.2 Síťové protokoly 109
13.2.1 NetBIOS, NetBEUI 109
13.2.2 IPX/SPX 111
13.2.3 TCP/IP 113
13.3 Směrování 115

13.3.1 RIP 116
13.3.2 OSPF 117

14 Správa lokálních sítí **119**
14.1 Síťové analyzátory 119
14.2 CMIS/CMIP 120
14.3 SNMP 122
14.4 RMON 123

15 Síťové operační systémy **124**

16 Novell Netware **128**
16.1 Komunikační protokoly v sítích Novell 128
16.2 Klient systému NetWare 129
16.3 Novell Directory Services 130
16.3.1 Objekty NDS 132
16.3.2 Přístupová práva k objektům NDS 133
16.3.3 Identifikace objektů NDS 133
16.4 Synchronizace času 134
16.5 Operační systém NetWare 134
16.6 Souborový systém 135
16.6.1 Atributy souborů a adresářů 136
16.6.2 Přístupová práva k souborům a adresářům 137
16.6.3 Ochrana před selháním diskového systému 138
16.7 Audit 138

17 IBM: PC-LAN, LAN Server a Warp Connect **139**

18 Microsoft: LAN Manager, Windows (NT) **142**

19 Banyan VINES **145**

20 DEC Pathworks **146**

21 UNIX: NFS, AFS, DCE **147**

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 isochronní Ethernet. Přepojovací technologie ATM, která se začíná prosazovat v páteřích lokálních sítí, ale i při připojování výkonnějších počítačů, 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 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.

Obr. 2.1: Přenos v soustředěné a rozlehlé síti

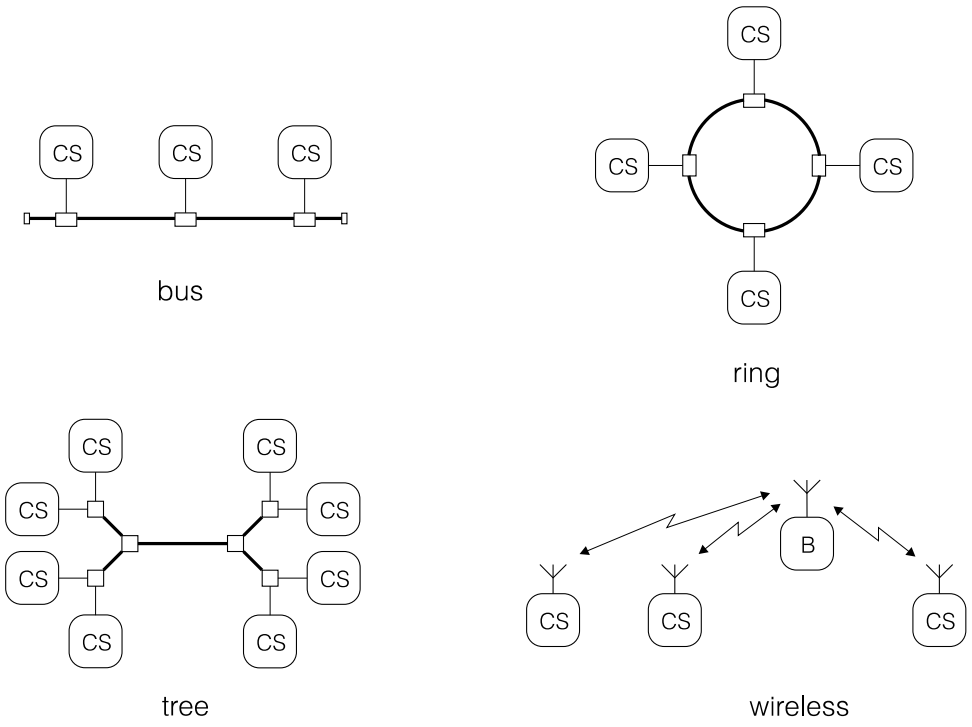
Mezi sítě, které takto charakterizujeme jako rozlehlé, patří i sítě s vysokou rychlostí přenosu a středními překonávanými vzdálenostmi (optické městské sítě). Soustředěné sítě zahrnují běžné sítě lokální a sítě rádiové (pro jejich malou přenosovou rychlost). Pro řadu metod řízení musíme zajistit velmi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

2.1 Topologie

Topologií se 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*. Lokální sítě využívají přímého propojení komunikačních stanic sdíleným kanálem, signál vyslaný jednou ze stanic je přijímán ostatními stanicemi sítě. Tyto 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,
- spolehlivost – odolnost sítě proti výpadkům komponent,
- složitost obsluhy,
- výkonnost – využití přenosové kapacity média, zpoždění zprávy.

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



Obr. 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.

Stromové (hvězdicové) sítě používají podobných metod řízení jako sítě sběrnicové.

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.

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. Nejčastěji se setkáváme s nesymetrickým (*koaxiální kabel*) a symetrickým (*kroucený dvoudrát – twisted pair*) vedením. Řada sítí se opírá o optická vlákna a ta jsou alternativním médiem i pro klasické technologie. Začínají se objevovat 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 v 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 20 Mb/s. 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). 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, 70 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 Ethernet 100BASE-T, FDDI a ATM na vzdálenost 100 m, přenosové rychlosti jsou zde do 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.

Dalším 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,
Type 9 - jako Type 1, ale levnější.

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).

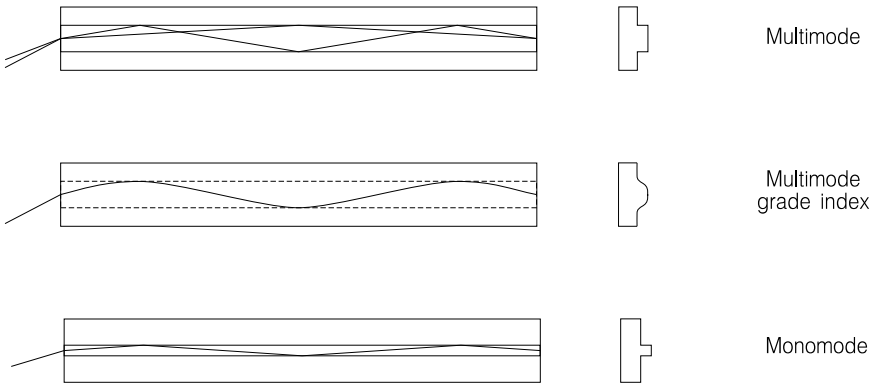
Strukturovaná kabeláž

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. V poslední době se objevují čtyřpárové kabely se společným stíněním označované jako *FTP* (Foiled Twisted Pair – fólií stíněné zkroucené páry) nebo *S(FTP)* (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 S(FTP)) 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 2.5 Gb/s na kilometrové vzdálenosti. 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.



Obr. 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 světelný paprsek se médiem šíří s více úhly odrazu (více vidy). Takových diskrétních hodnot jsou u mnohavidových vláken tisíce. Důsledkem odlišných úhlů odrazu je rozdíl v absolvované délce cesty vláknem a z toho vyplývající rozptyl světelného výkonu v čase na výstupu z vlákna. Mluvíme o *vidové disperzi*, ta je hlavním limitem překlenutelné vzdálenosti.

	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

Obr. 2.4: Parametry mnohavidových vláken

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 snížení počtu módů při zachování průměru jádra, které usnadňuje propojování kabelů (ve srovnání s vlákny jednovidovými). Gradientní vlákna s průměrem 65/125 μm používaná v lokální síti FDDI dnes v oblasti lokálních sítí převažují nad vlákny 50/125 μm používanými v telekomunikační technice. 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 (GHz.km) 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. Překlenutelné vzdálenosti jsou pro vlákna se skokovou změnou indexu do 10 km a pro vlákna gradientní do 35 km.

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 9/100 μm, horním limitem pro vlnové délky 1300 a 1550 nm a realizovatelné poměry indexu lomu je zhruba 15 μm). Jejich útlum je 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 1 km délky kabelu) 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 jednak primární ochranou, kterou je tenká vrstvička polyimidu, jednak skundární ochranou. Primární ochrana má sílu do 1 μm a chrání materiál vlákna před vlhkostí. V kritických aplikacích bývá doplňována o tenoučkou uhlíkovou vrstvu nanesenou pod ní na vlákno. Sekundární ochrana má průměr kolem 1 mm a je tvořena vhodnou plastickou hmotou (kevlar, nylon). Kromě kabelů s těsným uložením vlákna v materiálu sekundární ochrany (vnitřní kabely) existují kabely s volným uložením vláken v konstrukci kabelu (vnější kabely).

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 existují konektory, potřebná úprava konce vlákna a montáž konektoru je náročnou operací.

Jako zdroje světla pro světlovodné kabely jsou používány světloemitující diody *LED* (Light Emitting Diode) nebo rychlejší laserové diody *ILD* (Injection Laser Diode) – materiálem je GaAs (850 nm), AlGaAs (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. Jinak řečeno, 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

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

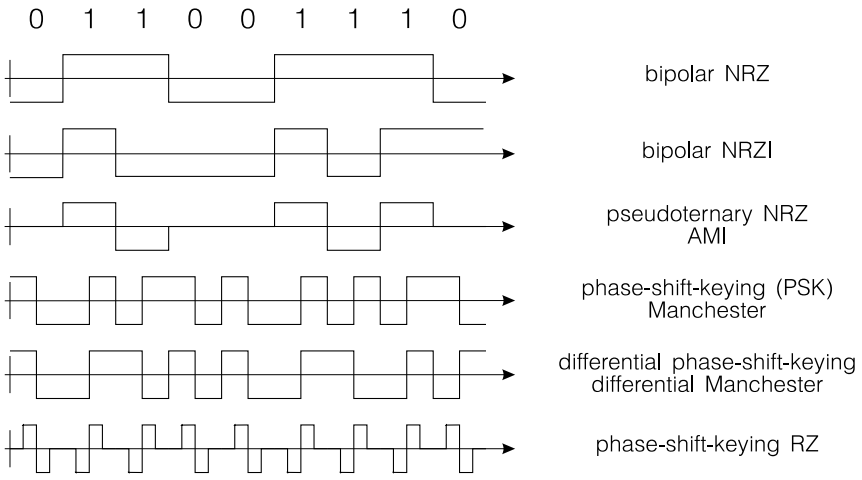
Počet úrovní signálu V nelze s ohledem na poškození spojitého signálu při přenosu (obvykle toto poškození charakterizujeme přídavným signálem – šumem) libovolně zvyšovat; teoretický

limit přenosové rychlosti C kanálu s pásmem o šířce W a odstupem signálu od šumu S/N udává Shannonova věta

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

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.



Obr. 2.5: Kódování datového signálu v lokálních sítích

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 sítí moderních).

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

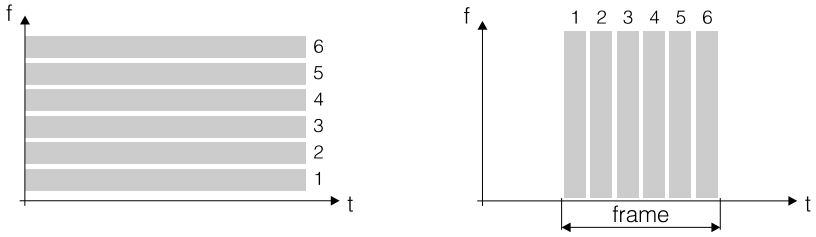
$$u(t) = U \sin(\omega.t + \varphi),$$

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. 99) se setkáme s *multiplexem kódovým* (CDMA – Code Division Multiple Access).



Obr. 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

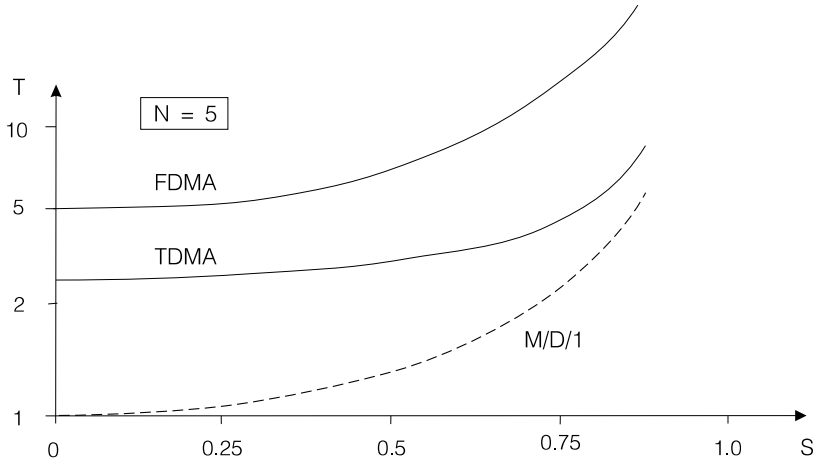
Při časovém multiplexu (*TDMA – Time Division Multiple Access*) přidělujeme přenosový kanál postupně jednotlivým stanicím. Každé stanici je vyhrazen časový úsek (*slot*), ve kterém může vyslat paket určité délky. Časové úseky jednotlivých stanic se pravidelně střídají s periodou, kterou obvykle označujeme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



Obr. 2.7: Závislost zpoždění paketu na zátěži

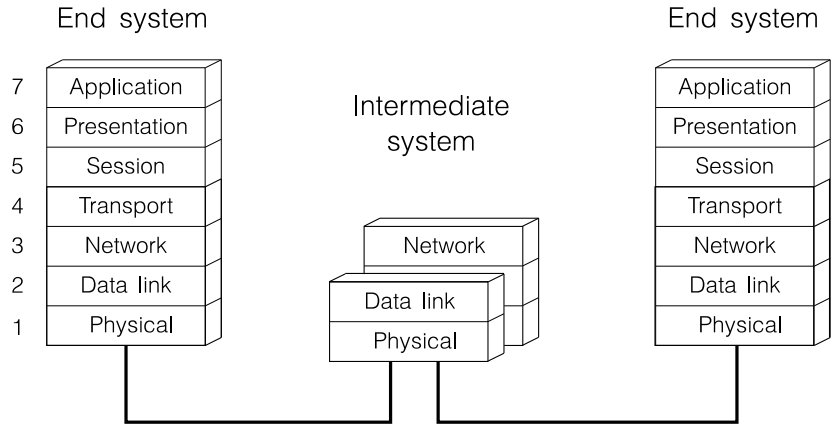
2.3 Architektura komunikačních funkcí

Současné lokální sítě se opírají o technologie, které jsou vesměs definovány standardy normalizačních organizací jako jsou *IEEE* (Institute of Electrical and Electronics Engineers), *ANSI* (American National Standards Institute) a *ISO* (International Organization for Standardization). Patří sem několik variant Ethernetu, kruhová síť IBM Token Ring a sítě pro technologické řízení. Tyto technologie jsou využívány i jako základ standardů sítí pro státní správu GOSIP, sítí pro průmyslové aplikace MAP a sítí pro administrativu TSAP. K historii už patří mimo standardy ležící a dříve často používaná síť ARCNet, význam ztrácí i síť AppleTalk. Dobře definovaný a zavedený je ANSI standard rychlé optické kruhové sítě FDDI. Mimo standardy stojí klasické širokopásmové sítě, v návrhu jsou standardy pro využití rychlých kanálů ATM (Asynchronous Transfer Mode) v lokálních sítích a standardy IEEE pro bezdrátové připojení počítačů k lokálním sítím a pro kombinaci sítí širokopásmových a optických.

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*). Model OSI popisuje komunikaci zajišťovanou počítači, jako hierarchii sedmi vrstev technických a/nebo programových prostředků, kde každá z vrstev zajišťuje funkce potřebné pro vrstvu vyšší a využívá služeb vrstvy nižší. Mezi jednotlivými vrstvami jsou (formou standardů a doporučení)

definována rozhraní (mezivrstvové protokoly), mezi prvky stejné vrstvy jsou definována pravidla komunikace (vrstvové protokoly). Architekturu vrstev modelu OSI ilustruje obr. 2.8.



Obr. 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.

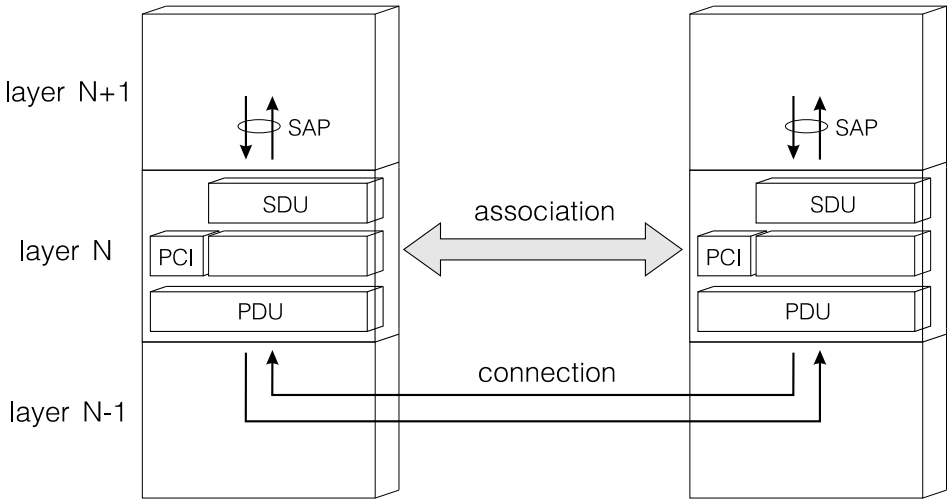
Relační vrstva (Session Layer) vytváří logické rozhraní pro aplikační programy, které používají služeb sítě. Definuje způsob komunikace programů a uživatelský pohled na komunikační kanál.

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.

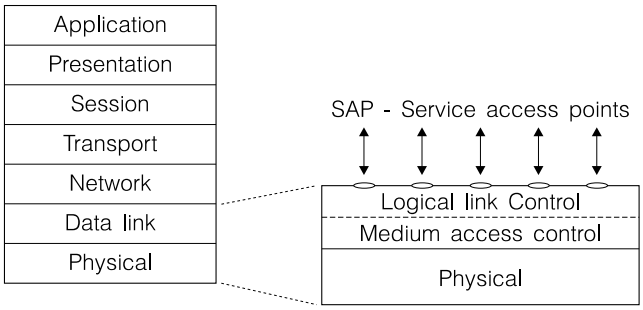
Standardy jednotlivých vrstev definují služby, které vrstva poskytuje (přenos bloků dat *SDU – Service Data Unit*), a způsob, kterým lze těchto služeb využívat (*SAP– Service Access Point*). Popisuje komunikaci uvnitř vrstvy (s protistanicí) a způsob využití služeb nižší vrstvy (přenos bloků dat *PDA – 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*.



Obr. 2.9: Vnitřní struktura vrstvy ISO OSI

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.

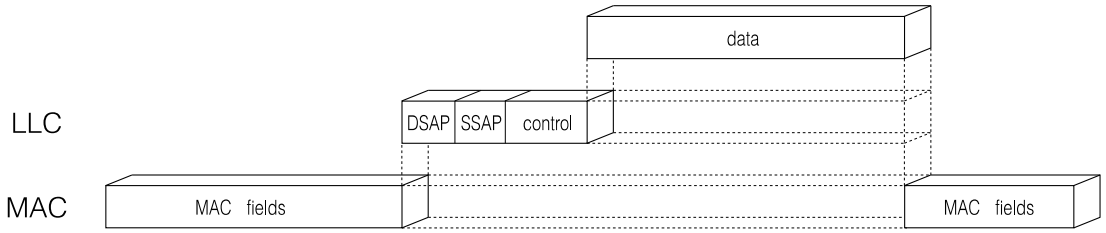


Obr. 2.10: Architektura lokálních sítí IEEE 802

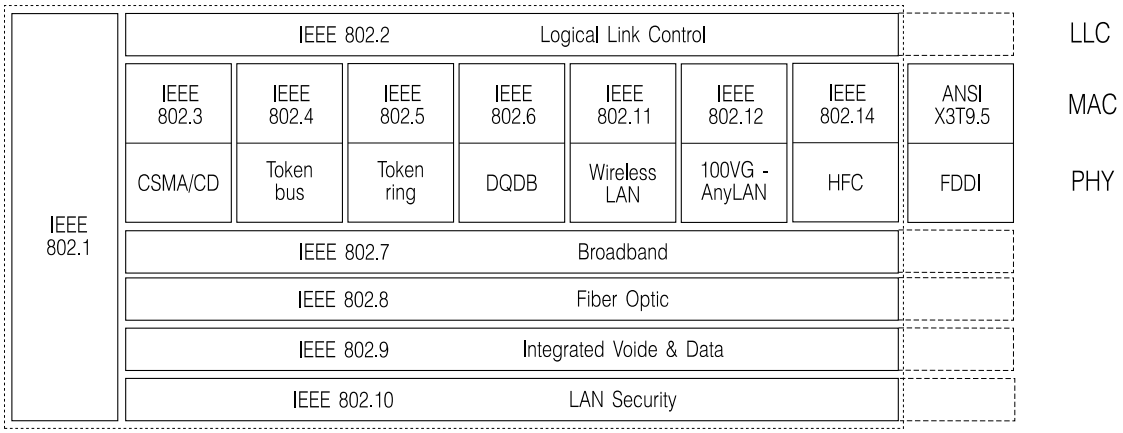
Doporučení IEEE 802 člení nejnižší vrstvy poněkud odlišně od architektury ISO (obr. 2.10). Vytváří vrstvu fyzickou, která definuje média, konektory, signály, a nad ní staví vrstvu řízení přístupu ke sdílenému komunikačnímu kanálu *MAC* (Medium Access Control). Ta definuje formáty rámců, adresaci stanic, 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.

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.



Obr. 2.11: Struktura rámců IEEE 802



Obr. 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.

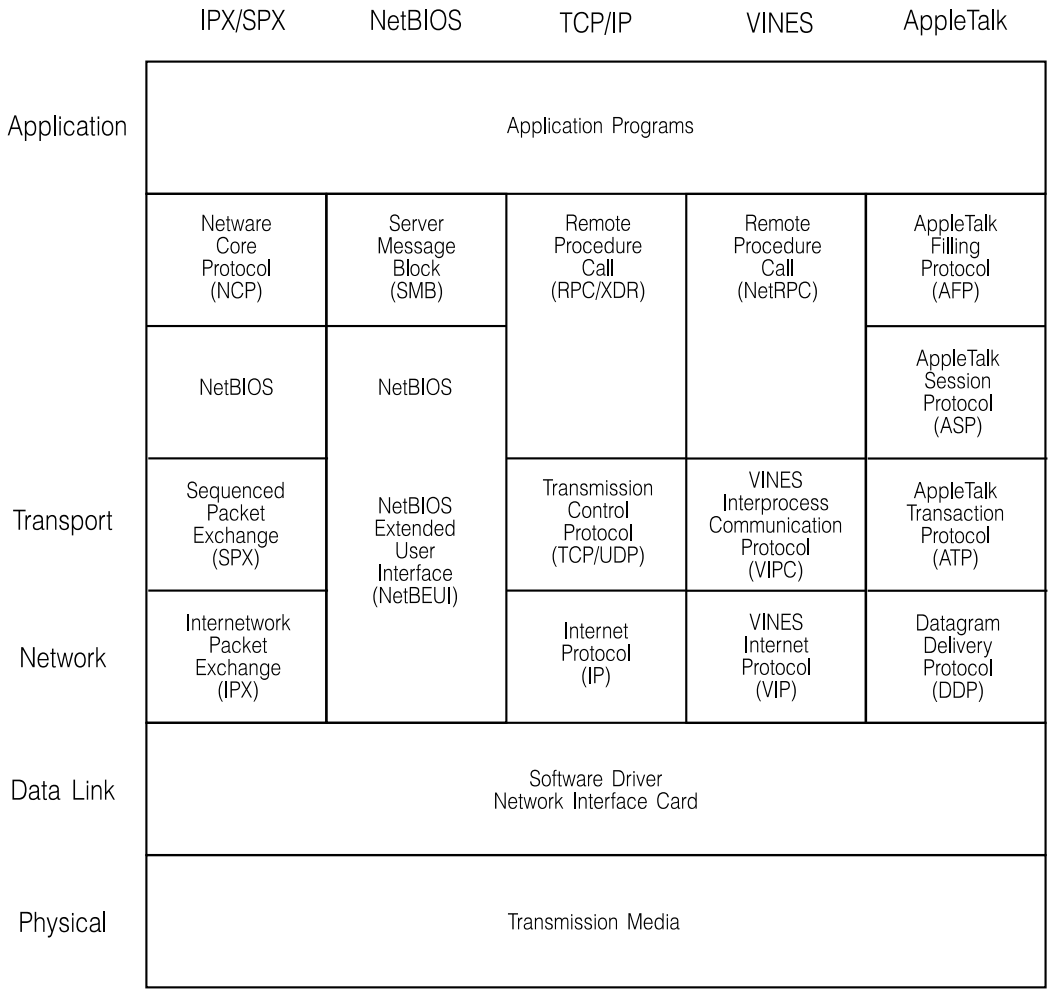
Doporučení *IEEE 802.3, 802.4, 802.5, 802.6, 802.11, 802.12 a 802.14* popisují fyzickou vrstvu a přístup k médiu pro lokální sítě různého typu – pro sběrnicové lokální sítě s náhodným řízením metodou CSMA/CD Ethernet, lokální sítě s deterministickým řízením, kruhové lokální sítě IBM Token Ring, rozhraní metropolitních sítí DQDB, bezdrátové sítě, síť 100 VG-AnyLAN a kombinované širokopásmové 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.

Obr. 2.12 vedle technologií IEEE 802 uvádí jako další specifikaci kruhovou síť FDDI ANSI X3T9.5, která předpokládá přenos rámců se strukturou odpovídající IEEE 802.2 LLC. Původní Ethernet, obvykle označovaný jako Ethernet II nebo DIX (podle jeho specifikace vytvořené firmami Digital, Intel a Xerox), není v obrázku explicitně uveden.

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).



Obr. 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). Obrázek situaci poněkud zjednodušuje, přesnější strukturu některých protokolových sad najdeme v kapitole věnované jednotlivým protokolům a síťovým systémům.

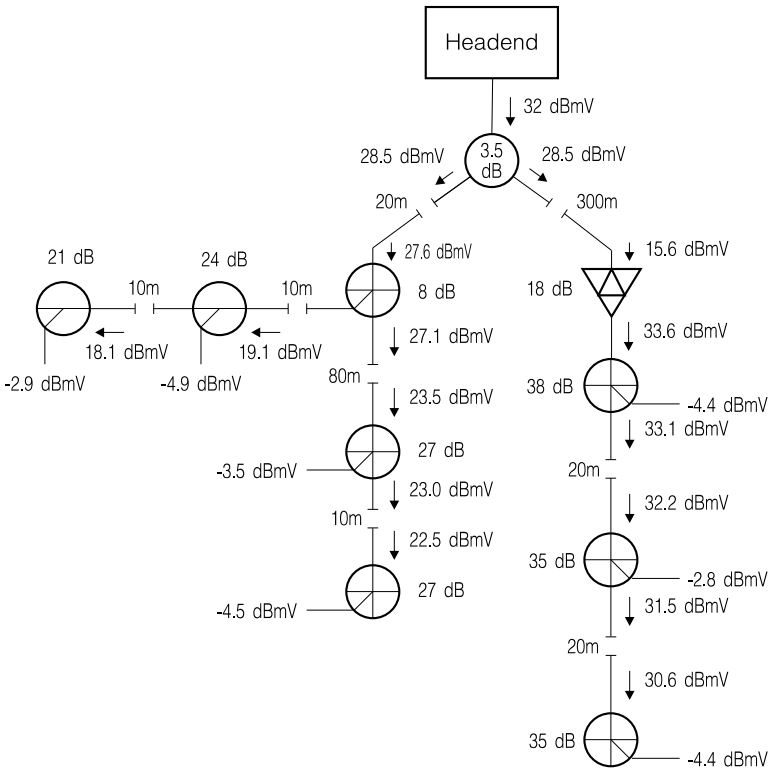
3. Širokopásmové sítě

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.



Obr. 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

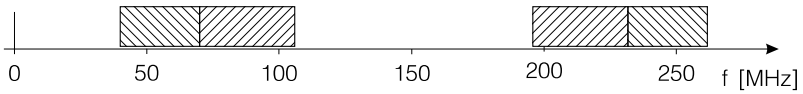
V širokopásmových lokálních sítích jsou využívány metody řízení, které poznáme u sběrnicových sítí s náhodným a deterministickým přístupem. Metody náhodného přístupu CSMA/CD jsou použitelné pro menší lokální sítě, u rozsáhlejších sítí z principu klesá jejich efektivita. Důvodem je jednak doba šíření 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. 65). Častěji se setkáváme s deterministickým řízením (Token-Passing Bus), síť pracující v přeloženém pásmu s deterministickým řízením je základem doporučení IEEE 802.4 (str. 39).

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.



Obr. 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. 109).

Wangnet

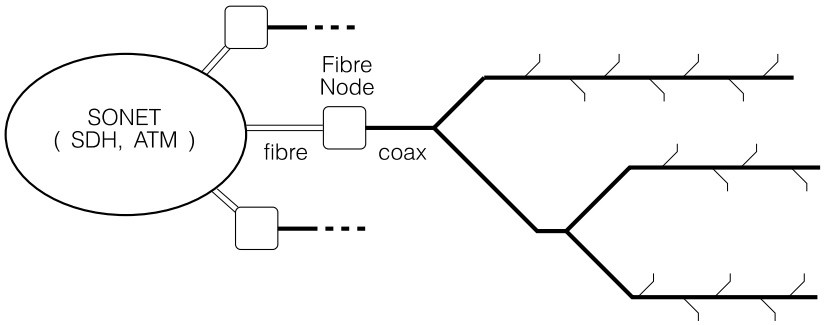
Jako příklad sítě se strukturou kabeláže Dual-Cable si uvedeme síť Wangnet. Má stromovou topologii, pro přenos je využívána dvojice koaxiálních kabelů. Na jeden jsou připojeny vysílače stanic, na druhý přijímače. Kabely, rozbočovače, odbočovače a zesilovače odpovídají běžné kabelové televizi.

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. Podle realizace centrálního prvku označujeme tyto optické systémy jako *pasivní* nebo *aktivní hvězdu*.

HFC – Hybrid-Fibre-Coax

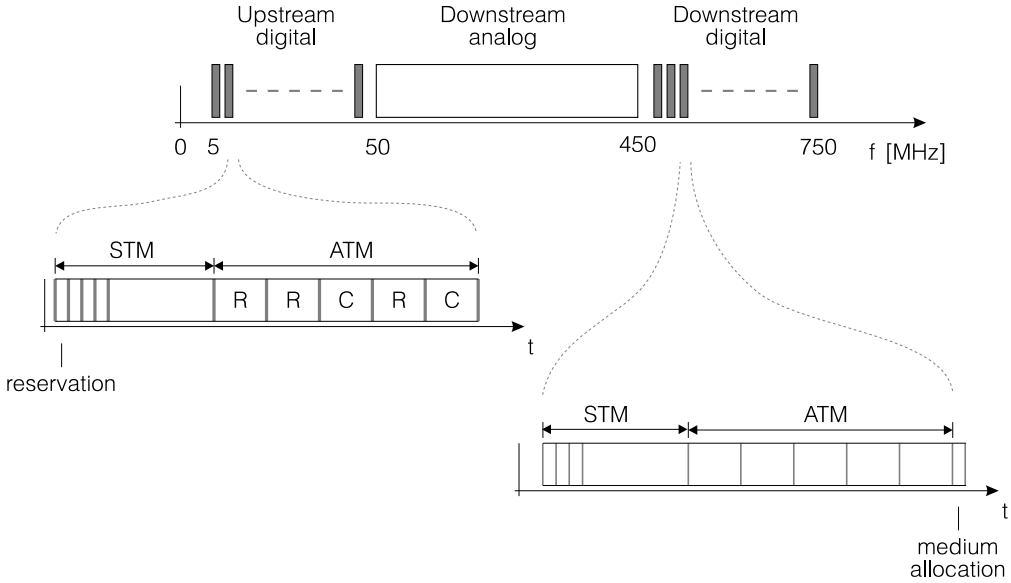
Z předchozích příkladů by se mohlo zdát, že širokopásmová technologie opírající se o koaxiální kabely CATV je spíše otázkou minulosti, alespoň v příkladech, které jsme si zde uvedli, se jedná o poměrně stará řešení. Opak je však pravdou. Využití kabelů CATV pro zpřístupnění moderních telekomunikačních služeb pro území pokrytá (nebo pokrývaná) sítěmi kabelové televize je otázkou blízké budoucnosti. Technologie již mají klíčoví výrobci připravené, v současné době je v rámci IEEE normalizační komise dokončováno doporučení, jehož respektování dovolí spolupráci zařízení různých producentů v jednom systému definovaném doporučením IEEE 802.14 *Hybrid-Fibre-Coax System*.



Obr. 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.



Obr. 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. 82). 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. 22), 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.

4. Náhodný přístup ke sdílenému médiu

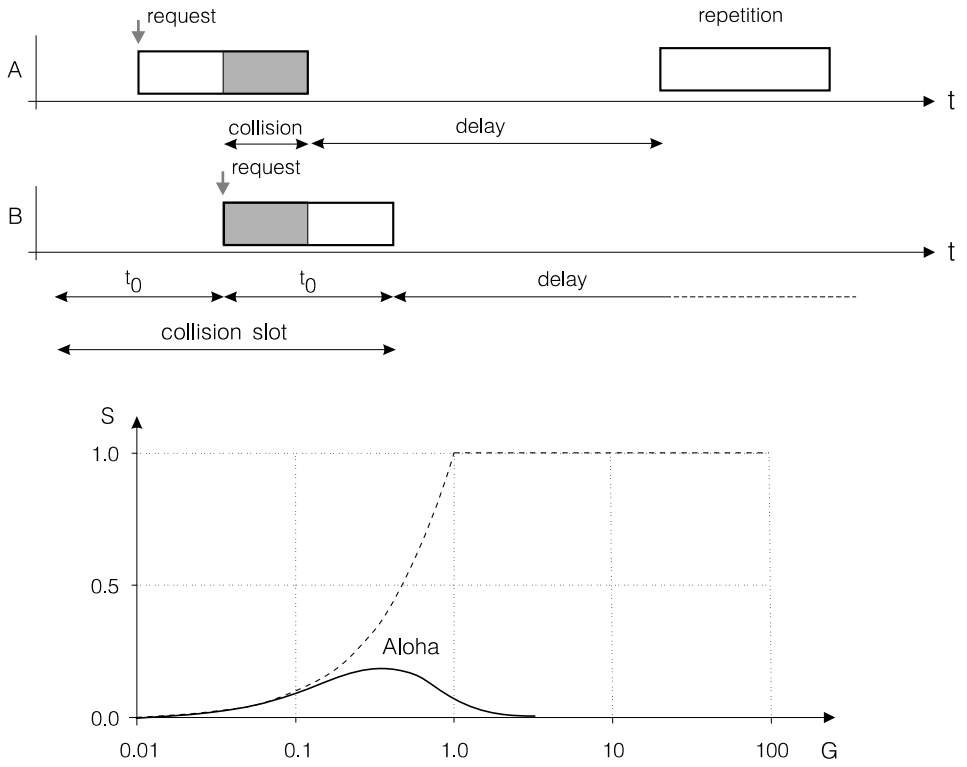
Náhodný přístup ke sdílenému přenosovému kanálu můžeme považovat za nejjednodušší techniku přístupu a za protipól deterministických metod, které si popíšeme později. Jednotlivé stanice podřizují přístup na kanál pouze svému odhadu nebo pozorování.

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.



Obr. 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

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

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

$$S = G.P_0,$$

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

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

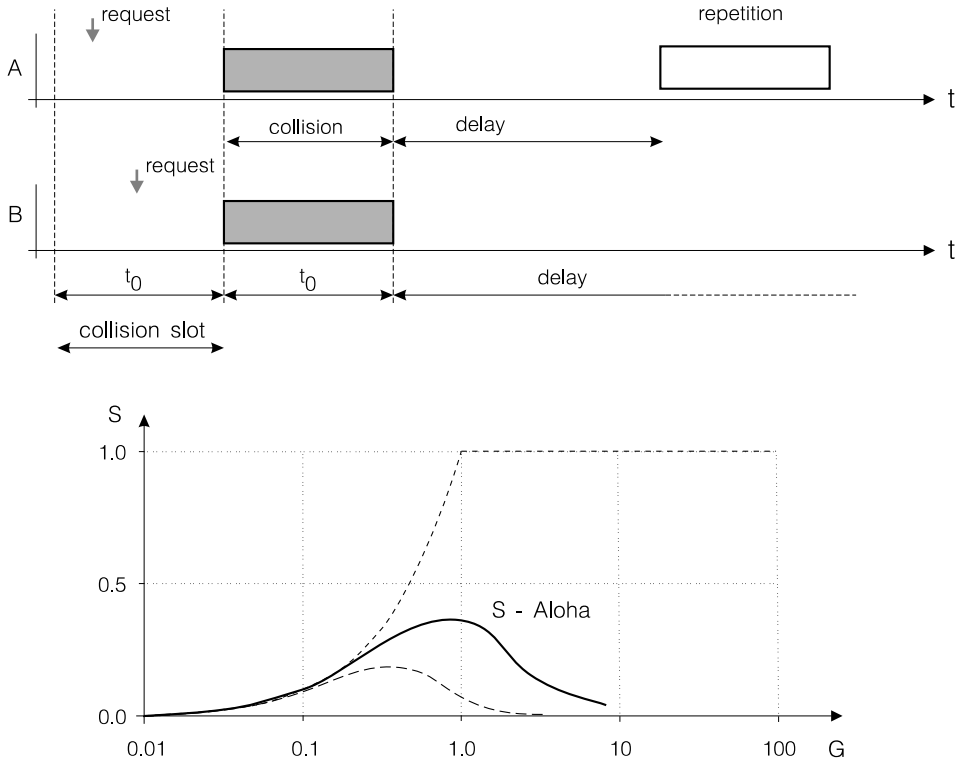
a tedy jednoduchým dosazením

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

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).



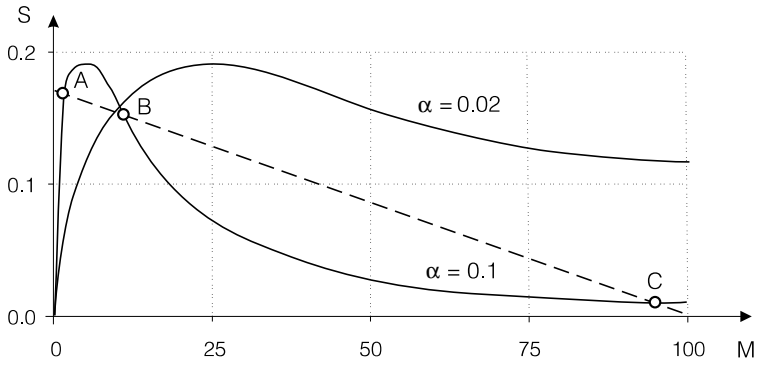
Obr. 4.2: Taktovaná Aloha

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

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

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.



Obr. 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

$$\alpha = \frac{e^{-\mathrm{G}}}{(\mathrm{N}+1)} = \frac{\mathrm{P}_0}{(\mathrm{N}+1)}.$$

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

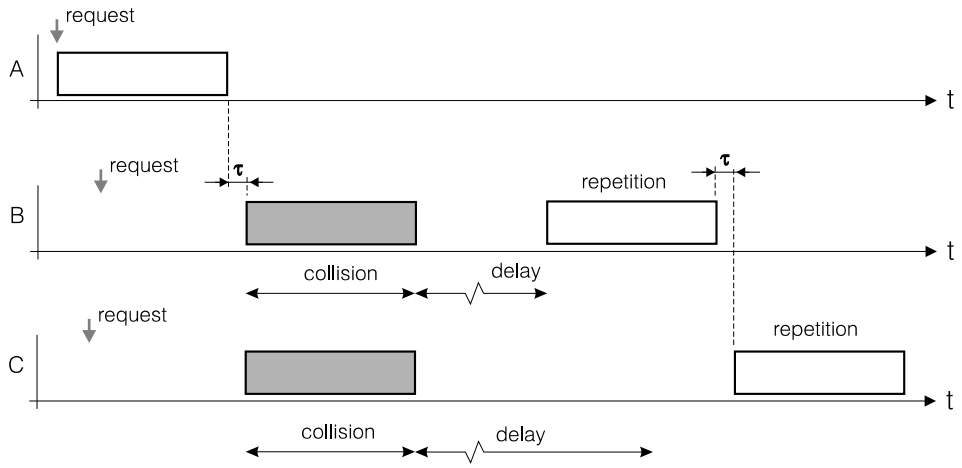
Metody Aloha jsou často využívány pro rezervaci kanálu časového nebo frekvenčního multiplexu, stanice pak může kanálu využívat po delší dobu. S tímto postupem se setkáváme u rádiových sítí, příklad použití metody Aloha pro bezdrátové sítě najdeme na str. 100.

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.

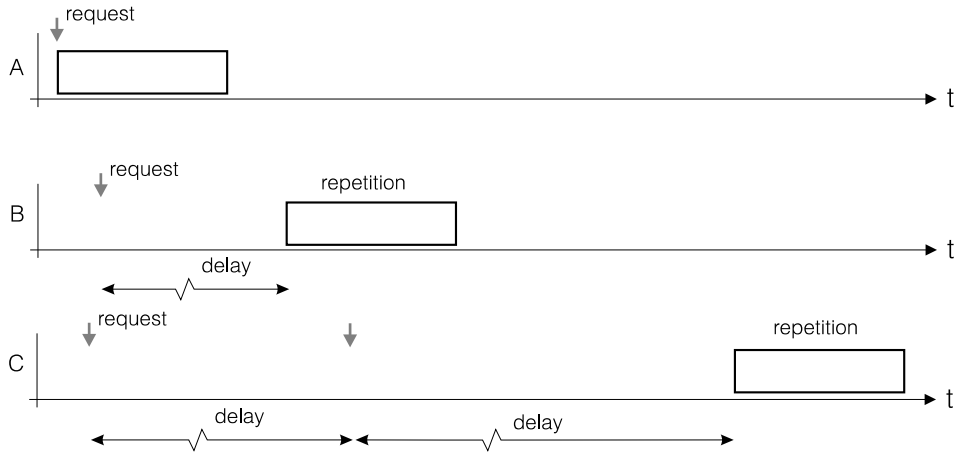


Obr. 4.4: Naléhající CSMA

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.

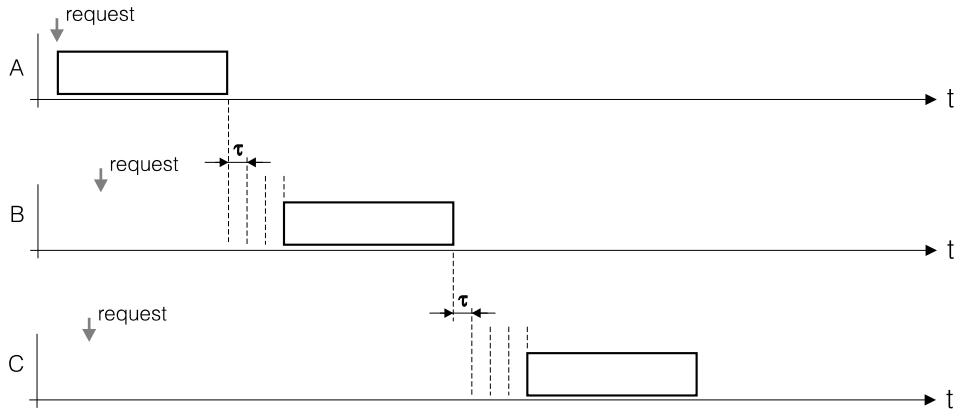


Obr. 4.5: Nenaléhající CSMA

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

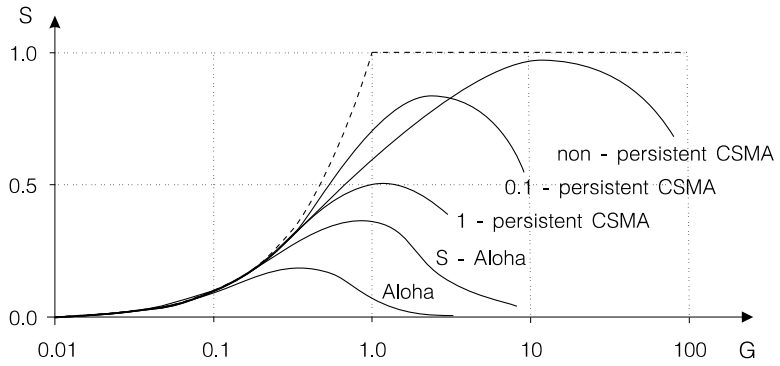
Stanice, která používá metodu *p-naléhající CSMA* (p-persistent CSMA), před odesláním rámce testuje stav kanálu. Je-li kanál volný, stanice zahájí vysílání. Pokud je kanál obsazen, stanice počká na uvolnění kanálu. Byl-li kanál volný nebo se právě uvolnil, začne stanice s pravděpodobností p vysílat a 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.



Obr. 4.6: p-naléhající CSMA

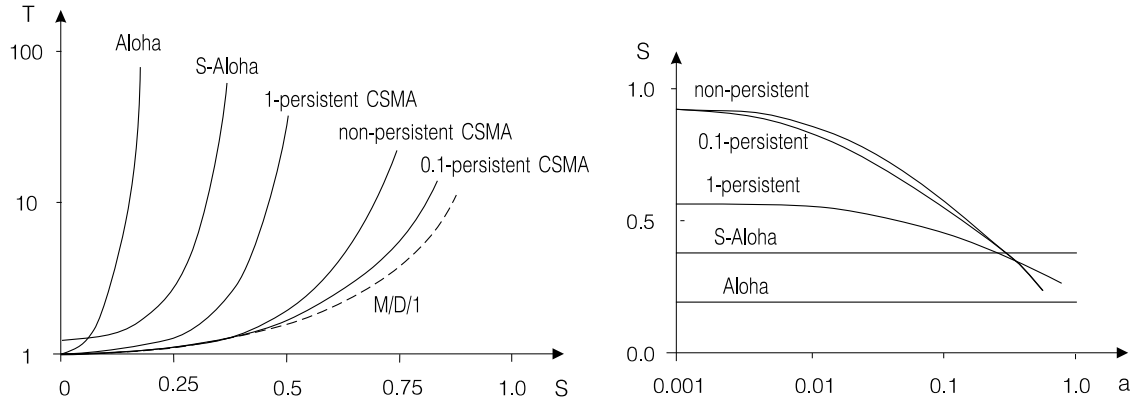
Volba parametru p dovolí optimálně nastavit využití kanálu a střední zpoždění rámce vzhledem k zátěži. Pro p=1 metoda přechází v naléhající CSMA, pro $p \to 0$ se sice průchodnost kanálu blíží hodnotě S=1, ale střední doba přenosu rámce roste nade všechny meze.

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).



Obr. 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.



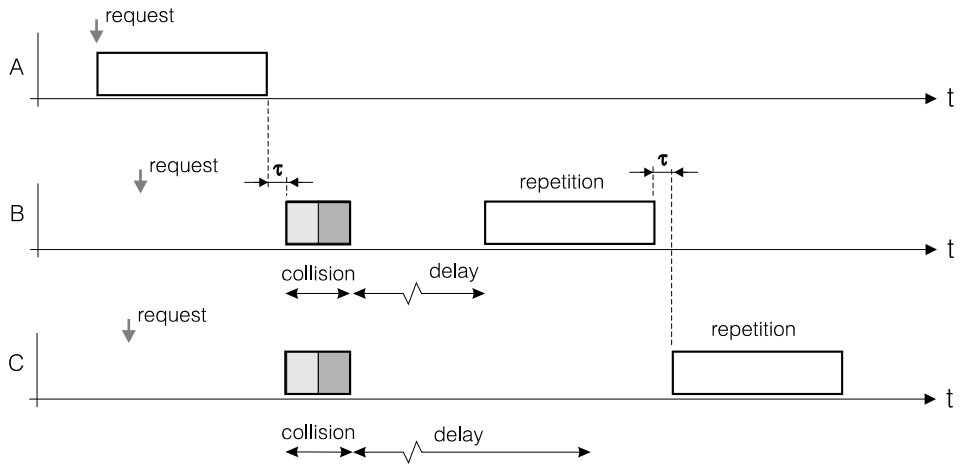
Obr. 4.8: Zpoždění a efektivita u metod CSMA

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. 32.

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).



Obr. 4.9: Metoda CSMA/CD

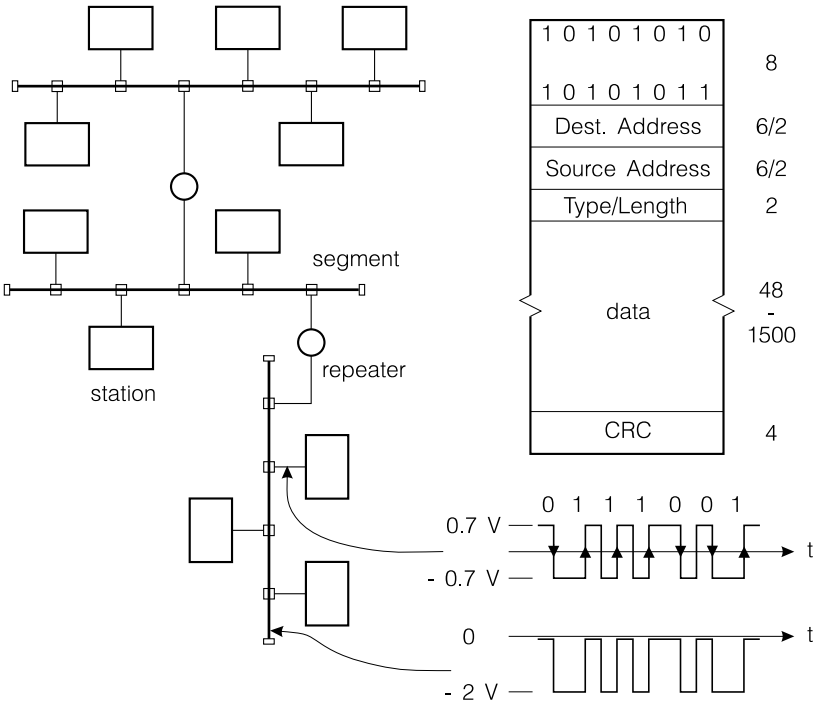
Použití metod CSMA/CD vyžaduje použít kanálu, na kterém lze kolizi zjistit. Nejjednodušším kanálem, který detekci kolize umožňuje, je sběrnice typu otevřený kolektor. V praxi však obvykle kolizi detekujeme jinak (např. sledováním napětí na médiu, které je buzeno proudovými zdroji vysílačů).

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. 24). 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. 61). Dnes se zřejmě jedná o nejrozšířenější technologii a lze očekávat, že bude (alespoň dosti dlouho) používána i k připojování stanic k sítím využívajícím vnitřně technologii jinou (například k sítím ATM).



Obr. 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 n, 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.

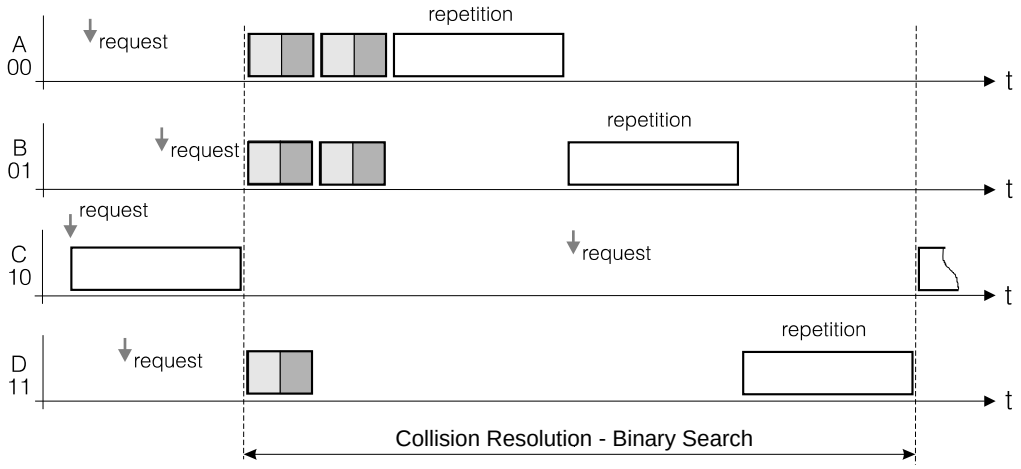
Funkci speciálního detektoru kolize v této síti nahrazuje zvláštní způsob rezervace kanálu pro přenos zprávy. Stanice, která chce získat neobsazený kanál (to zjistí detektorem signálu média stejně jako u metod CSMA), vyšle krátký rámec adresátovi zprávy a vlastní zprávu vysílá až po potvrzení tohoto 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.

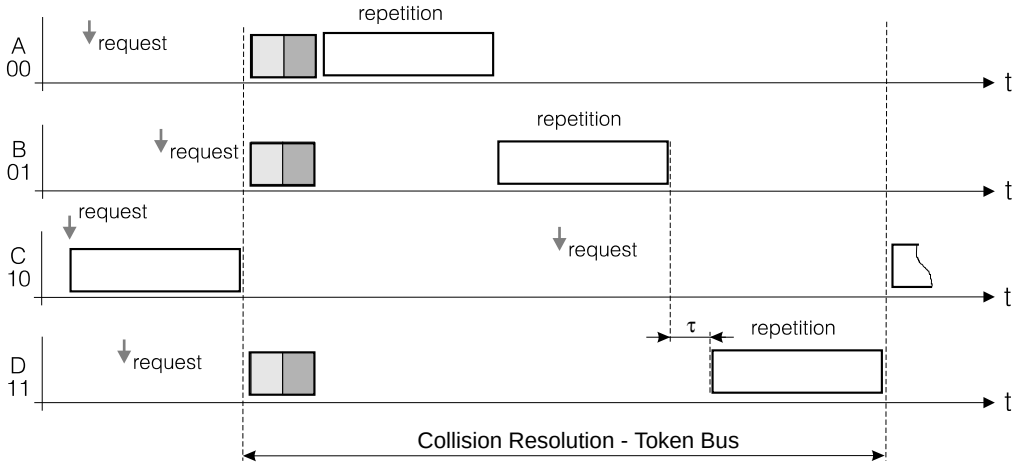
Nejjednodušší metodou řešení kolize je vyhledávání aktivních stanic v binárním stromu. Dojde-li ke kolizi v režimu CSMA/CD, stanice, které se kolize účastnily, se rozdělí do dvou skupin (například podle nejvýznamnějšího bitu adresy). Stanice z prvé skupiny se pokusí o vyslání zprávy, stanice druhé skupiny 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



Obr. 4.11: Deterministické řešení kolize – binární výběr

skupiny o jediné stanici, který připomíná deterministickou rezervaci kanálu metodou "round-robin" nebo virtuální logický kruh (obr. 4.12). Takového řešení používá firma Intel pro komunikaci mezi jednočipovými mikropočítači i80132, přenosová rychlost je 2 Mb/s.

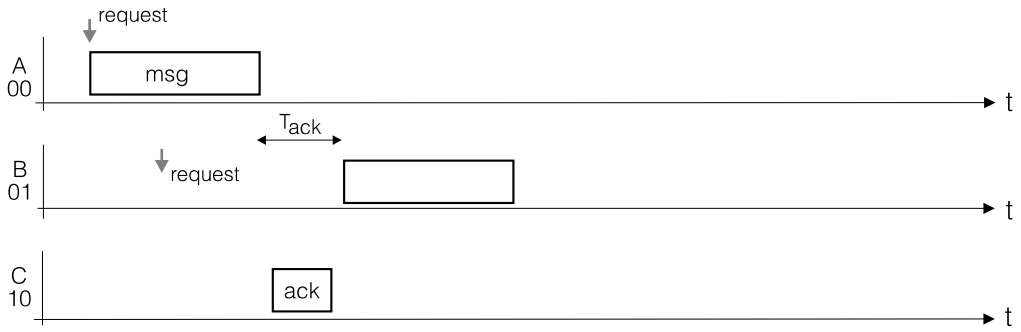


Obr. 4.12: Deterministické řešení kolize – logický kruh

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.

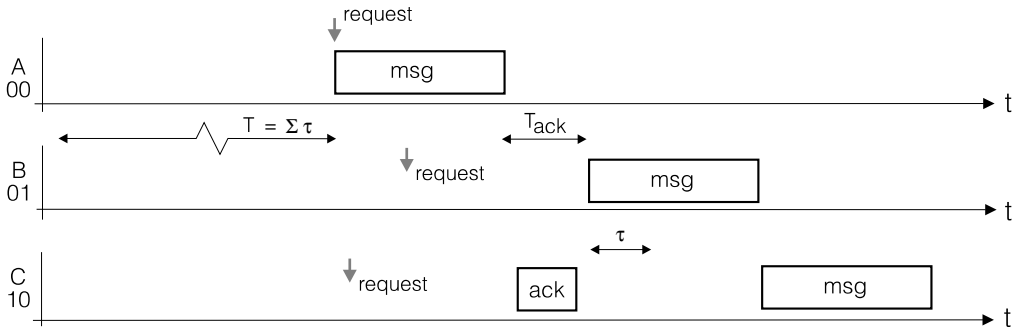
4.5 Metody CSMA/CA

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).



Obr. 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).τ po uvolnění média stanicí s adresou n (N je celkový počet stanic sítě a τ je doba šíření signálu médiem).



Obr. 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.τ 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* (viz str. 37).

Další úpravu CSMA/CA nalezneme u rádiových sítí podle IEEE 802.11 (str. 101). 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

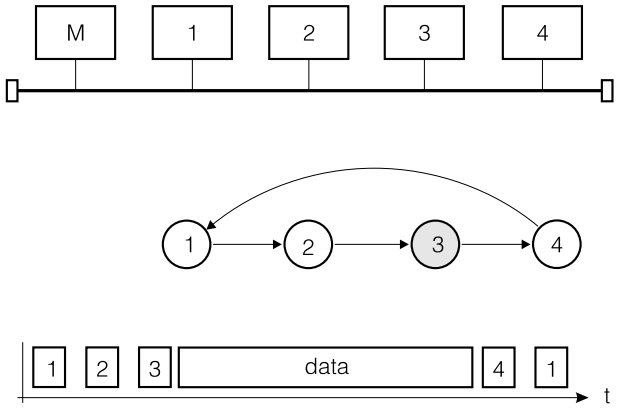
5.1 Centralizované řízení

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.



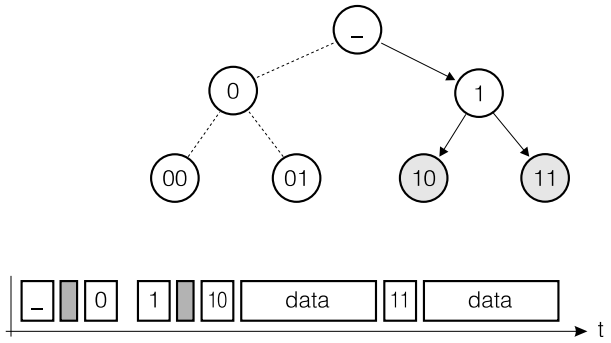
Obr. 5.1: Řízení kanálu cyklickou výzvou

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.



Obr. 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. 75).

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

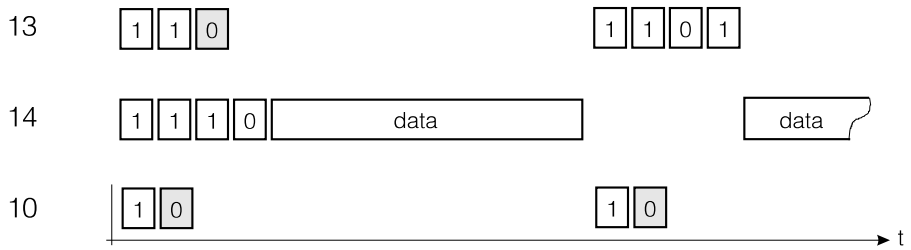
Rezervační metody jsou distribuovanou variantou přidělování kanálu na žádost. Vyčleňují z přenosového kanálu *rezervační rámec*, ve kterém si aktivní stanice rezervují přidělení kanálu datového. Rezervační rámec má charakter *bitové mapy* – každé stanici je přidělen slot o délce větší (alespoň dvojnásobně) 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.

Obr. 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.

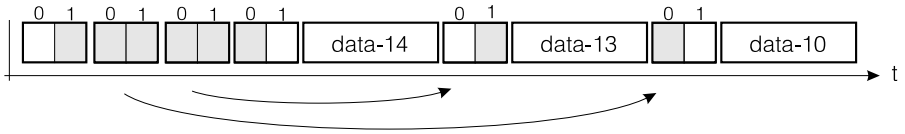


Obr. 5.4: Prioritní přístup

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.

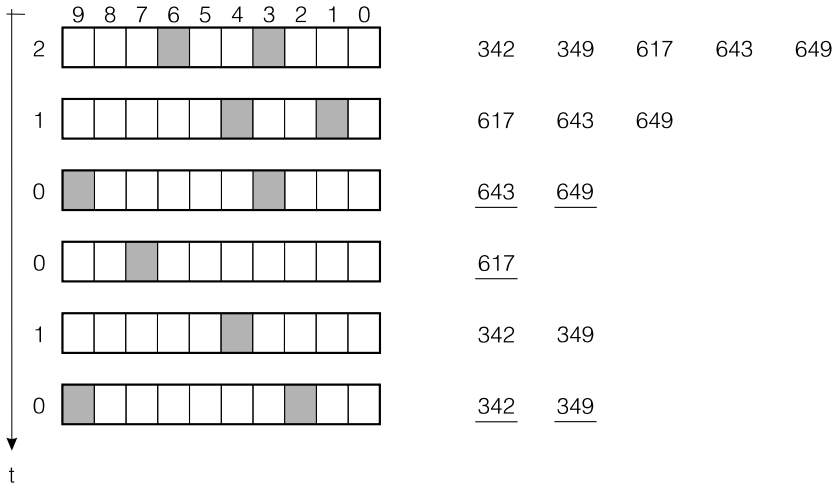


Obr. 5.5: Binární vyhledávání

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

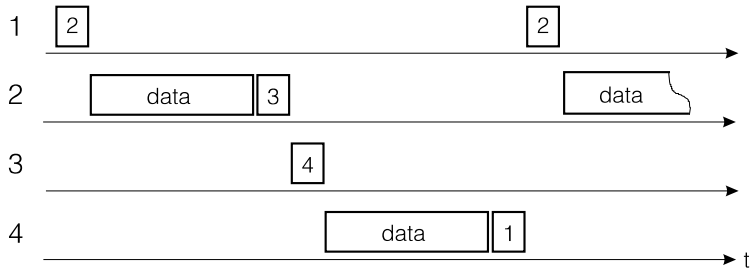
Další možnou úpravou vyhledávání je použití adres (a stromu vyhledávání) s jinou aritou. Příklad vyhledávání aktivních stanic v systému s třímístnou dekadickou adresou uvádí obr. 5.6. Metoda je uváděna pod názvem *MLMA* (Multiple Level Multiple Access), pro předání informace o aktivitách stanic v jednotlivých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



Obr. 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.

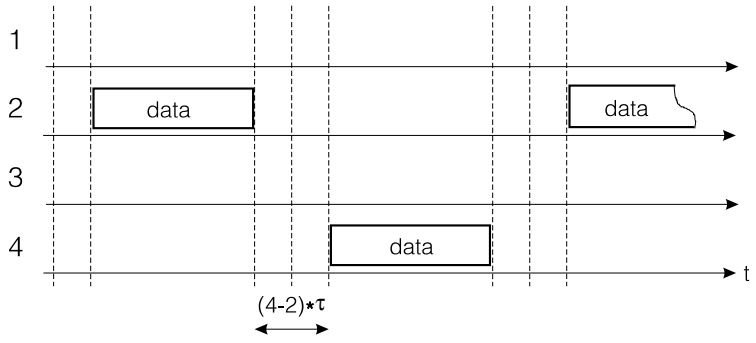


Obr. 5.7: Logický kruh

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.



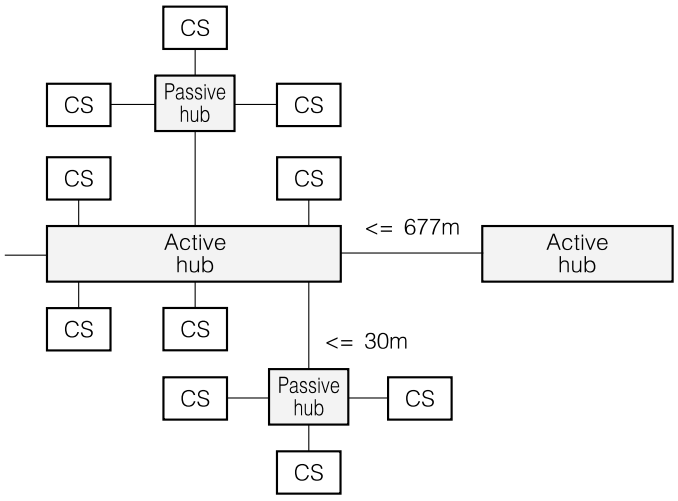
Obr. 5.8: Virtuální logický kruh

Stanice (nechť má adresu m) sleduje provoz na médiu a dojde-li po ukončení vysílání stanice s adresou n k uvolnění média na dobu $((m - n) \bmod N).\tau$, 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. 32).

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.



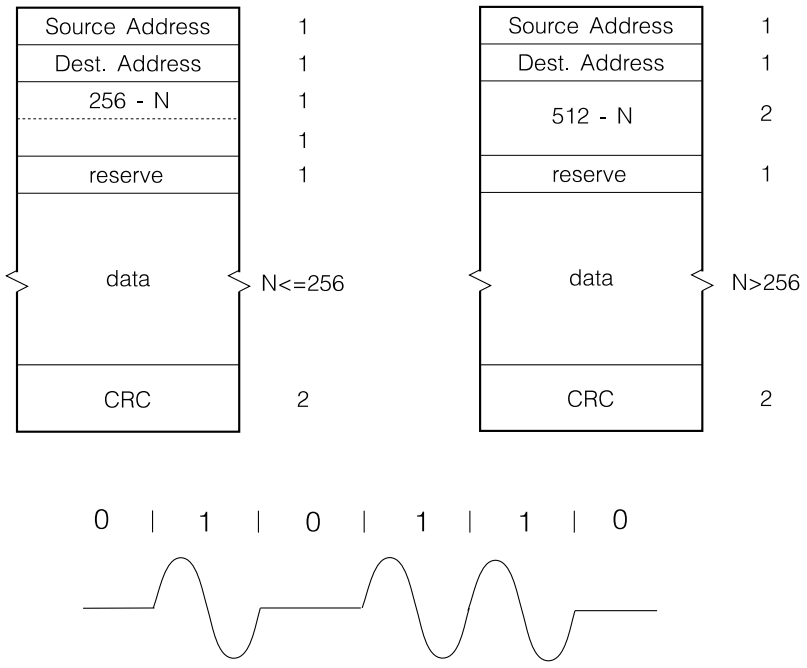
Obr. 5.9: ARCNet – topologie

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.



Obr. 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.

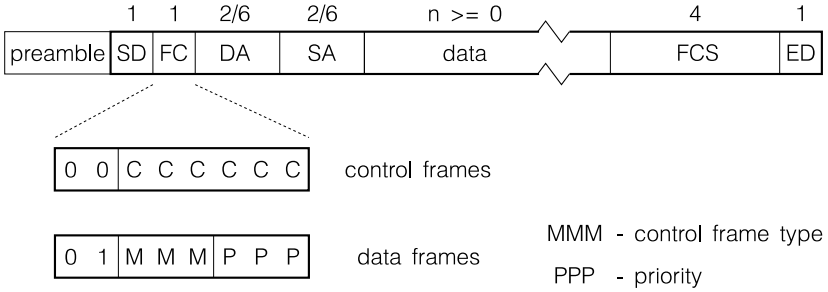
5.4 IEEE 802.4

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

Obr. 5.11: Média IEEE 802.4



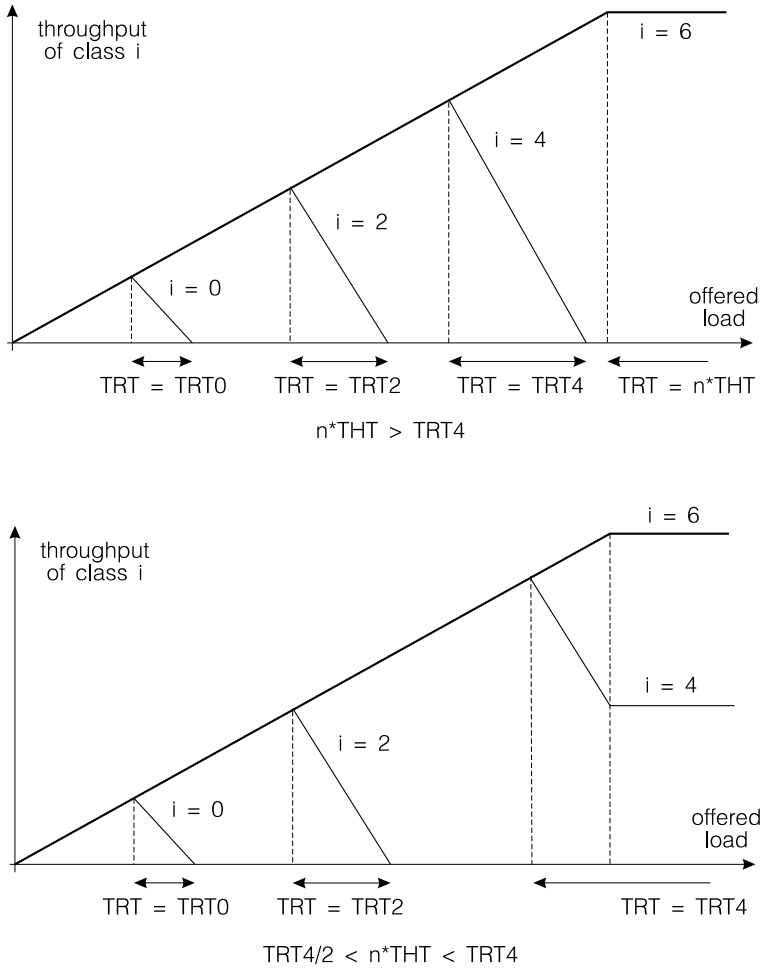
Obr. 5.12: IEEE 802.4 – formáty rámců

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.

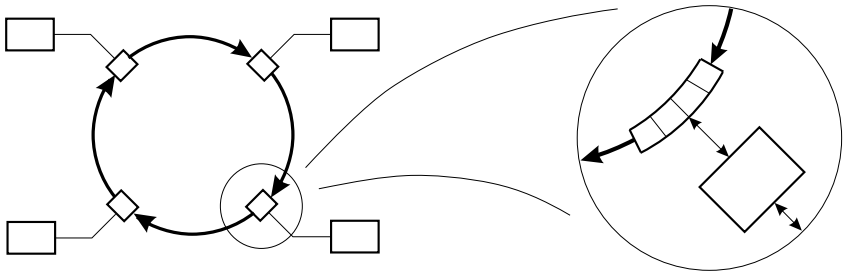
Spuštění logického kruhu je realizováno vysláním rámce *Claim-Token* stanicí, která indikuje klid na médiu. Délka rámce závisí na dvou nejvýznamnějších bitech adresy, pokud stanice po ukončení vysílání zjistí signál na médiu je to důsledek kolize a přenechá spustění kruhu soupeři. V dalším kroku použije 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.



Obr. 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).



Obr. 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 N 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.

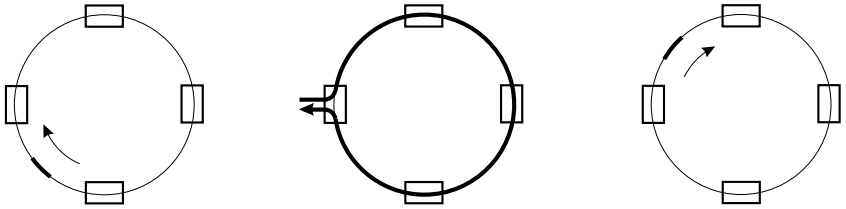
Kruhové sítě mají mnoho výhodných vlastností. Zjednodušují nasazení metod distribuovaného deterministického řízení přístupu i v případech, kdy stanice jsou velmi vzdálené (desítky kilometrů). Náhodný přístup se využívá pouze okrajově, například pro rozběh sítě. Metody zajišťují ohraničenou dobu zpoždění 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.

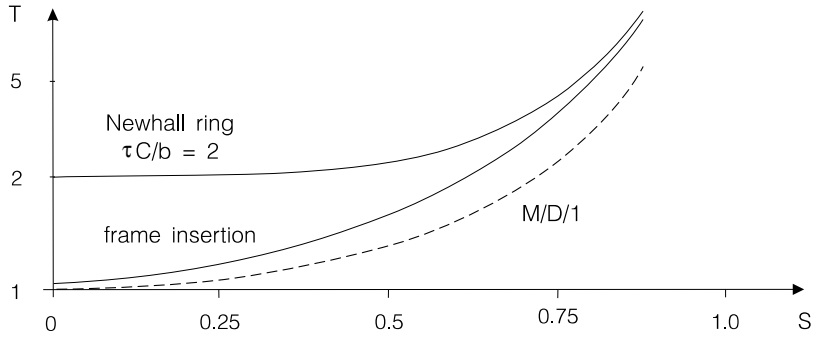
6.1 Newhallův kruh

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.



Obr. 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.



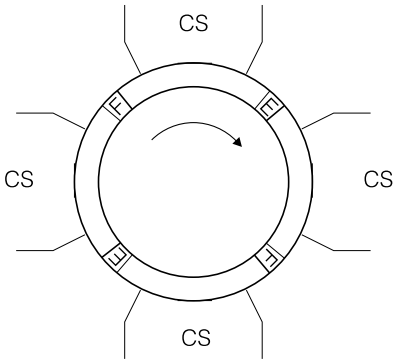
Obr. 6.3: Zpoždění v kruhové síti

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 síť 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.



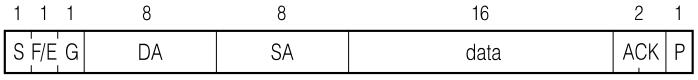
Obr. 6.4: Kruhová síť Pierceova typu

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 síť 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.



Obr. 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.

Obr. 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.

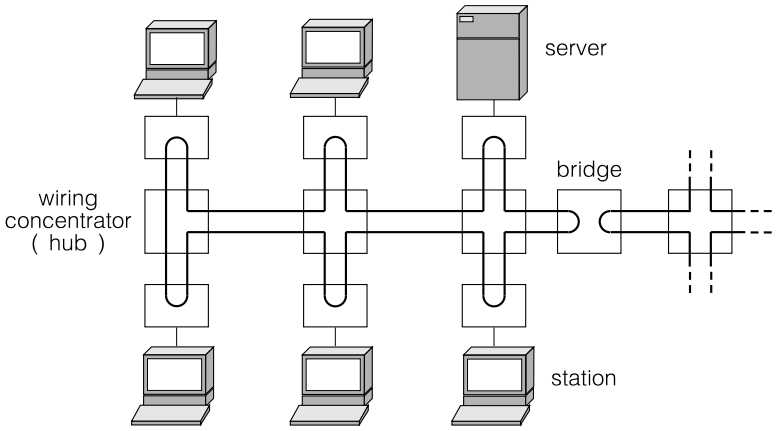
Kruhová síť SILK, která na tomto principu pracuje, používá pro přenos rychlostí 16 Mb/s koaxiální kabel 75 Ω. Datové pakety přenášejí šestnáctibitová slova.

6.4 IBM Token Ring (IEEE 802.5)

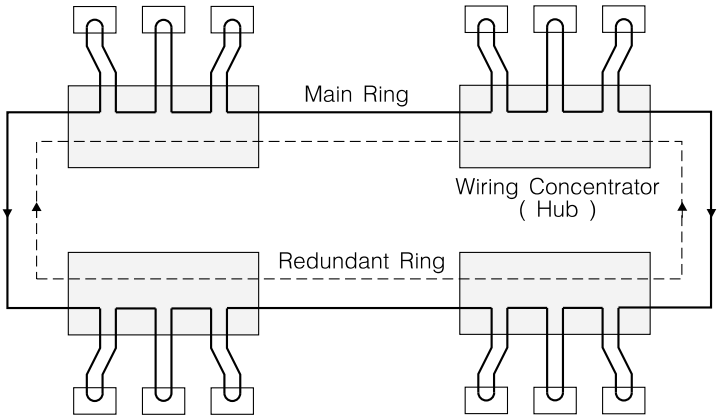
Nejběžnější kruhovou sítí je síť definovaná normou IEEE 802.5, známá pod názvem (IBM) Token Ring. Je tvořena stanicemi propojenými jednosměrnými dvoubodovými spoji do jednoduchého kruhu. Spoje mezi stanicemi jsou vedeny přes *koncentrátory* (Cabling Concentrator, někdy je označujeme jako rozbočovače) 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.



Obr. 6.7: Struktura sítě Token Ring



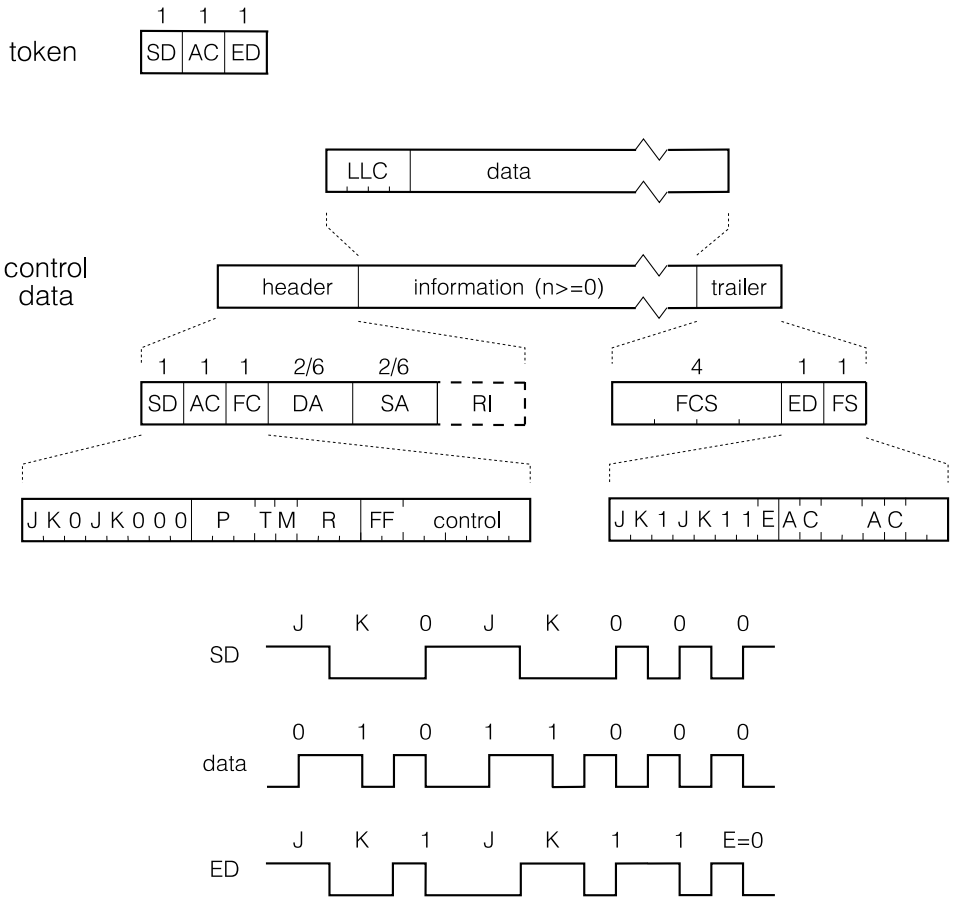
Obr. 6.8: Redundantní kruh Token Ring (Ring of Stars)

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 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)



Obr. 6.9: Diferenciální Manchester a struktura rámce IEEE 802.5

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 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.

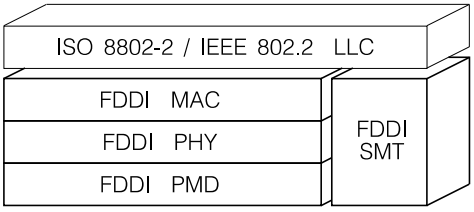
Důležitou funkci plní další MAC rámec – *Beacon*. Stanice, které vyprší časový limit No-Token, začne vysílat rámce Beacon. Na příjem rámce Beacon reaguje stanice, podobně jako u rámce Claim Token vysláním rámce Beacon s vyšší adresou. To dovolí identifikovat místo závady a síť rekonfigurovat. Pokud je 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.

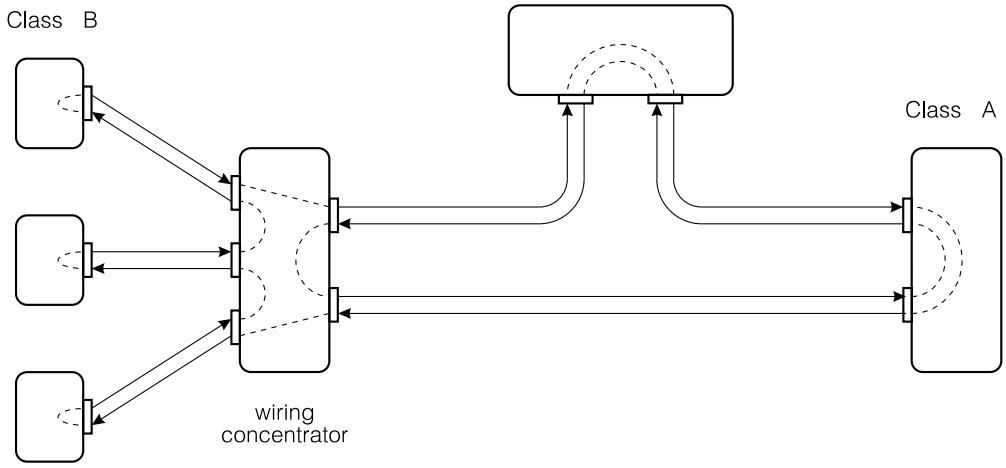
V názvu sítě se obráží fakt, že primárním přenosovým médiem jsou optická vlákna provozovaná na vlnové délce 1350 nm. Běžně používaná mnohavidová optická vlákna 62.5/125 μm (nebo někdy i levnější 50/125 μm) dovolují dosáhnout vzdálenosti mezi stanicemi až 2 km (limit útlumu mezi stanicemi je 11 dB, včetně 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).



Obr. 6.10: Architektura sítě FDDI

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 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).



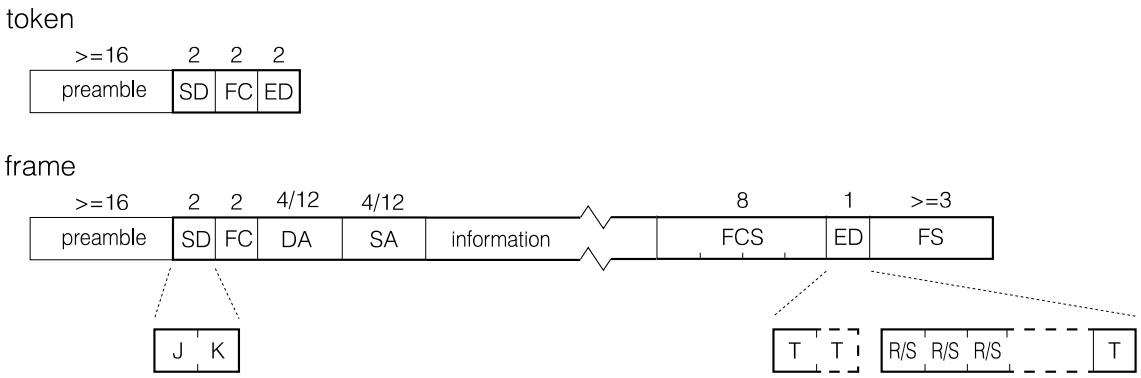
Obr. 6.11: Struktura sítě FDDI

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.



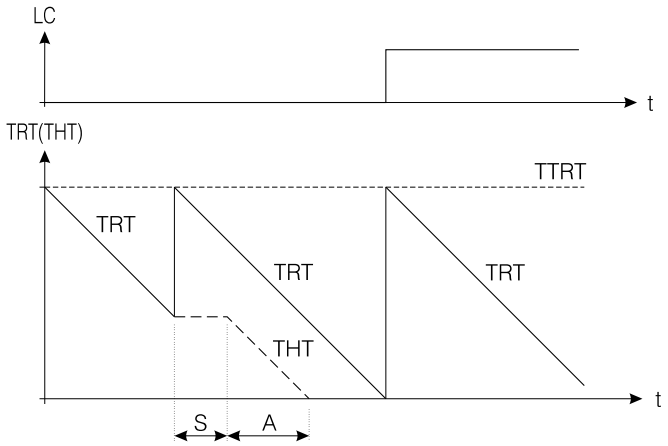
Obr. 6.12: Formát rámce

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



Obr. 6.13: Přidělování kapacity

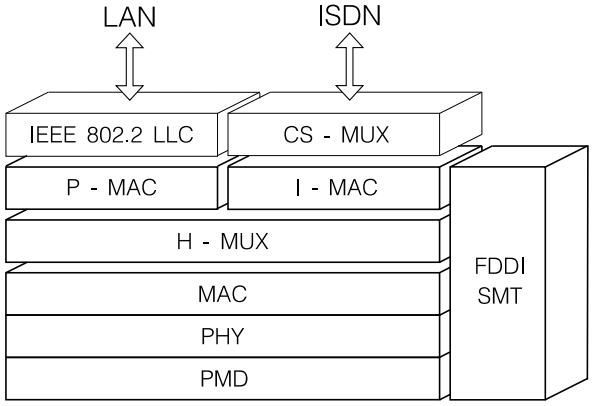
kruh (vysílá MAC rámec Claim).

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 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.

6.6 FDDI II

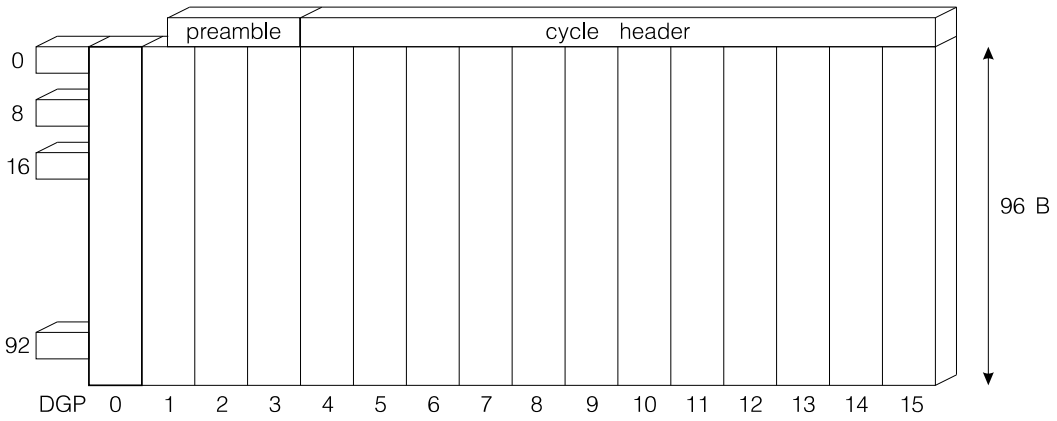
Síť FDDI podporuje provoz označovaný jako synchronní, rozumí se tím, že stanice má zaručenu možnost předání svých synchronních rámců při každém příchodu „pravidelně“ přicházejícího pověření. Takové chápání pojmu „synchronní provoz“ se liší od jeho definice v telekomunikačních systémech, tam synchronní 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.



Obr. 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.



Obr. 6.15: Struktura cyklu sítě FDDI II

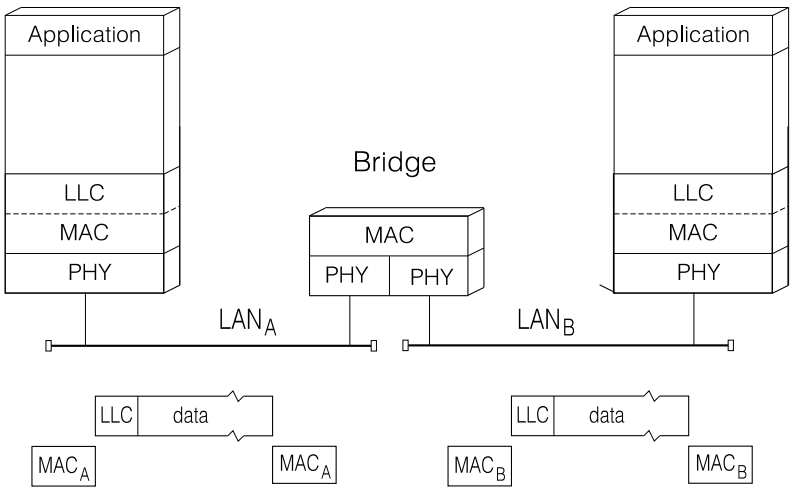
Každý cykl je tvořen preambulí o délce pěti (čtyřbitových) symbolů následovanou dvanáctislabičnou hlavičkou cyklu. Vlastní tělo cyklu je rozděleno na 16 skupin po 96 slabikách, každá skupina vytváří rychlý kanál WBC (Wide Band Channel) o přenosové rychlosti 6.144 Mb/s. Zbývajících 12 slabik tvoří kanál 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*.



Obr. 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. 69) 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. 58). 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).

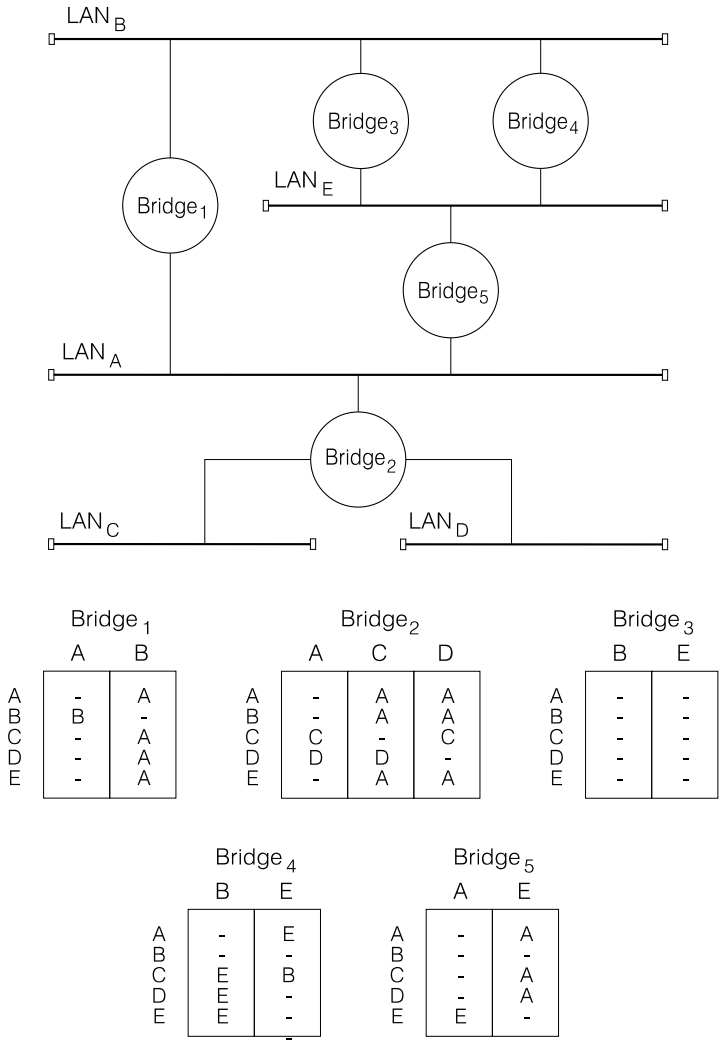
2 Na každou zprávu, která je přijata mostem z některé připojené sítě, most reaguje některým ze tří způsobů:

   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



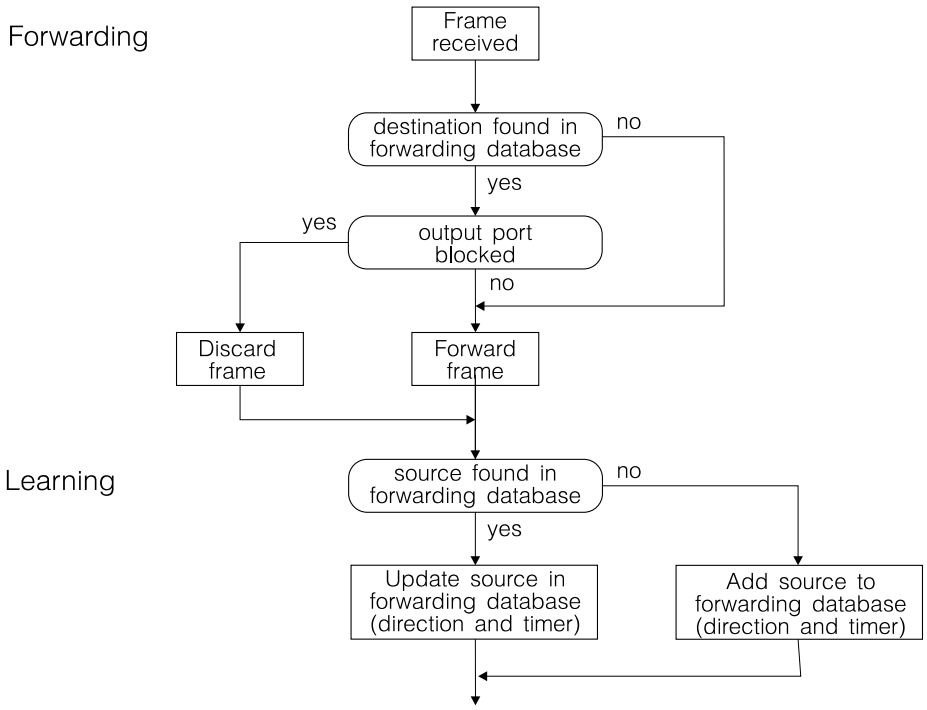
Obr. 7.2: Mosty se statickými směrovacími tabulkami

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.

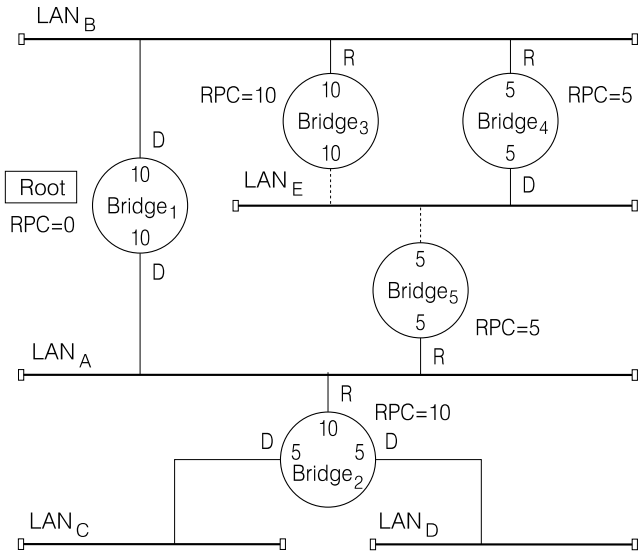
Transparentní most pracuje pouze v sítích se stromovou strukturou, v níž uzly reprezentují mosty a hrany reprezentují propojované lokální sítě. V propojených sítích nesmí vzniknout uzavřená cesta – cykl. Pokud potřebujeme propojit sítě více mosty a zajistit tak odolnost proti jejich výpadkům, musí být 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.



Obr. 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).



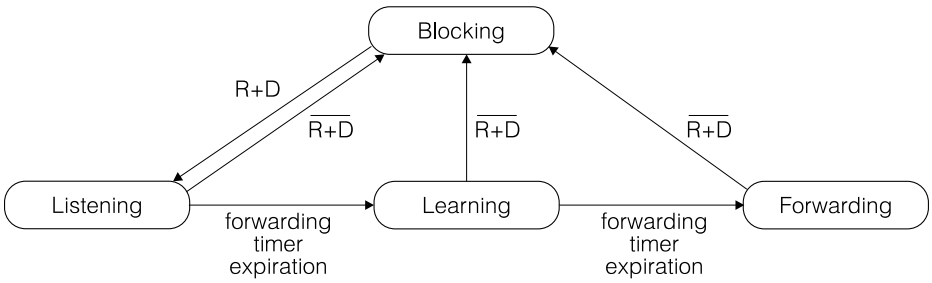
Obr. 7.4: Spanning-Tree algoritmus

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).



Obr. 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).

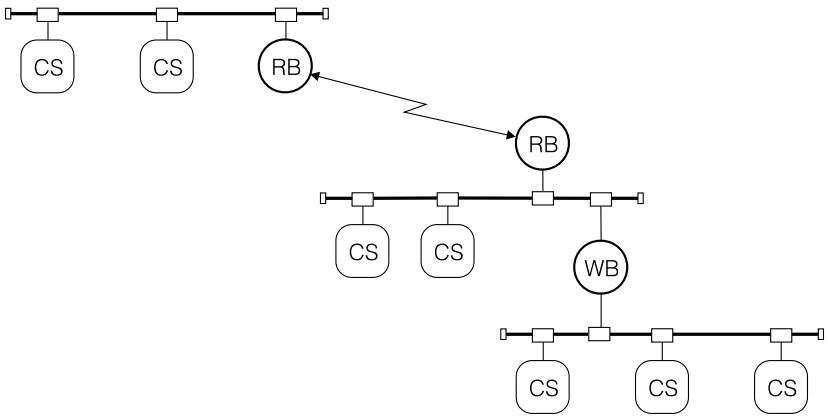
Jak už jsme uvedli, rozesílání rámců BPDU kořenem stromu je periodické (perioda je označována jako *Hello Time*). Při běžném provozu mosty evidují, že je vše v pořádku; výpadek některého z mostů nebo portů může vyvolat změnu root portu a vyhrazeného rozhraní. Každou takovou změnu most hlásí kořeni stromu 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.



Obr. 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. 69). 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"*.

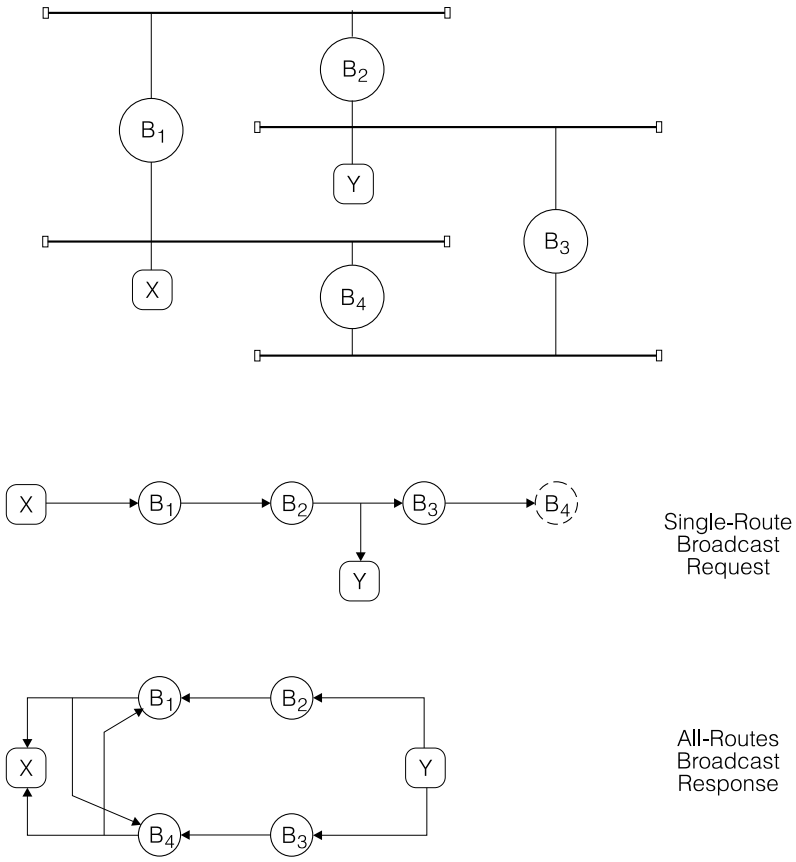
Zdrojové směrování

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.



Obr. 7.7: Zdrojové směrování

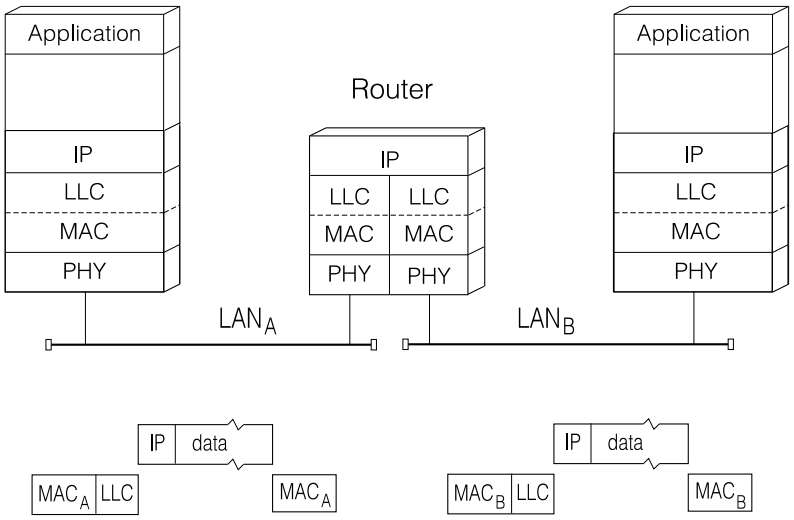
Z hlediska počtu zpráv v síti je výhodnější řešení uvedené na obr. 7.7. Žádost je rozesílána kostrou (Single-Route Broadcast), adresát vrací odpověď záplavou (All-Route Broadcast), z více odpovědí si žádající stanice vybere nejvýhodnější cestu.

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.

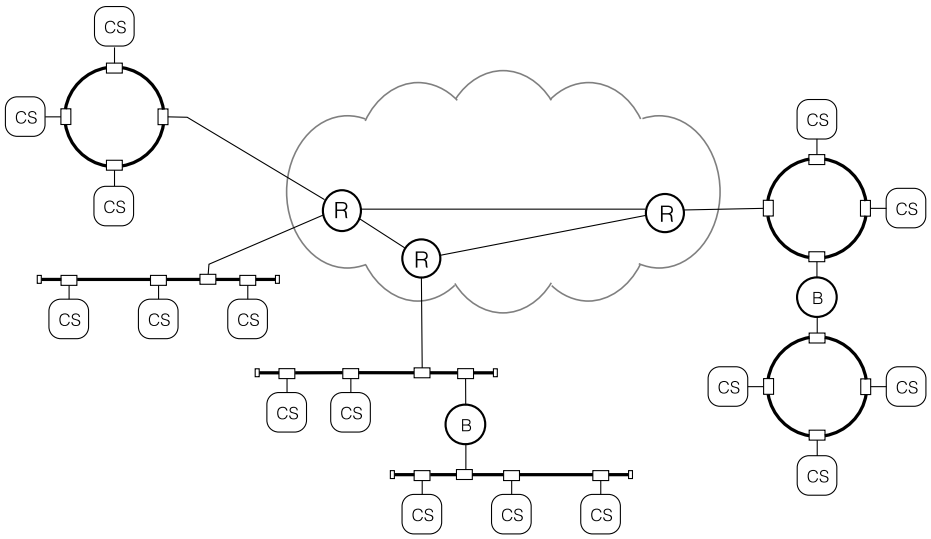
Z pohledu mostů jako součástí lokálních sítí je adresace sítí jako Internet IP nebo Novell IPX neviditelná, mosty (pokud nemají doplněnu filtraci opírající se o typ protokolu) považujeme za *protokolově transparentní*. Síťové adresy jsou přenášeny v hlavičkách *paketů*, které jsou pro prvky lokální sítě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



Obr. 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.

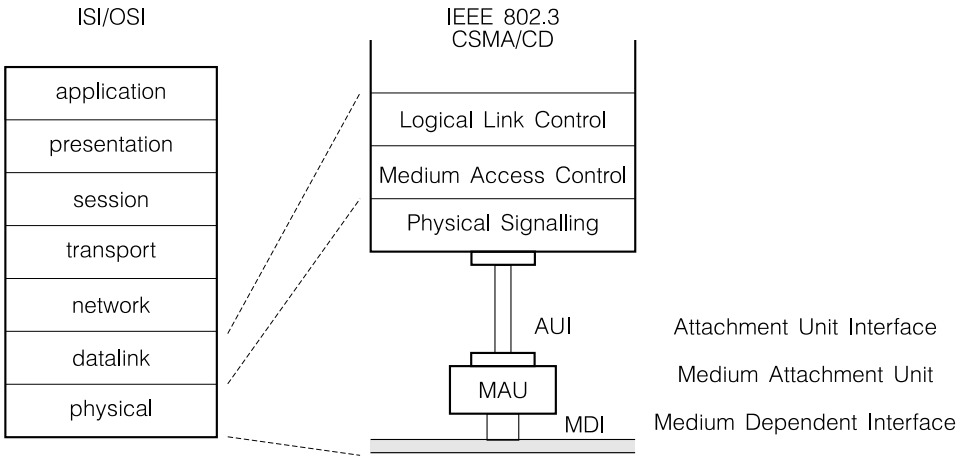


Obr. 7.9: Propojení sítí mosty a směrovači

Činnosti směrovačů se budeme podrobněji zabývat v kapitole věnované síťovým protokolům, na str. 115.

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. 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.



Obr. 8.1: Architektura standardu Ethernetu IEEE 802.3

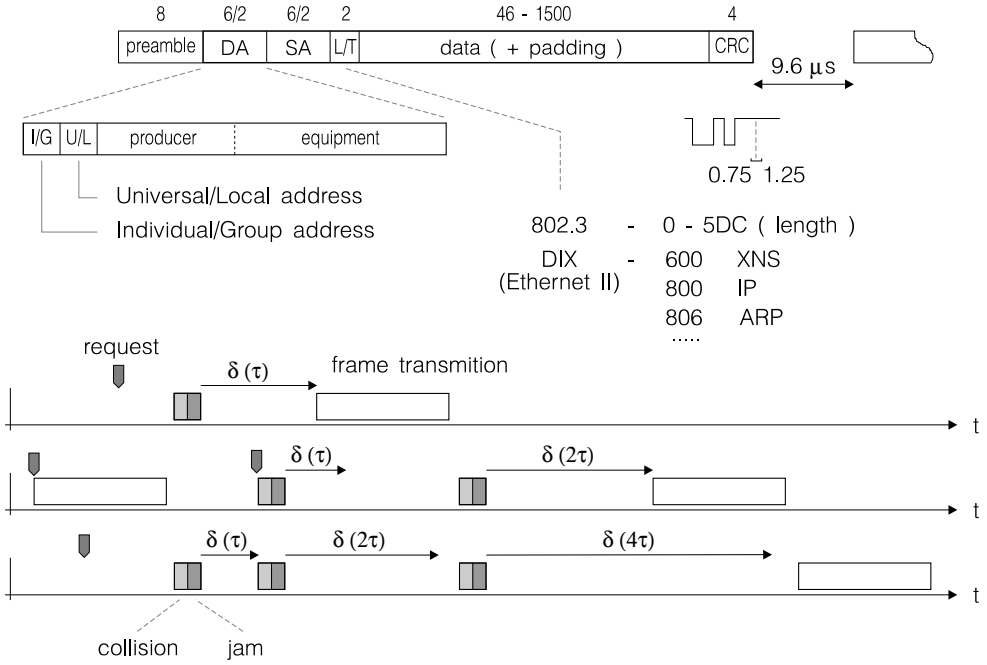
Nejnižší úroveň standardu je označována jako rozhraní *MDI* (Medium Dependent Interface) a definuje přenosové médium (tím dnes může být koaxiální kabel, kroucený dvoudrát nebo optické vlákno), signál na médiu a konektor. Přenosové médium podstatně ovlivňuje vlastnosti sítě. Jednotlivým technologiím lišícím 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 DIX), nebo 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*. Rámce kratší než 64 oktetů obr. 8.2 označujeme jako *runts*.



Obr. 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

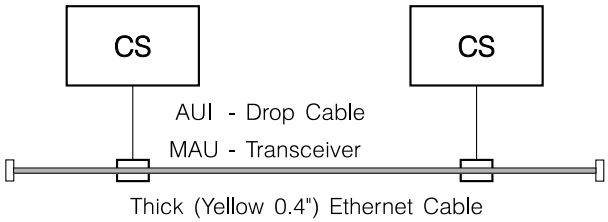
definovanou charakteristickou impedancí, detektor kolize se pak opírá o měření střední hodnoty signálu na kabelu. Podle nastaveného limitu je schopen detekovat kolizi vysílající stanice s jinou stanicí na kabelu (Transmit Mode), nebo kolizi dvou jiných stanic na stanici v klidu (Receive Mode). Pro testování 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 Technologie 10BASE5

Technologie 10BASE5 (10 Mb/s, přenos v základním pásmu, délka segmentu do 500 m) vychází z původního Ethernetu II a specifikace DIX (str. 29). (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.

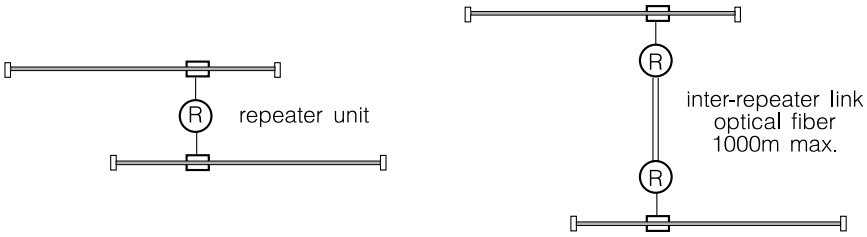


Obr. 8.3: Prvky sítě 10BASE5

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.



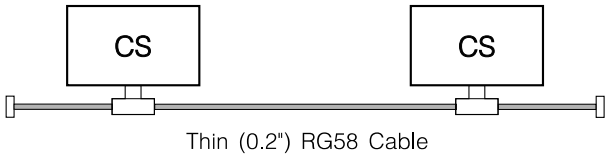
Obr. 8.4: Opakovače v síti 10BASE5

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*.

8.2 Technologie 10BASE2

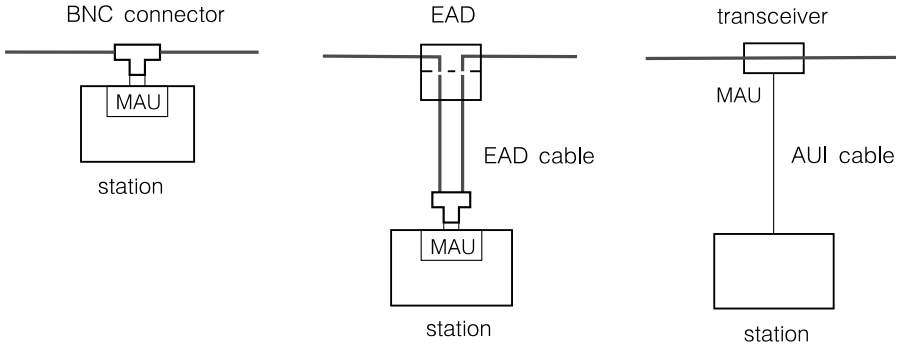
Kvalita standardního kabelu u technologie 10BASE5 (specifikace IEEE 802.3b z roku 1988) je bohužel zaplacena vysokou cenou, instalace je navíc značně komplikovaná. Využijeme ho pro propojování výkonných počítačů a pracovních stanic, pro výstavbu páteřních segmentů. Pro propojení většího množství osobních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



Obr. 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

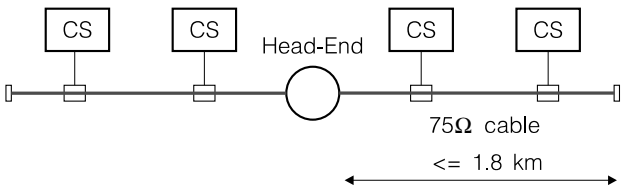


Obr. 8.6: Varianty kabeláže 10BASE2

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).

8.3 Technologie 10BROAD36

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



Obr. 8.7: Technologie 10BROAD36

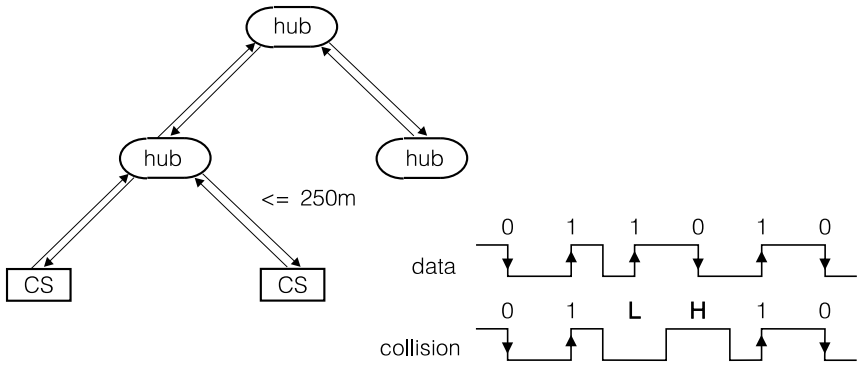
Stanice jsou připojeny k segmentům koaxiálního kabelu o maximální délce 1.8 km, segmenty jsou připojené k centrálnímu prvku označovanému jako *Head-End*. Existují dvě možné funkční konfigurace sítě: Prvá používá dvojitou kabeláž (*Dual-Cable System*) – jeden kabel přenáší signál od stanice k centrálnímu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

8.4 StarLAN

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).

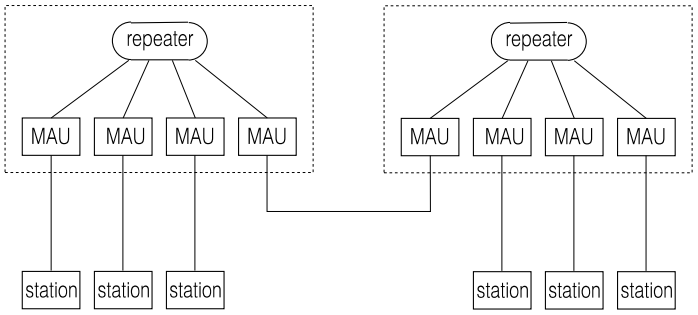


Obr. 8.8: Síť StarLAN

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.

8.5 Technologie 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.



Obr. 8.9: Struktura sítě 10BASE-T

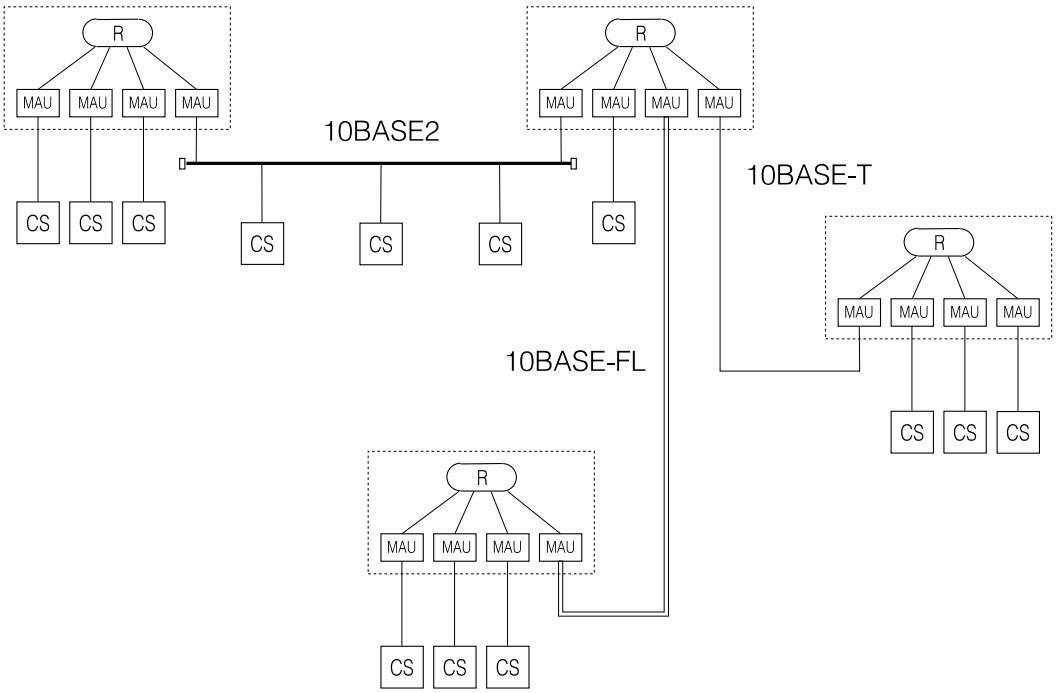
Ze čtyř vodičových párů kabelu UTP jsou využity dva, jeden pár přenáší signál od stanice k opakovači, druhý přenáší signál ve směru opačném. Kabel UTP musí splňovat podmínky na šířku pásma, charakteristickou impedanci a přeslech. (Přeslech signálu z vysílacího vedení do přijímacího může být považován 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. 68), 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).

Při rozhodování o volbě technologie Ethernetu pro lokální síť hraje často podstatnou roli cena řešení. „Nespolehlivý“ segment Ethernetu 10BASE2 lze postavit za cenu komunikačních



Obr. 8.10: Struktura moderní sítě Ethernet

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).

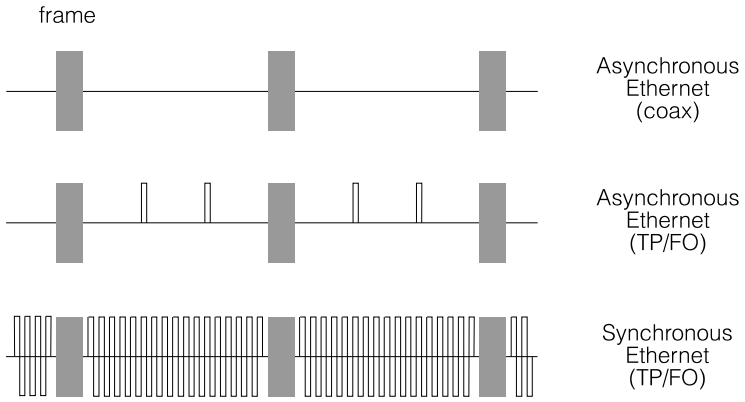
Moderní koncentrátory jsou vybavovány správou SNMP, které dovolí informovat o jejich funkci a ovládat je na dálku (str. 119). Existují i typy, které dovolují omezit přenos na jednotlivých vedeních na konkrétní adresy, takové koncentrátory zvyšují bezpečnost (ve významu „nezneužitelnost“) sítě.

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.

8.6 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) používá mnohavidové vlákno a dovoluje propojit opakovače na vzdálenost do 1000 m.



Obr. 8.11: Synchronní Ethernet

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. Prvky 10BASE-FL mohou spolupracovat s prvky podle FOIRL (limitem je vzdálenost 1000 m).

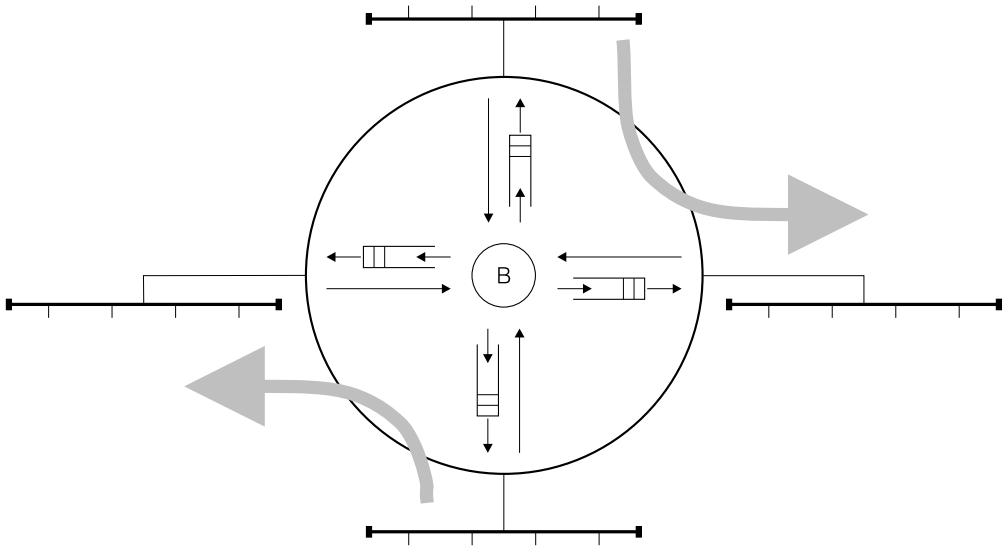
Specifikace *10BASE-FB* (Fiber Backbone) definuje synchronní dvoubodový spoj, určený pro propojení opakovačů. Dovoluje překročit limit počtu opakovačů mezi dvěma stanicemi, využití optického spoje 10BASE-FB mezi opakovači je obdobou *synchronního Ethernetu*. Konečně, specifikace *10BASE-FP* (Fiber Passive 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 33 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.

8.7 Přepojovaný Ethernet

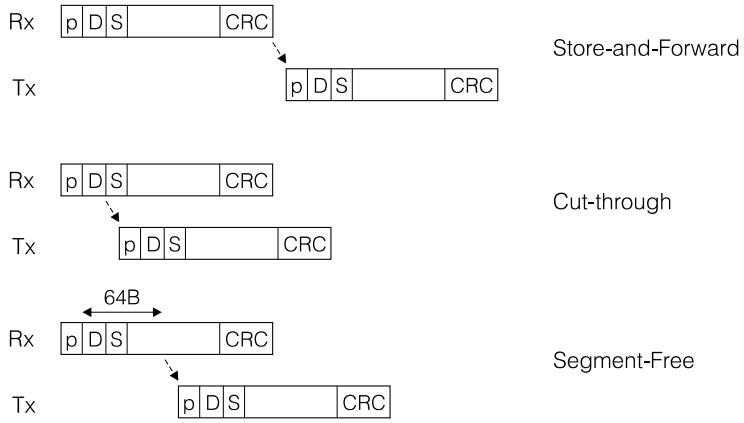
Mosty Ethernetu dovolují rozdělit rozsáhlejší síť na *kolizní domény*, provoz v jedné části sítě nemá vliv na provoz v části druhé a součtový tok v síti může být vyšší než je limit v každé z kolizních domén. U víceportových mostů, které propojují čtyři a více kolizních domén, se objevuje další zajímavý 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*).

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



Obr. 8.12: Princip přepojovaného Ethernetu

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*.



Obr. 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 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 snaží zmírnit i jiná 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.

8.8 Technologie 100BASE-TX a 100BASE-FX

Výrazně technologickou modifikací hvězdicového Ethernetu 10BASE-T je standard označovaný jako 100BASE-T a zvyšující přenosovou rychlost na 100 Mb/s na kabelovém rozvodu UTP Cat.5 (ale modifikace 100BASE-T4 vystačí dokonce i s UTP Cat.3), na kabelech STP a na vícevidových optických vláknech (62.5/125 μm). Specifikace rychlého Ethernetu je poměrně nová, pod označením IEEE 802.3u byla schválena v červnu 1995. Technologie rychlého Ethernetu je založena na efektivnějším využití přenosového média. Kódování Manchester je nahrazeno efektivnějším kódováním 4B5B, se kterým jsme se již setkali u sítě FDDI a víceúrovňovým signálem na metalických vedeních (MLT-3 Multi-Level Transmit). To dovolí dosáhnout přenosové rychlosti 100 Mb/s (na médiu 125 Mb/s) při běžné kabeláži UTP Cat.5 nebo STP. Vzdálenost mezi stanicí a koncentrátorem je stejně jako u sítě 10BASE-T do 100 m, optické vlákno dovolí jít až na 400 m (mezi dvěma stanicemi nebo mezi stanicí a přepínačem) a na 2000 m při duplexním provozu.

Rychlý Ethernet definuje tři rozdílné realizace fyzického kanálu. Základem jsou kanály 100BASE-TX – dva páry kabelu UTP nebo STP, a 100BASE-FX – dvojice optických vláken. Zajímavým doplňkem je kanál 100BASE-T4, který využívá tří párů kabelu UTP Cat.3 k přenosu dat a čtvrtého páru k detekci kolize. Podobně jako u běžného Ethernetu je definováno rozhraní mezi fyzickou vrstvou a vrstvou MAC, na místě rozhraní AUI a patnáctipinového konektoru zde najdeme čtyřicetipinový konektor *rozhraní MII* (Media Independent Interface).

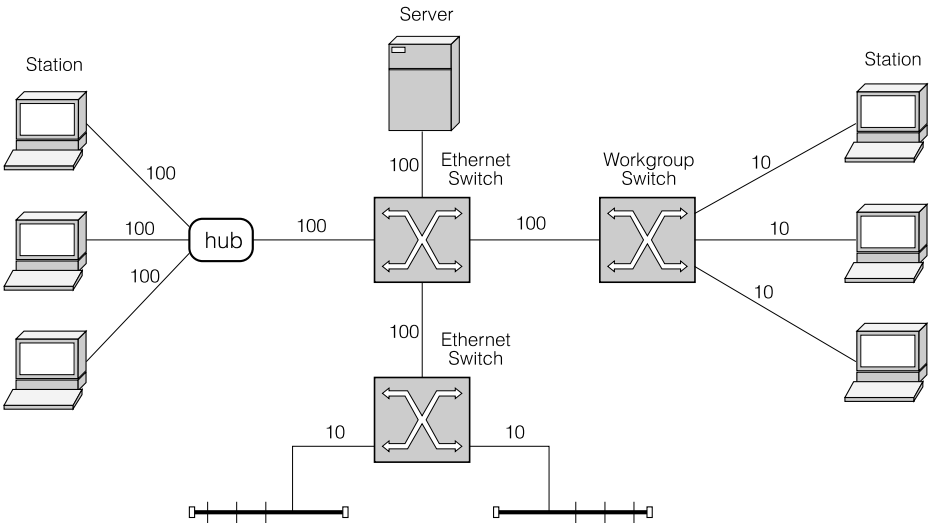
Zvýšení přenosové rychlosti při zachování ostatních vlastností Ethernetu (metoda přístupu CSMA/CD, formáty rámců) si pochopitelně vyžádalo určitou cenu, a tou je snížení maximálně překlenutelné vzdálenosti. Ta je zde omezena na o něco více než 300 m (a to pouze při použití optického vlákna). Pokud jde o vícevstupové opakovače, rychlý Ethernet definuje dva odlišné typy. První z nich (*Class 1*) umožňuje použití různých fyzických rozhraní na vstupech a smí být mezi stanicemi jediný. Druhý typ opakovače (*Class 2*) pracuje se stejnými fyzickými rozhraními, mezi stanicemi smí být nejvýše dva opakovače tohoto typu, navzájem propojené na vzdálenost do 5 m.

Opakovače v síti 100BASE-T slouží spíše pro napojení stanic z poměrně malé lokality na sdílený kanál, vlastní výstavba sítě se opírá častěji o přepínače přepojovaného Ethernetu. Běžně je přitom využívána možnost bezkolizního *duplexního provozu*; na dvoubodovém propojení přepínačů nebo na dvoubodovém připojení serveru 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 (mikrosegmentace) k přepínači, na který jsou rychlými kanály připojeny servery a další části sítě. Pro náročné aplikace je k dispozici možnost sdílení rychlého kanálu 100 Mb/s, nebo mikrosegmentace s plným vyhrazením kanálů 100Mb/s. Příklad možné topologie sítě na technologii 100BASE-TX uvádí obr. 8.14.

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 v budoucnu zřejmě i rychlejších) se projevuje problém známý z oblasti přepojovaných sítí – *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.



Obr. 8.14: Topologie sítí 100BASE-TX a 100BASE-FX

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.

Gigabitový Ethernet

Přenosová rychlost 100 Mb/s nezůstala nadlouho limitem. Z iniciativy skupiny výrobců známé jako *GEA* (Gigabit Ethernet Alliance) je vytvářen standard sítě založené na principech Ethernetu s přenosovou rychlostí 1 Gb/s. Tato rychlost sice omezuje fyzický průměr kolizní domény na 25 m, což je současně limit pro délku metalického spoje – krouceného dvoudrátu. Využití bezkolizního duplexního provozu dovoluje překlenout až 2 km při použití mnohavidového vlákna a 30 km při použití jednovidového vlákna.

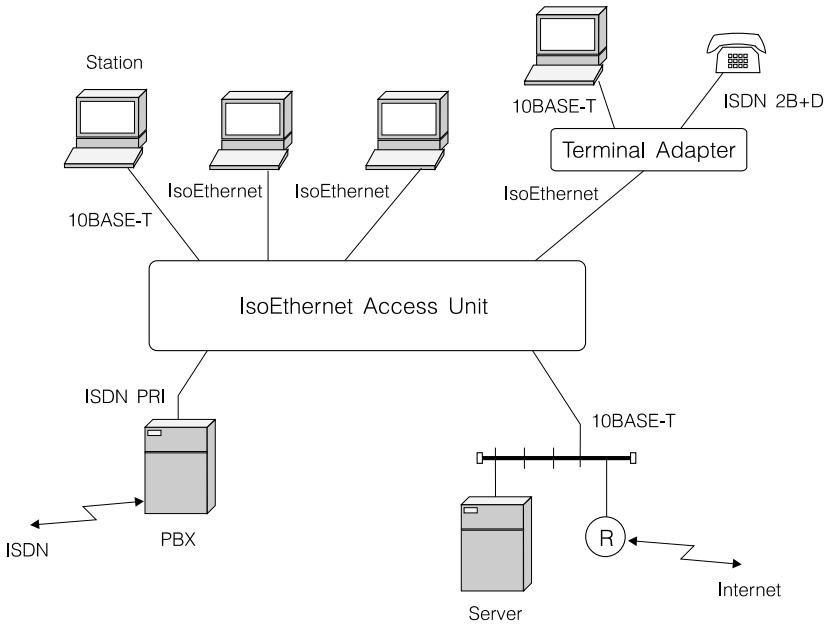
Technologicky se gigabitový Ethernet opírá o ověřené technologie vyvinuté pro spoje přepojovací sítě Fiber Channel. Standardizace gigabitového Ethernetu v rámci IEEE 802.3 je očekávána v roce 1997, v současnosti již existují přepínače dovolující vytvářet jednoduché sítě s těmito spoji.

8.9 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.



Obr. 8.15: Struktura sítě postavené na isochronním Ethernetu

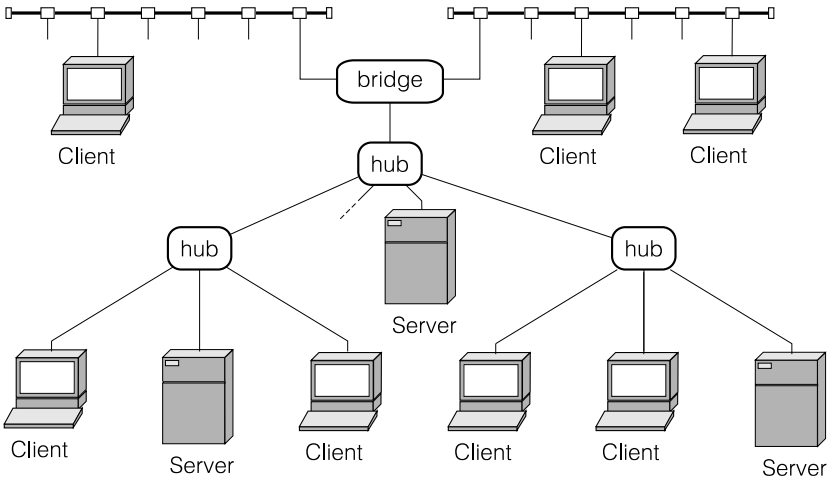
Isochronní Ethernet dovoluje vytvořit moderní ISDN systém (hlasová komunikace, videokonference) s využitím původní kabeláže Ethernetu (kabely UTP a optická vlákna, ne koaxiální kabely). Vyžaduje však pochopitelně náhradu původních opakovačů speciálními prvky, označovanými jako *jednotky AU* (Access Unit). 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. Pro připojení stanic, které nebudou kanál Ethernet (P Channel) využívat (např. telefonní ústředna, která propojí lokální systém na běžnou ISDN síť), lze využít plnou rychlost přenosového kanálu (16.144 Mb/s) pro vytvoření 248 synchronních kanálů (ISDN B Channel) s rychlostí 64 kb/s, jednoho kanálu pro signalizaci (ISDN D Channel) s rychlostí 64 kb/s a jednoho kanálu řídícího (ISDN M Channel) s rychlostí 96 kb/s.

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.

Technologie isochronního Ethernetu je poměrně nová, výběr prvků je zatím omezen na řadiče ISTE a AU jednotky s funkcí opakovače pro kanál Ethernet (ISDN P Channel). Prvky složitější (s funkcí mostu, přepínače nebo směrovače) zatím dostupné nejsou, vzhledem k ohromnému funkčnímu potenciálu standardu a vedoucí pozici firem jako AT&T, Ericson, IBM, National Semiconductors lze očekávat rychlý rozvoj.

9. 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.

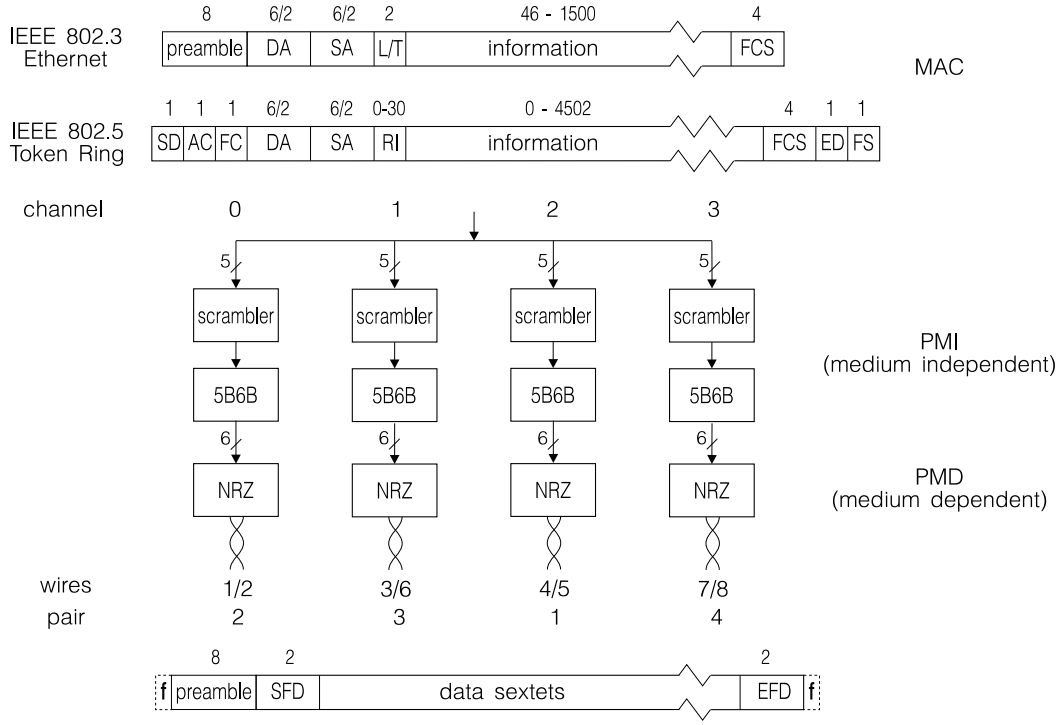


Obr. 9.1: Struktura sítě 100VG-AnyLAN

Síť má hvězdicovou topologii (obr. 9.1), 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*).

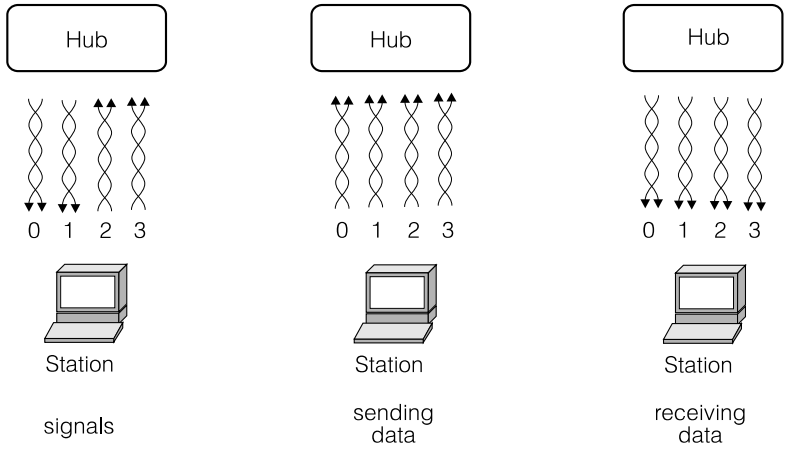


Obr. 9.2: Kódování a struktura rámců sítě 100VG-AnyLAN

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.

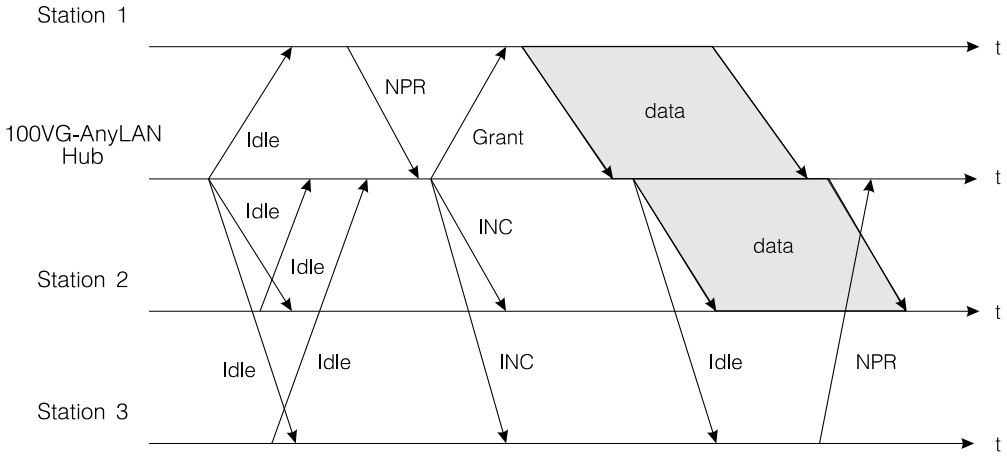
Detekci chyby ve fyzické vrstvě pochopitelně doplňuje zabezpečení 32-bitovým cyklickým kódem v přenášených datových rámcích IEEE 802.3 nebo IEEE 802.5.



Obr. 9.3: 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).



Obr. 9.4: 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.

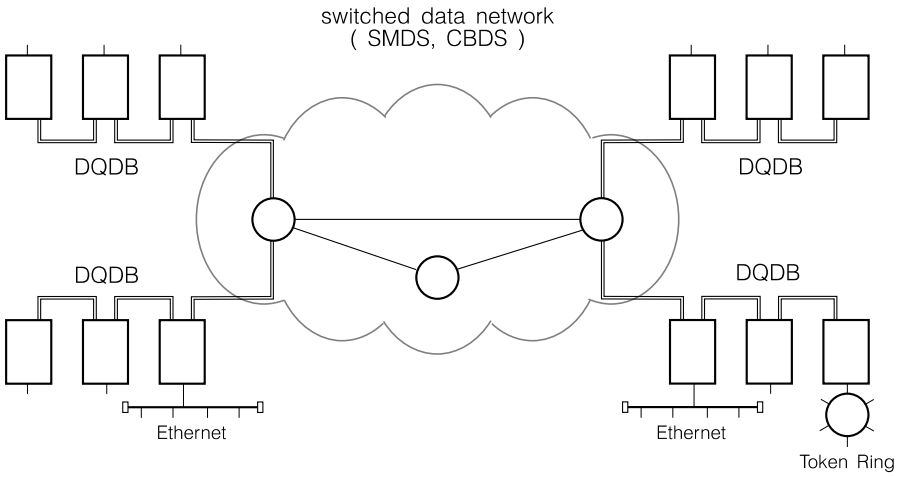
Stanice, která dostane souhlas k odeslání rámce (signál Grant) začne vysílat po všech čtyřech párech. Řadič přebírá rámec, analyzuje adresu cílové stanice a rozhoduje se, na které výstupy rámec předá. Možnost filtrace toku dat zvyšuje bezpečnost sítě, požadavek stanice na předávání pouze jí adresovaných 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). Podobně, síť 100VG-AnyLAN může být cenově výhodnou alternativou páteřní sítě k technologii FDDI; na rozdíl od FDDI však nedovoluje zprostředkovat současný provoz IEEE 802.3 CSMA/CD i IEEE 802.5 Token Ring.

10. Metropolitní síť, 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.

Řešením je připojení koncových účastníků rychlými sdílenými kanály, v úvahu by mohly přicházet kruhy FDDI nebo FDDI II, ale nejuvažovanějším řešením je velice zajímavé rozhraní označované jako DQDB (Double Queue – Double Bus). Jeho použití v metropolitní síti uvádí obr. 10.1.



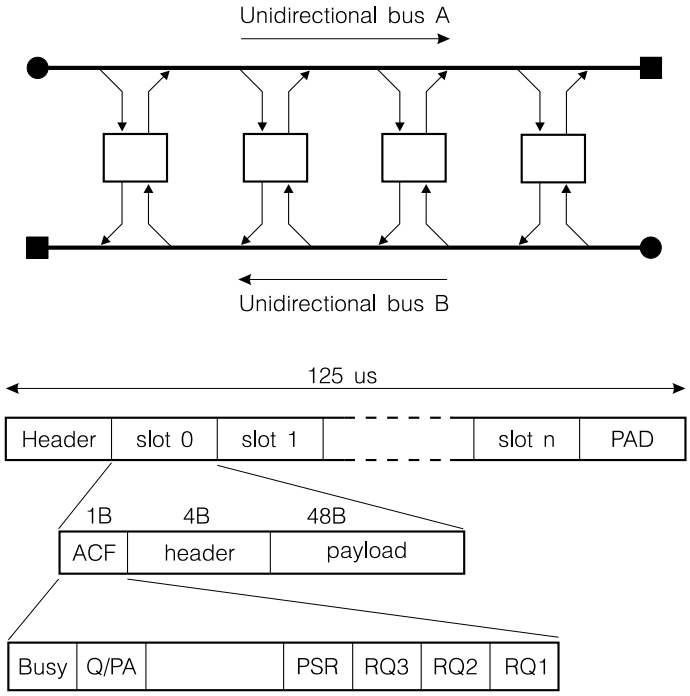
Obr. 10.1: DQDB – Architektura metropolitní sítě s rohraním DQDB

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.10.2).

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



Obr. 10.2: DQDB – Struktura sítě DQDB a formát buňky

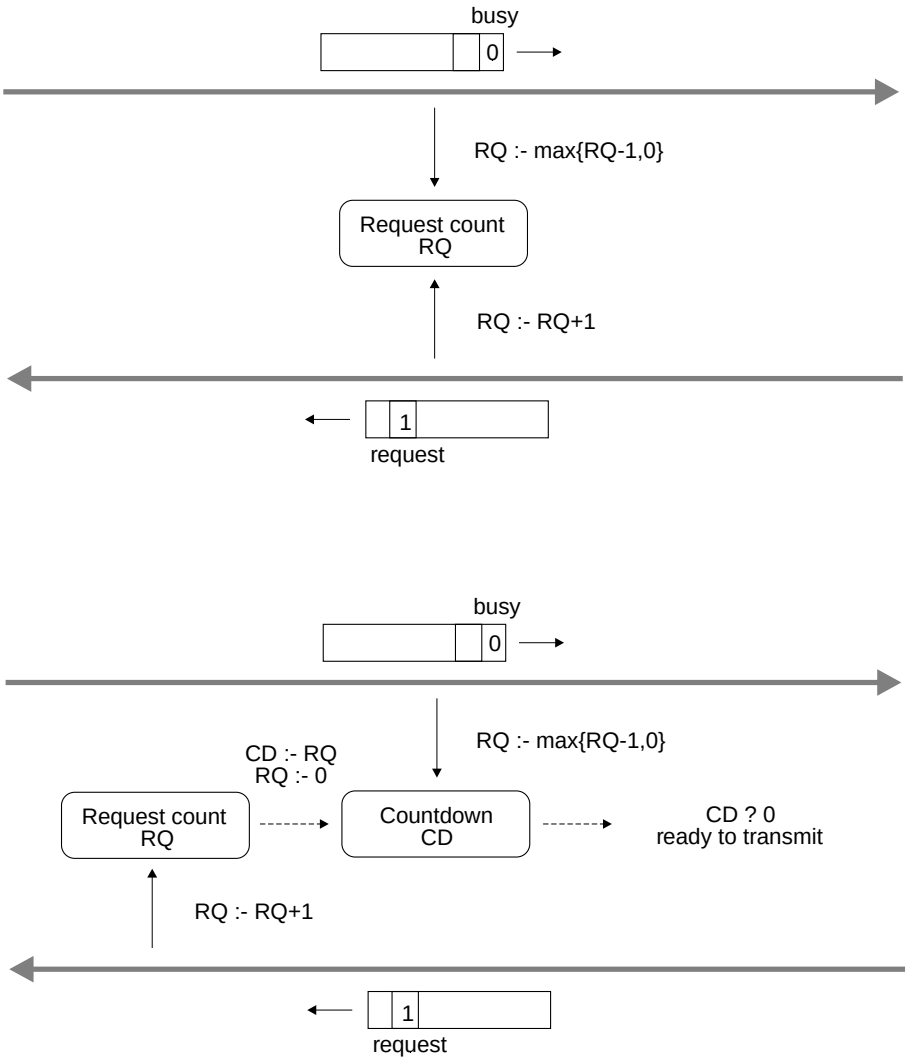
zajímavějším, režimem činnosti je přidělování jednotlivých slotů stanicím na jejich žádost. Tyto sloty jsou tedy využívány v režimu adaptivního časového multiplexu. Rozhraní DQDB poskytuje služby označované jako isochronní služba, datagram (Connectionless Data Transfer) a virtuální kanál (Connection-Oriented 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.10.3). 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.



Obr. 10.3: 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.

11. 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 dovolují přenos rychlostí stovek kilobitů na kilometrové vzdálenosti) nebo lépe digitálních kanálů (základní a primární ISDN, digitální spoje E1 nebo E3). S rozvojem překryvné digitální sítě se objevuje 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 dnes rozhodně není chápána pouze jako metoda dovolující velmi efektivní propojování lokálních sítí moderní digitální překryvnou sítí. Setkáváme se s ní stále častěji 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, nadějně vypadá i současný rozvoj prvků pro přenos ATM rychlostí 25 Mb/s po kabelech UTP Cat.3. 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 již dnes konkurují kruhovým sítím FDDI a vzhledem k jejich vlastnostem lze očekávat jejich další rozvoj a velké rozšíření v oblasti páteřních sítí a pro podporu multimediálních aplikací. Sítě ATM jsou, pokud jde o dosažitelnou přenosovou kapacitu, překonávány pouze paralelními přepojovacími sítěmi *HIPPI* (High-Performance Paralel Interface) a sítěmi využívajícími technologii *Fiber Channel*. Ty jsou však přes možnost vazby na synchronní optické sítě vyhrazeny spíše pro propojování počítačů v multipočítačových systémech na velmi malé vzdálenosti.

11.1 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 a systémy synchronní hierarchie.

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. 11.1.

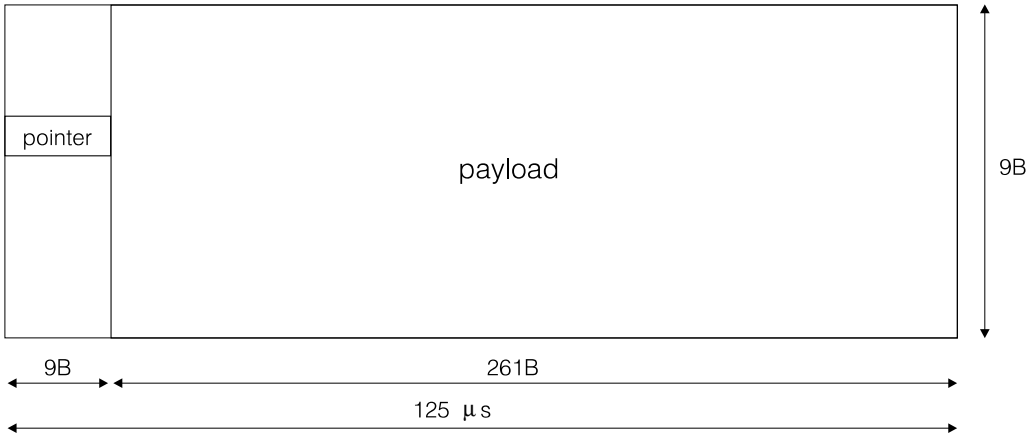
Europe	America	Japan	Number of 64 kb/s circuits	Digital Rate [Mb/s]
	T1	J1	24	1.544
E1			30	2.048
	T2	J2	96	6.312
E2			120	8.448
		J3	480	33.064
E3			480	34.368
	T3		672	44.736

Obr. 11.1: 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.



Obr. 11.2: 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. 11.3.

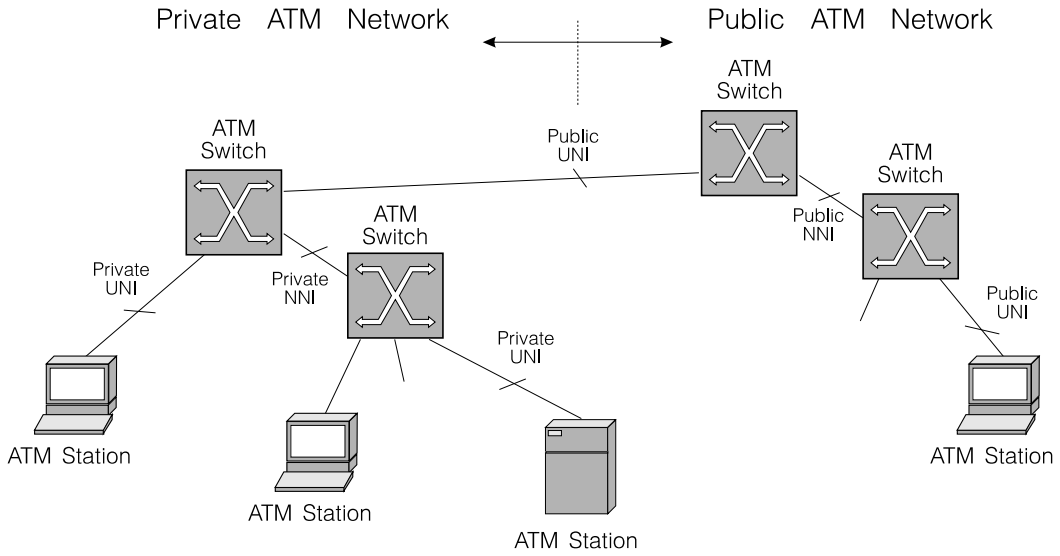
SDH STM-n	SONET STS-n	Digital Rate [Mb/s]
	STS-1	51.84
STM-1	STS-3	155.52
	STS-9	466.56
STM-4	STS-12	622.08
	STS-18	933.12
	STS-24	1244.16
	STS-36	1866.24
STM-16	STS-48	2488.32

Obr. 11.3: Synchronní přenosové systémy

11.2 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).

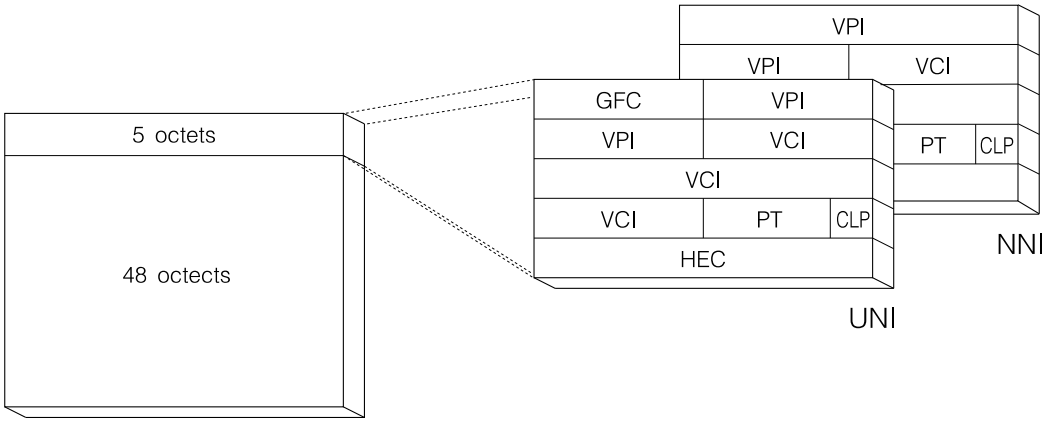
Síť ATM je tvořena přepínači ATM, mezi kterými jsou vedeny rychlé dvoubodové spoje, a na které jsou připojena koncová zařízení ATM (obr. 11.4). Struktura, funkce a chování rozsáhlých veřejných sítí je definováno materiály ITU-T, pro malé sítě privátní se o rychlé vytvoření podkladů stará skupina výrobců ATM technologie označovaná jako ATM Forum.



Obr. 11.4: Struktura sitě ATM

Data jsou mezi koncovými zařízeními ATM předávána v krátkých *ATM buňkách* (obr. 11.5) 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.



Obr. 11.5: 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

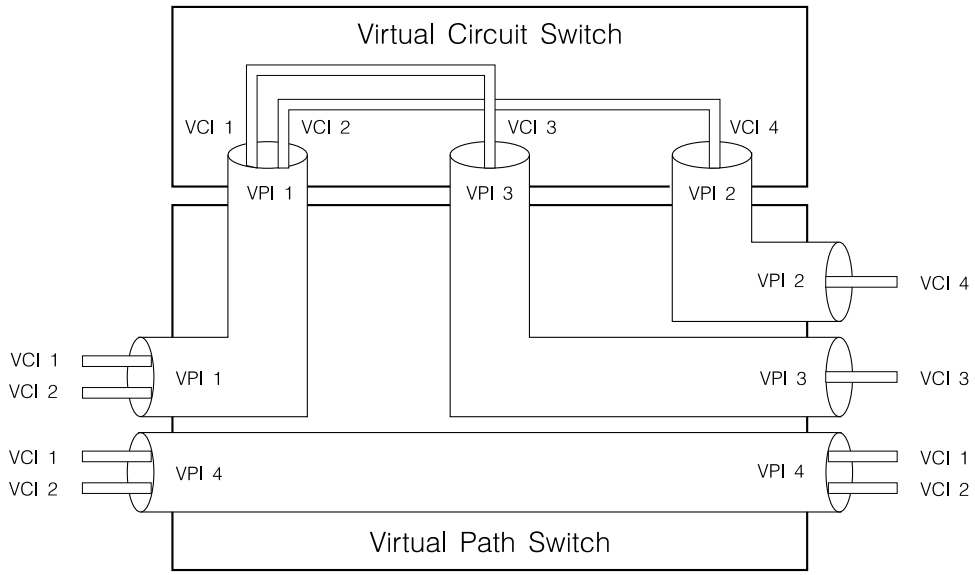
$$x^8 + x^2 + x + 1$$

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. 11.6). 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).



Obr. 11.6: Přepojování virtuálních kanálů a cest

Permanentní kanály PVC – Permanent Virtual Circuits

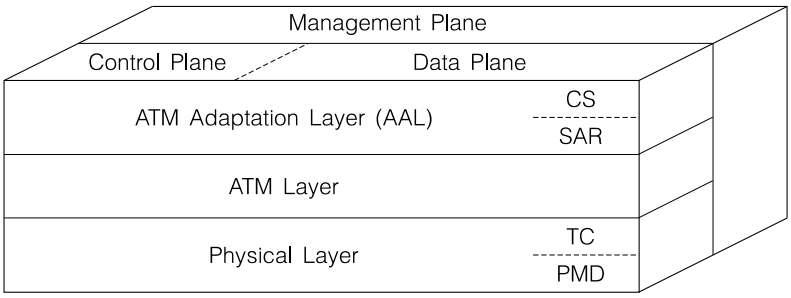
V přepojovacích tabulkách jsou položky definující virtuální kanál předdefinovány nebo nastavovány externě, typicky prostředky správy (například SNMP) a často manuálně. Permanentní spojení mají statický charakter, jejich použití se omezuje na některé vnitřní funkce sítě (signalizace, správa, virtuální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

11.2.1 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 11.6. 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.



Obr. 11.7: Architektura ATM

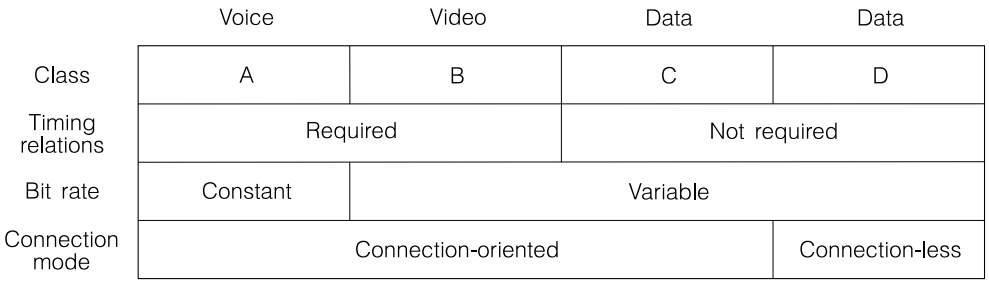
Architektura ATM dělí *fyzickou vrstvu* na část nezávislou na médiu (*Transmition Convergence Sublayer*), ta definuje strukturu buněk a využití informací v hlavičce, a na část závislou na použitém médiu (*Physical Medium Dependent Sublayer*), ta popisuje přenosové

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. 11.8) a jednotlivé třídy charakterizuje nutností dodržet přenosovou rychlost, časové relace (rozptyl zpoždění buněk) a zajistit potvrzování.



Obr. 11.8: 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.

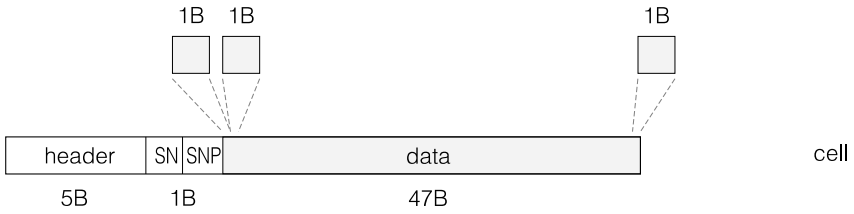
UBR – Unspecified Bit Rate

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

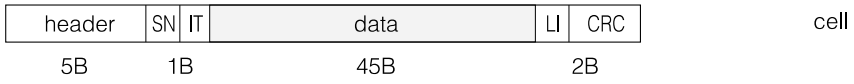
Slouží k uložení toku oktetů provozu CBR (produkovaných např. převodníkem hlasového signálu) do buněk ATM. Adaptační vrstva AAL1 nepodporuje ochranu proti chybám, pouze dovoluje detekovat ztracené buňky. Buňky jsou číslovány čtyřbitovým polem SN (Sequence Number), zabezpečeným proti chybám čtyřbitovým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



Obr. 11.9: 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.

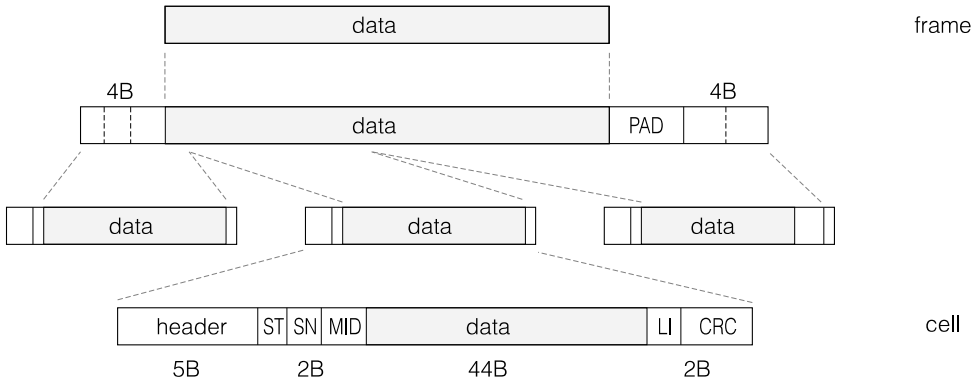


Obr. 11.10: Buňka AAL2

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).

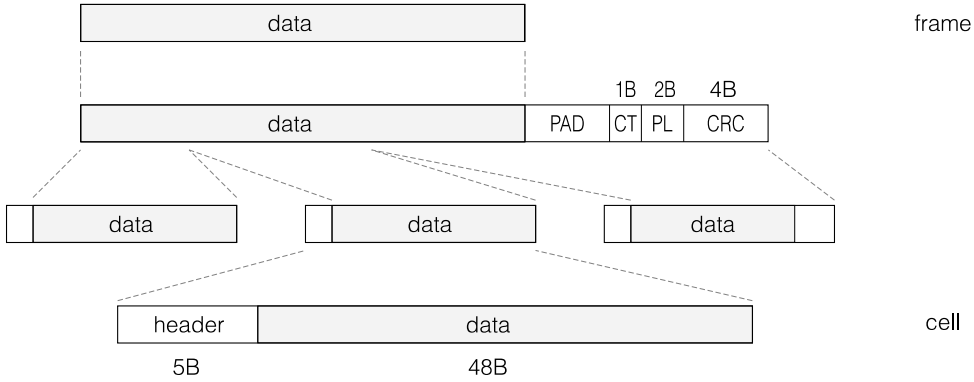
Každá buňka obsahuje šestibitovou informaci o délce přenášených dat LI (Length Indicator) a je zajištěna desetibitovým cyklickým kódem CRC. Desetibitové pole MID (Multiplexing Identification) dovoluje současný přenos více aplikačních rámců po jediném virtuálním kanále ATM. Pro data je v buňce k dispozici 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.



Obr. 11.11: 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.



Obr. 11.12: Adaptační vrstva AAL5

11.2.2 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

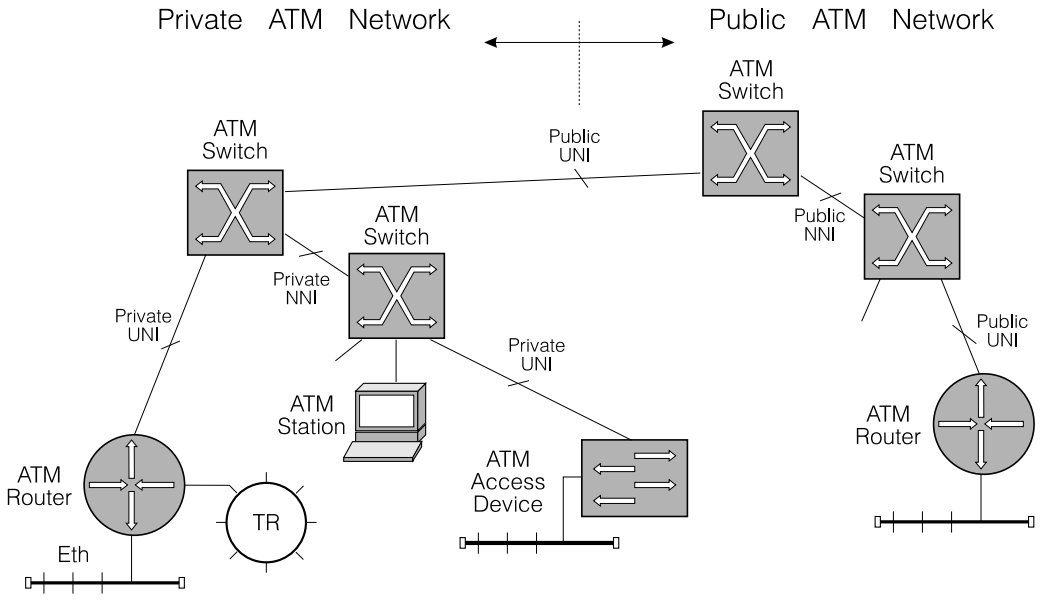
virtuálního kanálu odesláním žádosti Setup (obsahuje adresu cílové stanice a požadavky na parametry kanálu) po služebním kanálu (VPI=0,VCI=5) a obdrží od prvého ATM přepínače potvrzení Call Proceeding. Žádost Setup je mezitím předávána ATM přepínači sítě k cílové stanici a současně je budován virtuální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

11.3 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.

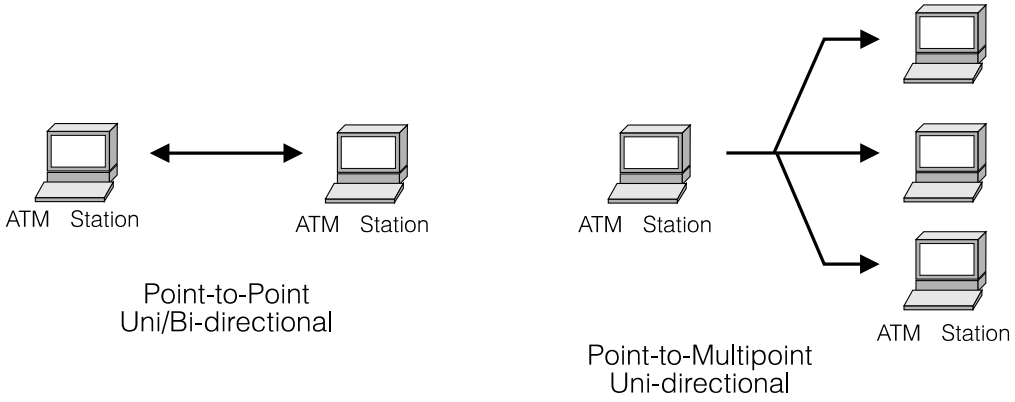


Obr. 11.13: Struktura sítě ATM s emulací LAN

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. 11.13), 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. 11.14). 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.



Obr. 11.14: 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. 11.15):

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.

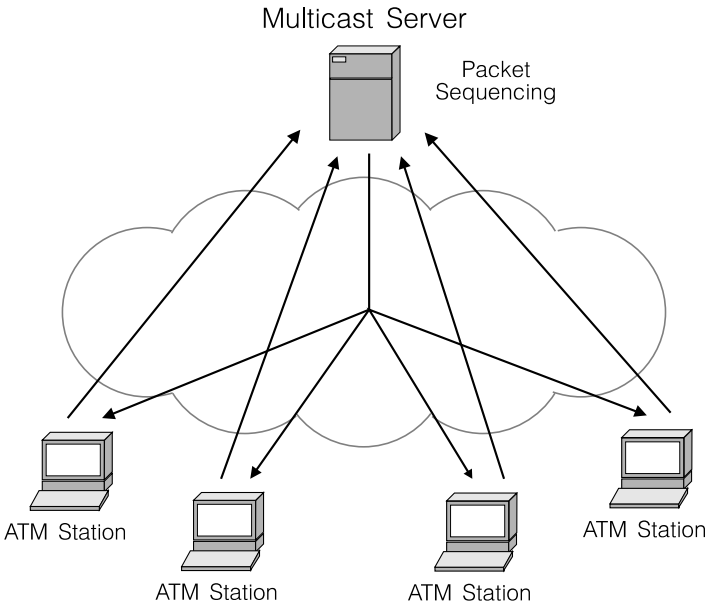
Multicast Server

Koncová stanice odesílá datový rámec vyhrazenému serveru (Multicast Server – obr. 11.15) 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

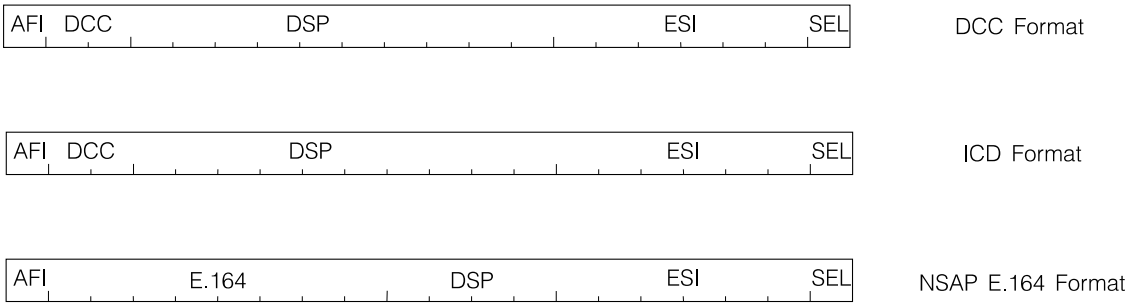
ostatních stanic.



Obr. 11.15: Realizace vícebodového kanálu Multipoint-to-Multipoint

11.3.1 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. 11.16.



Obr. 11.16: 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.

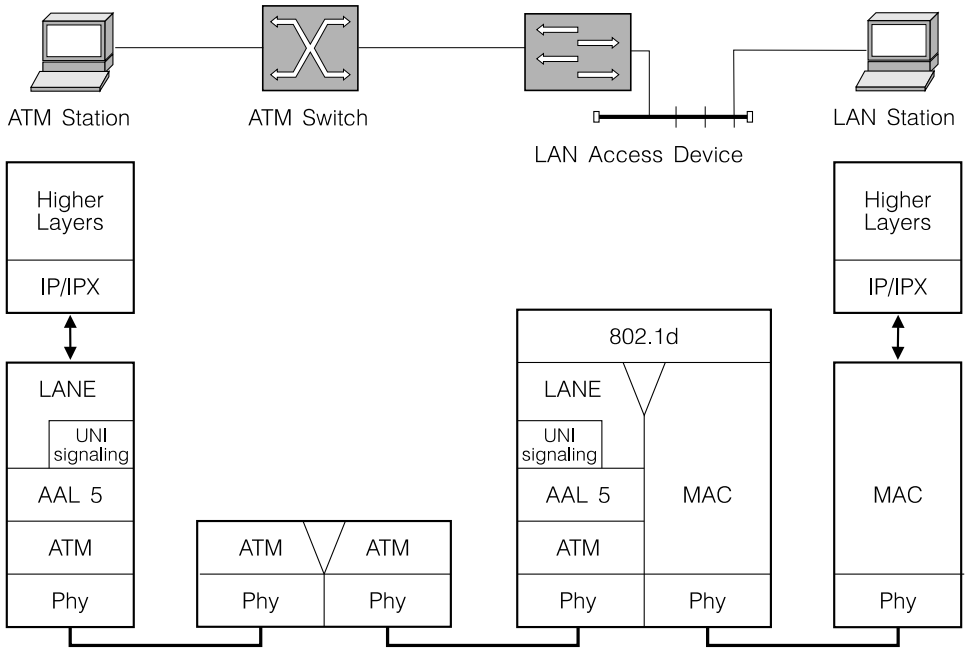
P-NNI Phase 0 (IISP – Interim Inter-Switch Signaling Protocol)

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.

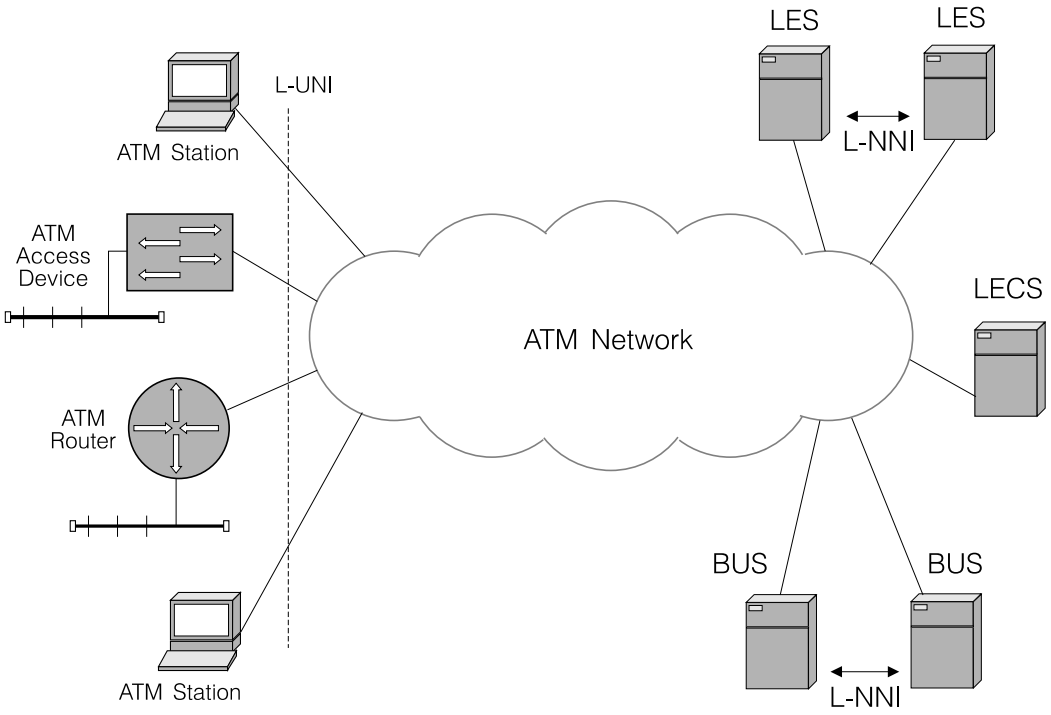
11.4 Virtuální sítě, emulace LAN

Plná náhrada technologií sdíleného kanálu pro lokální komunikaci plně přepojovanou sítí ATM zřejmě není v současnosti reálná. Zajímavé je ale využití sítě ATM pro přenos rámců odpovídajících standardům současných lokálních sítí.



Obr. 11.17: 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).



Obr. 11.18: 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.

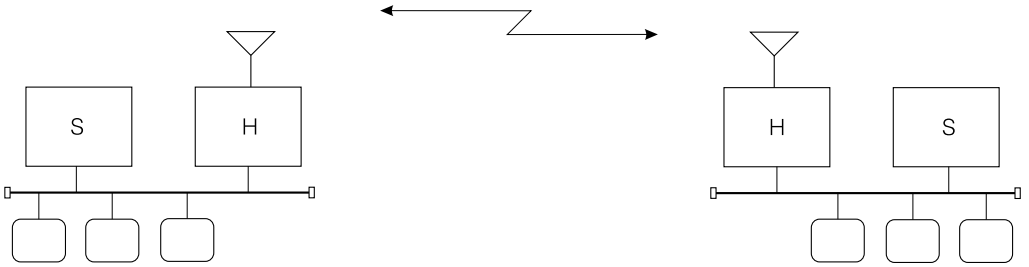
12. Bezdrátové sítě

Klasické lokální sítě využívají jako přenosové médium elektrických vedení nebo optických vláken a jsou vhodné pro propojení stacionárních zařízení. Pevné připojení je však málo pružné pro moderní přenosné osobní počítače (ale i další zařízení, jako jsou PDA, jednoúčelové terminály pro obchody, ap.), jejich nasazení vyžaduje použití bezdrátových spojů – *rádiových* nebo *optických*.

12.1 Rádiové spoje

Rádiové spoje jsou již po dlouhou dobu používané pro přenos dat mezi mobilními pracovišti některých služeb (lékařská záchranná služba, policie) a základnovými stanicemi. Požadavky na rychlost přenosu (nebo spíš možnosti takových systémů) jsou většinou omezené, při typickém využívání analogových hovorových rádiových kanálů nepřekračuje rychlost přenosu dat 9.6 až 14.4 kb/s, sítě však dovolují pokrýt území o průměru několika kilometrů. Rozšiřování moderních digitálních systémů rádiové telefonie (u nás je používaný *GSM* – Groupe Spèciale Mobile) pracujících s kombinací frekvenčního a časového multiplexu v buněčně rozdělených oblastech dovoluje přenos malých množství dat i uživatelům z jiných oborů. Modernější systémy (jako *PCN* – Personal Cellular System) přenos dat jako základní službu předpokládají. V tomto textu si pomalých spojů opřených o hovorové rádiové kanály (ať už analogové nebo digitální) příliš všímat nebudeme, uvedeme si především technologie, které jsou zajímavé pro lokální sítě a poskytují vyšší přenosové rychlosti.

Použití rádiových spojů v lokálních sítích je vhodné ve dvou případech. Jednodušší je jejich nasazení tam, kde je potřeba překlenout menší vzdálenosti mezi částmi klasické lokální sítě oddělenými prostorem, ve kterém buď nelze pro potřebnou dobu získat nebo vybudovat spoje drátové nebo optické, nebo kde by pronájmutí nebo vybudování takových spojů bylo neekonomické. Takový rádiový spoj je pevně instalovaný, zpravidla dvoubodový duplexní – *směrový*. S vhodně volenými antennimi systémy lze v mikrovlnných pásmech překlenout vzdálenosti až desítek kilometrů při přenosových rychlostech do 10 Mb/s, vzhledem k používaným kmitočtovým pásmům je požadována přímá viditelnost. Pro překonání větších vzdáleností, nebo když se potřebujeme vyhnout terénní nebo stavební překážce na trase, můžeme využít retranslace. Úzké směrování paprsků dovoluje využít shodných kmitočtů i na omezeném území, podmínkou spolehlivé činnosti je však plánovité přidělování kmitočtů jednotlivým spojům a povolovací řízení.

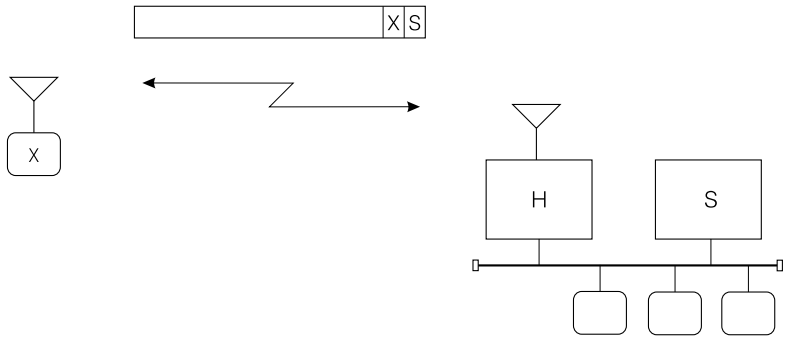


Obr. 12.1: Propojení lokálních sítí směrovým spojem

Příkladem takového řešení jsou směrové spoje firmy Motorola pro pásmo 18 GHz, systémy pracující s pevnými přidělenými kmitočty jsou označovány jako *úzkopásmové* (*Narrow Band*). Problém přidělování kmitočtů, které má zabránit interferenci, lze obejít použitím technik *rozprostřeného pásma* (*Spread Spectrum*). V pásmech určených pro průmyslové aplikace (ale i např. mikrovlnné trouby), vědecké experimenty a lékařskou techniku se tak lze vyhnout

nejen problémům s interferencí ale i povolovacímu řízení – pásma jsou označována jako *ISM* (Industrial, Science, Medicine). Příklad propojení dvou lokálních sítí směrovým rádiovým spojem uvádí obr. 12.1. Oddělení obou sítí mostem (nebo ještě raději směrovačem) omezí přenos dat na nutné minimum.

Druhou, a zřejmě zajímavější, oblastí nasazení rádiových spojů je připojování mobilních zařízení. Používány jsou převážně vícebodové – *všesměrové* spoje, které zajišťují komunikaci mobilních zařízení se základnovými stanicemi (princip připojení mobilního zařízení k lokální síti ilustruje obr. 12.2). Běžně se používá dvojice kanálů, v jednom vysílají mobilní zařízení, ve druhém základnová stanice; z pohledu základnové stanice se jedná o duplexní provoz.



Obr. 12.2: Připojení mobilního zařízení k lokální síti všesměrovým spojem

Základnové stanice jsou připojené do běžné lokální sítě a plní současně funkci mostu nebo směrovače. Vzdálenost mezi mobilním zařízením a základnovou stanicí je typicky do 300 m (menší v budovách – není vyžadována viditelnost – než ve volném prostoru) při přenosové rychlosti kolem 1 Mb/s. Pokrytí větších území vyžaduje použití více základnových stanic napojených na kabeláž.

Na rozdíl od dvoubodových směrových spojů je u vícebodových všesměrových spojů nutné řešit problém vícenásobného přístupu ke kanálu (dostřednému, na němž vysílají mobilní zařízení a přijímá základnová stanice, u odstředného kanálu, na kterém vysílá základnová stanice, tento problém nevzniká). Řešením je typicky *časový multiplex* dovolující rozdělit přenosovou rychlost kanálu mezi proměnlivý počet mobilních zařízení; jinou (a častěji využívanou) možností jsou techniky *rozprostřeného pásma*. Určitým problémem všesměrových spojů jsou interference mezi dvěma nebo více sítěmi na stejném území, nebo interference mezi základnovými stanicemi v téže síti. Problém lze řešit kmitočtovým plánem (přidělit sousedním základnovým stanicím různé kanály) nebo prací v rozprostřeném pásmu.

Rádiové spoje používají řadu kmitočtových pásem, některá z nich vyžadují přidělení (kromě jiného chránící uživatele před interferencemi), jiná takové přidělení nevyžadují a jejich použití buď přináší riziko interference (u úzkopásmových systémů) nebo se tomuto riziku určitým způsobem provozu vyhýbáme (u systémů s rozprostřením pásma, bez něj by například nebylo možné používat pro přenos dat pásem ISM). Pro zajímavost si uvedeme přehled pásem využívaných typickými zařízeními pro rádiový přenos dat v lokálních sítích (obr. 12.3).

12.1.1 Rozprostřené pásmo

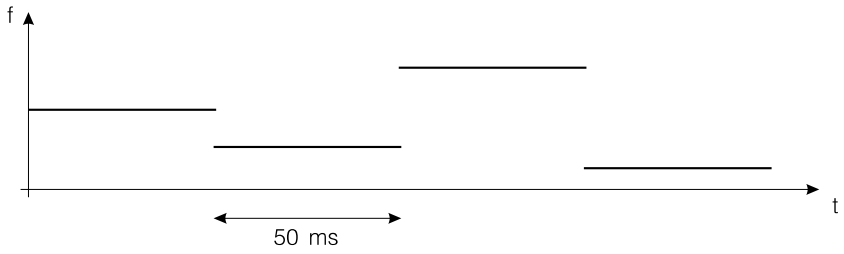
Vícebodová komunikace opírající se o všesměrový kanál vychází z principů známých od čtyřicátých let a používaných k utajení komunikace pro vojenské účely. Dnes jsou tyto techniky běžně využívány v civilních aplikacích a řeší řadu problémů spojených s bezdrátovým připojováním mobilních zařízení.

Licenced	18 GHz FDMA	Motorola
Digital Telephony	890 - 915 MHz 935 - 960 MHz TDMA 8/16 channels 200 kHz 1.7 - 1.9 GHz TDMA 8/16 channels 200 kHz, DSSS	GSM PCN
Industry Science Medicine	902 - 928 MHz FHSS 52(50) channels 0.5 MHz, DSSS 2.4 - 2.4835 GHz FHSS 83(75) channels 1 MHz, DSSS 5.725 - 5.850 GHz FHSS 125(75) channels 1 MHz, DSSS	

Obr. 12.3: Kmitočtová pásma pro rádiovou komunikaci v lokálních sítích

Rozprostření pásma FHSS

Technologie rozprostření pásma označovaná jako *FHSS* (Frequency Hopping Spread Spectrum) využívá pro komunikaci stanic skupinu více kanálů. Komunikující stanice mění během provozu pracovní kmitočet, na každém kanále pracují po omezenou dobu. Posloupnost přechodů mezi kanály je pseudonáhodná, komunikující stanice mění pracovní kmitočet synchronně a vnějšímu pozorovateli mohou tyto změny připadat jako náhodné. Volba různých (ortogonálních) posloupností dovolí současnou práci více stanic v jednom místě.



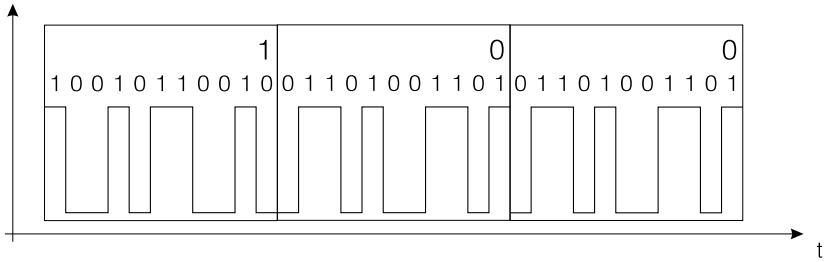
Obr. 12.4: Rozprostření pásma FHSS

Podle frekvence přechodů rozdělujeme systémy FHSS na systémy s pomalou (několik změn za sekundu) a s rychlou změnou kmitočtu (stovky změn za sekundu). Provoz v režimu FHSS je využíván ve všech pásmech ISM. Pásmo 2.4 – 2.4835 GHz je pro tento druh provozu rozděleno na 83 kanálů o šířce 1 MHz, pásmo 902 – 928 MHz na 52 kanálů o šířce 0.5 MHz a konečně pásmo 5.725 – 5.850 GHz na 125 kanálů o šířce 1 MHz. Pro provoz v pásmech ISM jsou definována určitá omezení: výkon vysílače musí být omezen na 1 W, práce na jednom kanálu v pásmu 2.4 GHz a 5.7 GHz smí trvat nejvýše 0.4 s během 30 s provozu stanice a kanály mají být využívané rovnoměrně. Pro pásmo 902 – 928 MHz je povolená doba vysílání 0.4 s během 20 s provozu. Tato omezení jsou definována FCC pro Spojené státy, ale jsou aplikována celosvětově. Uvedená omezení vyžadují vystřídat alespoň 75 kanálů v pásmu 2.4 GHz a 5.7 GHz, nebo 50 kanálů v pásmu 902 – 928 MHz.

Do limitu 0.4 s lze odeslat po jednom kanálu celý rámec, k opakování rámce, u kterého došlo k poškození, například interferencí, se již využije kanálu jiného. To, že k provozu není nutné využít všech kanálů pásma, dovolí vyhnout se kanálům rušeným interferencí. Rozdělení pásma na kanály limituje přenosovou rychlost na 1 Mb/s i při použití efektivních modulačních technik.

DSSS

Technologie rozprostření pásma označovaná jako *DSSS* (Direct Sequence Spread Spectrum), někdy nazývaná také *kódový multiplex – CDMA*(Code Division Multiple Access) se opírá o poněkud jiný princip. Namísto jednotlivých bitů (symbolů) jsou na nosnou frekvenci namodulovány pseudonáhodné posloupnosti bitů o délce od deseti do tisíců bitů. Nule originálních dat odpovídá určitá bitová posloupnost, jednotce odpovídá posloupnost jiná (většinou inverzní). Délka posloupnosti se liší podle předpokládané aplikace, běžné civilní aplikace používají krátké posloupnosti, vojenské aplikace (u kterých je důležité utajení provozu před odposlechem) používají až tisíců bitů. Vnější pozorovatel má dojem, že je vysílán šum, přijímač, který zná pseudonáhodnou posloupnost, používá pro detekci uložených dat korelační algoritmus.



Obr. 12.5: Rozprostření pásma DSSS

Podobně, jako je u provozu FHSS omezena doba práce na každém z kanálů, je u provozu DSSS zdola omezena délka bitové sekvence pro jeden symbol. Limit (opět stanovený FCC pro Spojené státy) je deset bitů na symbol. Omezení na deset bitů dovolí dosáhnout přenosové rychlosti 2 Mb/s v pásmu 902 – 928 MHz nebo 8 Mb/s v pásmu 2.400 – 2.435 GHz. Vzhledem k možnosti rušení v úzkém pásmu je výhodné rozdělit pásmo 2.4 GHz na několik kanálů a pro provoz DSSS vybrat ten z nich, ve kterém k interferenci nedochází.

Technika DSSS začíná efektivně potlačovat interferenci při zhruba 100 bitech na symbol, při nižších poměrech používaných v lokálních rádiových sítích je důležité zajistit, aby základnová stanice slyšela všechna pohyblivá zařízení zhruba stejně silně. Toho lze dosáhnout řízením jejich vysílacího signálu povely v odstředném kanále.

12.1.2 Směrové spoje

Princip a použití směrových spojů jsme si již uvedli v předcházejích odstavcích, jejich nejčastější využití, které dovoluje využít i nižších přenosových rychlostí, uvádí obr. 12.1. Zde si uvedeme pouze příklady konkrétních zařízení určených pro jejich výstavbu.

Altair

Zařízení Altair firmy Motorola využívá mikrovlnné pásmo 18.825 – 19.205 GHz vyhrazené firmě Motorola, ta přiděluje každému realizovanému spoji konkrétní kmitočet tak, aby nedošlo k interferenci s jiným spojem. Zařízení proto mohou pracovat pouze na místech a s kmitočtem, který jim byl přidělen. Dovolují přenášet data rychlostí 5.3 Mb/s na vzdálenost do 40 km.

SkyWalker

Zařízení SkyWalker české firmy Miracle pracuje v pásmu 10.3 až 10.7 GHz, které u nás nevyžaduje povolení, vzhledem k použití pevného kmitočtu je nutné ověřit, zda nedochází k interferenci s jiným provozem v pásmu. Přenosová rychlost je 4 Mb/s, překlenutelná vzdálenost 35 km.

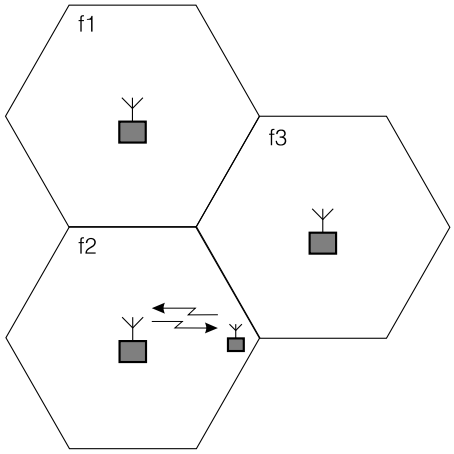
Airlink

Zařízení AirLink firmy Cylink jsou rádiové modemy pracující v pásmu 2.4 GHz technikou rozprostřeného pásma (DSSS). Jsou určeny pro směrové spoje, dovolují překlenout vzdálenost 50 km a jejich přenosová rychlost je (podle typu) 64 až 512 kb/s. Pro propojení lokálních sítí lze většinou použít i zařízení primárně určená pro bezdrátové připojování mobilních zařízení (například AirLAN firmy Solectec, viz str. 102). Potřebujeme-li překonat větší vzdálenosti, je nutné je vybavit směrovými anténními systémy.

Směrové kanály mohou být použity i pro propojení stacionárních zařízení (a výstavbu vnitřní struktury lokální sítě) v případě, že se chceme vyhnout kabeláži (časově omezená instalace, nemožnost realizovat pevnou kabeláž). Tento cíl sleduje evropská specifikace HIPERLAN (HIgh PErformance Radio Local Area Network), pro kterou jsou vyhrazena kmitočtová pásma 5.12 – 5.30 GHz a 17.1 – 17.3 GHz.

12.1.3 Rádiové sítě LAN

Rádiové lokální sítě se opírají o strukturu odpovídající obr. 12.2, mobilní zařízení jsou rádiovými kanály připojena k základnovým stanicím, které jsou propojené mezi sebou a se servery běžnou kabeláží. Vhodné rozložení základnových stanic dovoluje využít týchž kanálů v několika lokalitách, princip návrhu sítě a rozložení základnových stanic je obdobou celulárních sítí, jak je známe u mobilních telefonů.



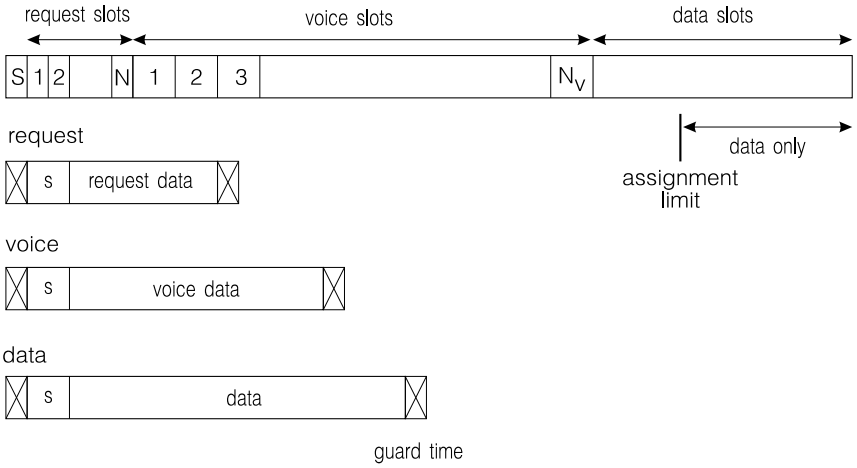
Obr. 12.6: Topologie rádiových lokálních sítí

PCN

Celulární síť se základnovými stanicemi propojenými kabeláží využívá například systém *PCN* (Personal Cellural Network), jehož funkci si nyní popíšeme. Struktura sítě PCN odpovídá obr. 12.6, a opírá se o rozdělení pásma 1.7 – 1.9 GHz na 16 kanálů a o jejich přidělení sousedním buňkám tak, aby nedocházelo k interferenci. Šířka kanálů je 200 kHz, přenosová rychlost v kanálu je 270.833 kb/s.

Pokud má být jeden pracovní kmitočet přidělený buňce využíván pro současnou komunikaci více mobilních stanic, musíme zajistit nějakou formu časového multiplexu. Ten může být i dosti složitý, (obr. 12.7) uvádí řešení časového multiplexu pro síť PCN.

Komunikace mezi mobilními stanicemi a základnou probíhá v časových rámcích dostředného kanálu. Každý z nich je rozdělen na několik částí. Prvou částí, která následuje za synchronizačním slotem, je skupina rezervačních slotů. V nich mobilní stanice může požádat



Obr. 12.7: Časový multiplex PCN

o přidělení synchronního slotu, nebo o odeslání rámce v asynchronním režimu. Kolize při podávání žádosti vede na opakovanou žádost po určité prodlevě (metoda Aloha). Následující synchronní sloty slouží přenosům, které vyžadují přenesení pevného množství dat v každém rámci, např. pro přenos digitalizovaného hovorového signálu. Synchronní slot, který mobilní stanice neobsadí, může základnová stanice přidělit jinému zájemci. Zbývající část rámce je využitelná pro asynchronní provoz – pro přenosy, které nevyžadují doručení do časového limitu. Hranice mezi synchronními sloty a intervalem pro přenos dat je pohyblivá, s určitým omezením, které dovolí zachovat určitý objem asynchronního provozu při velkém množství požadavků na přenosy synchronní.

Alternativou k využití pásma v časovém multiplexu je technika rozprostřeného pásma DSSS. Ta dovolí současné vysílání většího počtu stanic a detekování jimi předávaných dat v základnové stanici (obr. 12.8).

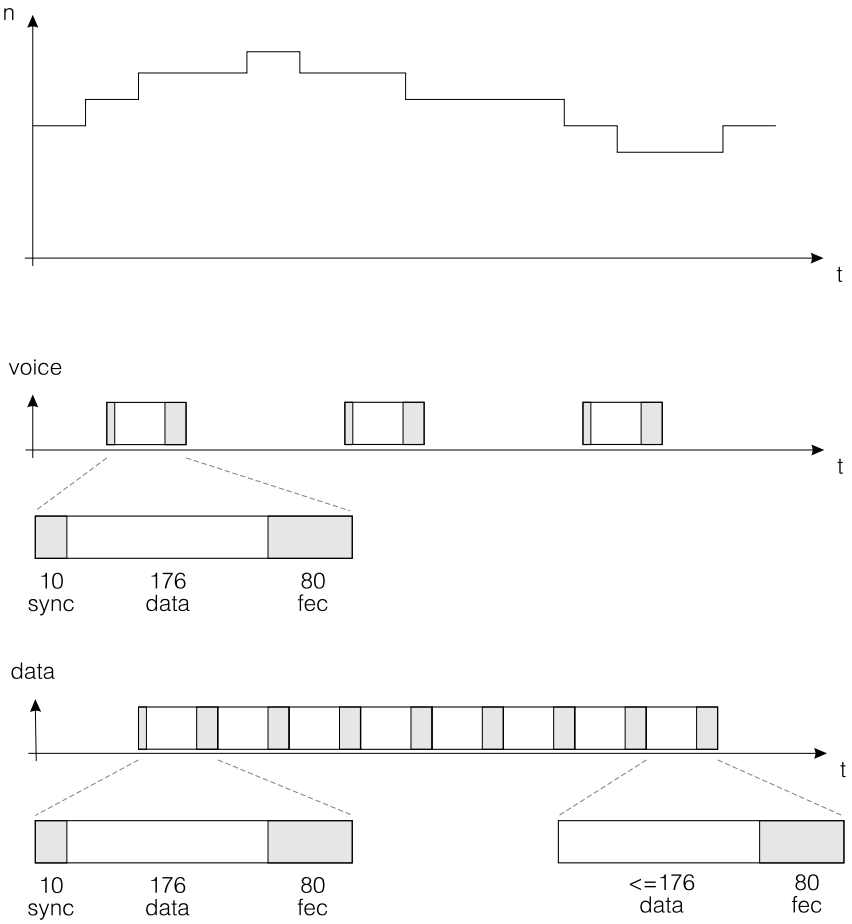
Podobně jako v případě časového multiplexu i u multiplexu kódového lze zajistit synchronní i asynchronní provoz. U synchronního provozu to znamená v pravidelných časových intervalech přenést datový rámec. Asynchronnímu provozu odpovídá přenesení posloupnosti rámců, délka této posloupnosti závisí na délce datového bloku, který potřebujeme přenést.

Při přenosu v rozprostřeném pásmu je sice možné odfiltrovat signál jednotlivé stanice, postup je však pochopitelně podstatně náchylnější k chybám než přenos úzkopásmový (časový multiplex). Data (synchronní i asynchronní) jsou proto přenášena v krátkých rámcích o délce 176 bitů a zajištěna cyklickým kódem BCH o délce 80 bitů. Tento kód dovolí opravit v přijatém rámci až deset bitových chyb.

Specifikace IEEE 802.11

Pro rádiové lokální sítě je v rámci IEEE 802 vytvářen standard s označením IEEE 802.11. Počítá s využitím pásma ISM 2.400 – 2.4835 GHz, kterému dává vzhledem k jeho téměř celosvětovému vyhrazení přednost před pásmy 902 – 928 MHz a 5.725 – 5.850 GHz. Předpokládá práci v rozprostřeném pásmu technikami FHSS i DSSS.

Pro FHSS je použita modulace GPSK, přenosová rychlost je 1 Mb/s. V pásmu 2.4 GHz je pro provoz FHSS využíváno 79 kanálů o šířce 1 MHz, vzhledem k požadavku FCC je nutné využít alespoň 75 z nich. Pro DSSS se používá modulace QPSK, přenosová rychlost je 2 Mb/s. Pásmo ISM je pro provoz DSSS rozděleno na pět kanálů o šířce 26 MHz, které se poněkud překrývají. To dovolí vyhnout se interferenci a problémům s odrazy v některém z kanálů. Podobně, jako je u FHSS omezena doba práce na každém z kanálů, je u provozu DSSS zdola



Obr. 12.8: Kódový multiplex PCN

omezena délka bitové sekvence pro jeden symbol. Limit (opět stanovený FCC pro Spojené státy) je deset bitů na symbol, specifikace IEEE 802.11 využívá 11-bitové posloupnosti. Alternativní technologií fyzické vrstvy lokální sítě IEEE 802.11 je difuzní optický spoj (str. 103).

WaveLAN

Systém pracující technikou rozprostřeného pásma vyráběný NCR Corporation a AT&T pracuje v pásmu 902 – 928 MHz. Opírá se o technologii DSSS, základním prvkem je dvoubitový symbol, každý symbol je zakódován pro přenos 11-bitovou posloupností. Přenosová rychlost je 2 Mb/s, šířka kanálu potřebného pro přenos je 22 MHz, překlenutelná vzdálenost je 250 m. Systém WaveLAN je současným průmyslovým standardem, kompatibilní řešení nabízí pod názvem AirLAN Solectec, nebo pod názvem RoamAbout DEC.

RangeLAN

Systém RangeLAN firmy Proxim je určený pro připojení pohyblivých zařízení (např. přenosných osobních počítačů) k základnovým stanicím. Opírá se o přenos v rozprostřeném pásmu, ale používá technologii FHSS. Má dvě varianty, lišící se využívaným kmitočtovým pásmem, rychlostí přenosu a dosahem. První varianta označovaná jako RangeLAN pracuje v pásmu 902 – 928 MHz a dovoluje komunikaci na vzdálenost do 150 m v budově a do 300 m ve volném prostoru. Lze provozovat tři vzájemně nezávislé sítě ve stejném místě. Přenosová rychlost sítě je relativně nízká (242 kb/s). Druhá varianta systému (RangeLAN2) používá pásmo 2.4 GHz. Překlenutelná vzdálenost je stejná jako u varianty pro pásmo 902 – 928 MHz. V jednom místě lze provozovat až patnáct nezávislých sítí, přenosová rychlost je 1.6 Mb/s. Obě

varianty jsou vybaveny běžnými ovladači ODI a NDIS a lze je použít v prakticky libovolném síťovém operačním systému.

Freeport

Systém Freeport firmy Cabletron dovoluje komunikaci až 62 stanic přes základnovou stanici na vzdálenost do 80 m. Využívá dvě pásma ISM pro dva nezávislé kanály, základnová stanice vysílá v pásmu 5.7 GHz, pohyblivé stanice vysílají v pásmu 2.4 GHz. Pro přenos je využito rozprostření pásma technikou DSSS, délka pseudonáhodné posloupnosti pro jeden přenášený bit je 32 bitů. Šestnáctiúrovňové fázové modulaci předchází překódování dat Trellisovým kódem, dosažitelná přenosová rychlost je 5.7 Mb/s.

12.2 Optické spoje

Rádiové spoje dnes mají v oblasti bezdrátového propojování lokálních sítí a připojování mobilních zařízení převahu, přesto je však možné setkat se i s další technologií, s využitím vzdušných optických spojů – *směrových* i *všesměrových*.

Směrové optické spoje jsou používány pro propojení částí lokálních sítí. Zařízení využívající LED diod (v oblasti infračerveného záření) postačí pro nižší přenosové rychlosti (do 16 Mb/s, tedy pro pomalejší sítě Ethernet a sítě Token Ring) na vzdálenost stovek metrů (a pochopitelně přímou viditelnost). Pro větší rychlosti a vzdálenosti (až 150 Mb/s do zhruba 2 km) jsou využívány infračervené polovodičové lasery (GaAlAs) nevyžadující zvláštní povolení. Světelné směrové spoje lze budovat velice rychle, mají však určitá principiální omezení (je dobré se vyvarovat míst se silnou turbulencí vzduchu, je nutné se vyhnout silným zdrojů infračerveného záření ve směru k vysílači – např. zapadajícímu Slunci, nepříjemný je i vliv povětrnostních podmínek – mlhy, deště a sněžení). Směrové optické spoje jsou vhodné hlavně jako dočasná řešení.

Pro připojování mobilních zařízení k základnovým stanicím lze využít i *všesměrové optické spoje*, které dovolí zvládnout vzdálenosti do 10 m. Proti rádiovým spojům mají menší dosah a je požadována přímá viditelnost mezi mobilním zařízením a základnovou stanicí. Jejich použití však může být výhodné vzhledem k omezení interferencí a větší bezpečnosti. S použitím optických všesměrových spojů počítá i standard IEEE 802.11 (uvažuje přenosovou rychlost 1 Mb/s).

IrDA

Specifikace *IrDA* (Infrared Data Association) navržená firmou Hewlett-Packard definuje částečně směrovaný přenos mezi zařízením a základnovou stanicí (všesměrová základnová stanice, na kterou je potřeba přibližně zaměřit komunikační modul mobilního zařízení – úhel maxima je kolem 30 deg) na vzdálenost do 8 m. Původní specifikace dovoluje dosáhnout přenosové rychlosti 115.2 kb/s, současná specifikace má limit na 4 Mb/s. Přenos využívá šířkové modulace světelného signálu, podpůrné obvody vyrábí řada firem a technologie se dnes využívá např. pro připojování tiskáren nebo PDA k lokálním sítím.

IBM Infrared Wireless LAN

Požadavky kladené doporučením IEEE 802.11 na přenosový kanál splňuje i technologie IBM využívající difuzního světla pro vytvoření kanálu, který může pokrýt území o velikosti 10×10 m. Přenosová rychlost je 1 Mb/s.

13. Komunikační protokoly

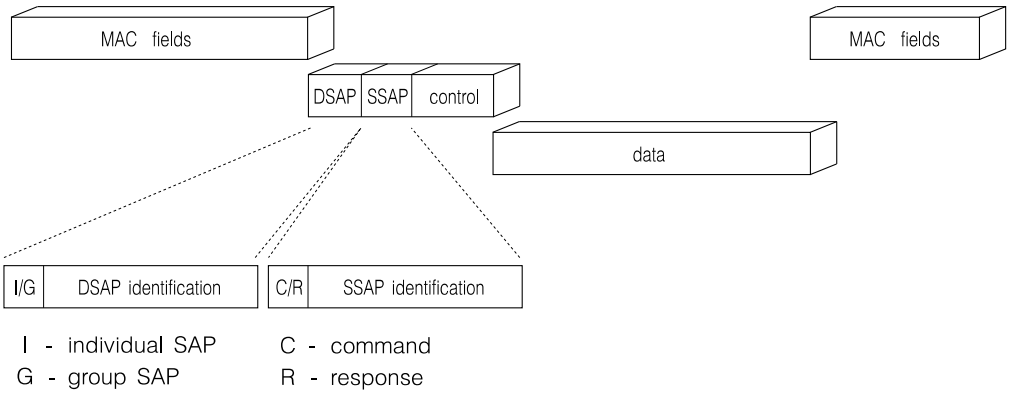
Síťová podpora aplikací musí být opřena o systém komunikačních protokolů, které zajistí předání dat v prostředí lokální sítě. Patří sem protokoly, které zajišťují *potvrzování* předávaných dat (na úrovni linkové nebo síťové vrstvy) a *směrování* (na úrovni síťové vrstvy). Jako příklad *protokolu linkové 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.

13.1 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 zajištuje 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. 13.1, seznam typů rámců uvádí obr. 13.2.



Obr. 13.1: 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:

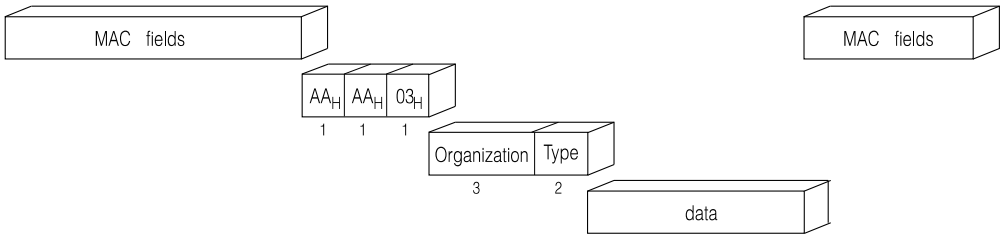
04	- SNA Path Control (individual)
AA	- SNAP
E0	- Novell Netware
F0	- IBM NetBIOS
FE	- ISO Network Layer

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

Obr. 13.2: 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. 13.3.

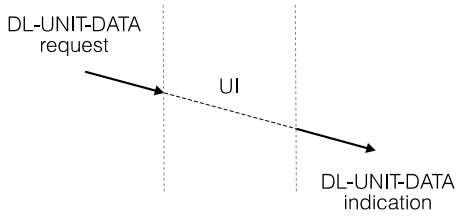


Obr. 13.3: Rámce protokolu SNAP

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. 13.4.



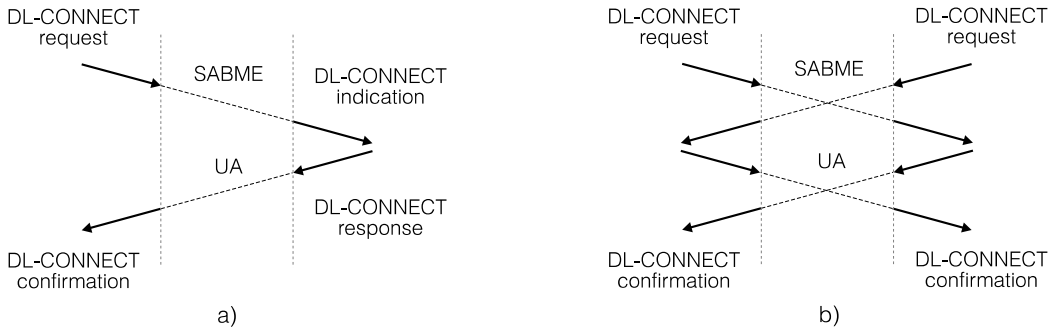
Obr. 13.4: Nepotvrzovaný datagram

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.

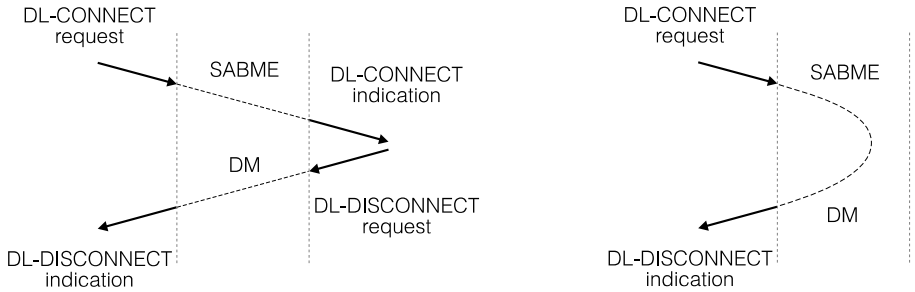
LLC2 – Logické spojení (Connection-Mode Service)

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. 13.5 a obr. 13.6.



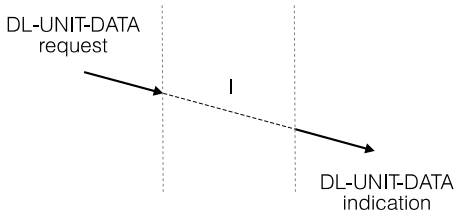
Obr. 13.5: Úspěšné navázání logického spoje

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.



Obr. 13.6: 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.



Obr. 13.7: Přenos dat

Po navázání spojení mohou oba účastníci zahájit *přenos dat* (obr. 13.7). 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. 13.8.

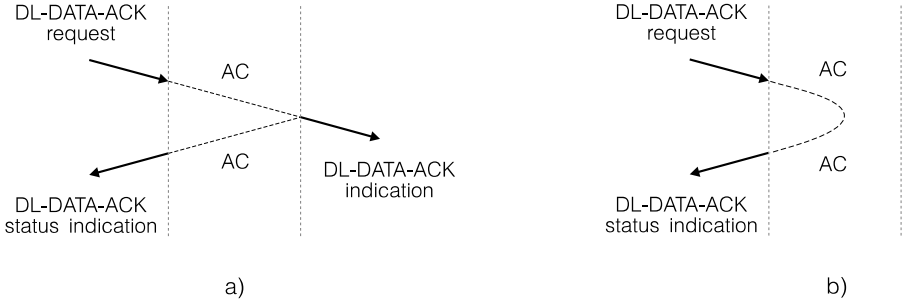
Obr. 13.8: Rozpojení logického spoje

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. 13.9.

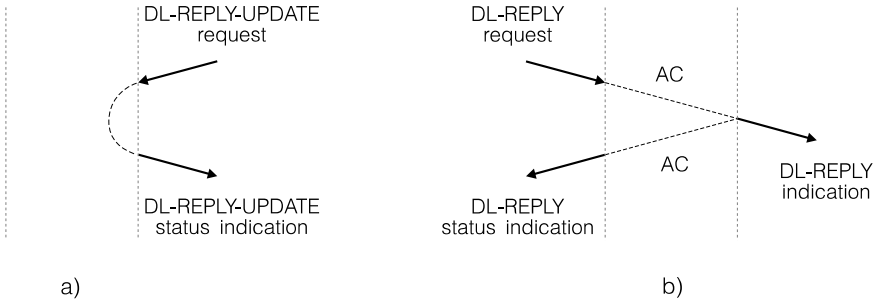


Obr. 13.9: Služba DL-DATA-ACK

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. 13.10.



Obr. 13.10: Služba DL-REPLY

13.2 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.

13.2.1 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

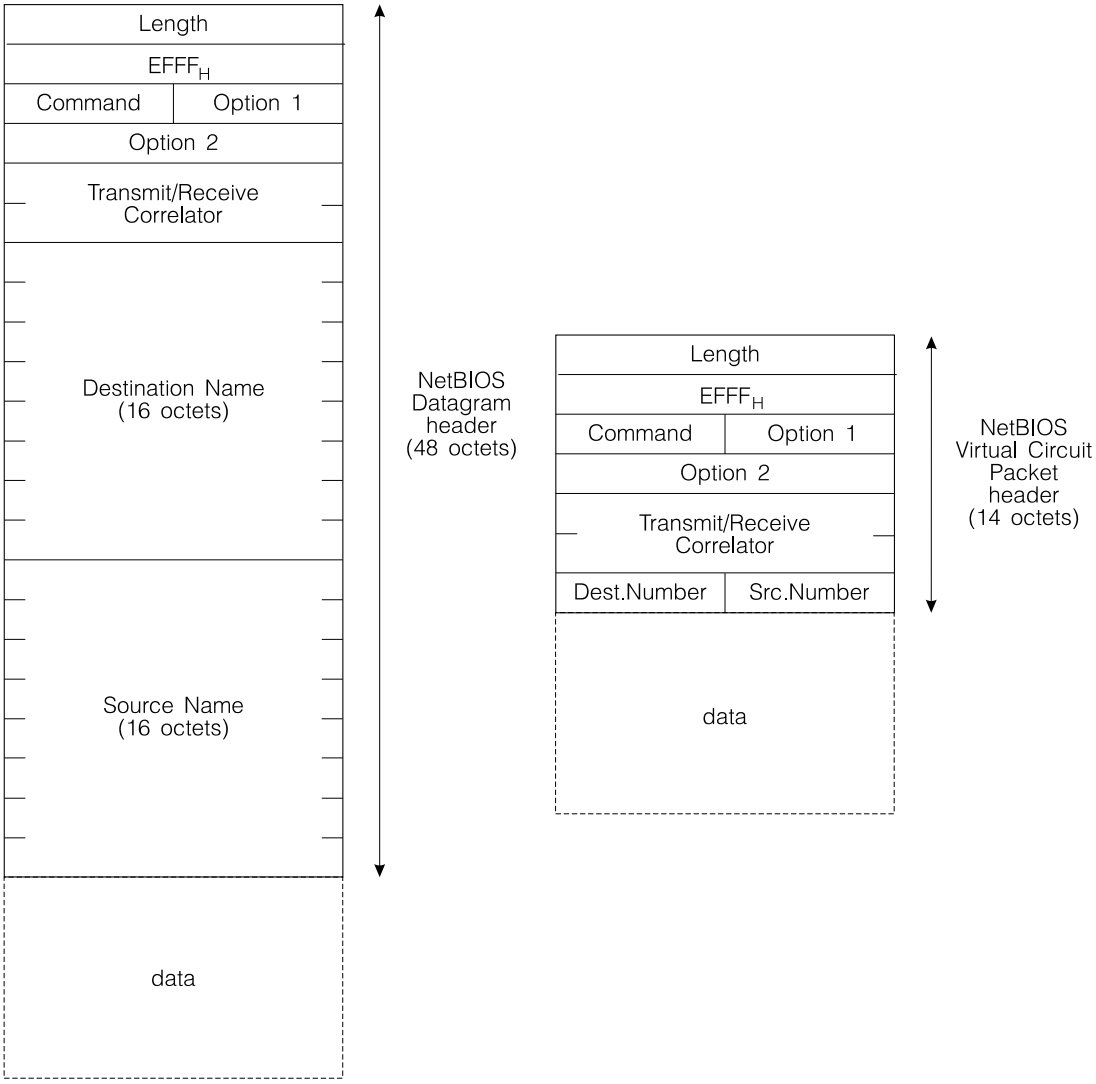
Základní služba, kterou NetBIOS podporuje, je *datagramová služba* (u protokolu NetBEUI jí odpovídá služba *MailSlot*) dovolující předání zprávy o délce do 512 B jednomu adresátovi nebo libovolné stanici na síti, která takovou zprávu očekává (*Broadcast*). Pro práci s datagramy slouží primitiva:

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).



Obr. 13.11: Pakety protokolu NetBIOS

Funkce NetBIOSu jsou podporovány dvaadvaceti typy předávaných paketů, formát uvádí obr. 13.11. 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.

13.2.2 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.

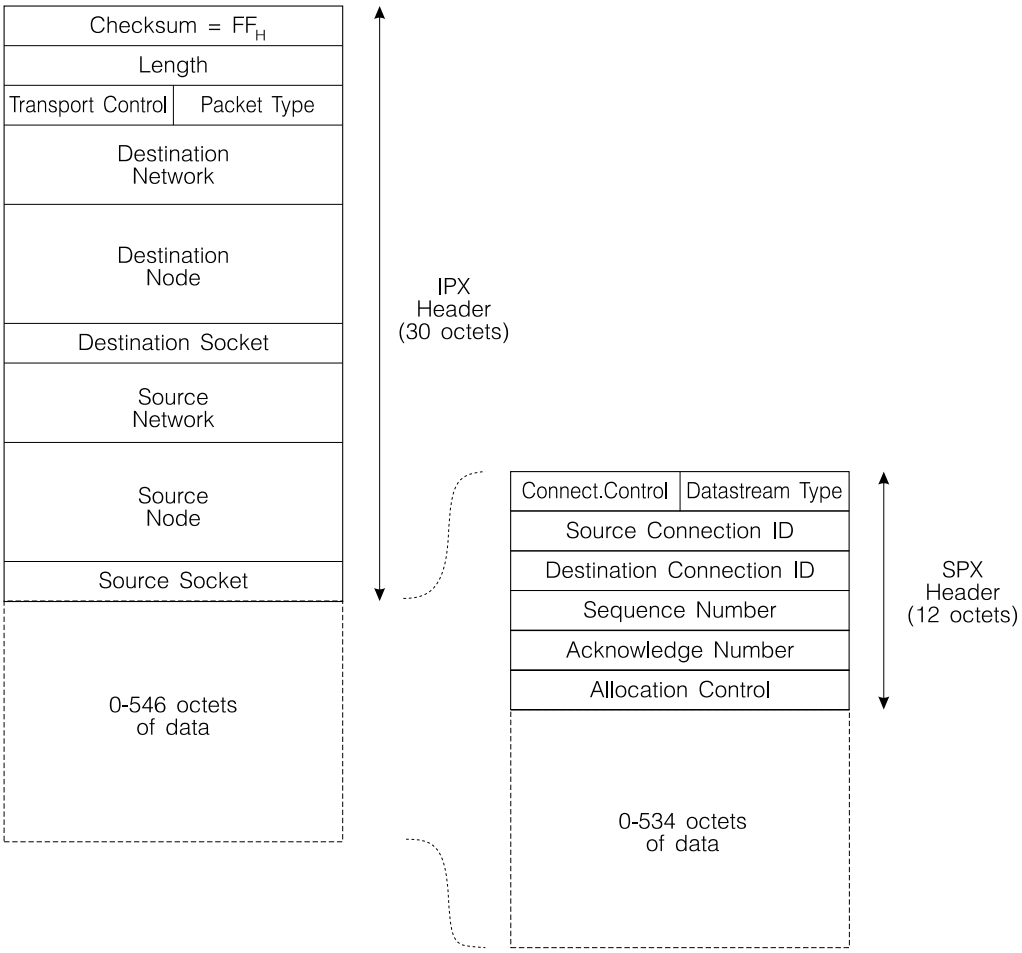
Komunikační funkce IPX/SPX vyžadují, aby aplikace uložila potřebné parametry do požadavkového bloku *ECB* (Event Control Block), obsluha požadavků může být asynchronní k dalšímu běhu aplikace. Aplikace může na ukončení požadované funkce aktivně čekat nebo může být přerušena dokončovací rutinou.

Formát paketů odpovídá obr. 13.12. 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



Obr. 13.12: 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

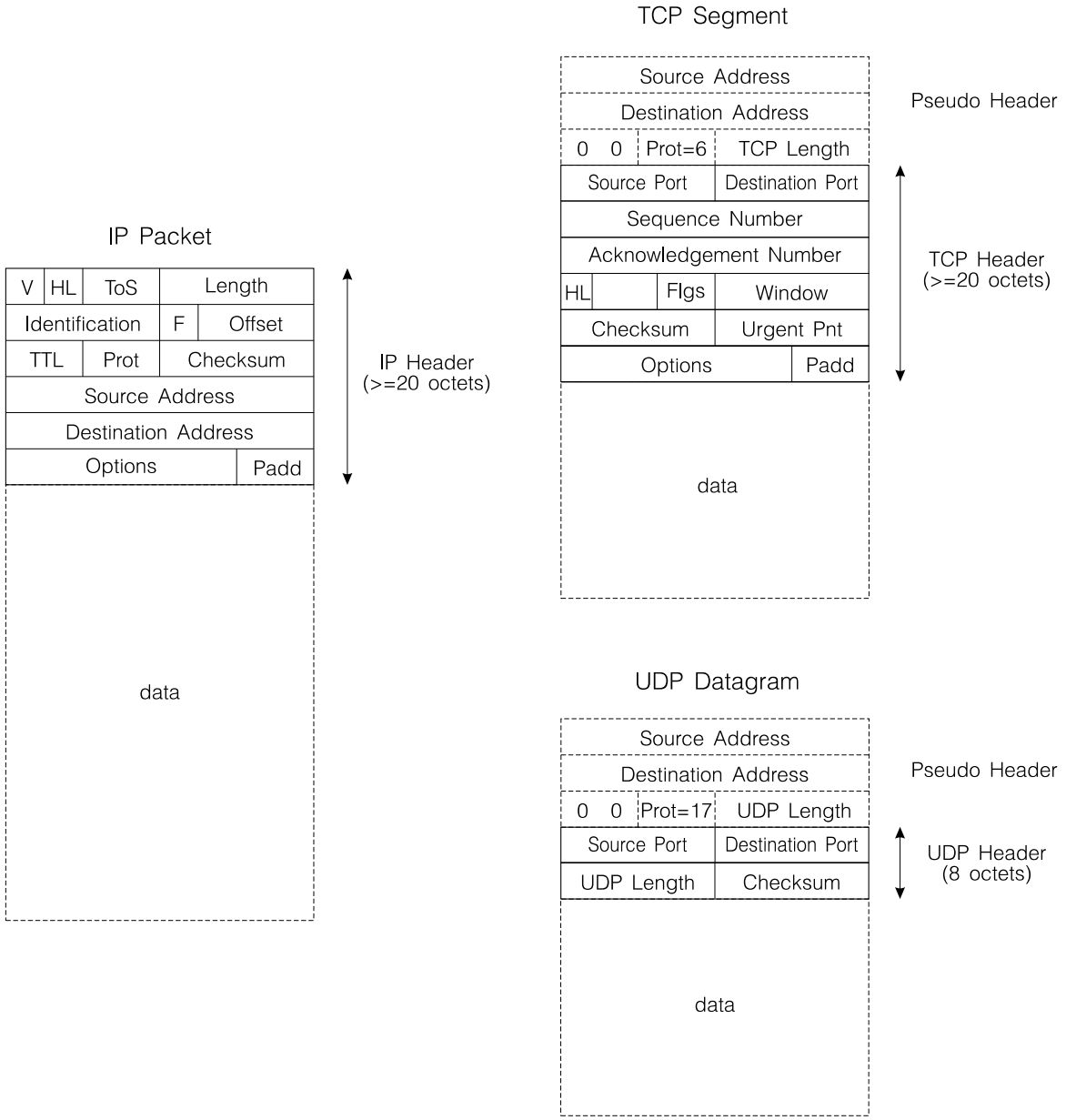
Pole Datastream Type je využíváno k indikaci ukončení práce na virtuálním kanále:

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.

13.2.3 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 zajišťuje 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).



Obr. 13.13: 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. 13.13.

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. 13.13 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.

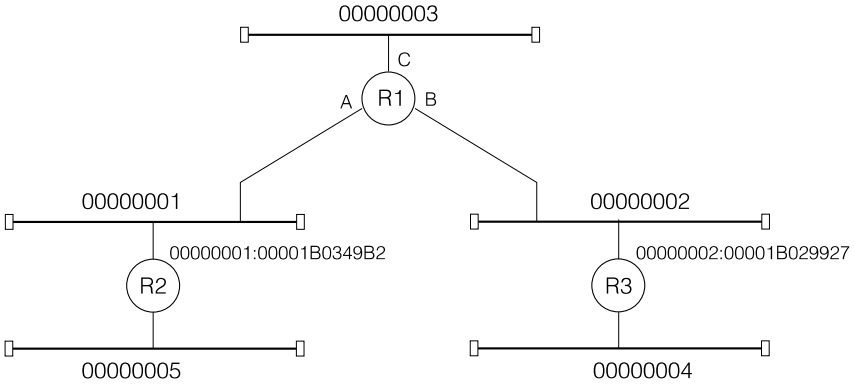
Konečně, hlavička *UDP datagramu* nese pouze čísla portů, délku UDP datagramu a kontrolní součet.

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.

13.3 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. 13.14.



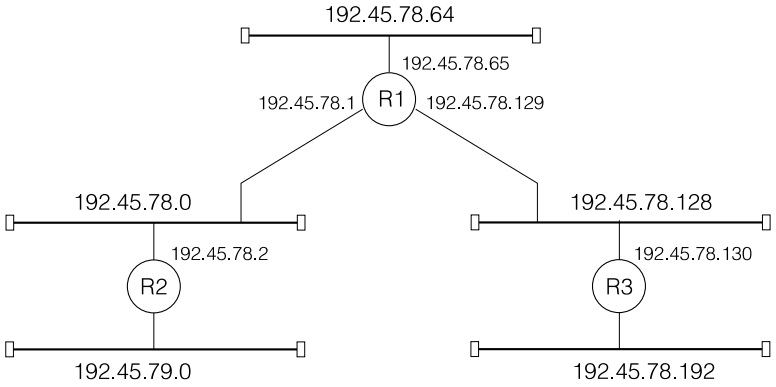
Obr. 13.14: Propojení lokálních sítí směrovači IPX

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. 13.15.

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 algoritmus



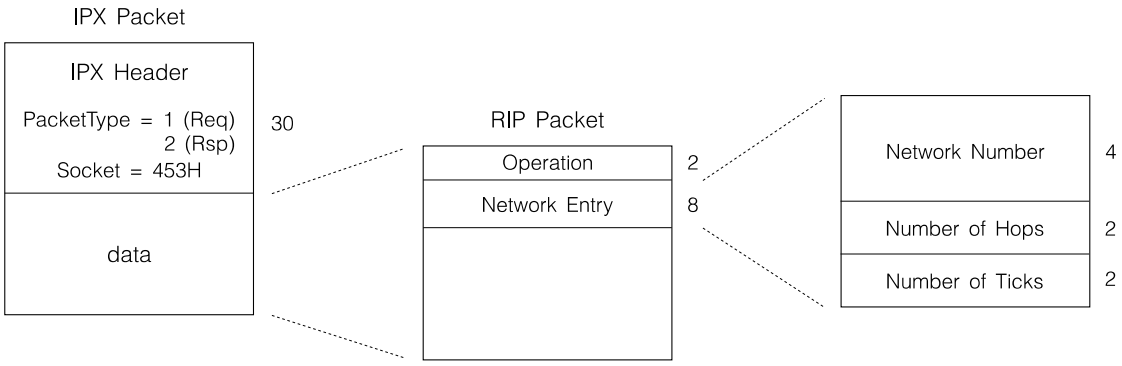
Obr. 13.15: Propojení lokálních sítí směrovači IP

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.

13.3.1 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. 13.16.



Obr. 13.16: 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. 13.17.

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

Obr. 13.17: 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.

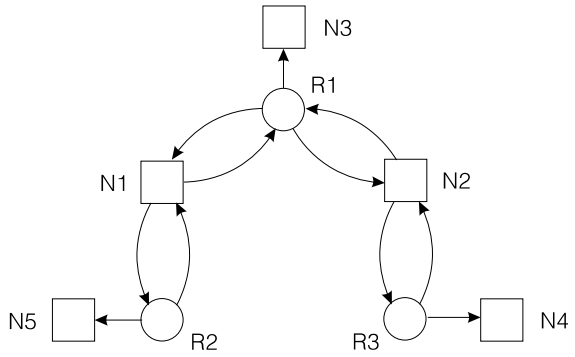
Výpadky rozhraní (nebo připojené sítě) směrovač oznamuje rozesláním RIP paketů s údajem Hops=16 v příslušné položce, tato hodnota má pro algoritmus RIP význam „nekonečna“. Paket RIP s údajem Hops=16 pro všechny připojené sítě směrovač rozesílá při regulárním ukončení své činnosti, výpadek směrovače zjistí 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.

13.3.2 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



Obr. 13.18: Topologická informace pro protokol OSPF

z obr. 13.15 najdeme na obr. 13.18. Aktuální informace o stavu linek je uložena jako ohodnocení orientovaných hran a využívána pro lokální výpočet směrovacích tabulek (příklad směrovací tabulky pro směrovač R1 z obr. 13.15 uvádí obr. 13.19). 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

Obr. 13.19: 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).

14. 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.

14.1 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.

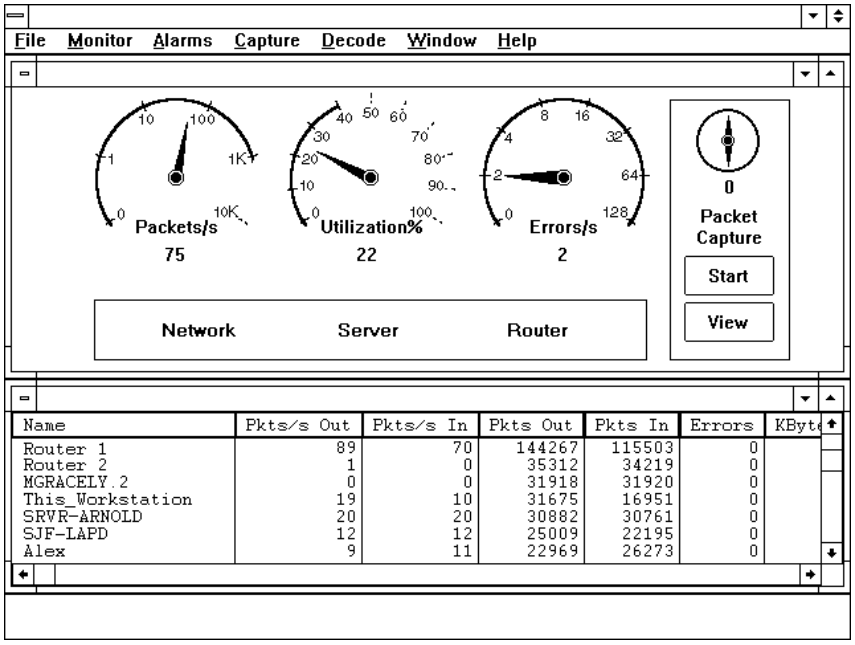
Struktura síťového analyzátoru je velice jednoduchá. Většinou dnes jde o přenosný osobní počítač, vybavený potřebným síťovým rozhraním. Vedle rozhraní pro lokální sítě, které nás v tomto textu zajímají, je obvykle pevně vestavěno sériové rozhraní schopné analyzovat dvoubodové spoje rozsáhlých sítí (patří 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. 14.1).



Obr. 14.1: Obrazovka síťového analyzátoru

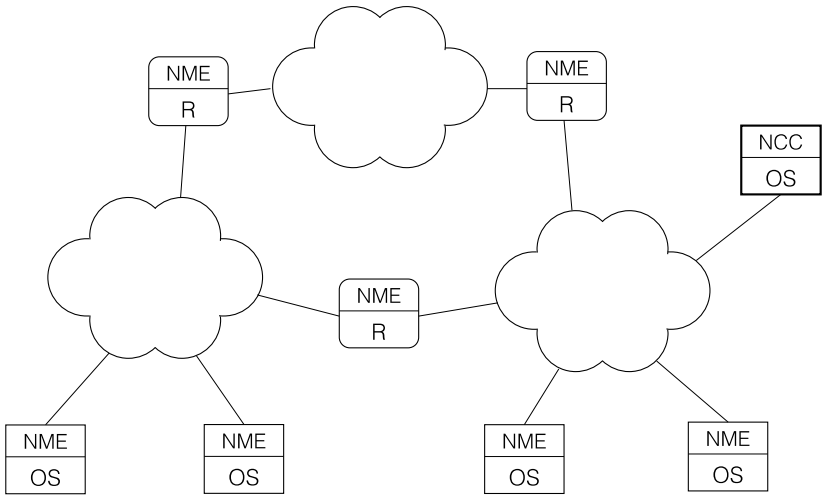
Podmínky, podle kterých vybíráme z toku dat rámce (nebo spíše jejich začátky), jejichž příspěvek k celkovému toku chceme indikovat v reálném čase, a které ukládáme do paměti počítače pro následnou statistiku a/nebo detailní analýzu, zahrnují výběr linkových a síťových protokolů (např. IP, ICMP, ARP pro 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.

14.2 CMIS/CMIP

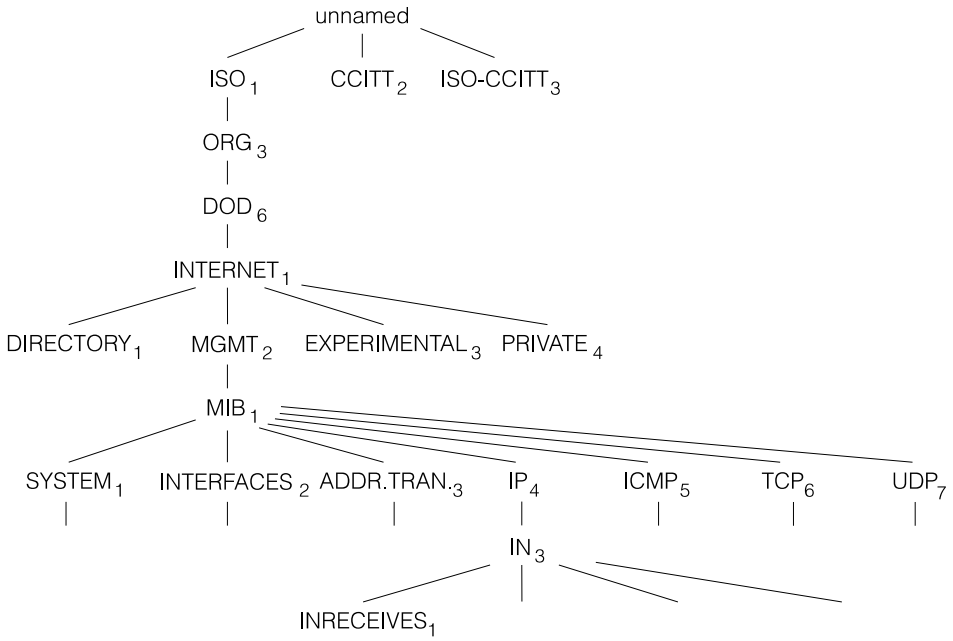
Podívejme se nejprve na obecné principy v kontextu systému správy ISO CMIS/CMIP. Systém správy je tvořen ovládanými prvky a pracovištěm pro správu sítě (obr. 14.2).

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* –



Obr. 14.2: Architektura ISO CMIS/CMIP

Network Management Entity). Tento modul má za úkol sbírat statistické údaje o provozu 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

Obr. 14.3: 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).

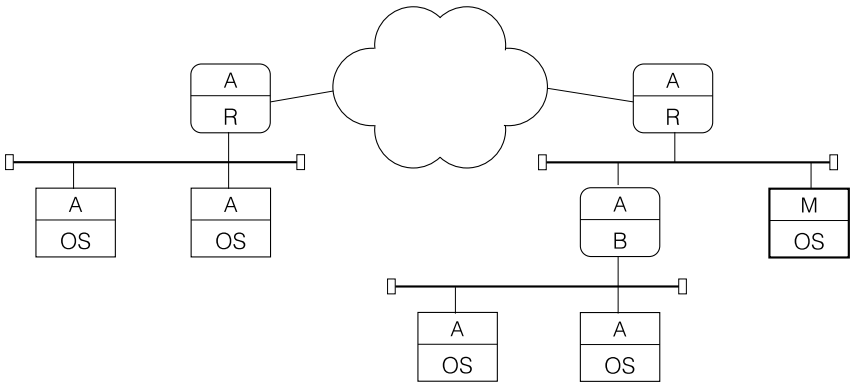
Pracoviště pro správu sítě (*NCC* – Network Control Center) je vybaveno programem, který komunikuje s moduly NME ovládaných prvků, získává od nich stavové a statistické informace, výsledky presentuje správci sítě a příkazy správce (nebo příkazy automaticky generované) modulům MME rozesílá. Kromě této 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.

14.3 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. 14.4).

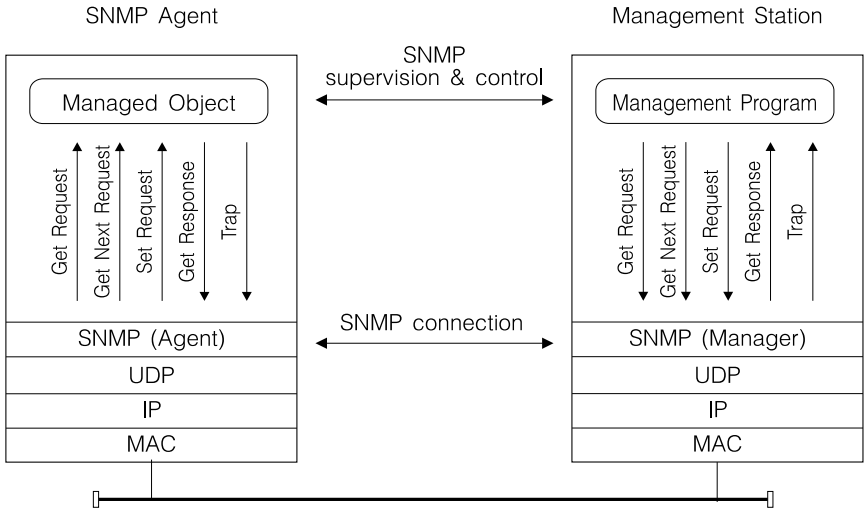


Obr. 14.4: Architektura SNMP

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

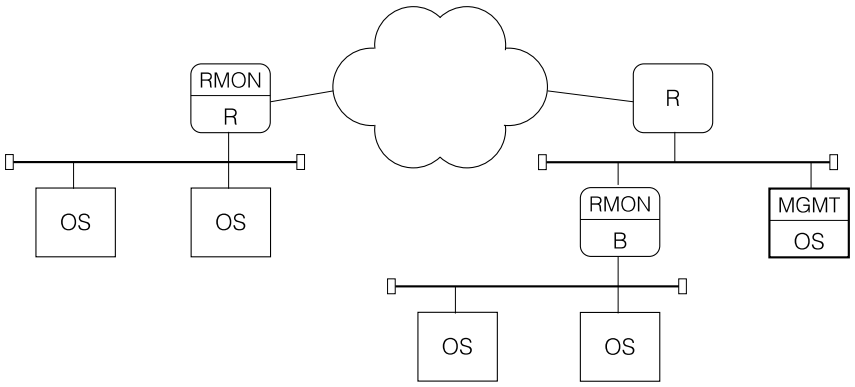


Obr. 14.5: Komunikace SNMP

síťových prvků (např. Synoptics Optivity). Tyto programy dovolují správci získat informaci o okamžitém stavu sítě a upravovat její konfiguraci nebo parametry, a to často ve velice přehledné grafické formě a s možností intuitivního ovládání.

14.4 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.



Obr. 14.6: 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.

15. 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.

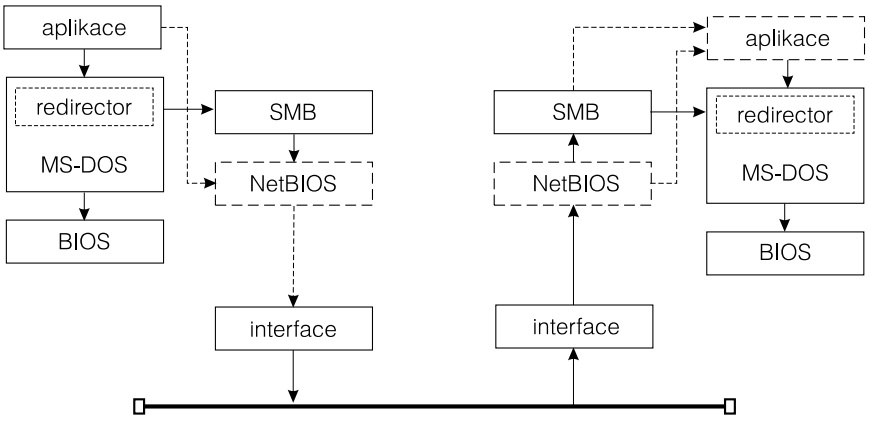
Ponechme stranou historické systémy, z nichž se dnešní síťové systémy vyvinuly, a jejichž cílem bylo poskytnout primitivně vybaveným mikropočítačům podporu jednoduchého řídícího programu se systémem souborů, se standardizovaným ovládáním periférií a primitivním řízením úloh. U takového řídícího programu 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



Obr. 15.1: Struktura síťového rozšíření operačního systému MS-DOS MS-Net

vzdáleném 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.

16. Novell Netware

NetWare je synonymem pro několik pojmů. Jednak jde o specializovaný operační systém, který dovoluje na jednom počítači poskytovat služby souborového serveru, tiskového serveru, může být směrovačem v rozlehlých sítích, případně provozovat další služby. Zároveň tímto pojmem někdy bývají označovány 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 (MS DOS, MS Windows, Windows95, Windows NT, OS/2, Macintosh) sdílet souborové, tiskové i jiné služby poskytované těmito servery. Pomocí dalších produktů firmy Novell lze do sítě integrovat i jiné typy počítačů a uživatelům sítě poskytovat rozšířené služby.

Serverem sítě je nejčastěji počítač typu PC. Na něm běží operační systém NetWare, který je optimalizovaný pro funkci souborového serveru. Podpora serveru specializovaným „operačním systémem“ je sice cestou k jeho maximální efektivitě, podstatně však komplikuje rozšiřování serveru o aplikačně orientované procesy.

Též se lze setkat se serverem NetWare provozovaným jako jedna z úloh systému OS/2, Unix nebo OpenVMS. V takových případech se obvykle jedná o doplňkovou službu, která tyto systémy integruje do lokální sítě.

16.1 Komunikační protokoly v sítích Novell

V novellské síti lze používat všechny běžně používané technologie pro výstavbu lokálních sítí. Obvyklý je Ethernet nebo rychlý Ethernet, Token Ring, FDDI, ATM, na ústupu je Arcnet.

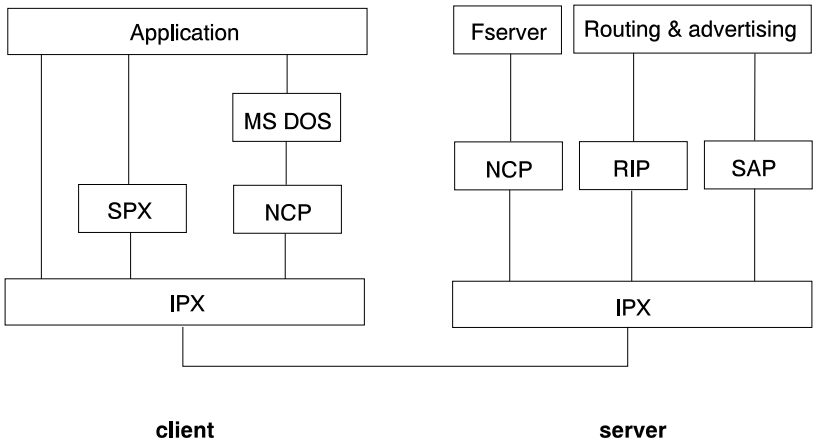
Komunikační podpora Novell Netware se opírá o protokoly IPX/SPX. Protokol IPX (Internetwork Packet Exchange) představuje nespojovanou a nepotvrzovanou komunikaci, tedy klasickou datagramovou službu. Pro identifikaci jednotlivých stanic je použita hierarchická adresa. Ta se skládá z adresy sítě (4 byty) 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.

Protokoly IPX a SPX patří mezi univerzální protokoly. Lze je používat pro vzájenou komunikaci libovolných dvou pracovišť, resp. aplikačních programů.

Pro vlastní komunikaci mezi serverem NetWare a jeho klienty je použit protokol NCP (*NetWare Core Protocol*) implementovaný prostřednictvím IPX. Služby operačního systému klientské stanice se v případě práce s adresáři a soubory uloženými na serveru převádějí na komunikaci protokolem NCP.

Informace o existujících serverech a jimi poskytovaných službách jsou mezi servery šířeny protokolem SAP (*Service Advertising Protocol*). Informace o topologii sítě potřebné pro správné směrování jsou zveřejňovány protokolem RIP (*Routing Information Protocol*). V obou případech jsou tyto informace zveřejňovány pravidelně a šířeny jako broadcast. Jednotliví klienti tyto informace získávají v případě potřeby dotazem od serveru. Tuto protokolovou strukturu ve zjednodušené podobě přibližuje obr. 16.1.

V případě velmi rozsáhlých sítí může docházet k situacím, že broadcasty budou tvořit nezanedbatelný podíl na počtu celkově přenášených zpráv. Navíc mohou být vysílány v těsném sledu za sebou (*broadcast storm*). Proto lze v rozsáhlých sítích pro šíření informací mezi



Obr. 16.1: Struktura protokolů Novell Netware

jednotlivými servery a routery používat protokol NLSP (*NetWare Link Services Protocol*), který je obdobou OSPF, jako náhradu dosavadních protokolů RIP a SAP. Předností NLSP je podstatně nižší počet přenášených zpráv. Zjednodušeně lze říci, že se nepřenášejí informace o celé síti, ale jen změny oproti předchozímu stavu.

Používání protokolu SPX se omezuje především na komunikaci mezi souborovými a tiskovými servery NetWare a také pro vzdálenou administraci serveru (remote console). Další oblastí jeho využití je komunikace databázových klientů se serverem provozovaným jako rozšiřující modul novellského serveru.

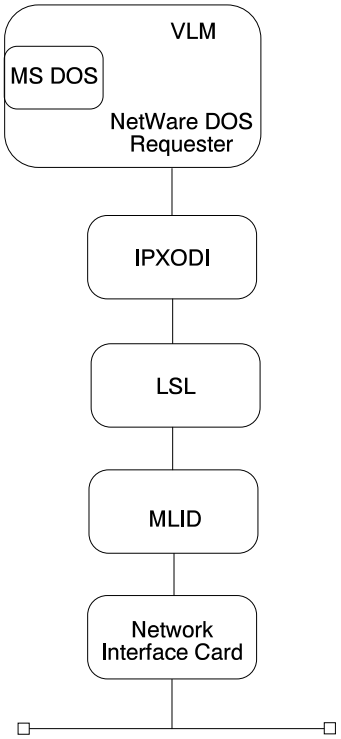
S postupným rozšiřováním Internetu firma Novell začala podporovat i protokoly TCP/IP. Zpočátku servery NetWare dokázaly pracovat jen jako routery pro TCP/IP. Dnes lze protokol IP použít jako rovnocennou náhradu protokolů IPX/SPX. Pro komunikaci mezi klientem a serverem v protokolu NCP již není jako nosný protokol využíván jen protokol IPX, ale lze použít i transportní protokol UDP z rodiny internetovských protokolů.

Server NetWare dnes nabízí i další služby, které byly dříve obvykle poskytovány jen unixovými servery. Patří mezi ně přístup k souborům uloženým na novellském serveru službou ftp a integrace tiskových služeb NetWare a Unixu. Prostřednictvím protokolu NFS pro sdílení souborů lze navzájem propojit souborové systémy NetWare a Unixu (či jiného operačního systému). Obvyklé je i propojení lokální novellské elektronické pošty s poštou Internetu. Na serveru NetWare lze provozovat i informační služby gopher a WWW.

16.2 Klient systému NetWare

Pro ilustraci si uveďme, čím je tvořeno programové vybavení na straně klienta serveru Netware. Budeme uvažovat počítač vybavený klasickým operačním systémem MS DOS. Zde jsou jednotlivé programové vrstvy dostatečně zřetelně odděleny. Struktura programového vybavení je zachycena na obr. 16.2.

Název programu `LSL` je zkratkou z *Link Support Layer*. Jeho úkolem je vytvořit jednotné programové prostředí, na které je pak navázán ovladač konkrétního komunikačního adaptéru. V této souvislosti je komunikační ovladač označován jako MLID (*Multiple Link Interface Driver*). Konkrétní ovladače pak mají názvy odvozeny od komunikačních adaptérů, například `NE2000`. Program `LSL` směrem vzhůru poskytuje rozhraní ODI (*Open Data-Link Interface*). Toto rozhraní se snaží být do značné míry univerzálním, takže nad ním pracují jak vyšší vrstvy klienta NetWare, tak i klienti pro TCP/IP nebo NetBEUI. Program IPXODI poskytuje



Obr. 16.2: MS DOSový klient serveru NetWare

komunikační rozhraní pro protokol IPX. Může být využíváno jak *redirektorem* souborových operací VLM, tak současně i jinými aplikačními programy. Redirektor VLM je navázán na interní programové rozhraní sytému MS DOS. Přebírá od něj požadavky na práci se síťovými diskovými jednotkami a transformuje je na komunikaci se serverem v protokolu NCP/IPX. Všechny uvedené programy používají společný konfigurační soubor `net.cfg`.

16.3 Novell Directory Services

Ve starších verzích NetWare řady 3.x má každý server svůj vlastní katalog oprávněných uživatelů serveru. Tento katalog je označován termínem *bindery*. Jsou v něm i údaje o existujících skupinách uživatelů, tiskových frontách a dalších objektech. Pokud je v síti více serverů a uživatel potřebuje přistupovat k datům uložených na několika serverech, musí být zaregistrován na těchto serverech a musí mu na nich být poskytnuta přístupová práva.

Při zahájení práce v síti se uživatel nejprve přihlásí ke svému hlavnímu, domácímu serveru. Poté se musí ještě přihlásit na všechny další servery, ke kterým bude chtít přistupovat. K tomu používá uživatelská jména a hesla registrovaná v katalogu ostatních serverů. To poněkud komplikuje správu i používání rozsáhlejší sítě.

Proto byla v NetWare verze 4.x zavedena společná databáze objektů NDS (*Novell Directory Services*). Soustřeďuje informace o jednotlivých objektech sítě — uživatelích, serverech apod. Díky této databázi se celá síť s případným větším počtem serverů jeví jako jeden homogenní celek.

Novell Directory Services jsou distribuovanou databází, ve které jsou uloženy informace o všech možných objektech sítě. Tato databáze 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

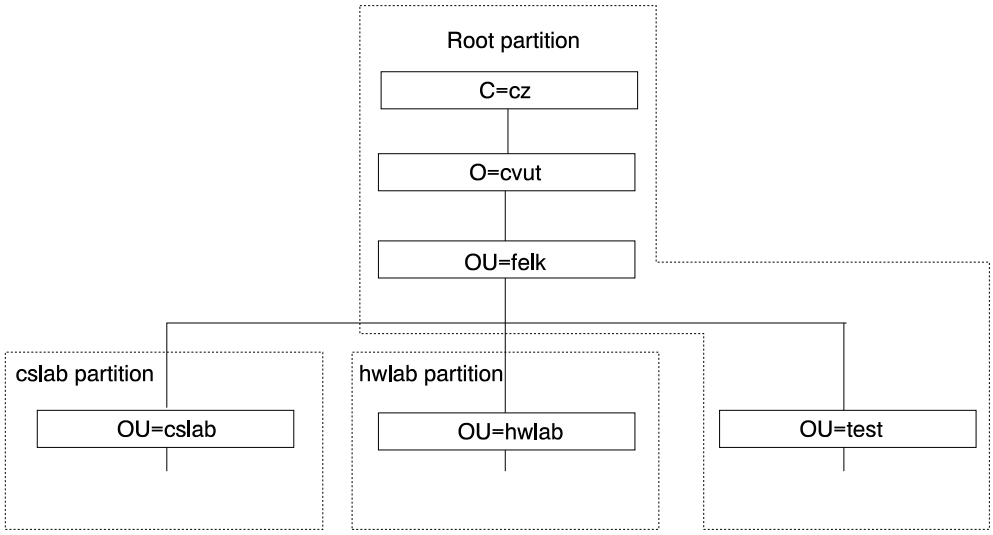
může odpovídat organizačnímu uspořádání podniku. V případě velkých firem lze zohlednit i geografická hlediska.

Existence databáze, na kterou můžeme zjednodušeně pohlížet jako na společný centrální katalog uživatelů (a dalších objektů), zjednodušuje správu rozlehlých sítí s více servery. Tuto výhodu dokládá například postup při zřizování uživatelského účtu. Administrátor sítě NetWare 4.x nejprve vytvoří v databázi NDS 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 NDS 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 NDS 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 obsažené v objektech NDS se poměrně často mění. Ke změně dochází např. i při každém přihlášení a odhlášení uživatele ze sítě, které v NDS objektu typu uživatel vede ke změně aktuální síťové adresy. Vždy po vytvoření nového objektu, zrušení nebo změně některého z objektů NDS 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 NDS stromu s více kontejnerovými objekty lze informace NDS 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. 16.3. Z pohledu správy jednotlivých objektů NDS je rozdělení databáze na několik částí zcela transparentní.



Obr. 16.3: Rozdělení NDS stromu na oblasti

Správnou volbou struktury NDS stromu, jeho částí a replik spolu s jejich uložením na vhodné servery lze jak minimalizovat objem dat přenášených při synchronizaci replik po

pomalejších komunikačních linkách, tak i zvýšit odolnost a dostupnost NDS i při výpadcích serverů a komunikačních kanálů.

16.3.1 Objekty NDS

Mezi kontejnerové objekty NDS patří samotný kořen stromu [Root], dále objekty Country, Locality, Organization a Organizational Unit. V užším slova smyslu, a s ohledem na předchozí text, mezi kontejnerové objekty řadíme jen [Root], objekty Organization a Organizational Unit.

[Root]. Kořen stromu [Root] vzniká při instalaci prvého serveru a vytváření databáze NDS.

Country. Objekt Country (zkratka C) je nepovinným objektem vytvářeným bezprostředně pod objektem [Root].

Locality. I objekt Locality (L) je nepovinný. Spolu s Country pomáhá v databázi držet obraz geografické podoby rozlehlé sítě. Objekt typu Locality může být vytvořen o jednu úroveň níže pod objekty Country, Organization nebo Organizational Unit.

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 mohou být objekty Country a Locality.

Organizational Unit. Nepovinné objekty Organization Unit (OU) se vytvářejí pod úrovní Organization. Tyto kontejnerové objekty jako jediné v sobě mohou obsahovat další objekty typu OU. Počet takto vytvořených úrovní není omezen.

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:

AFP Server. Objekt typu Apple Talk Filling Protocol Server představuje uzel sítě NetWare. Jde o router připojující do novellské sítě počítače Apple Macintosh soustředěné v síti AppleTalk.

Alias. Alias lze používat jako odkaz na jiný objekt. Použitím alias objektu lze uživatelům sítě usnadnit práci s objekty v jiné části NDS 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 i 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 NDS. Nezaměňovat s objektem Group, se kterým lze spojit přístupová práva k souborům a adresářům.

Print Server. Tiskový server sítě. Může být provozován na stejném počítači jako souborový server nebo na samostatném počítači.

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.

16.3.2 Přístupová práva k objektům NDS

Každý objekt obsahuje několik různých informací, které jsou v terminologii NDS označovány jako *properties* (vlastnosti objektu). 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 vlastnostmi (*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 NDS jsou shrnuta v tabulkách 16.1 a 16.2.

Název	Význam
Supervisor	Všechna práva k objektu i ke všem jeho vlastnostem
Browse	Právo číst (vidět) názvy objektu a vyhledávat jej v NDS
Create	Možnost vytvořit nový objekt uvnitř kontejnerového objektu
Delete	Právo objekt zrušit
Rename	Právo změnit název objektu

Tab. 16.1: Přístupová práva k objektům NDS

Název	Význam
Add or Delete Itself	Možnost přidat nebo vyřadit sám sebe z vlastnosti objektu typu seznam; nejčastěji jako právo začlenit se sám do určité skupiny uživatelů (objekt typu group)
Compare	Právo testovat hodnotu nějaké vlastnosti objektu bez oprávnění ji přímo přečíst; výsledkem porovnání je ano/ne
Read	Možnost zjistit hodnotu dotyčné vlastnosti objektu
Write	Právo zapsat, změnit hodnotu; zahrnuje v sobě i právo Add or Delete Itself
Supervisor	Všechna práva k dotyčné vlastnosti objektu

Tab. 16.2: Přístupová práva k vlastnostem objektů NDS

16.3.3 Identifikace objektů NDS

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 NDS stromu. Při práci s objekty uloženými v dotyčném kontejneru totožném s nastaveným kontextem stačí totiž uvádět jen vlastní jména objektů (Common Names, CN). Kontext lze v případě potřeby změnit programem `CX`.

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 zkrácený 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 zkráceným zápisem identifikace objektu, platí jednoduché pravidlo. Zápis začínající tečkou je považován za zkrácený 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`.

16.4 Synchronizace času

Operace s objekty NDS by měly být prováděny v tom pořadí, v jakém byly vznášeny požadavky na jejich provedení. Každá žádost o práci s objekty NDS 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 NDS.

Po zahájení činnosti si tedy server musí zasynchronizovat svůj lokální čas se síťovým. K tomu nesmí dojít skokovou změnou, nýbrž dočasným zrychlením nebo zpomalením lokálních hodin. Pokud je dotyčný server naopak zdrojem přesnějších časových údajů, pak se mu ostatní servery postupně přizpůsobí.

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, například radiovým přijímačem časového signálu z vysílače DCF.

Secondary. Sekundární servery přebírají přesný čas z výše uvedených serverů a navzájem jej synchronizují s ostatními Secondary servery.

16.5 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 jednotlivých procesů a threadů, poskytuje semafory a signály pro synchronizaci procesů.

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).

Po spuštění serveru se začnou provádět příkazy ze souboru `startup.ncf`. Především je zde předepsáno zavedení diskových ovladačů. Po jejich začlenění do operačního systému lze začít pracovat se souborovým systémem NetWare. Od této chvíle již není nutné přistupovat k souborovému systému MS DOSu. Server si vyhledá systémový svazek `SYS:`, připojí si jej (přimontuje) a z jeho adresáře `SYSTEM` začne provádět příkazy uložené v souboru `AUTOEXEC.NCF`. Mezi obvyklé příkazy patří nastavení jména serveru a jeho dalších vlastností, zavedení komunikačních ovladačů, připojení zbývajících diskových svazků a zavedení dalších potřebných modulů NLM.

Případná změna konfigurace serveru a sledování jeho chodu se provádí prostřednictvím příkazů operačního systému nebo pomocí integrovaných modulů (utilit) pro administraci serveru.

16.6 Souborový systém

Server pracuje se svým vlastním souborovým systémem. Při inicializaci disku se vyhradí malá oblast (partition) pro MS DOS potřebná jen pro počáteční fázi spuštění serveru. Na zbytku disku se vytvoří novellská oblast. Na případných dalších discích se vytváří jen novellská oblast. 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.

Server si při běhu v operační paměti udržuje též tabulku FAT s informacemi o fyzickém umístění souborů na svazku. Zbývající volnou operační paměť používá jako vyrovnávací paměť pro diskové operace. Z toho plyne, že nároky na kapacitu operační paměti jsou úměrné instalované diskové kapacitě. Při inicializaci svazku lze definovat větší alokační bloky a tím zmenšit velikost FAT tabulky. S růstem velikosti alokačního bloku se ale zvětšuje i disková kapacita ztracená v neúplně využitých posledních alokačních blocích souborů.

Protože alokační blok může mít velikost až 64 kB, ztráta diskové kapacity 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.

V případech, kdy je třeba mít k dispozici řádově desítky a více GB dat v souborech, s nimiž se nepříliš často pracuje, lze zavést sekundární paměťový systém. Tato velkokapacitní paměťová zařízení se označují zkratkou HCSC (*High Capacity Storage System*). Jde obvykle o knihovnu optických disků, které jsou v případě potřeby vybírány a automaticky vkládány do pracovní jednotky *jukebox*. Vlastní disky serveru pak slouží jako cache paměť pro přístup k souborům na sekundárním paměťovém zařízení. Pro přesuny souborů se používá termín migrace.

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 Windows95 či OS/2, 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.

16.6.1 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 shrnuty v tabulkách 16.3 a 16.4.

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	soubor je sdílitelný více uživateli
System	Sy	význam totožný s MS DOSem
Transactional	T	transakční operace jsou podporovány systémem pro sledování transakcí (TTS)

Tab. 16.3: 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

Tab. 16.4: Atributy adresářů

Kromě atributů lze u spustitelných souborů nastavovat způsob vyhledávání datových souborů (*search modes*). Jde o určitou obdobu příkazu `append` z MS DOSu. V závislosti na nastaveném modu se mění chování systému v okamžiku, kdy se program snaží otevřít neexistující soubor. V takovém případě může být soubor hledán také v aktuálním adresáři nebo v adresářích, kde server vyhledává spustitelné programy a dávky.

Pro jednotlivé adresáře nebo celé svazky lze stanovit limity (kvóty) na čerpání diskové kapacity jednotlivými uživateli.

16.6.2 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 16.5.

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

Tab. 16.5: Přístupová práva k adresářům a souborům

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 (Inherited Rights Filter).

16.6.3 Ochrana před selháním diskového systému

Nestačí jen nabízet systém propracovaných přístupových práv. Je nutné nabídnout i prostředky ochrany před ztrátou dat v případě poruchy diskového subsystému (porucha disku nebo jeho řadiče). V NetWare je tato prevence soustředěna do několik oblastí a její jednotlivé prvky jsou označovány jako stupně SFT (*System Fault Tolerant*):

- Po zápisu dat na disk server provede jejich kontrolní čtení. Při neshodě zapisovaných a čtených dat je diskový blok prohlášen za vadný a místo něj se začne používat náhradní blok z předem rezervované oblasti náhradních bloků (*Hot Fix Redirection Area*). V případě inteligentních diskových řadičů může zpětné čtení provádět samotný řadič, čímž klesne počet vstupně-výstupních operací prováděných operačním systémem. Tato nejnižší úroveň zabezpečení je označována jako SFT 1.
- Kritické části diskového svazku (adresář, tabulka FAT) jsou na disku uloženy ve dvou kopiích.
- Zvýšenou ochranu představuje zdvojení disků. Mohou být připojeny ke společnému diskovému řadiči (*mirroring*) nebo pro případ poruchy řadiče mohou být připojeny ke druhému řadiči (*duplexing*). Veškeré informace jsou uloženy ve dvou nezávislých kopiích. V případě poruchy kteréhokoliv z disků je k dispozici disk druhý s aktuální kopií dat. Tento stupeň zabezpečení je označován jako SFT 2.
- Stupeň zabezpečení SFT 3 se používá pro obzvláště kritické aplikace. Jde o dva zcela identické servery navzájem propojené rychlým komunikačním spojem. Navenek vůči celé síti tato dvojice vystupuje jako jediný server. Diskové operace se provádějí paralelně na obou serverech. Při výpadku některého ze serverů na sebe obsluhu sítě samočinně přebere zbývající server.

16.7 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 NDS. V tom je auditor zcela nezávislý na administrátorovi sítě a v konečném důsledku tak kontroluje i jeho činnost.

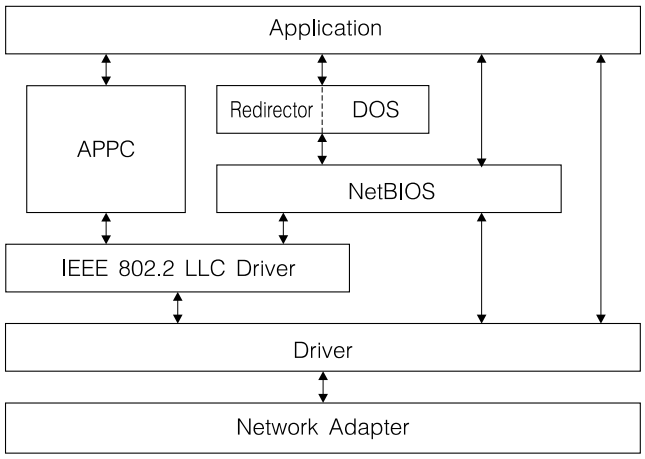
Auditor stanoví, jaké typy operací budou sledovány a zaznamenávány. Lze sledovat prakticky všechny typy operací s objekty NDS, tedy jejich vytváření, rušení, změny objektů a přístupových práv k nim. V souborovém systému lze sledovat změny určitých souborů a jejich původce, nebo naopak lze zaznamenávat souborové aktivity konkrétního uživatele sítě. Záznamy lze následně vyhodnocovat podle různých kritérií, jakými jsou čas, typ události nebo její původce.

17. IBM: PC-LAN, LAN Server a Warp Connect

V této části si shrneme řešení vyvinutá v průběhu let pro podporu lokálních sítí firmou IBM, od historické PC-LAN k současnému OS/2 Warp Serveru a systému AIX.

PC-LAN

PC-LAN byla jedním z prvních programových produktů pro lokální sítě. Síť PC LAN se opírala o přenos v přeloženém pásmu po koaxiálním kabelu, později byla používána na technologii Token Ring. Dovolovala sdílení prostředků stanic metodou Peer-to-Peer. Síť PC-LAN podporovala klasické přesměrování I/O požadavků, které převedla na *SMB bloky* a ty předávala protokolem *NetBIOS*. Kromě toho zajišťovala předávání dat mezi programy komunikujícími firemním rozhraním *APPC* (Application Program-to-Program Communication). Doplňkem sítě byl i jednoduchý program pro elektronickou poštu. Komunikační architekturu sítě PC-LAN ilustruje obr. 17.1.

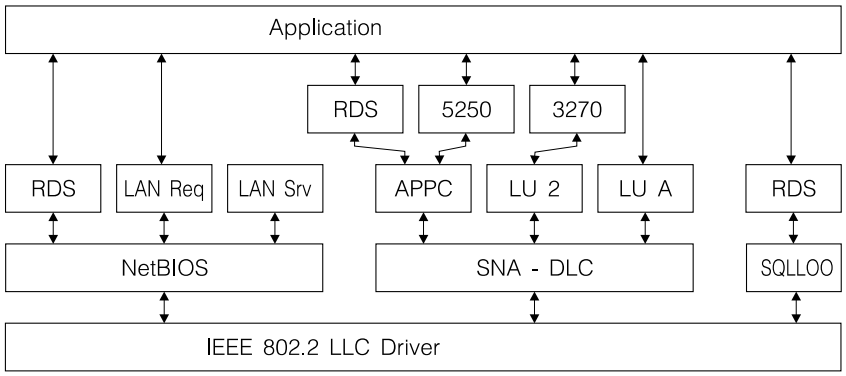


Obr. 17.1: Architektura protokolů sítě PC-LAN

OS/2 LAN Server (2.0, 3.0 a 4.0)

Výkonný server lokální sítě systém OS/2 LAN Server vychází ze struktury LAN Manageru a je vystavěn nad operačním systémem OS/2. Je plně kompatibilní s prostředky starší sítě PC-LAN, servery vybavené systémem OS/2 LAN Server tedy mohly podporovat stanice sítě PC-LAN. Souborový server OS/2 LAN Server je (podobně jako LAN Manager) vystavěn nad univerzálním operačním systémem OS/2 nebo OS/2 Warp. Oba tyto systémy mají plnohodnotný multitasking s podporou vláken výpočtu; ten dovoluje využít výkon i více procesorů nad společnou pamětí (*SMP – Symmetric MultiProcessing*). Opírají se o výkonný systém souborů *HPFS* (High Performance File System) s efektivně implementovanou strukturou alokačních bloků a využívající technologii vyrovnávacích pamětí cache. Díky vlastnostem operačního systému bývá souborový server často kombinován s podporou aplikací. Těmi bývají databázový SQL Server, elektronická pošta nebo podpora pracovních skupin Lotus Notes.

Komunikační architekturu systému OS/2 LAN Server ilustruje obr. 17.2. Protokol *NetBIOS* podporuje vzdálený přístup k souborům a zařízením vyžádaný moduly *RDS* (Remote Data Services), *OS/2 LAN Requester* (redirector pro DOS nebo OS/2) a *OS/2 LAN Server*. Vedle něj jsou implementovány protokoly APPC, LU A a LU 2 nad modulem *SNA LAN DLC* (Data Link Control), ten převádí linkovou komunikaci emulovaných terminálů 3270 a 5250 na rámce lokální



Obr. 17.2: Komunikační architektura sítě OS/2 LAN Server

sítě. Konečně, poslední sada protokolů podporuje komunikaci v jazyce SQL s databázovým systémem *OS/2 Database Manager*.

Systém OS/2 LAN Server byl vytvořen pro prostředí operačního systému OS/2 na počítačích s procesory Intel, k dispozici jsou však i varianty LAN Serveru pro operační systémy AIX, AS/400, MVS a VM. Klientská pracoviště tak získávají přístup k systémům souborů a zařízením výkonných počítačů.

OS/2 Warp Server

Operační systém OS/2 prodělal poměrně dlouhý vývoj, jeho poslední verze jsou označovány jako OS/2 3.0 Warp a OS/2 4.0 Merlin. Pro operační systém OS/2 Warp byl upraven i systém OS/2 LAN Server dodávaný v sestavě s podporou TCP/IP a vzdálených pracovišť a s vylepšenou správou, tiskovými službami a zálohováním jako *OS/2 Warp Server*. Moderním rysem systému OS/2 Warp Server je *podpora mobilních počítačů* – specificky synchronizace replikovaných souborů (automatická úprava replik po připojení klientského pracoviště) a podpůrný systém AskPSP.

OS/2 LAN Requester

Ke každému ze síťových serverů je běžně dodávána podpora klientských pracovišť: v případě serveru OS/2 LAN Server je jím OS/2 LAN Requester, který dovoluje klientskému pracovišti přístup k prostředkům výkonných serverů a k prostředkům zpřístupněným jinými klientskými pracovišti v režimu Peer-to-Peer (např. modulem Peer for OS/2 souboru OS/2 Warp Connect). Kromě modulu OS/2 LAN Requester Peer for OS/2 lze služeb serverů OS/2 LAN Server a OS/2 Warp Server využívat z klientských pracovišť opírajících se o protokoly SMB a NetBIOS, jako jsou klienti DOS, Windows, Windows for Workgroups, Windows 95 a Windows NT Workstation.

OS/2 Warp Connect

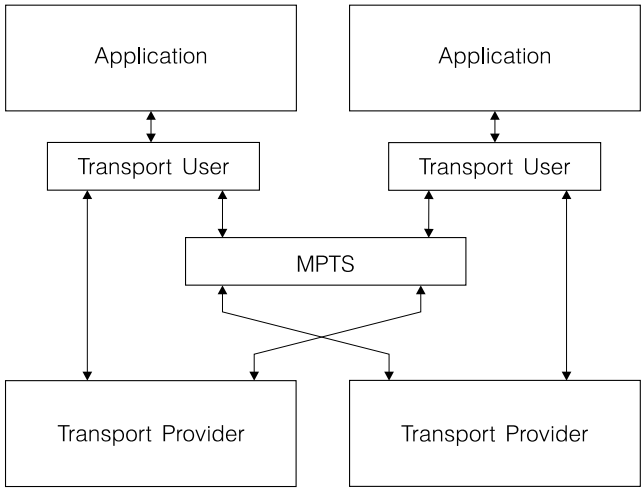
Moderní podporou klientských pracovišť je soubor programů OS/2 Warp Connect, vystavěný nad operačním systémem OS/2 Warp. Je stavěn modulárně, konfiguraci klientského pracoviště lze přizpůsobit konkrétním požadavkům.

Modul *Peer for OS/2* systému OS/2 Warp Connect dovoluje zpřístupnit prostředky jiných pracovišť (vybavených moduly Peer for OS/2) a výkonných serverů OS/2 LAN Server a OS/2 Warp Server a současně dovoluje přístup k vlastním adresářům, souborům a zařízením jiným klientům. Lze tak vybudovat jednoduchou síť typu Peer-to-Peer.

Modul *OS/2 LAN Requester* dovoluje zpřístupnit prostředky jiných pracovišť (vybavených moduly Peer for OS/2) a výkonné servery OS/2 LAN Server a OS/2 Warp Server. Kromě toho lze OS/2 LAN Requester použít pro administraci sítě.

Doplnění modulu *Novell Netware Client* dovolí zpřístupnit služby serverů Novell Netware. Podobně modul *Internet Access* (TCP/IP) dovoluje přístup k serverům UNIX (podporovány jsou standardní protokoly – Telnet, FTP, SMTP, lpr a rexec, doplnit lze podporu služeb NFS, X Windows, MOTIF, News, Gopher a WWW). Konečně s využitím modulu *LAN Distance Remote* lze připojit pracoviště k lokální síti telefonní linkou s modemem.

Z pohledu správy (a přístupnosti) lze rozsáhlé sítě se servery IBM rozdělit na *samostatně spravované domény*, každá doména může obsahovat více výkonných serverů OS/2 LAN Server a OS/2 Warp Server. Současně s prostředky těchto serverů jsou spravovány i prostředky pracovišť zpřístupněné moduly Peer for OS/2.



Obr. 17.3: Architektura MPTS

Zajímavým rysem OS/2 Warp Server a OS/2 Warp Connect je jejich vybavení univerzálním transportním rozhraním *MPTS* (Multi-Protocol Transport Service/AnyNet). To zpřístupňuje protokoly NetBIOS, TCP/IP, emulátor NetBIOSu nad TCP/IP a emulátor NetBIOSu nad IPX. Vedle standardních protokolových sad může MPTS využívat rozhraní IrDA (str. 103) a běžné paralelní rozhraní. Služby serveru OS/2 Warp Server, přístup k prostřeedkům OS/2 Warp Connect a síťové aplikace opírající se o rozhraní MPTS jsou tak nezávislé na konkrétně použité protokolové sadě.

AIX

Mezi servery, poskytující služby klientským pracovištím, si můžeme na závěr uvést systém AIX 4.2. V tomto případě jde o stabilní systém UNIX, s plně preemptivním jádrem respektujícím standard POSIX a s podporou multiprocesorů včetně systémů System/6000 SP. Systém je modulární, typické konfigurace jsou označované jako AIX Client, AIX Workgroup a AIX Server.

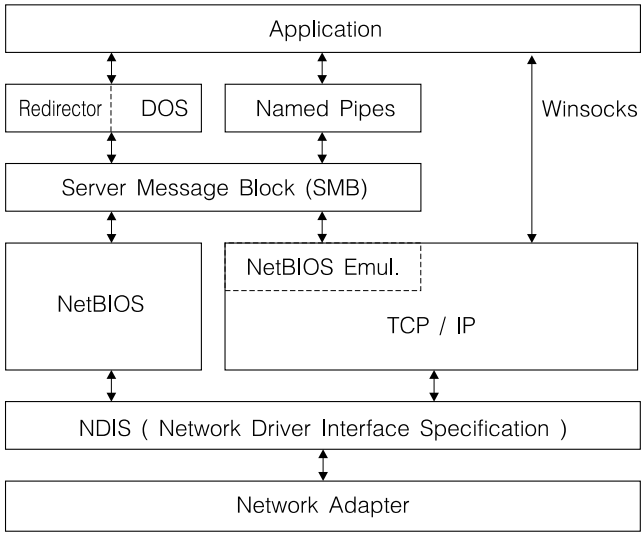
Servery AIX podporují komunikaci pod TCP/IP, po doplnění o modul AIX Connections k nim lze připojit klientská pracoviště a servery Netware (protokoly IPX/SPX a NCP), LAN Manager, OS/2, DOS, Windows a Windows NT (protokoly NetBIOS a SMB) a klientská pracoviště Apple Macintosh. Při spolupráci se servery jiných architektur jsou podporovány adresářové služby DCE Cell Directory Services, NT Trusted Domains, Novell Netware Directory Services.

18. Microsoft: LAN Manager, Windows (NT)

Historie programového vybavení pro lokální sítě firmy Microsoft je spojena se síťovými operačními systémy MS Net, LAN Manager, Windows 3.1, Windows for Workgroups, Windows 95 a Windows NT. Vnitřní strukturu sítě MS Net jsme si již uvedli na str. 124, zde si stručně uvedeme některé základní rysy řešení použitých v síťových funkcích systémů LAN Manager a Windows (v historickém pořadí), podrobnosti jistě zájemce najde v množství dostupné firemní literatury.

LAN Manager

LAN Manager byl vyvinut firmou 3Com na základech definovaných sítěmi PC LAN a MS Net. Jeho nosičem se stal tehdy perspektivní operační systém OS/2, jeho paralelismus dává LAN Manageru žádoucí pružnost a rozšiřitelnost. Technologii LAN Manager firma Microsoft odkoupila a po řadu let rozvíjela, LAN Manager se stal i základem pro současný Windows NT Server pod operačním systémem Windows NT.



Obr. 18.1: Struktura protokolů LAN Manageru

Protokoly, o které se opírá síť LAN Manager, uvádí obr. 18.1 Základem je implementace protokolu NetBIOS, později rozšířená a označovaná jako *NetBEUI* (NetBIOS Extended User Interface), postavená přímo nad ovladač komunikační karty *NDIS* (Network Driver Interface Standard). NetBIOS poskytuje rozhraní redirectoru, který se opírá o soubor funkcí SMB pro přístup aplikace ke vzdálenému serveru. Pro rychlejší komunikaci mohou aplikace využít i programátorsky přívětivější datagramy a kanály NetBEUI (Mail Slots, Named Pipes).

Vedle protokolu NetBIOS LAN Manager implementuje i protokoly TCP/IP, které podporují aplikace pod Windows (rozhraní WinSock), a protokoly ISO. Nad protokoly TCP/IP a ISO je k dispozici emulátor rozhraní NetBIOS.

Windows 3.1

Operační systém Windows 3.1 je použitelný pouze pro klientská pracoviště lokálních sítí a je vybaven podporou pro sítě Windows NT, LAN Mananager a Netware. Výhodnější však často bývá podpora dodávaná s těmito, ale i dalšími, servery (např. LAN WorkPlace pro

Netware). Pro přístup k serverům v lokální síti se využívá protokol NetBIOS, pro přístup ke vzdáleným službám může být systém Windows 3.1 vybaven protokolovou sadou TCP/IP (rozhraní WinSocks) a emulátorem NetBIOSu.

Windows for Workgroups 3.11

Windows for Workgroups 3.11 dovoluje oproti Windows 3.1 zpřístupnit lokální adresáře a zařízení pro práci v režimu Peer-to-Peer. Navíc je doplněný o elektronickou poštu mezi pracovišti a o sdílený časový rozvrh. Lze s ním vybudovat jednoduchou lokální síť s několika pracovišti bez vyhrazeného serveru. Klientská pracoviště přitom současně zajišťují přístup k serverům Windows NT Server a LAN Manager protokolem NetBIOS, k serverům Netware protokoly IPX/SPX a přístup ke vzdáleným systémům protokoly TCP/IP.

Windows 95

Podpora komunikace v lokální síti byly zahrnuta i do dalšího operačního systému Windows 95, a to jak pro servery Windows NT Server, ale i pro LAN Manager a Netware. Windows 95 dovoluje podobně jako Windows 3.1 nebo Windows for Workgroups 3.11 zpřístupnění vlastních adresářů a zařízení jiným klientům a lze s ním vybudovat jednoduchou síť typu Peer-to-Peer.

Windows NT Workstation

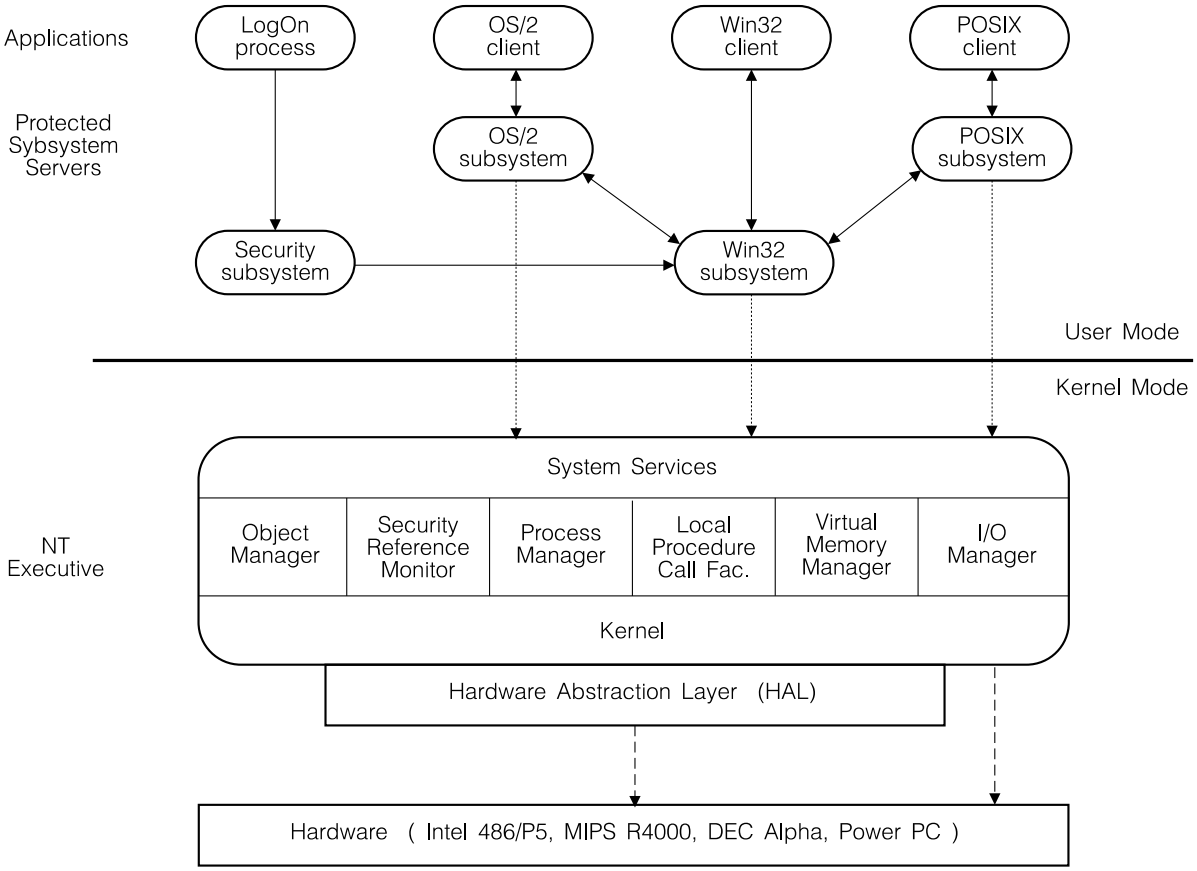
Windows NT Workstation pro operační systém Windows NT je přizpůsoben spolupráci se servery Windows NT Server. Podobně jako u jiných pracovišť s operačním systémem této řady (Windows for Workgroups 3.11, Windows 95), lze i u Windows NT Workstation zpřístupnit lokální adresáře a zařízení pod libovolně volenými jmény (*alias*). Samozřejmostí je vestavěná podpora TCP/IP.

Windows NT Server

Windows NT Server je programové vybavení pro souborové servery, podporuje klientská pracoviště LAN Manageru (pro DOS a OS/2), Windows 3.1, Windows for Workgroups, Windows 95 a Windows NT Workstation.

Windows NT Server se opírá o operační systém Windows NT. Vnitřní struktura systému Windows NT je založena na technologii mikrojádra (obr. 18.2) a poskytuje rozhraní pro různé formy programů pro osobní počítače PC (Win16, Win32, OS/2), ale také pro programy využívající služeb POSIXu. Implementaci systému pro různé procesory (v současnosti procesory Intel 486/P5, MIPS R4000, DEC Alpha a Power PC) usnadňuje definice rozhraní *HAL* (Hardware Abstraction Layer). Mikrojádro usnadňuje podporu i víceprocesorových systémů, verze souborového serveru využívající až 32 procesorů nad společnou pamětí (*SMP* – Symmetric MultiProcessing) je označována jako *Windows NT Advanced Server*. Systém souborů *NTFS* (Windows NT File System) zajišťuje potřebnou efektivitu a ochranu dat.

Komunikace Windows NT Serveru s klientskými pracovišti se opírá o protokol *NetBEUI*. Vedle toho je k dispozici protokolová sada TCP/IP s emulátorem NetBIOSu pro vzdálená připojení. Pro komunikaci s klienty sítě Novell Netware je doplněn protokol NWLink, který je kompatibilní s protokoly IPX/SPX.



Obr. 18.2: Vnitřní struktura systému Windows NT

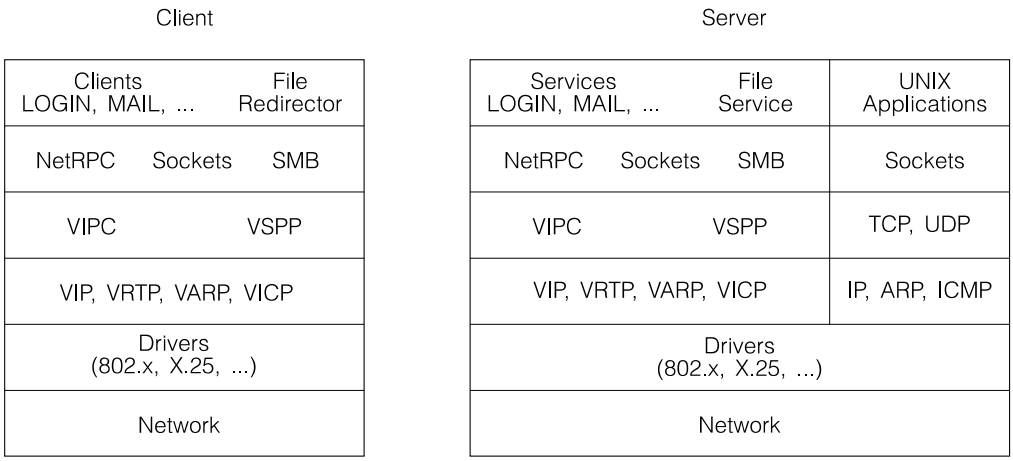
Slučitelnost Windows NT Serveru si kromě zahrnutí výběru komunikačních protokolů vyžádala i zajištění podpory několika systémů souborů, které najdeme u technologie osobních počítačů PC. Windows NT Server podporuje *FAT* (File Allocation Table), *HPFS* (High Performance File System) a *NTFS* (Windows NT File System).

Windows NT Server má propracovaný systém přístupových práv. Uživateli, který se k síťovému systému přihlašuje, je možné omezit přístup na určité hodiny, vázat jeho přihlášení na konkrétní pracoviště, dovolit mu přístup jen do určité oblasti. Systém Windows NT Server dovoluje řídit skupinu serverů sdružených do domén. Doména může být tvořena jedním nebo více servery, jeden z nich funguje jako primární server domény a udržuje databázi uživatelů. Další servery (Backup Domain Controllers) mají k dispozici kopie této databáze. Potřeba mít pro uživatele přístupová práva v každé doméně se obchází globálním zpřístupněním jedné domény (*trusting*) uživatelům domény jiné (*trusted*). Vhodným rozdělením serverů do domén a definovaním přístupových práv lze dosáhnout jak globální dostupnosti, tak potřebného oddělení zdrojů sítě jednotlivým uživatelům.

Uživatelé jsou rozděleni do několika kategorií. Správce má kompletní kontrolu nad konfigurací a organizací sítě, omezená práva mají operátoři serverů, správci zálohovacího systému, tiskových služeb a uživatelských kont. Koncovým uživatelům lze přiřadit jednu ze dvou úrovní přístupových práv, liší se možnostmi spojenými s vytvářením a rušením adresářů a souborů.

19. Banyan VINES

Operační systém lokální sítě VINES (*VIrtual NEtwork System*) firmy Banyan Inc. se opírá o souborový server, který je vystavěn nad operačním systémem UNIX. Klientská pracoviště existují ve verzích pro operační systémy DOS, Windows, OS/2, MacOS a UNIX. Systém VINES byl, na rozdíl od ostatních systémů, již od počátku orientován na vytváření velkých sítí na rozsáhlém území a na transparentní integraci lokálních sítí a dálkových spojů. Komunikační protokoly VINES vycházejí ze sady protokolů *XNS*, pro server jsou pochopitelně k dispozici i protokoly TCP/IP (obr. 19.1).



Obr. 19.1: Protokoly sítě Banyan VINES

Sítě Banyan VINES dovolují využít libovolné síťové technologie (lokální sítě, veřejné datové sítě, pronajaté spoje), nad nimi je vystavěna síťová vrstva s protokoly *VIP* (VINES Internet Protocol), *VICP* (VINES Internet Control Protocol), *VRTP* (VINES Routing Update Protocol) a *VARP* (VINES Address Resolution Protocol). Transportní rozhraní vytváří protokoly *VIPC* (VINES Interprocess Communication Protocol) a *VSPP* (VINES Sequenced Packet Protocol). Aplikace mohou pro komunikaci využívat sockety nebo procedurální rozhraní NetRPC. Služby lokální sítě (souborový server, elektronická pošta) jsou podporovány zprávami SMB.

Zajímavostí systému VINES je jeho adresářový systém *StreetTalk*. Ten byl předchůdcem systémů jako jsou ITU-T X.500 nebo na něm založený NDS (Network Directory Service) v systému Netware. StreetTalk vytváří globální adresář, aplikace nemusí rozlišovat mezi lokálními a vzdálenými zdroji, to je záležitostí adresářových služeb (VINES Redirector).

Ve srovnání se staršími systémy Netware je zde *jednodušší přihlašování*. Uživatel se přihlašuje do systému jako celku, ne k jednotlivým serverům. Přihlašovací mechanismus samozřejmě obsahuje řadu ochranných prvků (např. omezení na konkrétní místo a čas práce).

Systému VINES byla často dávána přednost díky propracovanému systému přístupových práv (samozřejmě vedle schopnosti pracovat v rozsáhlých konfiguracích). Přístup k adresářům a souborům lze omezit *přístupovými právy*, uživateli je možné povolit prohlížení adresáře (Search), čtení souborů (Read-Only), spouštění aplikací (Execute), provádět změny v adresářích (Write Directories), měnit obsah souborů (Write Files), mazat adresáře a soubory (Delete) a konečně definovat tato přístupová práva (Control). S vlastními adresáři a soubory jsou spojené *atributy*, které dovolí zakázat výmaz (No Delete), přejmenování (No Rename), dovolí sdílet adresář nebo soubor (Shared) nebo pouze spouštět program ze souboru (Executable). Zvláštní přístupová práva se vztahují k tiskárnám a tiskovým frontám, uživatel může manipulovat pouze se svými požadavky, operátor se všemi soubory v tiskových frontách a správce i s konfigurací.

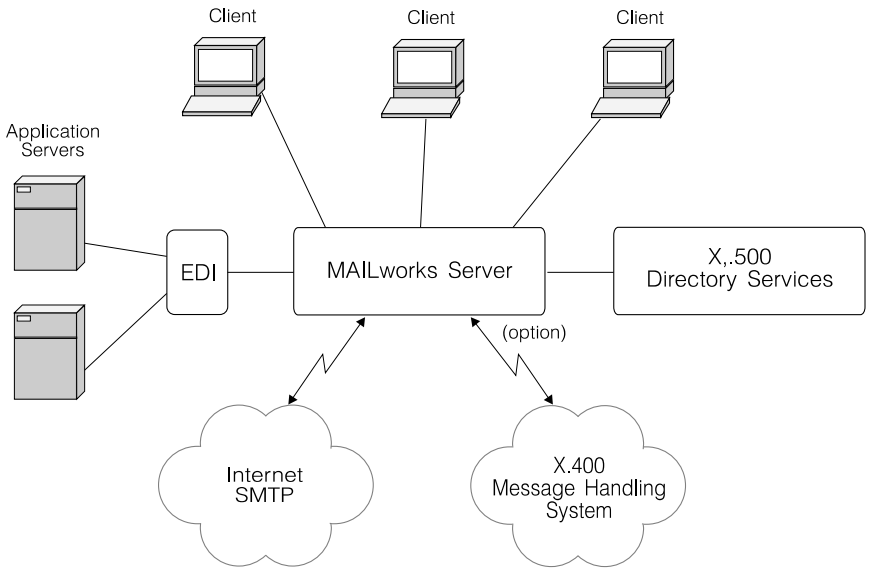
20. DEC Pathworks

V prostředí sítí vybavených počítači firmy Digital je často používaným prostředkem, integrujícím klientská pracoviště s osobními počítači a výkonné souborové a aplikační servery, síťový operační systém Pathworks. Struktura Pathworks je obdobou systémů, které jsme si uvedli dříve, zajímavé jsou platformy a komunikační prostředky, které systém podporuje.

Servery systému Pathworks jsou určeny pro práci pod firemními operačními systémy OpenVMS a ULTRIX, mohou však pracovat i pod systémy Digital UNIX (OSF-1), SCO UNIX a OS/2. Klientská pracoviště existují pro DOS, Windows, Windows NT, OS/2 a MacOS. Vedle běžných služeb jako je zpřístupnění souborů a sdílení tiskáren poskytují Pathworks podporu elektronické pošty a emulaci terminálu pro práci s aplikacemi běžícími na serverech.

K protokolovým sadám využívaným jinými systémy (IPX, TCP/IP, NetBIOS, AppleTalk) Pathworks přidávají firemní protokoly DECNet. Podpora technologií lokálních sítí Ethernet a IBM Token Ring je doplněna o podporu FDDI a o rychlou komunikaci *CI* (Computer-room Interconnect Bus) podporující vícepočítačové sestavy (*VAX-clusters*). Vedle lokálních technologií jsou transparentně podporovány i dvoubodové spoje, lze využít protokoly DDCMP (Digital Data Communication Message Protocol), PPP (Point-to-Point Protocol) a protokoly veřejných datových sítí X.25.

Vedle funkcí běžných v jiných systémech lokálních sítí Pathworks integrují i systém elektronické pošty MAILworks, jeho strukturu si zde jako koncepčně čisté řešení uvedeme (obr. 20.1).



Obr. 20.1: Elektronická pošta MAILworks

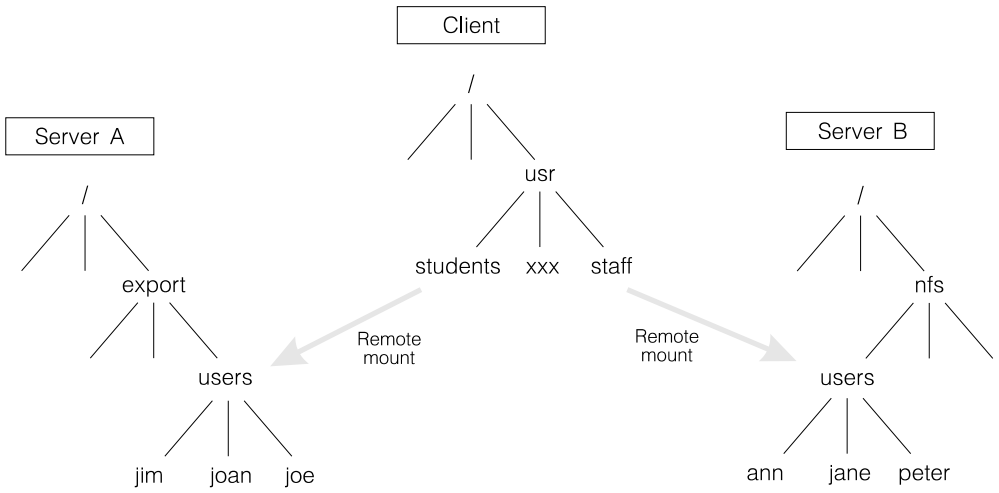
Jádrem elektronické pošty je *Mail Server*, který odesílá zprávy a udržuje paměť přijatých zpráv pro uživatele. Uživatelé mohou pracovat na emulátorech textových nebo grafických (Motif) terminálů, případně mohou využívat klientská pracoviště systémů cc:Mail, Microsoft Mail a dalších. S vnějším světem mail server komunikuje protokolem *SMTP* (Simple Mail Transfer Protocol) a opírá se o adresaci *DNS* (Domain Name Service). Pro spojení se systémy podle *ITU-T X.400 MHS* (Message Handling System) je doplněn o modul MAILbus 400 a o modul adresářových služeb podle *ITU-T X.500* (Directory Services). Vedle výměny zpráv pro uživatele (textových, zvukových, obrazových) poskytuje mail server podporu i aplikacím využívajícím standardy pro data v elektronické formě *EDI* (Electronic Data Information).

21. 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. 21.1). 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).

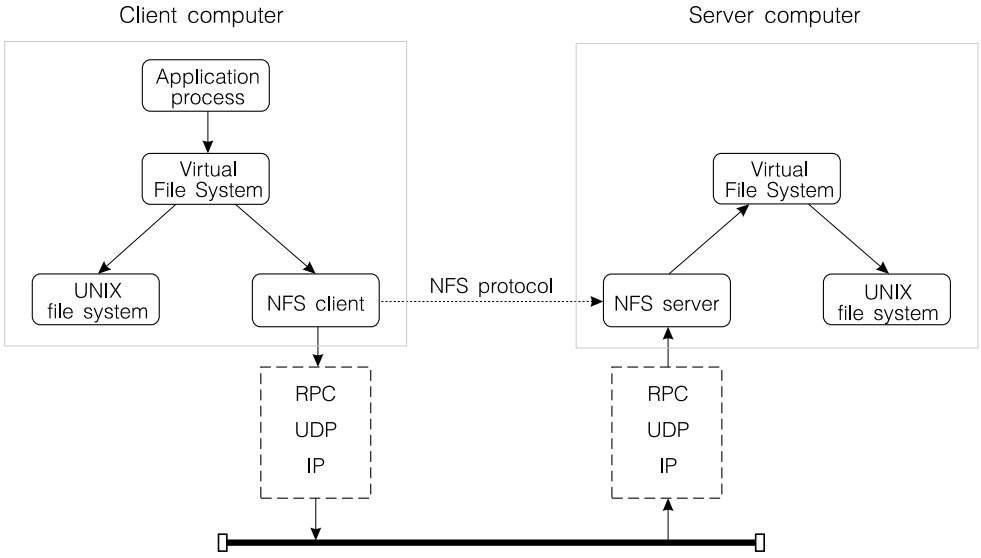


Obr. 21.1: Adresářové vazby v systému NFS

Přístup k lokálním i vzdáleným souborům se opírá o logické spoje mezi stromovými adresáři fyzicky oddělených počítačů (obr. 21.2). 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.



Obr. 21.2: 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.

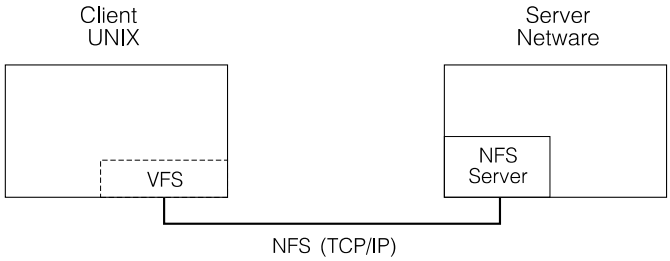
Interoperabilita s jinými sítěmi

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. 141). Jindy je server konkrétní lokální sítě realizován jako proces spustitelný pod operačním systémem UNIX, jako přiklad může sloužit implementaci Pathworks pro UNIX (str. 146). 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,

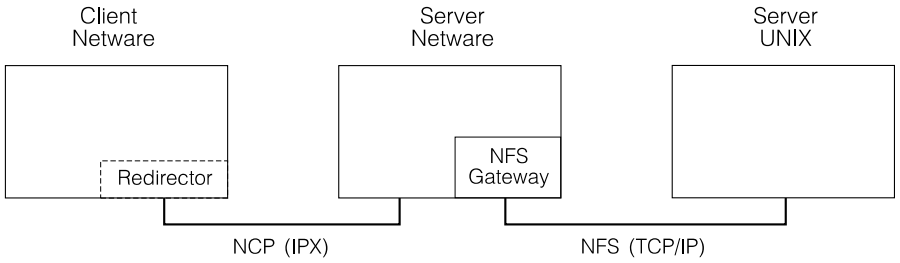
nmbd - name server podporující emulaci NetBIOSu nad TCP/IP a

smbclient - klientské pracoviště běžící pod systémem UNIX.



Obr. 21.3: Modul NFS serveru lokální sítě

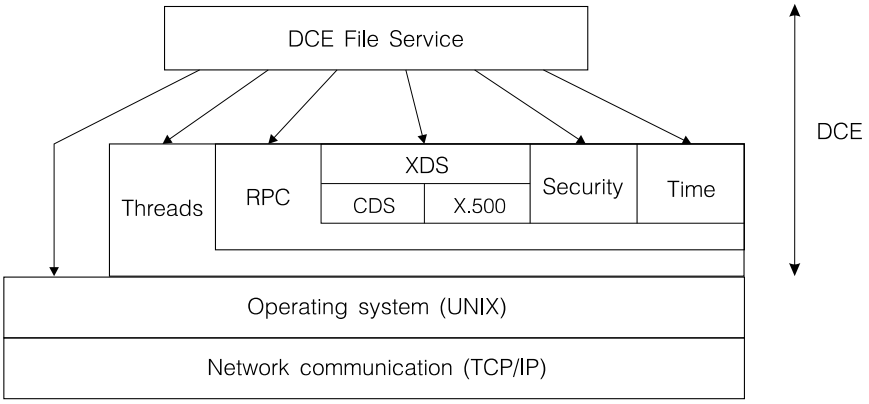
Často se setkáme i s opačným postupem, zpřístupněním souborů a tiskových front serverů lokální sítě (Netware, Windows NT) „klientským pracovištím“ pod systémem UNIX využívajícím protokoly TCP/IP. Takové moduly označujeme, podobně jako pod UNIXem, jako *FTP servery*, *NFS servery* (obr. 21.3 pro přístup 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. 21.4) a *lpr gateway*.



Obr. 21.4: 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. 21.5).



Obr. 21.5: 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.

Odkazy a doporučená literatura

Tento text vychází z informací v literatuře uvedené v následujícím 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:

[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

Index

adresa MAC 64
AIX 143
Aloha 24,29
- prostá 24
- rezervační 27
- řízená 26
- stabilita 26
- taktovaná 25
analyzátor sítě 121
Appletalk 32,34
ARCNet 40
ATM 84,86
- adaptační vrstva AAL1 90
- adaptační vrstva AAL2 90
- adaptační vrstva AAL3/4 90
- adaptační vrstva AAL5 91
- adresace 91,94
- ATM most 93
- buňka 23,86
- P-NNI Phase 0 95
- P-NNI Phase 1 95
- režim ABR – Available Bit Rate 90
- režim CBR – Constant Bit Rate 89
- režim UBR – Unspecified Bit Rate 90
- režim VBR – Variable Bit Rate 89
- signalizace 91
- směrování 94
- virtuální cesta 87
- virtuální kanál 86,87
  - PVC 88
  - SVC 88
AUI (Attachment Unit Interface) 31
Banyan VINES 147
- StreetTalk 147
CSMA – Carrier Sense Multiple Access 27
- naléhající 27,29
- nenaléhající 28,29
- p-naléhající 28,29
CSMA/DCR – Collision Resolution 32
CSMA/CA – Collision Avoidance 29,34
CSMA/CD – Collision Detection 30
- kolizní posloupnost 30
- kolizní slot 30,31
- naléhající CSMA/CD 30,64
- ustupování 32,64
DEC Pathworks 148
deterministický přístup 35
- centralizované řízení 35
- distribuované řízení 37
distribuované řízení 37
- binární vyhledávání 37,38
- dekadické vyhledávání 38
- prioritní přístup 38
- rezervace 37
doména
- broadcast 62
- kolizní 64,71
DQDB – Double Queue Double Bus 81
EAD zásuvky 67
elektronická pošta 148
emulace LAN, LANE 95,96
Ethernet 31,63
- 10BASE2 66
- 10BASE5 65
- 10BASE-FB 71
- 10BASE-FL 71
- 10BASE-FP 71
- 10BASE-T 69
- 10BROAD36 67
- 100BASE-TX 74
- 100BASE-T4 74
- 100BASE-FX 74
- asynchronní 70
- duplexní provoz 73,74
- gigabitový 75
- isochronní 75
- mikrosegmentace 71
- segment 31
- segmentace 71
- PACE 73
- přepojovaný 71
- synchronní 70
- širokopásmový 67
FDDI 50
FDDI II - isochronní FDDI 53
hub 8,69,77
- aktivní 8,40
- pasivní 8,40
- vícevstupový 69
IBM Token Ring 47
- rozbočovač 47
IEEE 802
- 802.1 18
- 802.2 Logical Link Control 18,106
- 802.3 CSMA/CD (Ethernet) 18
- 802.4 Token Bus 18,41
- 802.5 Token Ring 18,47
- 802.6 Metropolitan (DQDB) 18,81

- 802.7 Broadband 18
- 802.8 Fibre Optic 18
- 802.9 Integrated Voice/Data 18,75
- 802.10 Security 18
- 802.11 Wireless 18,103
- 802.12 100VG-AnyLAN 18,77
- 802.14 Hybrid-Fibre-Coax 18,22

IPX/SPX 19,113
ISDN 75,85
kabel
- FTP (Foiled Twisted Pair) 10
- koaxiální 9
- kroucený dvoudrát 10
- STP (Shielded Twisted Pair) 10
- STP Type 10
- UTP (Unshielded Twisted Pair) 10,69
- UTP Category 10

kódování 13
- 4B5B 51
- 5B6B 78
- diferenciální Manchester 13
- Manchester 13
- scrambling 13

kruhové sítě 44
- Cambridge Ring 46
- monitor 44
- Newhallova 45
- Pierceova 46
- vkládání rámců 47

LAN Manager 144
logický kruh 39
- virtuální 33,34,39

MAU (Medium Attachment Unit) 63
most - bridge 55,56
- brouter 55
- remote bridge 59
- Spanning Tree 57
- statické směrování 56
- transparentní 56
- učení 56
- víceportový 60
- workgroup bridge 59

NetBEUI 19,111,127
NetBIOS 19,111,127,141
- emulátor 111,117

Novell Netware 130
- audit 140
- bindery 132
- broadcast storm 130
- IPX/SPX 130
- klient 131
- kontext 135
- LSL 131
- MLID 131
- NCP 130
- NDS 132
- NLSP 131
- ODI 131
- RIP 130
- SAP 130
- server 136
- souborový systém 137
- synchronizace času 136
- VLM 132

opakovač 66
- remote repeater 66

optické spoje vláknové 70
- FOIRL 66,70
- 10BASE-FB 71
- 10BASE-FL 71
- 10BASE-FP 71

optické spoje vzdušné 105
- směrové 105
- všesměrové 105
- IBM Infrared Wireless LAN 105
- IrDA 105

OS/2
- LAN Requester 142
- LAN Server 141
- MPTS 143
- Warp Connect 142
- Warp Server 142

PC-LAN 141
- SMB blok 141

priorita 49,52,77
protokoly 106
- linkové 106
  - LLC1 107
  - LLC2 108
  - LLC3 110
- síťové 111
  - NetBIOS, NetBEUI 111
  - IPX/SPX 113
  - TCP/IP 115

provoz
- asynchronní 52
- synchronní 23,52,84

přepínač - switch 55,57,60,71
- cut-through 72
- fragment-free 73
- store-and-forward 72

přidělování na výzvu 35
- adaptivní výzva 36
- binární vyhledávání 35

- Bitbus 36
- cyklická výzva 35
přidělování na žádost 36,77
- 100VG-AnyLAN 77
rádiové sítě 98
- CDMA 101
- DSSS 101
- FHSS 100
- GSM – Groupe Spèciale Mobile 98
- PCN – Personal Cellular System 98
- rádiové sítě LAN 102
  - Freeport 105
  - PCN 102
  - RangeLAN 104
  - WaveLAN 104
- rozprostřené pásmo 98,99
- směrový spoj 98,101
  - Airlink 102
  - Altair 101
  - Skywalker 101
- úzkopásmové 98
- všesměrový spoj 99,102
redirector 126
rekonfigurace 39,51
sdílení kanálu 14
- časový multiplex (TDMA) 14
- kmitočtový multiplex (FDMA) 14
- kódový multiplex (CDMA) 14
server 126
- souborový 126
- aplikační 126,128
síťový operační systém 126
- Client-Server 126,128
- Peer-to-Peer 128
směrovač - router 55,61,62,117
- víceprotokolový 55
směrování 117
- cut-through 55,60,72
- fragment-free 73
- OSPF 119
- RIP 118
- store-and-forward 55,60,72
- zdrojové 49,60
správa – management 121
- CMIS/CMIP 121,122
- MIB databáze 123
- RMON 125
- SNMP 121,124
stabilita 26,28,30
StarLAN 68
strukturovaná kabeláž 10
světlovodná vlákna 11
- disperze
  - chromatická 12
  - vidová 11
- gradientní 11
- jednovidová 11
- mnohavidová 11
symetrický multiprocessing 141
synchronní hierarchie (SDH) 85
širokopásmové sítě 20
- Dual-Cable 20,68
- Localnet 21
- Mid-Split 20
- Split-Channel 20,68
- Wangnet 22
TCP/IP 19,115
- UDP 115
- TCP 115
Token Bus 39,41
Token Ring 45
transceiver 31,63
UNIX 149
- AFS 150
- AIX 143
- DCE 151
- interoperabilita 150
- NFS 149
- SunRPC 149
- XDR 149
Windows 3.1 144
Windows for Workgroups 3.11 145
Windows 95 145
Windows NT 145
- Server 145
- Workstation 145