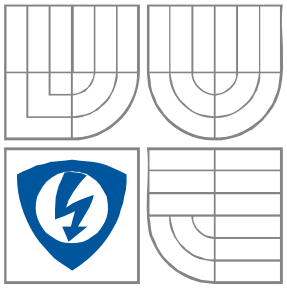
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ



Architektura sítí

Garant předmětu:
doc. Ing. Vít Novotný, PhD.

Autoři textu:
doc. Ing. Vít Novotný, PhD.

BRNO * 2011

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Vznik těchto skript byl podpořen projektem č. CZ.1.07/2.2.00/15.0139
Evropského sociálního fondu a státním rozpočtem České republiky.

Autor	doc. Ing. Vít Novotný, Ph.D.
Název	Architektura sítí
Vydavatel	Vysoké učení technické v Brně
	Fakulta elektrotechniky a komunikačních technologií
	Ústav telekomunikací
	Purkyňova 118, 612 00 Brno
Vydání	první
Rok vydání	2012
Náklad	elektronicky
ISBN	978-80-214-4450-8

Tato publikace neprošla redakční ani jazykovou úpravou

Obsah

Úvod

Oblast telekomunikačních sítí je v současnosti prezentována vesměs digitálními technologiemi. Z původně analogového světa telefonních sítí zčásti přežívá již pouze část označovaná jako „last mile“ nebo „first mile“ představovaná analogovými telefonními či faximilními přístroji a analogovým účastnickým vedením zakončeným analogovou účastnickou sadou, kde je však signál ihned digitalizován a dále již přenášen ve formě datového signálu. Digitální systémy poskytují mnohem širší možnosti zpracování informací, především však sjednocují přístup a metody přenosu, uchovávání a zpracování signálů od různých zdrojů, čímž umožnily zahájit postupnou integraci služeb do jednotné infrastruktury datových sítí se sjednoceným způsobem přenosu. Digitální technologie umožňují vytvářet mnohem pružnější komunikační systémy, které jsou odolnější vůči výpadkům dílčích síťových prvků, vyznačují se vysokou škálovatelností a jsou schopny se bez nutnosti významného přebudování sítě se přizpůsobit novým požadavkům, umožňují implementovat nové služby a poskytují možnosti propojení rozmanitých typů sítí. Jednotný digitální způsob zpracování libovolného typu informace nabízí možnost konvergence síťových a informačních technologií a integrace služeb, a tak optimalizovat využití síťových prostředků. Dnes jsme svědky snahy integrovat služby libovolného charakteru (hlas, video, obecná data) do datových sítí a potažmo do globální sítě Internet založené na protokolové sadě TCP/IP (Transmission Control Protocol/Internet Protocol). Integrace je podporována jednak zvyšujícími se přenosovými rychlostmi, ale také zaváděním mechanizmů pro zajištění nezbytné kvality požadované daným typem služby (chybovost, přenosové zpoždění, proměnlivost zpoždění). V současnosti existuje celá řada řešení, které se více či méně snaží vyhovět stále rostoucím potřebám uživatelů na zavádění nových služeb a zvyšování kvality služeb stávajících. Dobře se orientovat v problematice datových sítí a Internetu se dnes považuje u lidí zaměřených na telekomunikační techniku a informatiku za nezbytný základ, který se snaží tento učební text poskytnout.

Učební texty „Architektura sítí“ se snaží poskytnout dostatečně rozsáhlý náhled do oblasti telekomunikačních sítí se zaměřením na současný stav a vývoj, který charakterizuje mohutný rozvoj digitálních sítí s přepojováním datových jednotek souhrnně označovaných jako datové sítě. Počáteční kapitoly uvádí čtenáře do problematiky architektury, typů a principů digitálních telekomunikačních sítí. Významná část textu je věnována lokálním datovým sítím, kde se čtenář dozví relativně podrobné informace o různých typech kabelových a také dnes velmi populárních bezdrátových sítí. Další díl je pak věnován problematice protokolů vyšších vrstev modelu komunikačních sítí, kam patří především dnes nejrozšířenější sada protokolů TCP/IP.

Kurz Architektura sítí je jedním z řady předmětů orientovaných na problematiku telekomunikačních sítí. I když učební text v úvodní části obsahuje přehled základních termínů telekomunikační techniky, včetně objasnění jejich významu, je vhodné, aby byl student obeznámen se základní problematikou digitálního zpracování informace (vzorkování, zdrojové kódování, komprese digitální informace, zabezpečovací techniky proti chybám, apod.) a se základy komunikační techniky (struktura telekomunikační sítě, telekomunikační služby, telekomunikační kanál, okruh, spoj, přenos signálu, zkreslení signálu, šum v kanálu, signalizace, synchronizace, symbolové kódování, modulace, spojení, apod.).

1 Informace, sítě a služby přenosu informace

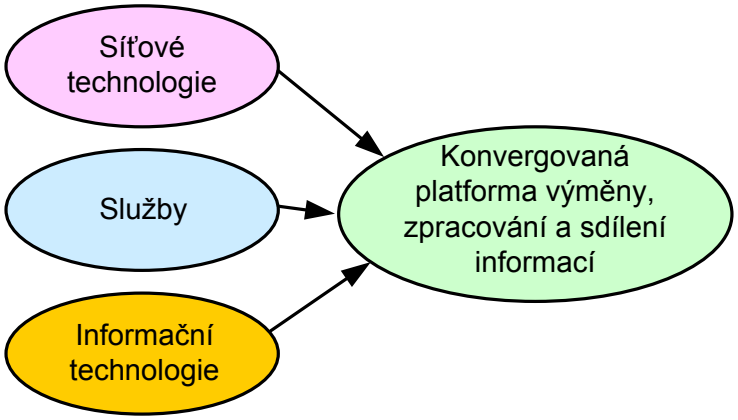
Základem každého života na naší planetě je potřeba získávání a zpracovávání informací o prostředí, kde se daný život odehrává a které se ho týká, neboť to umožňuje adaptovat se aktuálním podmínkám, případně se připravit i na možné změny životních podmínek, a tak nejenom přežít, ale i dosáhnout cílů k uspokojení dalších potřeb. Živé organizmy jsou proto vybaveny řadou více či méně dokonalých **smyslových orgánů**, kterými mohou okolní svět vnímat, tedy přijímat informace, napojených na **nervovou soustavou**, která umožňuje zpracování a ukládání získaných informací, a **výkonnými prvky**, kterými případně organizmus reaguje na povely nervového systému vzniklé jako výsledek zpracování informace.

Informace živý organizmus může získávat:

- poznáváním **za použití pouze vlastních smyslů přímým vnímáním** všech neživých i živých součástí našeho okolí,
- **přímým předáváním informací od ostatních živých organizmů svého druhu** přes výkonné a smyslové orgány - kontaktem na vzdálenost umožňující přímou detekci informace prezentovanou výkonnými prvky organizmu – mechanicky, akusticky, vizuálně, chemicky, elektricky,
- **zprostředkovaně** (i na velkou vzdálenost, buď v reálném čase nebo i s různě dlouhým časovým odstupem) **prostřednictvím jiného typu nosiče informace**, než těch, co přímo ovlivňují výkonné prvky organizmů, jenž jsou zdrojem informace,
    - od ostatních živých organizmů svého druhu – pomocí řeči, písma, obrazu, či jiných mechanických způsobů záznamu, které cílový organizmus umí svými smysly vnímat, a přenosu informace
    - od uměle vytvořených výpočetních systémů umožňující získávání, ukládání, zpracovávání a prezentaci informace, případně i ovládání výkonných prvků vlastního systému či vzdálených systémů.

Zprostředkovaný způsob získávání informace může být realizován pomocí:

- lokálních zdrojů – místní knihovny, muzea, archivy, kroniky, atd.
- přenosem po přirozených komunikačních sítích – říční sítě, mořské proudy, vzdušné proudy,
- přenosem po umělých komunikačních sítích:
    - využívající cvičené živé organizmy jako nosiče – lidi jako posly, dále nejčastěji ptáky (např. holuby) nebo savce (psy, kočky, delfíny), apod.
    - mechanických – umělé vodní kanály, různé potrubní systémy (např. potrubní pošta), aj.
    - akustických – např. pomocí bubnů,
    - optických – světelné či kouřové signály,
    - využívající různých forem elektromagnetického signálu jako nosiče informace = **telekomunikační sítě**.



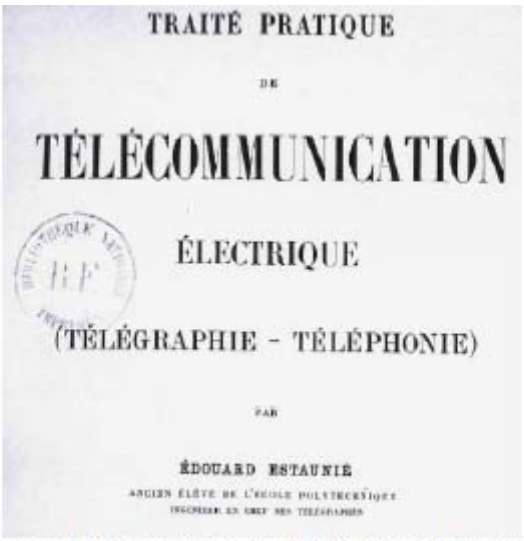
Obr. 1.1: **Proces konvergence a integrace v oblasti přenosu, zpracování a sdílení informací**

1.1 Komunikační sítě jako systémy vazeb

Komunikační síť obecně je systém skládající se ze souboru či množiny uzlů a množiny spojů či vazeb, které mezi uzly spojují do jednoho vzájemně na sebe působícího souboru. Uzly jsou objekty, které mohou být zdrojem, příjemcem a nebo přeposílatelem médií. Médium může mít obecně formu materiálu, živých organizmů, chemických sloučenin, elektromagnetického signálu, apod., jenž jsou mezi uzly přenášeny po spojích. Cílové uzly jsou příjemci médií, které dále zpracovávají, ale i mezilehlé uzly mohou z předávaných médií získávat informace, které mohou využít mnoha způsoby, například k různým statistickým výpočtům jako vyhodnocování vytížení spojů i samotného uzlu, skladba (profil) toků (z jakých typů a v jakém objemu média tok tvoří), doba obsluhy požadavku (předání média ze vstupu na odpovídající výstup), ztráty na daných spojích a v uzlech a jiné. Přenosem médií dochází ke vzájemnému působení mezi uzly, což může v případě adaptivní sítě modifikovat její chování a případně i celou strukturu sítě. Příkladem komunikačních sítí jsou dopravní sítě, telekomunikační sítě, biologické sítě (neuronové sítě, vazby mezi enzymy, proteiny, apod.), vztahy mezi živými organizmy (potravní řetězec či sociální sítě), potrubní systémy, kanalizační systémy, chemické vazby mezi molekulami a mnoho dalších.

1.2 Základní pojmy v oblasti telekomunikačních sítí

Telekomunikace – komunikace na dálku pomocí „elektřiny“ (přesněji elektromagnetické energie), viz **Obr. 1.2**, dnes chápaná především za pomoci elektronických systémů; dříve i mechanických, optických a elektromechanických systémů.


TRAITÉ PRATIQUE

DE

TÉLÉCOMMUNICATION

ÉLECTRIQUE

(TÉLÉGRAPHIE - TÉLÉPHONIE)

PAR

ÉDOUARD ESTAUNIÉ

First appearance of *Télécommunication* (Bibliothèque Nationale de France)

Obr. 1.2**: První použití slova telekomunikace (francouzsky *Télécommunication*) v publikaci z roku 1904, [24]**

Telekomunikační systém - je komplex vytvořený pro zprostředkování přenosu informace (pro poskytování telekomunikačních služeb) za pomoci elektromagnetického signálu jako základního nosiče informace. Systém zahrnuje telekomunikační síť, soubor poskytovaných služeb a jejich parametrů, informační systém obsahující informace o účastnících, aktivovaných službách a data o realizovaných službách, a soubor organizačních pravidel definující jednotlivé činnosti prováděné na síti s důrazem na zabezpečení přenášené informace v síti proti nadměrnému zkreslení (chybám), nezákonnému odposlechu, změně či zničení a na zabezpečení chodu systému jako celku.

Telekomunikační síť - je soubor ***koncových zařízení***, ***přenosových***, ***spojovacích***, ***signalizačních***, ***dohledových*** a ***řídicích*** prostředků pro zajištění poskytování telekomunikačních služeb v požadované kvalitě. Příkladem je telefonní síť a dnes především Internet.

Telekomunikační služba - je služba zprostředkovávající přenos uživatelské informace telekomunikační sítí prostřednictvím elektromagnetických vln jako nosiče informace. Je specifikována ***souborem technických, provozních a organizačních opatření***, která musí být telekomunikačním systémem zajištěna pro její úspěšné provozování. Typickým příkladem služby je hovorová (telefonní) služba, videokonverzační služba, faximilní služba, služba elektronického přenosu zpráv (e-mail), služba okamžité výměny zpráv (instant messaging), distribuční služby typu přenosu televizního a rozhlasového vysílání, video a audio streaming z video a audio serverů, hry po síti (internet gaming) a další, ale stále více a více se rozšiřují služby datového typu, jako je přístup k informačním zdrojům – především prostřednictvím služby www; dále přenos databázových dat z jednoho centra do druhého, dálkový sběr naměřených dat, stahování datových souborů (software, video, audio, e-knihy, aj.) a mnoho dalších.

Telekomunikační služba v reálném čase - je služba, kdy informace určená k přenosu není pevně předpřipravena a uložena na paměťovém médiu, ale vzniká ve zdrojích informace komunikujících uzlů až v průběhu vedení relace. Po vzniku je informace přenášena k cíli, u příjemce je informace během relace zpracována a vygenerována odpověď, která je zaslána zpět odesílateli, kde v závislosti na obdržené informaci je aktivována odpovídající reakce, a to vše v takových časových relacích, které odpovídají časovým požadavkům daného typu

služby. Příkladem je hovorová služba, která vyžaduje, aby pro její hladký průběh bylo zpoždění přenosu hlasu telekomunikačním systémem menší než 150 ms v jednom směru.

Koncový komunikační uzel sítě (koncové komunikační zařízení) – uzel, odkud je zahajován či kde je ukončován přenos informace v síti a kde je provozována výkonná jednotka (entita) provozované telekomunikační služby a nezajišťují funkce přepínání a směrování. Koncovými uzly mohou být:

- ***Účastnická koncová zařízení*** – koncové uzly, jejichž prostřednictvím zákazníci síťového operátora realizují telekomunikační služby. Tato zařízení jsou nejčastěji v osobním vlastnictví zákazníků (účastníků) jimiž mohou být jak fyzické, tak i právnické osoby (organizace). Tato zařízení bývají jak iniciátorem tak i cílem telekomunikačních služeb
- ***Servery*** – uzly nabízející služby a očekávají příchod požadavků na službu od účastnických koncových zařízení případně i od jiných serverů.

Přenosové komunikační médium – fyzické prostředí mezi komunikujícími uzly (vysílačem a přijímačem) umožňující přenášet informaci pomocí elektromagnetického nosného signálu a vytvářející tak ***fyzický komunikační spoj***, neboli propojení mezi bezprostředně sousedícími komunikačními uzly (mezi nimi se podél komunikační cesty nenachází žádný mezilehlý komunikační uzel). Nejčastějšími typy jsou ***metalická vedení***, ***optická vlákna***, ***volný prostor*** s obsahem různých plynů či drobných částic (atmosféra), případně ***vlnovody***,

Transportní systém – systém zajišťující efektivní, spolehlivý a bezpečný přesun (transport) informace (aplikační, řídicí) mezi přepojovacími uzly nebo mezi přepojovacím uzlem a koncovým uzlem sítě.

Přepojovací (spojovací) uzel sítě – síťový prvek zajišťující přepojení toku dat na vstupu na požadovaný výstup za účelem vytvoření cesty od zdrojového ke koncovému komunikačnímu uzlu sítě

Spojovací systém – soustava mezilehlých přepojovacích uzlů sítě vzájemně propojených transportním systémem pro přenos aplikačních a řídicích dat za účelem realizace postupného předávání vyslané informace od zdroje směrem k cíli.

Přenos v síti (síťový přenos) – je obecně jakékoliv odeslání či příjem dat po telekomunikační síti.

Síťová informační transakce – je jakákoli obousměrná výměna zpráv po telekomunikační síti typu:

- dotaz-odpověď,
- příkaz-odpověď,
- ohlášení-odpověď,
- data-potvrzení,
- data-data+potvrzení,
- data+potvrzení-data+potvrzení.

Relace v komunikačních sítích – je komunikace mezi dvěma entitami (výkonnými jednotkami) koncových uzlů sítě, které jsou provozovány ve vrstvách nad úrovní intersítě. Tyto entity jsou buď samostatné jednotky (na samostatné vrstvě nazývané relační vrstva), nebo jsou součástí větších výkonných celků na transportní nebo aplikační vrstvě. Relační

entity v komunikujících koncových uzlech sítě vytvářejí záznamy, které obsahují informace o zdroji, cíli, typu služby, parametrech služby a stavu komunikace.

Komunikační (sdělovací) kanál – jednosměrný logický spoj mezi vysílačem a přijímačem. Vyznačuje se řadou vlastností, jako jsou:

- kmitočtová poloha kanálu,
- šířka pásma,
- přenosová charakteristika (modulová, fázová),
- rušení, příčiny a jeho charakter,
- dynamický rozsah pro nosný signál.

Výše uvedené vlastnosti pak určují maximální kapacitu komunikačního kanálu.

Fyzický komunikační segment (linka) – fyzické propojení mezi bezprostředně sousedícími komunikačními uzly mezi nimi se podél komunikační cesty nenachází žádný mezilehlý komunikační uzel. Ten může být buď dvoubodový (Point-to-Point) nebo mnohabodový (Multipoint).

Logický komunikační spoj – logické propojení koncových komunikačních uzlů přes mezilehlou síť (mezilehlé přepojovací uzly)

Komunikační spoje mohou mít několik podob:

- **pevné spoje** – spoj, který je permanentně sestaven, a tudíž stále k dispozici pro přenos informace.
- **komutované (přepojované) spoje** – spoj, který se sestavuje na žádost při zahajování realizace telekomunikační služby, prostředky jsou vyhrazeny jen po čas trvání služby a po jejím ukončení jsou prostředky uvolněny a k dispozici pro realizaci služeb ostatními uživateli.

Komunikační okruh – obousměrné propojení mezi dvěma koncovými uzly sítě. Okruh může být buď fyzický nebo virtuální.

- **Fyzický okruh** znamená vyčlenění síťových prostředků pro sestavení komunikačních kanálů v obou směrech buď **napevno**, nebo během procedury **sestavování spojení** (komutovaný či přepojovaný okruh). Tyto prostředky jsou vyhrazeny pouze pro daný logický komunikační spoj, dokud tento není ukončen a síťové prostředky nejsou uvolněny. Kapacita okruhu bývá ve většině případů během celého spojení konstantní. V případě sítě ISDN a doplňkové služby „Bandwidth on Demand“ se kapacita může měnit, avšak pouze v násobcích kapacity základního kanálu B, jenž činí 64 kb/s. Komunikace po fyzických okruzích vykazuje velice nízké zpoždění a také nízkou režii během přenosu, protože cesta a její přenosová kapacita je pevně dána a data tak nemusí obsahovat informaci pro směrování informace sítí. Nevýhodou je neefektivní využití přidělených síťových prostředků a nutnost sestavování nového okruhu při výpadku některé z částí okruhu.
- **Virtuální okruh** – je logický obousměrný spoj mezi koncovými komunikačními uzly sítě nad fyzickou sítí založenou na sdílení přenosových a spojovacích prostředků. Princip virtuálního okruhu je součástí specifikace dané síťové technologie, jde tedy o technologicky závislé řešení. Pro vytvoření virtuálního okruhu je třeba vyhledat cestu k cíli a ve přepojovacích prvcích podél nalezené cesty vložit záznam do přepojovací tabulky. Síťové prostředky však nejsou pevně vyhrazeny pro dané spojení, ale jsou sdíleny s ostatními toky. Množství a stálost přidělených síťových prostředků je pak

průběžně řešena plánovačem obsluhy datových jednotek v přepojovacích prvcích. Výhodou je z podstaty používané sítě s přepojováním datových jednotek efektivní využití síťových prostředků. Data však musí být rozdělena na datové jednotky, které obsahují identifikátor virtuálního okruhu, což zvyšuje režii přenosu. Příklady síťových technologií s tímto principem přenosu dat je ATM (Asynchronous Transport Mode) a FR (Frame Relay).

Orientace služeb na spojení – služby mohou či nemusí či dokonce z podstaty nesmí vytvářet spojení:

- ***spojově orientované služby*** – před zahájením přenosu aplikačních dat je vytvořen spoj (fyzický či virtuální). Příkladem jsou služby realizované v sítích ISDN, ATM a služby Internetu využívající spojově orientovaný transportní protokol TCP (Transmission Control Protocol).
- ***nespojově orientované služby*** – služby, kdy jsou aplikační data odesílána k cíli, aniž se navazuje spojení (ani virtuální). Důvodem pro tento typ komunikace je rychlost, jednoduchost odeslání dat (požadavku) v případě velmi malého objemu odesílaných dat (budování, údržba a ukončení spojení by trvalo déle než samotný přenos aplikačních dat) nebo vícebodovost komunikace, tj. zasílání dat skupině uzlů (multicast) či všem uzlům v síti (broadcast). Pro tento účel služby v síti Internet využívají transportní protokol UDP (User Datagram Protocol)

Fyzický end-to-end spoj – spoj mezi koncovými uzly v sítích pracujících na bázi fyzických okruhů.

Virtuální end-to-end spoj – sestavení end-to-end spojení na úrovni nad síťovou vrstvou, tedy transportní a vyšší. Před vlastní komunikací je nutné sestavit spojení (virtuální, tj. dojde k výměně zpráv obsahujících žádost o spojení, kladnou odezvu na žádost a sadu parametrů pro řízení komunikace), to je pak pomocí procedur protokolu virtuálního spoje udržováno a po skončení přenosu dat zase zrušeno. Tento typ spoje je nezávislý na síťové technologii a může tak být sestaven přes různé typy sítí.

Způsob přenosu informace sítí – na základě typu síťové technologie můžeme rozlišovat:

- ***služba přenosu po fyzických okruzích*** – v sítích založených na sestavování fyzických okruhů (např. telefonní síť). Informace lze přenášet buď v analogové formě po analogové telefonní síti nebo v digitální formě po digitální síti (ISDN) jako kontinuální proud zdrojově zakódovaných aplikačních dat (například u hovorové či videokonverzační služby v síti ISDN, kdy prioritou není zabezpečení dat vzhledem k nízké chybovosti sítě) nebo po blocích, a to z důvodu zabezpečení proti chybám (u přenosu obecných dat je bezchybnost přenosu prioritou) nebo proti přerušení spojení (u velkého objemu dat, aby při přerušení spojení nebylo nutné po jeho obnově přenášet všechna data znovu),
- ***služba přenosu po virtuálních okruzích*** – buď pevně nebo komutovaně je v síti sestavena cesta, tzv. virtuální okruh, kterému se pro každý segment cesty přidělí identifikátor okruhu s lokální platností a v přepínačích se vytvoří záznam, kam přepínat jednotky s daným identifikátorem okruhu. Po virtuálním okruhu se pak data předávají od zdroje k cíli. Vzhledem k tomu, že jsou prostředky sdílené, musí být data rozdělena na datové jednotky - rámce či buňky, které ve svém záhlaví nesou identifikátor virtuálního okruhu. K přepínání dochází typicky na spojové vrstvě.
- ***datagramová služba*** – jedná se o nespojově orientovanou službu přenosu dat. Data se rozdělí na datové jednotky, které nesou úplnou směrovací informaci pro cestu sítí

(adresy adresáta a odesílatele). Díky tomu mohou datové jednotky putovat sítí nezávisle na ostatních. V přepojovacích prvcích se o každé datové jednotce rozhoduje samostatně dle aktuální podoby směrových informací a díky mřížové struktuře intersítě (neboť tato služba je typicky poskytována na síťové vrstvě), kdy většinou existuje k cíli řada cest mohou datové jednotky dojít k cíli s různým zpožděním, či dokonce i v jiném pořadí, než byly vygenerovány.

Kódování – transformace datového signálu z jednoho abecedního prostoru do druhého. Rozlišujeme několik typů:

- ***zdrojové kódování*** – prezentace zpráv od zdroje informace posloupností prvků z jiné abecedy s cílem omezit stupeň redundance originálního toku zpráv,
- ***kanálové kódování*** – transformace zdrojového toku dat do podoby vhodné pro efektivní a věrný přenos informace daným komunikačním kanálem. Pod tento pojem zahrnujeme:
    - *protichybové kódování* – zvýšení redundance toku dat za účelem rozpoznání případného vzniku chyby (detekční kódy) nebo dokonce za účelem automatické opravy vzniklých chyb (korekční kódy).
    - *linkové kódování* – prezentace datového signálu pomocí symbolů vyjádřených pomocí elektrického napětí či proudu ve formě pulzů diskrétních v hodnotě a času svým průběhem přizpůsobených pro přenos daným fyzickým kanálem.
    - *pomocná kódování* – příprava datového signálu pro následující linkové kódování s cílem optimalizovat využití přenosového kanálu. Sem patří činnosti typu příprava pro odstranění stejnosměrné složky, vkládání synchronizační informace, odstranění periodicit datového signálu, úprava signálu pro snížení parametru PAPR (Peak to Average Power Ratio) u následné vícestavové modulace (u mobilních koncových uzlů), apod.
- ***kódování pro utajení přenášených dat*** – šifrování (kryptografie) dat pro přenos důvěrných dat přes nedůvěryhodnou telekomunikační síť.
- ***kódování pro zajištění autenticity zprávy*** – elektronický podpis, zakódování zprávy pro možnost ověření pravosti udávaného autora a konzistence zprávy

Datová jednotka - ucelený blok dat sestávající z řídicích částí (alespoň jedné) a z vlastní (aplikační či uživatelské) části (anglicky označovanou jako payload) nesoucí informaci pro cílovou výkonnou entitu (řídicí či aplikační). Datová jednotka může mít na různých úrovních telekomunikačního systému různou formu:

- ***zpráva*** - datová jednotka přenášená na úrovni aplikační vrstvy, je tedy technologicky nezávislá, délka zprávy je velmi proměnlivá, formát je specifikován aplikačním protokolem,
- ***blok*** – část zprávy vytvořená za účelem postupného přenosu velmi objemné zprávy po částech, především jako ochrana před nutností přenášet celou zprávu od začátku, když během přenosu dojde k přerušení spojení,
- ***segment*** - část zprávy vytvořená za účelem přenosu zprávy po síti s přepojováním datových jednotek, ve které je maximální velikost datové jednotky omezena, aby byl zajištěn princip sdílení síťových prostředků a aby docházelo při zpracování datové jednotky k obsazování těchto prostředků pouze na relativně krátkou dobu,

- *paket* – datová jednotka přenášená na úrovni síťové vrstvy, je tedy technologicky nezávislá, délka paketu je proměnlivá, příkladem může být IP paket,
- *rámec* – datová jednotka přenášená na úrovni spojové vrstvy, je tedy technologicky závislá, délka rámce je proměnlivá, příkladem mohou být rámce sítí Ethernet, Token Ring, Frame Relay a dalších,
- *buňka* – datová jednotka přenášená na úrovni spojové vrstvy, délka datové jednotky je však pevně dána a tedy konstantní. Příkladem je buňka sítě ATM (Asynchronous Transport Mode).

Sdílení komunikačního kanálu – využívání komunikačního kanálu pro přenos více datových toků. Rozlišujeme sdílení:

- ***multiplexováním*** (multiplex) – sdružování toků řeší jedno zařízení jménem multiplexor, který podle určitého schématu vkládá jednotlivé příspěvky do výstupního toku,
- ***vícenásobným přístupem*** (multiple access) – více přispěvatelů a případně řídicí uzel řeší, kdo může v daný okamžik do komunikačního kanálu vkládat data.

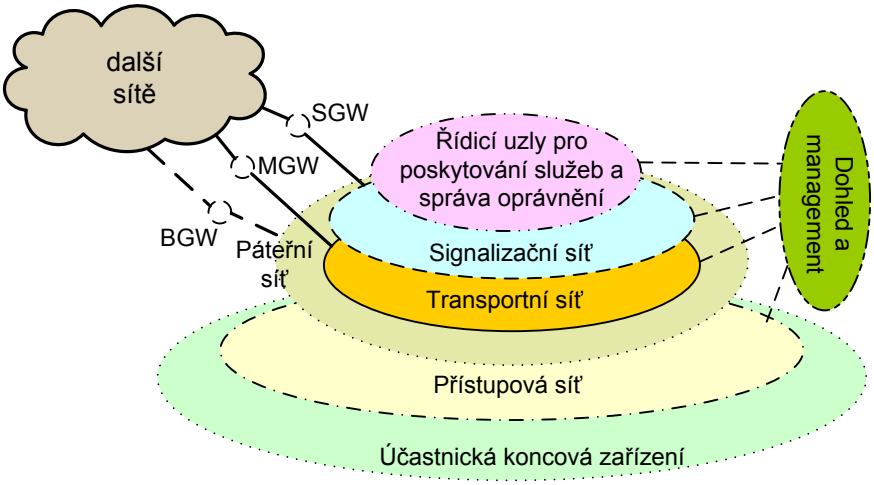
Multiplex toků je operace sdružování více toků do jednoho, která je prováděna jedním zařízením – multiplexorem. Rozlišujeme:

- **prostorový** multiplex (SDM),
- **kmitočtový** multiplex (FDM),
- **časový** multiplex (TDM),
- **statistický** časový multiplex (STDM),
- **kódový** multiplex (CDM),
- **ortogonální** kmitočtový multiplex (OFDM).

Vícenásobný přístup je procedura, která umožňuje více zdrojům datových toků podle určitého scénáře (algoritmu) přistupovat ke sdílenému přenosovému kanálu a vkládat do něj data tak, aby pokud možno nenastávaly kolize mezi přispěvateli, a pokud ano, aby kolize byly co nejdříve detekovány a aby bylo řešeno, jak se dalším kolizím vyhnout. Vše se děje s cílem, aby metoda přístupu nebyla příliš komplikovaná, aby nefunkčnost (výpadek) uzlu neměl vliv na fungování systému sdíleného přístupu a aby se co nejefektivněji využila dostupná kapacita kanálu. V současnosti k tomu dále přibývá i požadavek na prioritizaci toků citlivých na zpoždění, jeho proměnlivost a vyžadující určitou minimální přenosovou kapacitu.

1.3 Architektura telekomunikačních sítí

V průběhu vývoje vznikla celá řada typů telekomunikačních sítí, které se lišily či liší typem přenášené informace (telefonní, telegrafní, datové, rozhlasové, televizní, integrované), podobou přenášené informace (analogová a digitální), způsobem komunikace (se spojením, bez spojení), způsobem přepojování signálu v uzlech (se spojováním fyzických okruhů, zpráv, paketů, buněk), cestou přenosu (pozemní, satelitní), apod.



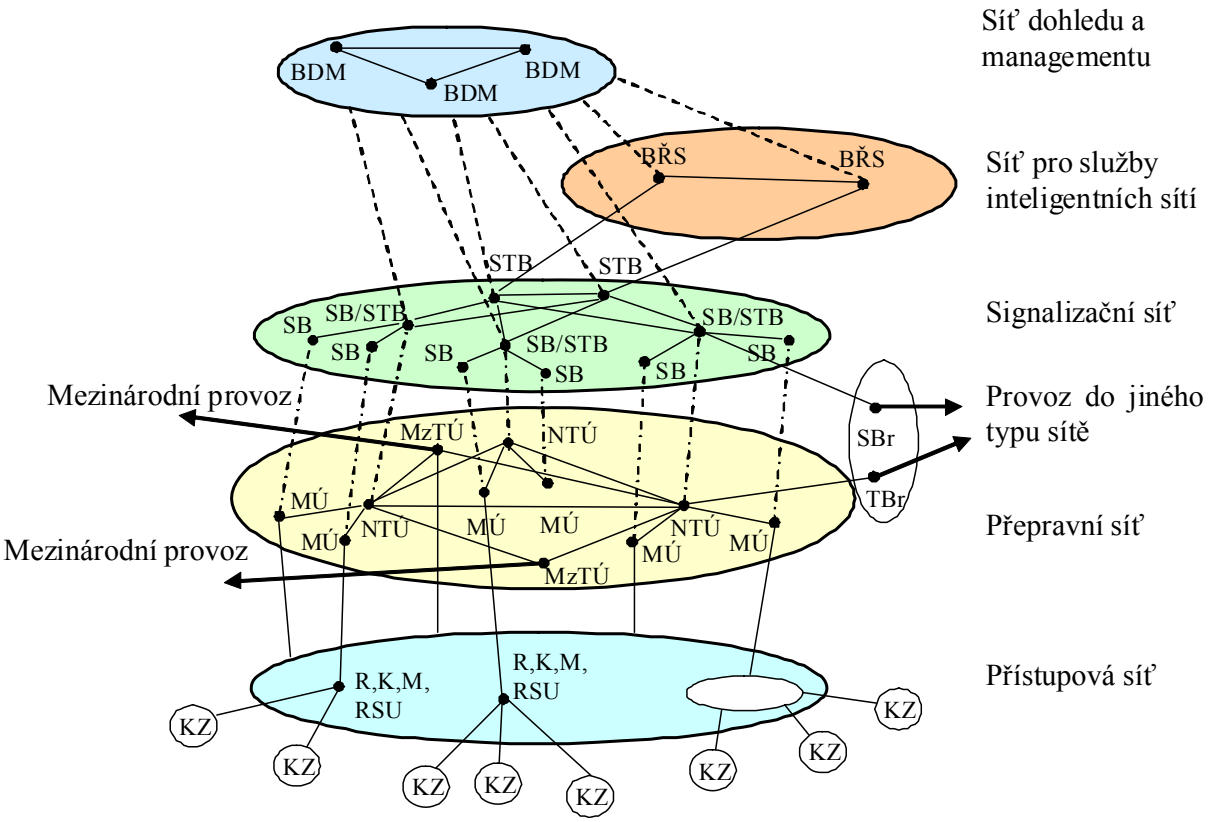
Obr. 1.3: Obecná architektura telekomunikační sítě

Obecná architektura telekomunikační sítě zobrazena na Obr. 1.3 a zahrnuje následující základní části:

- **účastnická koncová zařízení** – zařízení zajišťující přístup účastníků ke službám telekomunikační sítě, nejčastěji ve vlastnictví účastníků, případně ve vlastnictví majitele sítě nebo i dalších organizací, jako například poštovních úřadů, provozovatelů letišť, restaurací, hotelů, nákupních center, administrativních budov, apod. (sem patří například kromě standardních telefonů také veřejné telefonní automaty, internetové terminály, aj.),
- **přístupová síť** – zajišťuje přístup účastnických koncových zařízení k páteřní části sítě,
- **transportní síť** – zajišťuje přepravu datových toků poskytovaných služeb mezi hraničními transportními uzly, ke kterým jsou prostřednictvím přístupových sítí napojeny koncové uzly, mezi nimiž je sestaveno spojení či relace za účelem realizace služby,
- **signalizační síť** – síť zajišťující přenos řídicích zpráv sloužících k řadě procedur, jako přihlášení do sítě, autentizace, mobilita, přidělování síťových prostředků, budování, udržení, modifikace a rušení spojení či relace, účtování služeb, apod.,
- sada **řídicích uzlů** zahrnující:
    - **aplikační servery** - řídicí uzly pro poskytování základních služeb, poskytování nadstavbových služeb pomocí služeb inteligentních sítí (INAP – Intelligent Network Application Part) nebo nadstavby CAMEL (Customised Applications for Mobile network Enhanced Logic),
    - **pomocné (proxy) servery** - předzpracování a správné směrování požadavků účastníka na službu,
    - **databázové servery** - uzly s databázemi pro autentizaci, autorizaci, lokalizaci účastníků (databáze pro správu účtů účastníků), účtování za služby, ověření pravosti (např. u koncových terminálů mobilních sítí) apod.
- **síť dohledu a managementu** – přenos zpráv o stavu a využití síťových prostředků, o selhání určitých prvků sítě (alarmů), či přenos dat pro upgrade softwarové výbavy síťových prvků,

Transportní a signalizační síť včetně řídicích uzlů se často spojují do jednoho celku označovaného jako „**páteřní síť**“ (anglicky „Core Network“). Pak se pro rozlišení specifikace protokolové výbavy pro transport aplikačních dat a signalizace hovoří o přenosové rovině a o signalizační (řídicí) rovině.

Na Obr. 1.4 je zachycen příklad struktury telefonní sítě.



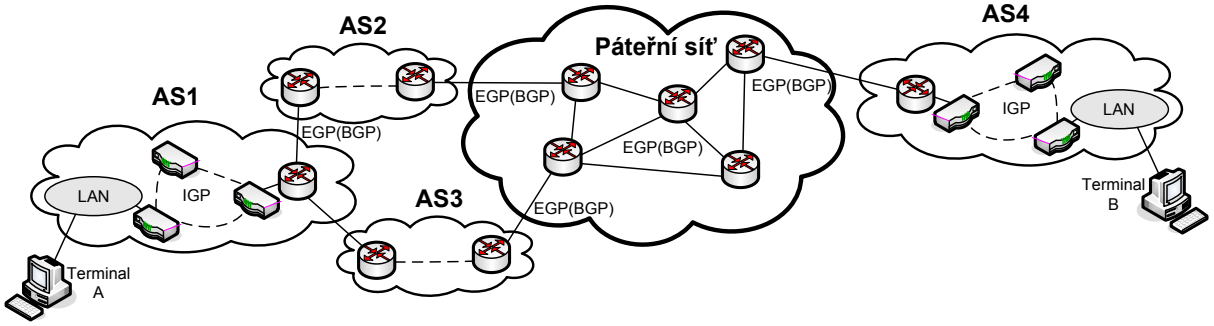
Obr. 1.4 Struktura digitální telekomunikační sítě se spojováním okruhů

MÚ – místní ústředna (LE – Local Exchange)
NTÚ – národní tranzitní ústředna (TrE – Transit Exchange)
MzTÚ – mezinárodní tranzitní ústředna (IE – International Exchange)
SB – signalizační bod (anglicky SP – Signalling Point)
STB – signalizační transportní bod (anglicky STP – Signalling Transport Point)
BŘS – bod řízení služeb inteligentních sítí (SCP – Service Control Point)
BDM – bod dohledu a managementu (OMC – Operational and Maintenance Centre)
TBr – transportní brána (anglicky MGW – Media Gateway)
SBr – signalizační brána (anglicky SGW – Signalling Gateway)
R – rozvaděč
K – koncentrátor
M - multiplexor
RSU – předsunutá účastnická jednotka (Remote Subscriber Unit)

Síť daného operátora se za účelem možnosti zprostředkování komunikace mezi účastníky (koncovými uzly) sítí dalších operátorů propojuje s dalšími sítěmi pomocí bran, a to dvou typů – signalizační (řídicí) brány (Signalling Gateway) a brány pro přenos aplikačních dat (Media Gateway). Tyto brány mohou být sloučené, pak se označují jako hraniční brány (Border Gateway). Základním úkolem bran je překlad formátů řídicích zpráv a aplikačních dat, předávání informací nezbytných pro správné sestavování relací/spojení, a přídavným úkolem pak ochrana vnitřní sítě před případnými útoky z venčí.

Dnešní globální síť Internet založený na protokolové sadě TCP/IP sestává z vzájemně propojených částí označovaných jako Autonomní systémy (AS), kde platí jednotná politika transportu (směrování) dat. Jeden autonomní systém bývá spravován nejčastěji jedním, ale i

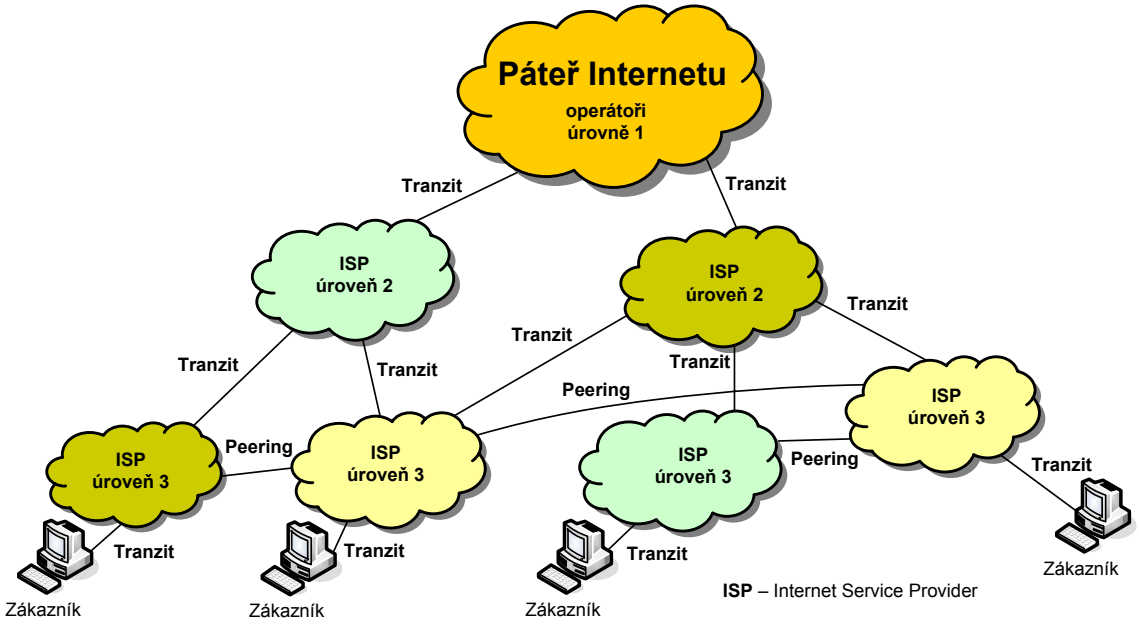
více operátory. V Internetu má každý AS přiřazen identifikátor ASN (AS Number), původně 16-bitový, dnes už 32-bitový.



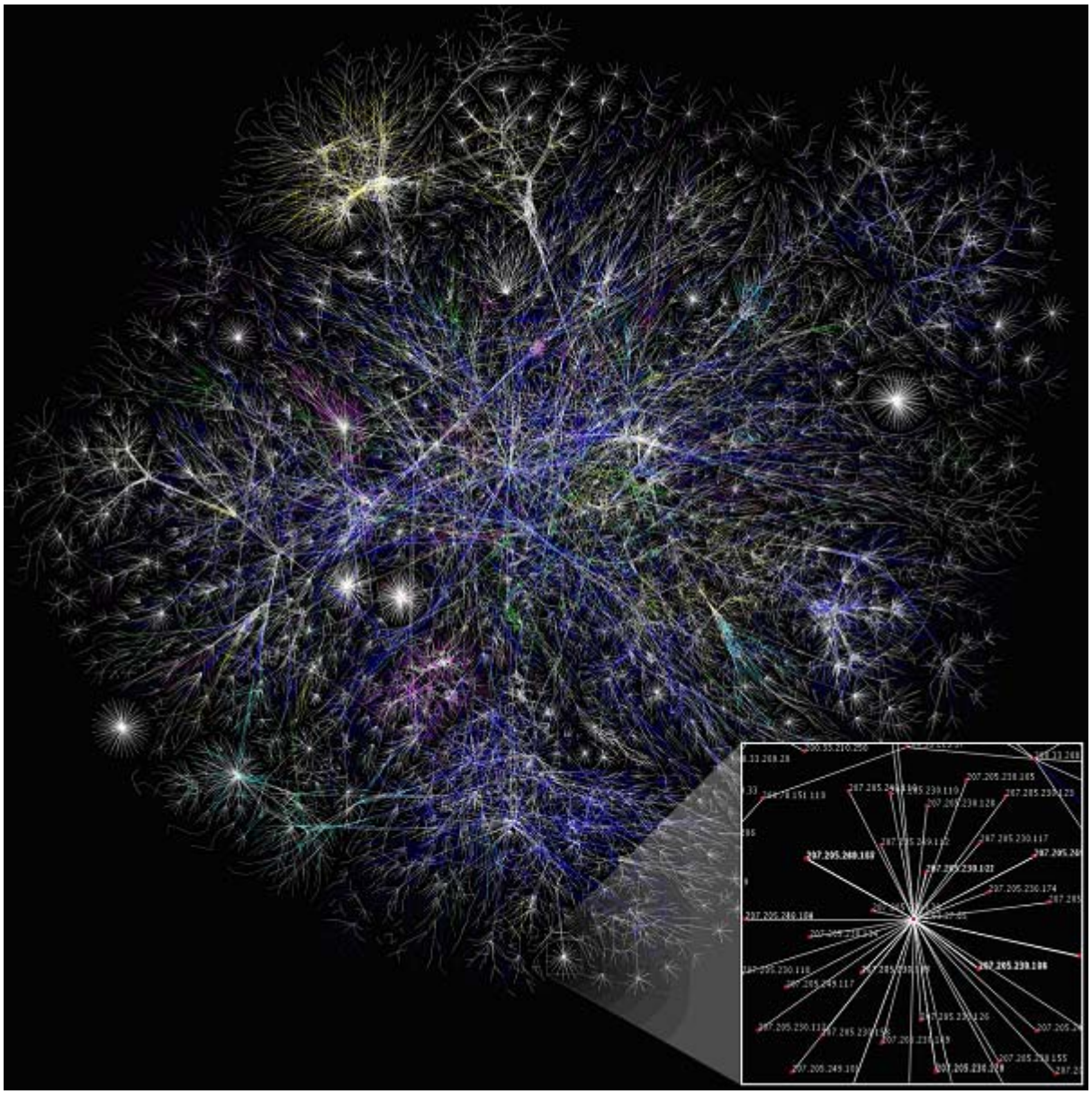
Obr. 1.5: Autonomní systémy a jejich propojování pro vytvoření globální datové sítě

Směrem k vyšším úrovním autonomních systémů dochází ke koncentraci provozu se zaměřením na pouhý tranzit provozu s co nejvyšším přepojovacím a přenosovým výkonem. Mezi operátory tak vznikají vztahy:

- **nižší k vyššímu** – poskytovatel sítě nižší úrovně platí poskytovateli vyšší úrovně za tranzit dat,
- **vyšší k nižšímu** – poskytovatel vyšší úrovně dostává zaplaceno od provozovatelů napojených sítí nižší úrovně (zákazníků),
- **rovný s rovným** – vznikají další propojení označované jako peeringové spoje vytvářející polygonální strukturu sítě, kdy si poskytovatelé sítí stejné úrovně navzájem bezplatně poskytují výměnu a transport provozu směrem k cíli za účelem:
    - snížení nákladů za transport dat – všechna data nejsou přenášena přes operátora sítě vyšší úrovně,
    - zvýšení redundance v konektivitě – snížení nebezpečí „odříznutí“ operátora od zbytku sítě při výpadku jednoho spoje,
    - zvýšení propustnosti sítě daného operátora směrem do globální sítě,
    - možnost rozkládání zátěže,



Obr. 1.6: Propojení poskytovatelů přístupu k Internetu



Obr. 1.7: Pokus o vytvoření mapy Internetu, zdroj
http://en.wikipedia.org/wiki/Computer_network

1.4 Základní typy telekomunikačních sítí

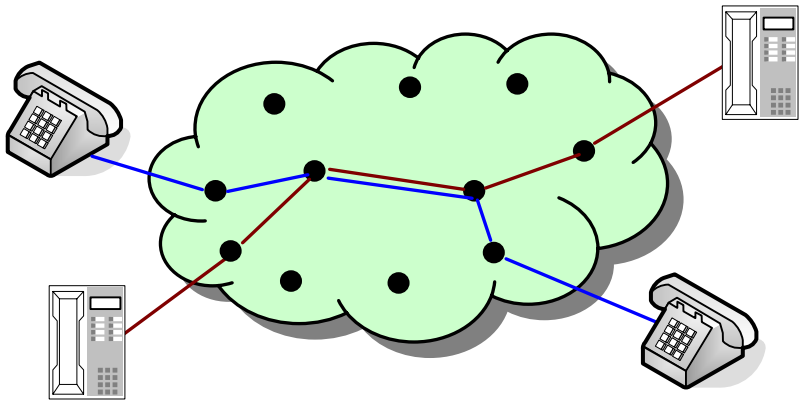
Telekomunikační sítě lze rozdělit do dvou základních skupin podle toho, jakým způsobem se realizuje předávání dat mezi koncovými uzly:

- sítě se **spojováním fyzických okruhů**,
- sítě s **přepojováním datových jednotek**.

Každý z uvedených typů má své přednosti, ale také i nevýhody. Kromě přepojovaných komunikačních technik ještě existují také **permanentní (pevné) okruhy**, které existují stále, a nedochází tedy k jejich sestavování a rušení. Jejich výhodou je stálá dostupnost síťových prostředků, nevýhodou pak je vysoká cena pronájmu pevného spoje.

1.4.1 Sítě se spojováním fyzických okruhů

V sítích se spojováním fyzických okruhů se mezi koncovými uzly služby před vlastním přenosem informace sestavuje **fyzický okruh** (komunikační kanál tam i zpět), viz Obr. 1.8, kde okruh představuje soubor přenosových, spojovacích a výpočetních prostředků pro zajištění obousměrného přenosu dat mezi koncovými aplikacemi.



Obr. 1.8: Princip sítí se spojováním fyzických okruhů

V tomto typu sítě lze provozovat pouze spojově orientované služby. Sestavený fyzický okruh je vyhrazen pouze pro daný spoj a je k dispozici po celou dobu existence spojení. Prostředky sítě jsou tedy obsazeny bez ohledu na to, zda se v daný okamžik přenáší či nikoli. Výhodou tohoto řešení je, že síťové prostředky jsou vždy k dispozici, čehož výsledkem je malé a téměř konstantní zpoždění přenosu informace sítí, což je vhodné pro služby v reálném čase (přenos řeči, videa, vzdálené řízení systémů). Nevýhodou naopak je, že v případě výpadku libovolného spojovacího či přenosového prvku na cestě spojení dojde k přerušení spojení, případně i k ukončení služby, k nutnosti spojení znovu navazovat a v případě neošetření i opakovat přenos od samotného počátku. Další nevýhodou, a to dosti podstatnou, je neefektivní využití prostředků sítě, neboť prostředky sítě jsou vyhrazeny, i když nejsou právě využívány. Nejmarkantněji se to projevuje v přístupové části kabelových sítí se spojováním okruhů, každé koncové zařízení musí mít vlastní vedení dosahující až k místní ústředně. Přístupové sítě tak tvoří nejnákladnější část celé sítě. Přitom procentuální využití účastnického vedení je ve většině případů minimální. Například přenos hovoru je víceméně poloduplexní přenos, kdy v daný okamžik jeden uživatel mluví a druhý poslouchá, čímž je kanál pro opačný směr přenosu nevyužitý. Nemůže však být poskytnut jinému přenosu, pokud to není dosti složitým způsobem jinak řešeno. Navíc i řeč nepředstavuje spojitý tok informace a při standardním typu kódování „tvaru vlny“ (standard ITU-T G.711) se signál z mikrofonu stále vzorkuje a kóduje, ať už uživatel hovoří či ne. Tedy generuje se tak vysoce redundantní datový tok. I řečový signál samotný je značně redundantní, a při současných technikách zpracování signálů může být komprimován s relativně vysokým stupněm komprese (viz řada doporučení G.728, G.729, G.723) vyžadující i méně než jednu desetinu přenosové kapacity ve srovnání se standardem ITU-T G.711. Avšak zavedení nových kompresních technik do stávající sítě se spojováním fyzických okruhů je problematické, protože kapacita základního kanálu je pevná a výsledná kapacita je jeho násobkem. Tudíž by při zavedení účinnějšího způsobu zdrojového kódování bylo velmi komplikované a nákladné využít zbývající kapacitu přiděleného kanálu, a ve většině případů by tak zůstala ušetřená kapacita kanálu nevyužitá. Zavedení nového způsobu kódování by tak pro operátora představovalo výdaje, které by se mu nevrátily. Také zavádění nových služeb do sítě se spojováním fyzických okruhů je obtížné, zvláště je-li potřeba jiných přenosových kapacit (nižších i vyšších), nebo vytvářet

vícebodová spojení, či je-li potřeba doplnit síť o nové prvky pro zajištění funkčnosti dané služby, (například přenos dat, faximilních zpráv, realizace konferencí, aj.).

Příkladem tohoto typu sítí je analogová telefonní síť či síť ISDN (Integrated Services Digital Network).

Základní vlastnosti sítí s přepojováním fyzických okruhů lze shrnout takto:
výhody:

- **stálá dostupnost síťových prostředků** po sestavení spojení do jeho ukončení,
- **minimální a konstantní zpoždění** přenosu informace,

nevýhody:

- počáteční zpoždění přenosu - nutnost **sestavování fyzických okruhů** před vlastní komunikací,
- pouze **pro služby orientované na spojení**,
- **neefektivní využití prostředků sítí**,
- **nepružnost sítě** ke změnám, zavádění nových služeb a nových technik zpracování signálů,
- **nízká odolnost sítě** proti výpadkům spojů a uzlů – výpadek způsobí rozpad spojení a nutnost navazování nového spojení.

1.4.2 Sítě s přepojováním datových jednotek

Základní vlastností sítí založených na principu přepojování datových jednotek je sdílení síťových prostředků, a to již od samotného koncového zařízení, které často umožňuje provozování více typů komunikačních služeb současně, sdílejí se komunikační kanály mezi jednotlivými uzly sítě, i výkon přepojovacích uzlů, viz Obr. 1.9. Za tímto účelem sítě s přepojováním datových jednotek přenášejí uživatelská i řídicí data v datových blocích, které pro přenos sítí nesou různé identifikační údaje, především informaci o cíli a zdroji, případně i o cestě sítí. Dalšími informacemi může být typ přenášených dat, parametry pro řízení toku dat, a další. Některé z těchto informací jsou zpracovány v přepojovacích uzlech a datová jednotka je odeslána přes daný výstupní port dalšímu přepojovacímu uzlu či koncovému zařízení. Přitom platí, že daný přenosový kanál je sdílen mezi mnoha přenosy. V daný okamžik je samozřejmě posílána jedním kanálem pouze jedna datová jednotka. Princip sdílení přináší jak výhody, tak i problémy.
Mezi **výhody** patří:

- **efektivní využívání síťových prostředků** – když jedna služba negeneruje datové jednotky, jsou síťové prostředky k dispozici pro obsluhu toků dalších služeb;
- **robustnost sítě vzhledem k výpadkům** – preferuje se nespojovaný charakter transportu datových jednotek a dynamický způsob určování cest k cílovým sítí a zpravidla existuje více cest, které nefunkční část nahradí a nedojde tak k výpadku služeb),
- **větší pružnost sítě k nasazení nových technik zpracování signálů a nových služeb**,
- **nižší náklady na síť** pro stejnou úroveň provozu, tedy **nižší cena za službu**.

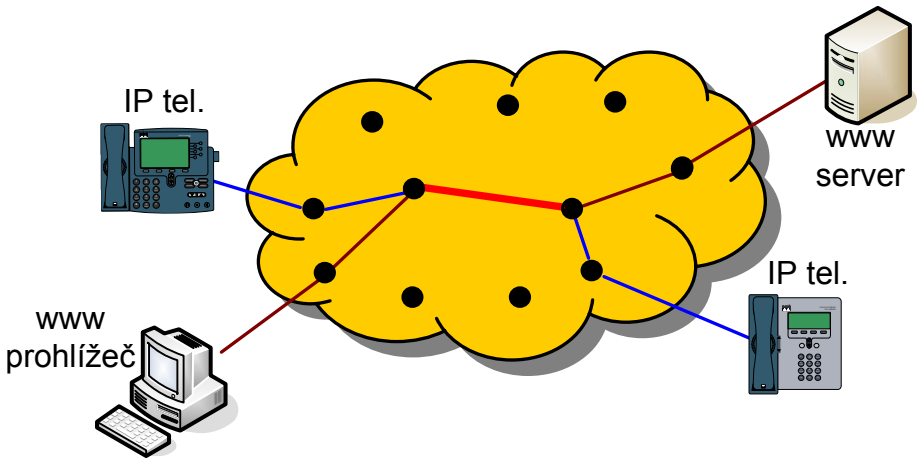
Mezi **problémy** z důvodu sdílení patří:

- **větší zpoždění** doručování datových jednotek,
- **proměnlivost zpoždění** – tzv. jitter,

- **nutnost diferenciace toků** dle služeb a **prioritizace** toků služeb citlivých na zpoždění a jeho proměnlivost - bez další podpory nevhodnost tohoto typu sítí pro služby v reálném čase (konverzační služby),
- **nebezpečí nedostupnosti síťových zdrojů** - kolize či zahlcení síťových uzlů -> ztráta datových jednotek,
- **zahození celé datové jednotky** i z důvodu jednobitové chyby v případě použití pouze detekčních protichybových kódů pro zabezpečení datové jednotky,
- **navýšení režie přenosu** – datové jednotky musí obsahovat informace zajišťující správné doručení dat do cíle,
- nutnost řešit případný problém **doručování datových jednotek mimo pořadí**, nebo jejich **násobné doručení**,
- **nižší úroveň bezpečnosti** komunikace,

Existuje několik forem přepojování datových jednotek:

- **s přepojováním zpráv** – přepojuje se celá zpráva. Jedná se pouze o teoretickou možnost, která se pro přenos uživatelské informace nepoužívá, neboť délka uživatelské zprávy se může měnit od několika bajtů až po obrovské objemy dat o velikosti řádu GB či TB, což by vyžadovalo obrovské vyrovnávací paměti v přepojovacích uzlech, a také by při přenosu zprávy byl porušen princip sdílení síťových prostředků, neboť by objemná zpráva na dlouhou dobu obsadila síťové prostředky (přenosový kanál, spojovací uzel, aj.),
- **s přepojováním segmentů zpráv** – zpráva se ve zdrojovém koncovém zařízení rozdělí na menší části (segmenty), které se vybaví potřebnými informacemi pro cestu sítí a v cílovém koncovém zařízení dojde k opětovnému složení původní zprávy. Přenášejí se tedy pouze části zpráv (v případě krátké zprávy i celá), jejichž délka je limitována sítí a při cestě sítí může případně dojít i k dalšímu dělení datových jednotek na menší části. Patří sem přepojování
  - **paketů** – k přepojování dochází na síťové vrstvě. Délka paketu je proměnlivá. Příkladem může být síť Internet,
  - **rámců** – k přepojování dochází na spojové vrstvě. Délka rámce je proměnlivá. Příkladem mohou být sítě Ethernet a Frame Relay,
  - **buněk** – k přepojování dochází na spojové vrstvě. Délka datové jednotky je konstantní. Příkladem je síť ATM.



Obr. 1.9: Princip komunikace s přepojováním datových jednotek

Podle způsobu přepojování můžeme rozlišit sítě s

- **datagramovou službou** - datové jednotky nesou úplnou směrovací informaci pro cestu sítí. Přenosová síť mívá mřížovou strukturu, takže většinou existuje k cíli řada cest. Přepojovací uzly obsahují přepojovací tabulky, které se mohou dynamicky měnit se změnou stavu sítě a podle nich se rozhodují, kam bude datová jednotka přepojena. Datové jednotky jediné relace tedy mohou jít k cíli různými cestami, které jsou různě dlouhé a obsahují různě rychlé segmenty a jsou různě zatížené. Výsledkem jsou různá zpoždění průchodu datových jednotek sítí a případně i různé pořadí příchodu datových jednotek k cílovému koncovému zařízení.
- **virtuálními okruhy** - před vlastním přenosem uživatelských dat je zjištěna optimální cesta k cíli a ve vybraných přepojovacích uzlech jsou uloženy informace o výstupním portu pro daný přenos. Daným úsekům spoje je přidělen identifikátor, a v přepojovací tabulce je vytvořen záznam a tím určeno, na který port má být datová jednotka přicházející na určitý vstup a s určitým identifikátorem okruhu přepojena, a jaký identifikátor virtuálního okruhu dalšího úseku má být vložen do záhlaví odesílané datové jednotky. Všechny datové jednotky jdou v případě bezporuchového provozu jedinou vytyčenou cestou a do cíle přichází ve správném pořadí. Řídicí informace datových jednotek nesoucí uživatelskou informaci je jednodušší než v případě datagramové služby (tedy s přenosem se pojí nižší režie). Zpoždění také vykazuje menší proměnlivost než je tomu u datagramové služby. Nevýhodou je spojovaný charakter komunikace, problém výpadku přepojovacího uzlu, a tím rozpadu řady virtuálních okruhů, které nefunkčním uzlem procházejí.

1.5 Vývoj telekomunikačních sítí

Počátek vývoje telekomunikačních sítí se klade do konce první poloviny 19. století, přesněji do roku 1844, kdy se uskutečnil první přenos telegrafní sítí na spoji mezi lokalitami Washington a Baltimore.

Později pak přišly na řadu i sítě telefonní, jejichž hlavní službou je přenos řeči. Tento typ sítě se díky mnoha technologickým inovacím zkvalitňujícím poskytovanou hovorovou službu a díky rozšiřování nabídky různých doplňkových služeb udržel až dodnes. Telefonní sítě založené na různých technologiích spojování se označují jako generace nultá až čtvrtá (podrobněji skripta věnovaná spojovací technice):

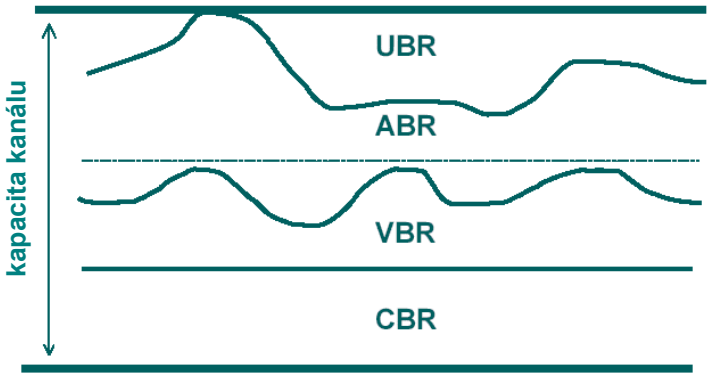
- manuální,
- voličové,
- s křížovými spínači,
- s kódovými spínači,
- s maticovými spínači,
- plně elektronické analogové,
- plně elektronické digitální.

Všechny výše uvedené typy jsou založené na technice spojování fyzických okruhů, což přináší problémy (viz. kap. 1.4.1) při zavádění nových služeb a technologií ve zpracování signálů a při přechodu k integrovaným sítím. Problémy s tím spojené se řešily různými způsoby:

- **přizpůsobením stávající sítě** – byla vyvinuta speciální zařízení, která umožňovala nasazení nové služby. Příkladem může být vznik modemů pro přenos dat po analogové telefonní síti.
- **vytvoření nové sítě pro danou skupinu služeb** – tak vznikly datové (počítačové), rozhlasové a televizní sítě
- **návrh integrovaných sítí** – vytvoření sítě umožňující přenášet informace různých typů služeb a snadno a efektivně se adaptovat na vznik nových služeb a technik ve

zpracování informace. Prvním pokusem byla **úzkopásmová síť ISDN** (N-ISDN = Narrowband Integrated Services Digital Network), jejíž návrh zahrnoval především část realizující přenos pomocí technologie spojování fyzických okruhů, i když se počítalo i s podporou paketové technologie X.25. Doporučení ITU-T X.31 specifikuje použití paketového přenosu po D-kanálu. Díky nepružnosti technologie X.25 se paketový způsob přenosu dat však nikdy v sítích ISDN příliš nerozšířil. Doporučení X.31 bylo implementováno pouze v několika zemích – Velká Británie, Francie a Japonsko. U okruhově orientované části sítě ISDN však přetrvávaly výše uvedené nevýhody sítí s přepojováním fyzických okruhů. Ukázalo se, že integrovaná síť budoucnosti musí být založena na technologii přepojovaní datových jednotek, ve které bude implementována podpora rozmanitých typů služeb (i s ohledem na budoucnost), tzn. že datové toky služeb budou diferencovány dle typu služby (tzv. třídy služeb), a datové jednotky budou přepojovacími uzly obsluhovány s různou prioritou tak, aby byly dodrženy technické parametry, které služba pro svůj hladký průběh (a tedy spokojenost uživatele) vyžaduje = podpora QoS (Quality of Service). Onou spásnou technologií a univerzální sítí měla být síť **ATM** (Asynchronous Transfer Mode). ATM síť podporuje různé třídy služeb, viz. Obr. 1.10. Standardy však byly vytvářeny specialisty z oblasti klasických telekomunikací, a proto nezahrnuly všechny potřebné aspekty datových přenosů specifické pro přenos dat, se kterými se dnes setkáváme v počítačových sítích. Základními nevýhodami sítí ATM, které způsobily, že se příliš neujala (až na páteřní sítě a sběrné sítě ADSL provozu), jsou:

- složitost, vysoká cena,
- spojovaný charakter přenosu – nevyhovuje standardnímu nespojovanému principu přenosu dat v počítačových sítích,
- neposkytuje vícesměrové a všesměrové vysílání zpráv,
- problematické přizpůsobení výše uvedeným požadavkům klasických počítačových sítí.



Obr. 1.10: Třídy QoS implementované v síti ATM a rozdělení kapacity kanálu těmto třídám

CBR – Constant Bit Rate,
VBR – Variable Bit Rate,
ABR – Available Bit Rate,
UBR – Unspecified Bit Rate

Zatímco u sítí ATM se předpokládalo, že klasické telekomunikace pohltí i oblast počítačových sítí, v současnosti je tomu naopak, kdy klasické telekomunikační služby, kam patří především hovorová služba, jsou postupně integrovány do počítačových sítí (dnes díky konvergenci technologií a integraci služeb označované jako **datové sítě**), založených na

principu přepojování datových jednotek a využívající protokolovou sadu TCP/IP. Datové sítě sice nebyly navrhovány pro služby, jako přenos hovoru či videa, zato však mnohem efektivněji využívají síťové prostředky a jsou mnohem adaptabilnější pro případné změny. To znamená, že vznikají standardy, které vnášejí do datových sítí podporu těchto služeb v podobě funkčních uzlů služby (pro telefonní službu např. telefonní server, telefonní datový terminál, telefonní brány, konferenční jednotka), řídicích (signalizačních) protokolů a podporu požadavků na QoS (techniky IntServ, DiffServ – viz dále) a umožňují napojení datových sítí na sítě telefonní - ISDN, mobilní - GSM,UMTS, a další. V datových sítích tak pro jednotlivé služby vznikají tzv. **překryvné sítě** (angl. overlay networks) vytvářející logické funkční spoje mezi jednotlivými funkčními uzly služby.

1.6 Telekomunikační služby

1.6.1 Členění telekomunikačních služeb

Pojem telekomunikační služba byl definován v kap. 1.2. Telekomunikační služby lze rozdělovat dle řady hledisek, nejobecnějším se jeví rozdělení na:

- **základní** – poskytují uživateli přenos základního druhu informace (například řeči),
- **doplňkové** – jsou doplňkem některé ze základních služeb a zvyšují tak komfort služby základní (například informace o čísle volajícího – CLIP – Calling Line Identification Presentation),
- **speciální** – jedná se o nestandardní služby pro specializované aplikace (hotelové služby, centra volání, nemocniční systémy, apod.).

Základní služby

Základní služby můžeme dále dělit na:

- **přenosové služby** - daná síť pouze zprostředkovává přenos obecných dat sítí,
- **relační služby** - uživatel služby navazuje s protějším koncovým uzlem spojení či obecněji relaci. Specifikace služeb zahrnuje i popis protokolů vyšších vrstev, tedy i co a v jakém formátu se přenáší. Sem patří například telefonní, videotelefonní, faximilní, teletex - přenos textu podle kódovací abecedy; služba přenosu souborů; služby uchování zpráv; služby sběru dat; služby vyhledávání informací, např. video na vyžádání, videotex, atd.;
- **podavatelské služby** - spojová organizace zprostředkovává uživateli i obsluhu koncového zařízení, např. veřejný telegraf, postfax - zasílání faximilní zprávy, apod.;
- **distribuční služby** - informace je šířena přenosovým prostředím nezávisle na uživateli - například televizní vysílání, rozhlasové vysílání, Teletext.

Pozn. Hrubším rozdělením základních služeb může být na **přenosové** (**transportní**) služby, kdy síť pouze poskytne transport obecných dat (nespecifikuje se obsah), a na **(telematické**, kdy popis služby zahrnuje i obsah a formu přenášené informace (např. hlas s kódováním G.711 A-law).

Doplňkové služby

Jak už z názvu vyplývá, doplňkové služby jsou služby poskytované jako doplněk ke službě základní a vyznačují se následujícími rysy:

- zvyšují komfort základní služby,
- nemohou být poskytovány samostatně,
- jeden typ doplňkové služby může být poskytován k více základním službám

Příklady doplňkových služeb mohou být:

- opakovaná volba,
- zkrácená volba,
- přímá volba - vybudování spojení s nastaveným koncovým zařízením pouhým zvednutím mikrotelefonu,
- provolba do pobočkových systémů,
- upozornění účastníka na příchod druhého hovoru,
- přesměrování hovorů
    - bezpodmínečné,
    - volaný neodpovídá,
    - volaný obsazen,
    - selektivní přesměrování podle tlf. čísla
- omezení hovorů v odchozím či příchozím směru,
- a mnohé další

Speciální služby

Speciální služby jsou služby poskytované na zvláštní přání zákazníka, například:

- hotelové a nemocniční systémy,
- dveřní systémy, elektronický vrátný,
- propojení se zabezpečovacími systémy, poplachové služby střežení objektů,
- dohledové systémy,
- dálkové ovládání zařízení po síti,
- záznamové, informační a objednací systémy, hlasové schránky a hlasová pošta, faxové schránky,
- podpora bezdrátových sítí,
- apod.

Každá telekomunikační služba je charakterizována sadou **atributů**, které mohou být rozděleny do několika skupin

- **funkční** – podstata služby,
    - ***typ*** – základní, doplňková, speciální,
    - ***obsah*** – hovor, videokonverzace, statický obraz, obecná data, informace o čísle volajícího, atd.
    - ***způsob řízení realizace služby*** – účastnická, podavatelská, distribuční služba,
    - ***stupeň mobility*** – pevná, bezšňůrová, mobilní pozemní, mobilní satelitní,
- **technické** – technické prostředky pro zajištění služby,
    - ***forma*** – typ zdrojového kódování obsahu a přenosový formát datových jednotek,
    - ***požadavky na technické zajištění služby*** = podpora kvalitativních požadavků služeb **QoS** (Quality of Service) pro zajištění parametrů, kam se především řadí:
        - potřebná přenosová rychlost (průměrná, maximální) – může být i různá pro různé směry přenosu,
        - maximální akceptovatelné zpoždění a jeho proměnlivost (jitter),
        - akceptovatelná chybovost (ztrátovost) sítě,
        - další parametry – například pořadí doručování datových jednotek, maximální velikost datové jednotky, požadavek na specifikaci

informace o formátu aplikačních dat, možnost doručení i chybných jednotek, priorita zahození datových jednotek, apod.

- **procedurální** – procedury realizace služby,
  - ***realizovatelnost služby*** – v čase, prostoru, rychlost zahájení služby, jednoduchost realizace služby, spolehlivost běhu služby,
  - mechanizmus zahájení, udržení a ukončení služby,
  - řešení nestandardních situací při realizaci služeb
- **administrativní** – řešení přístupu ke službě, poplatky za službu, apod.
  - autorizace uživatelů služeb,
  - zpoplatnění služeb - cena za jednotku (dobu, objem) služby,
  - zabezpečení přenášených dat proti neoprávněnému přístupu – proti odposlechu a změně

1.6.2 Požadavky telekomunikačních služeb a jejich uživatelů na síť a provozovatele

V definici pojmu Telekomunikační služba v kap. 1.2 je stanoveno, že telekomunikační systém (koncová zařízení a síť) musí pro úspěšné nasazení a komerční provozování služeb zajistit určitá opatření technického, provozního a organizačního charakteru, aby se zajistila požadovaná kvalita služby, a tím i spokojenost uživatelů – zákazníků telekomunikačního operátora.

Základní požadavky uživatelů telekomunikačních služeb na provozovatele služeb jsou:

- **věrnost přenášené informace** – informace je sítí přenesena bezchybně nebo s přijatelnou chybovostí či zkreslením a s přijatelným zpožděním a jeho změnami v rámci jednoho přenosu. Tato pravidla se zahrnují do tzv. „**sémantické**“ a „**časové transparence**“,
- **bezpečnost přenášené informace** – zajištění informace proti neoprávněnému přístupu za účelem jejího odposlechu či dokonce změny,
- **dostupnost služby** (prostorová a časová) – zahrnuje přístup ke službě prostoru a čase,
- **obtížnost realizace služby** - z časového hlediska a z hlediska náročnosti obsluhy koncového zařízení,
- **spolehlivost služby** – nízká poruchovost prostředků zajišťující činnost služby,
- **cena služby** – velmi důležitý parametr, který může rozhodnout o úspěchu či neúspěchu zavedení dané služby.
- dostupnost **zákaznické podpory**.

1.6.3 Ochrana proti zkreslení přenášené informace vlivem reálných vlastností přenosové cesty – sémantická transparence

Zajištění sémantické transparence spočívá v zajištění takových podmínek přenosu informace, aby nedošlo k jejímu nepřijatelnému zkreslení. Telekomunikační služby jsou různě citlivé na různé úrovně narušení přenášeného obsahu. Přijatelnou úrovní zkreslení přenášené informace je taková úroveň, při které především nedojde vlivem narušení k chybnému porozumění (vyhodnocení) vyslané informace (například srozumitelnosti řeči a schopnosti identifikovat mluvčího u telefonní služby) nebo i k výraznému poklesu spokojenosti uživatele s přijímaným obsahem vlivem jeho narušení (sledování videa či poslouchání hudby).

Například služby přenosu řeči či videa v nekomprimované podobě či s nízkým stupněm komprese jsou k úrovni značně tolerantní (až 10^{-3}), zatímco služba přenosu obecných dat vyžaduje chybovost víceméně nulovou, čehož v reálných podmínkách nelze dosáhnout, a proto je zapotřebí realizaci služby doplnit o zabezpečovacími mechanizmy pro detekci a opravu chyb.

1.6.3.1 Zdroje zkreslení a chyb přenášeného obsahu

Nosičem informace v telekomunikační síti je elektromagnetický signál, jehož průběh je při přenosu měněn vlivem:

- přenosové charakteristiky kanálu (modulové a fázové) jednotlivých úseků spoje,
- šumu přenosového kanálu,
- přeslechů ze sousedních kanálů,
- vnějších zdrojů rušení, jako jsou impulzní rušení z výbojů v atmosféře, z energetické sítě, ze silových rozvodů, z neodrušených strojů, apod.,
- nelineárního zkreslení při činnosti obvodů v nelineární oblasti (například vlivem přebuzení obvodů),
- nedokonalé impedanční přizpůsobení vstupů a výstupů uzlů impedanci komunikačního kanálu,
- apod.

V analogových systémech je hlavním kritériem odstup signál/šum či v časové oblasti tvarové zkreslení signálu.

V digitálních systémech jsou důležitými pojmy **bitová** a **paketová chybovost** (BER – bit error rate a PER – packet error rate)

Bitová chybovost je především důležitá pro digitální přenosy s nepřetržitým datovým tokem (přenos hlasu, videa, apod.) a je vyjádřena vztahem

$$\mathrm{BER} = \frac{\text{počet chybných bitů}}{\text{počet všech přenesených bitů}}$$

Paketová chybovost vyjadřuje poměr chybných paketů ku celkovému počtu přenesených paketů. Lze to vyjádřit vztahem

$$\mathrm{PER} = \frac{\text{počet chybných paketů}}{\text{celkový počet odeslaných paketů}},$$

přičemž chybnými pakety se myslí, že

- přijatý paket obsahoval chyby,
- paket nedošel do cíle do stanoveného okamžiku,
  - byl zahozen cestou sítí z důvodu chyby či zahlcení přepojovacího prvku,
  - byl směrován jinam z důvodu chyby ve směrovací informaci či chyby přepojovacího prvku,
- násobné přijetí paketu,
- přijetí cizího paketu.

Samozřejmě chybovost může být způsobena především poruchou či podstatnou změnou parametrů libovolného prostředku použitého pro realizaci telekomunikační služby, ale také chybným návrhem sítě. Sem lze zařadit

- použití nevhodné kabeláže,
- chybné propojení sítě,
- překročení maximální povolené délky kabeláže,
- impedanční nepřizpůsobení prvků přenosového řetězce,
- nevhodná výkonová úroveň signálu,
- poddimenzování síťových prvků (přenosové rychlosti komunikačního kanálu), kapacity přepojovacích prvků,

- chybná konfigurace síťových prvků,
- nekompatibilita síťových prvků,
- chybný řídicí software,
- apod.

1.6.3.2 Ochrana proti chybám

Zabezpečení přenosu informace proti chybám může probíhat na různých úrovních komunikačního systému. V počátcích datových sítí byl kladen důraz na to, aby se o bezchybný přenos starala síť. Příkladem je paketová síť X.25. Bylo třeba implementovat zabezpečení (detekce chyb a jejich oprava) již na linkové úrovni. To se však se zvyšováním kvality přenosových médií, s vývojem moderních modulačních a kódovacích technik, s rozvojem moderních výrobních technologií a s nárůstem provozu v síti ukázalo jako neudržitelné, neboť zabezpečení s sebou neslo velké množství režie (potvrzování, uchování odeslaných a nepotvrzených dat v paměti, kontrola časových limitů, opakování přenosu a další). To bránilo zvyšování propustnosti sítě. Proto v současnosti se zodpovědnost za bezchybný přenos přesouvá na koncové uzly a síť se pouze snaží o přenos s co nejnižší chybovostí („best effort“). Toto snažení spočívá v:

- použití co nejlepších přenosových technik – modulace, synchronizace,
- testování kvality spojení před vlastním přenosem, i v jeho průběhu (především u rádiových sítí),
- zabezpečení a detekce chyb v datových jednotkách – aby se zbytečně nepřenášely datové jednotky s chybami, chybné datové jednotky se zahazují,
- korekční mechanizmy – pro automatickou opravu chyb v
    - datových jednotkách při přenosu krátkých datových jednotek v kanálech s relativně vysokou pravděpodobností chyb (například při radiovém přenosu),
    - hlavičkách datových jednotek - oprava nízkobitových chyb pro zabránění nesprávného přepojování datových jednotek,

V případě výskytu a detekce chyby při přenosu datové jednotky sítí je nejčastější reakcí zahození datové jednotky a přenechání opravy této události na koncová zařízení. Síť se tedy snaží být co nejrychlejší. To vyžaduje dostatečné přepojovací kapacity spojovacích uzlů, neklade to však nároky na velké vyrovnávací paměti uzlů.

Ochrana proti chybám v koncových zařízeních se může nacházet na různých úrovních použitého vrstvového modelu (viz popis referenčního modelu ISO/OSI). Nejčastěji se to řeší na úrovni transportní vrstvy, jenž odpovídá první vrstvě nad vrstvami sítě. Na této úrovni se kontroluje, zda nedošlo při přenosu k chybě či zda přišly všechny datové jednotky, zda není přísun datových jednotek příliš rychlý vzhledem k rychlosti jejich zpracování a na základě vyhodnocení dochází k žádosti o opakování a případně k regulaci datového toku. Z výše uvedených faktů vyplývá, že mechanizmus zabezpečení je vysoce spolehlivý, avšak přináší velké množství režie a navíc se často pojí se spojovanou službou. Výsledkem je pomalejší služba bez možnosti vícesměrového a všesměrového předávání dat. Služba je tedy vhodná pro bezpečný dvoubodový přenos nezanedbatelného množství informace. V rámci některých služeb se však přenáší relativně málo dat, a pravděpodobnost chyby je proto velmi nízká. O to důležitější však bývá rychlost přenosu a rychlost odezvy a případná možnost současného vícesměrového předávání dat. Využije se tedy rychlá avšak nespolehlivá transportní služba a případná oprava chyb se přenechá na vyšších vrstvách, jakými jsou relační, presentační či aplikační (pokud je to zapotřebí).

Vlastní zabezpečení proti chybám se tedy řeší pomocí:

- korekčních (samoopravných) kódů – např. konvoluční kódy, turbo kódy, Reed-Solomonovy kódy, BCH kódy, aj.
- detekčních kódů (např. cyklických kódů) doplněných o mechanizmus potvrzování či žádání o opakování (systémy ARQ – Automatic Repeat reQuest).

1.6.4 Zpoždění, latence, časová transparence

Latence systému je termín odrážející **reakční čas** (odezvu) systému, což je doba mezi okamžikem vstupu elementu zprávy do systému (jednotkový impulz u analogového systému, symbol u digitálního systému zpracovávajícího symbol po symbolu nebo paket u datové sítě pracující na bázi přepojování paketů) a okamžikem objevení se reakce na výstupu ze systému (u paketové datové sítě to znamená příjem paketu v cílovém bodě).

V telekomunikační síti pojmem **latence sítě** je specifikována **doba reakce telekomunikační sítě**. Zde je možno tento pojem dále dělit na:

- **latenci řízení** znamenající *prodlevu* určité *řídicí procedury* způsobenou přenosem a zpracováním řídicích zpráv (například doba od vyslání žádosti na přidělení zdrojů do přijetí zprávy od sítě o přidělených síťových zdrojích, doba potřebná na provedení autentizace, doba mezi odesláním čísla volaného a přijetím kontrolního vyzváněcího tónu, apod.), a
- **latenci aplikační** znamenající *dobu přenosu elementu zprávy* s aplikačními daty (telekomunikační služby) mezi koncovými zařízeními na úrovni rozhraní mezi síťovou a transportní vrstvou

Dále ještě můžeme hovořit o **latenci end-to-end**, či latenci na aplikační úrovni, která zahrnuje i odezvu koncových zařízení.

Velmi často nás zajímá rychlost odezvy od cílového koncového uzlu, neboli **zpoždění ve smyčce**, tzv. **Round Trip Time** (RTT) či **Round Trip Delay** (RTD) zahrnující dobu přenosu zprávy ze zdrojového koncového uzlu sítí k cílovému uzlu, dobu zpracování zprávy systémem cílového uzlu, dobu vygenerování odezvy a dobu jejího přenosu zpět do zdrojového uzlu.

Pokud se velikost elementu zprávy mění, pak je výsledkem i jiná hodnota latence, i když jsou podmínky v síti naprosto stejné. Je to z důvodů kombinace sériového přenosu elementu po datových spojích (tzv. serializační zpoždění), a sériového a paralelního zpracování elementu zprávy v mezilehlých přepojovacích prvcích, tj. když element zprávy je na nižších vrstvách komunikačního systému rozdělován do více menších částí, které jsou postupně (sériově) přenášeny. Tak tomu například je u rádiové přístupové části mobilních sítí, kdy se paket dělí na více bloků tvořící rámce a ty pak jsou rozděleny dále na fyzické vrstvě do více fyzických rámců obsahující symboly tvořené daným modulačním schématem a případně i kódovým schématem, pak záleží na rychlostech přenosu zprávy jednotlivými spoji a rychlosti zpracování zpráv v přepojovacích i koncových uzlech. Tzn. čím kratší zpráva, tím kratší hodnoty latence se u datových sítí dosáhne.

Pokud je zkoumána latence pouze části sítě, pak její hodnota by měla být měřena pro element zprávy, který je danou částí sítě zpracováván jako celek (například u přístupové části mobilní sítě GPRS by to byl RLC blok).

Zpoždění přenosu zprávy je *doba přenosu celé zprávy* (dopředu připravené a uložené na paměťovém médiu) mezi koncovými aplikacemi a zahrnuje celkový čas od zahájení vysílání až do doby přijetí poslední datové jednotky zprávy v cílovém uzlu. U větších zpráv, např. řádově MB a více, má pak latence specifikující dobu přenosu jedné datové jednotky sítí na celkovém zpoždění celkem zanedbatelný vliv.

Zpoždění telekomunikační služby (Doba trvání telekomunikační služby) je doba *od aktivace služby až po její ukončení*, a zahrnuje tedy

- fázi přístupu k telekomunikační síti,
- žádost o poskytnutí služby a sestavování relace,
- přenos zprávy,
- potvrzení úplnosti přenosu,
- ukončení relace,
- uvolnění vyhrazených síťových prostředků.

Časová transparence v telekomunikační síti znamená zajištění přijatelných hodnot zpoždění transportu datových jednotek sítí (latence sítě) a jeho změn při přenosu informace sítí vzhledem k typu telekomunikační služby. Existují různé druhy služeb, které jsou různě citlivé na hodnotu zpoždění při přenosu a na proměnlivost tohoto zpoždění během přenosu. Například tzv. **služby v reálném čase**, kam patří telefonní a videokonferenční služby a služby dohledu řízení procesů, vyžadují co nejmenší latenci spoje (např. pro telefonní službu má být zpoždění < 150 ms pro jeden směr) a případně, aby bylo navíc konstantní, tzn. aby datové jednotky přicházely do cíle v pravidelných okamžicích a ve správném pořadí. Pokud je příchod datových jednotek nepravidelný, je třeba přenosový řetězec doplnit vyrovnávací pamětí, která však vnáší do přenosu další díl zpoždění. Naproti tomu například služba přenosu datových souborů není citlivá na hodnotu zpoždění ani na jeho variabilitu.

Z hlediska hodnoty a proměnlivosti zpoždění rozlišujeme:

- ***Pevné spoje*** – výhodou je stálá dostupnost spoje, tedy:
  - **minimální zpoždění před zahájením přenosu** aplikačních dat – není třeba sestavovat fyzický spoj, případně je pouze třeba sestavit relaci mezi aplikačními entitami.
  - **nízké a konstantní zpoždění** po dobu přenosu aplikačních dat, dané dopravním zpožděním, a tedy závislé na délce pevného spoje.
- ***Komutované spoje na bázi fyzických okruhů***
  - **zpoždění sestavením fyzického spoje před zahájením přenosu** aplikačních dat – nutné sestavení fyzického okruhu a navázání spojení. Jakmile vznikne požadavek na přenos dat, je zahájeno budování spojení a poté případné ověření komunikujících uzlů. Pak teprve může nastat přenos uživatelské informace. Po přenosu dojde k ukončení spojení a uvolnění vyhrazených síťových prostředků. Nevýhodou je zpoždění zahájení přenosu vlivem budování spojení.
  - **nízké a konstantní zpoždění** po dobu přenosu - zpoždění šířením elektromagnetického signálu přenosovým prostředím a zpoždění zpracováním informace v koncových a přepojovacích uzlech, a v transportních systémech. Zpoždění je tedy závislé na délce cesty mezi koncovými uzly sítě (na případném použití satelitní stanice) a na počtu přepojovacích uzlů a pohybuje se od desítek μs (spojení na krátké vzdálenosti v rámci místní ústředny) až po stovky ms (spojení přes satelit).
- ***Komutované spoje na bázi přepojování datových jednotek*** – zde mohou vzniknout dva druhy zpoždění, a to **při vytváření spoje** a **při vlastním vysílání aplikačních dat**, a proto je třeba rozlišovat:
  - **spojově orientované přenosy** - před vlastním přenosem se navazuje spojení, tedy zpoždění sestavení spojení. Uplatňují se tedy oba druhy zpoždění.
  - **nespojově orientované přenosy** – datové jednotky se vysílají do sítě bez navazování spoje a ověřování připravenosti cílového uzlu na příjem dat. Uplatňuje se tedy pouze druhý typ zpoždění.

U spojově orientovaných služeb může být zpoždění způsobeno:

- **zpoždění sestavením virtuálního okruhu** – pouze u sítí na bázi virtuálních okruhů,
- **zpoždění sestavením logického spojení před zahájením přenosu** aplikačních dat – vytvoření relace a domluva na parametrech přenosu,
- zpoždění přenosu datových jednotek

Co se týče zpoždění vlastního přenosu datových jednotek sítěmi s přepojováním datových jednotek, pak je třeba rozlišit:

- **zpoždění na virtuálním okruhu** – nižší a méně proměnná hodnota zpoždění
- **zpoždění v sítích s datagramovou službou** – zpravidla vyšší a více proměnná hodnota zpoždění

Co se týče detailnějšího rozboru zdrojů zpoždění v současných telekomunikačních sítích, tedy především datových sítí, pak je dále třeba rozlišovat, jestli se jedná o **službu v reálném čase** (viz definice v kap. 1.2) a nebo nikoli.

U **služeb neprobíhajících v reálném čase** se data nejprve připraví (zakódují, zkomprimují, případně i zašifrují) a uloží do paměti, a pak teprve se aktivuje služba přenosu, a proto je zpoždění před odesíláním dáno rychlostí načtení potřebného množství dat z paměti a vytvořením datové jednotky, která může být dostatečně velká, aby byl zajištěn příznivý poměr režijních informací vůči aplikačním datům. Například datová jednotka služby VoIP (Voice over IP) využívající transportní protokol UDP (User Datagram Protocol) nad IP a přenášená technologií Ethernet bude vykazovat režii alespoň 54 B (8B_UDP+20B_IP+18B_MAC_Ethernet+8B_PhPream_Ethernet).

U **služeb v reálném čase** data vznikají teprve v průběhu vedení relace, v případě získávání dat z okolí koncového uzlu musí dojít k převodu snímané veličiny (například akustického tlaku u řečového signálu) na elektrický signál, a u digitálních systémů se dále provádí vzorkování, kvantování a kódování vzorků. Vzniká zde relativně mále **zpoždění konverze**. Teprve až se nasbírá dostatečné množství vzorků dat pro zpracování v ***kodéru zdroje*** a pro naplnění datové jednotky s přijatelným poměrem režijních a aplikačních dat, tak se zahájí příprava k vyslání datové jednotky.

Například doporučení ITU-T G.711 je kodérem tvaru vlny, tzn., že se každý vzorek signálu řeči kóduje nezávisle na ostatních. Vzorkovací kmitočet je 8 kHz a délku slova 8 bitů, což vytváří čistý datový tok 64 kb/s. Tedy zpoždění kódováním je cca 125 μs (převod hodnoty vzorku do kódového slova je velice rychlý). U moderních způsobů kódování řeči, jako jsou kodeky dle doporučení ITU-T G.718, G.719, G.729, G.723.1 aj., je paketizační zpoždění několikanásobně větší, protože se jedná o parametrické kodéry, a pro výpočet parametrů řečového traktu mluvčího je zapotřebí nasbírat vzorky z úseku řeči určité délky, bývá to úsek 10, 20 i 30 ms. Teprve poté může být spuštěn proces zdrojového kódování. Zpoždění vlastního procesu kódování závisí na výpočetním výkonu kodéru a může činit i jednotky ms. Tento proces spolu se sběrem dat vytvářejí tzv. **algoritmické zpoždění**. Výsledná hodnota algoritmického zpoždění může pro kvalitní způsob kódování přesáhnout i 40 ms (http://www.itu.int/net/itu-t/sigdb/speaudio/Gseries.htm).

Vytvoření datového bloku vkládaného do datové jednotky vyvolá zpoždění, které se označuje jako „**paketizační**“. Velikost tohoto zpoždění závisí na velikosti datového bloku, vzorkovacím kmitočtu a typu zdrojového kódování (vyznačuje se kompresním poměrem, a výpočetní náročností). Například pro délku datového bloku 100 B a nekomprimovaný přenos řeči podle dop. G.711 (64 kb/s - vzorkovací kmitočet 8 kHz a délku slova 8 bitů) je zpoždění způsobené vzorkováním a kódováním dáno vztahem (1.1)

$$\delta_p = \frac{1}{8000} 100 \text{ s} = 12{,}5 \text{ ms} . \quad (1.1)$$

Při výběru parametrických kodeků pro kódování řeči se pak ještě specifikuje, kolik kódových bloků se bude vkládat do jednoho paketu, čímž se hodnota zpoždění násobí.

Tedy čím delší datová jednotka, tím větší paketizační zpoždění. Z hlediska služby v reálném čase je vhodnější kratší datová jednotka, což však znamená, že velkou část datové jednotky tvoří služební informace. Z hlediska provozovatele je naopak nejvhodnější co nejdelší část datové jednotky nesoucí uživatelská data vzhledem k celkové délce datové jednotky, neboť uživatel platí převážně za přenos uživatelské informace (platí-li podle objemu přenesených dat a ne podle doby připojení).

Určité zpoždění také vznikne, než je plně vybavená datová jednotka vybavena všemi potřebnými služebními (řídicími) informacemi a předána k přenosu podvrstvě přístupu k přenosovému kanálu. Označme si toto zpoždění jako **zpoždění přípravou datové jednotky** δ_w (w – wrap).

Je-li přenosový kanál sdílen s dalšími stanicemi, nebo s dalšími síťovými aplikacemi ve stejné stanici, musí být sdílení ošetřeno určitou přístupovou metodou, jejímž výsledkem je přidělení síťových zdrojů a odeslání datové jednotky. Metod řízení přístupu ke sdílenému médiu existuje celá řada. V datových sítích je dělíme do dvou skupin - statické a dynamické (ta druhá skupina nás zajímá) – viz. kapitola 3.4 o přístupových metodách. Dynamické metody pak dále dělíme na deterministické a stochastické. Například nejpoužívanější síť Ethernet používá stochastickou metodu CSMA/CD (podrobněji viz kapitola o sítích Ethernet). V mobilních sítích s podporou paketového přenosu dat (služba GPRS) se zase používá centralizovaná metoda poskytování zdrojů na žádost. Dobu (zpoždění), než se stanice dostane k úspěšnému odvysílání datové jednotky si označme jako **zpoždění přístupu** δ_a (a – access).

Jsou-li přiděleny síťové zdroje, je zahájeno vysílání datové jednotky. Doba od zahájení vysílání jednotky do kanálu do okamžiku odeslání posledního symbolu datové jednotky se označuje jako **serializační zpoždění** δ_{sr} (sr – serialization). Tato doba je závislá na velikosti datové jednotky, a bitové rychlosti spoje (počtu bitů na symbol, symbolové rychlosti a počtu paralelních kanálů).

Dalším zdrojem zpoždění jsou přepojovací uzly sítě. Tyto uzly pracují na linkové či síťové vrstvě (viz model ISO/OSI). Nejdříve musí přepojovací prvek přijmout alespoň část datové jednotky, aby získal informace potřebné pro přepojení. V případě vysoké úrovně provozu není datová jednotka obsloužena ihned, ale ukládá se do vstupní vyrovnávací paměti. Je-li paměť zaplněna, jsou příchozí datové jednotky zahazovány, nebo je aktivována některá z metod řízení provozu. Jakmile datová jednotka je zpracovávána prvek případně kontroluje, zda je přijímaná jednotka v pořádku či zda se nejedná o nedoručitelnou jednotku. Tedy, zda ji má dále někam přepojovat nebo zahodit a případně poslat chybovou zprávu. Pokud je jednotka bezchybná a doručitelná, následuje vyhledání směru (výstupního portu). V určitých případech (směrovače, přepínače sítí s virtuálními okruhy) navíc dochází k modifikaci záhlaví datové jednotky, na což se opět spotřebuje určitý čas. Pak se přepojovací uzel pokusí vyslat datovou jednotku na zjištěný port. Tím, že jsou přenosové cesty v paketových sítích sdíleny mezi mnoha službami, přepojovací prvek často nemůže okamžitě přepojit datovou jednotku do daného směru a ukládá jednotku do výstupní vyrovnávací paměti. V současnosti se do přepojovacích prvků začínají implementovat mechanismy pro zajištění požadované kvality služeb, které se zajišťují pomocí přednostního zpracování datových jednotek s vyšší prioritou.

Má-li datová jednotka nižší prioritu, musí čekat, než jsou zpracovány jednotky s vyšší prioritou. Zpoždění vyvolané průchodem přepojovacími prvky si označme jako **zpoždění přepojováním** δ_{sw} (s - switching).

V cílovém koncovém zařízení pak dochází k depaketizaci a blok uživatelských dat je předán aplikačnímu procesu. Zpoždění předání se označuje jako **depaketizační zkreslení** δ_u (u - unwrap).

Pokud daná služba požaduje pravidelný přísun dat, jsou datové bloky ukládány nejprve do vyrovnávací paměti a odtud v pravidelných okamžicích vybírány ke zpracování a k převodu do vhodného tvaru (řeč, hudba, video, …). Velikost vyrovnávací paměti a základní doba zpoždění by měla být volena tak, aby nedošlo k „podtečení“ ani „přetečení“ paměti. Zpoždění si označme jako **zpoždění bufferováním** δ_b (b - buffering).

Někdy se k výše uvedeným zpožděním přidává i zpoždění zpracováním v koncovém zařízení, a to jak ve zdrojovém, tak i cílovém. Jedná se o dobu převodu informace z/do originálního tvaru (například akustický signál nesoucí hlas) do/z elektrického a dále digitálního formátu. Toto zpoždění může nabývat i relativně značných hodnot (i desítky ms) u multifunkčních koncových zařízení (počítačů) vybavených obyčejnými zvukovými a grafickými adaptéry (kartami) a provozující velký počet aplikací žádající strojový čas hlavního procesoru koncového zařízení. Označme si toto zpoždění jako δ_c (c - conversion).

Celkové zpoždění je tedy dáno vztahem

$$\delta = \delta_{cs} + \delta_p + \delta_w + \delta_a + \sum_j \delta_{swj} + \sum_i \delta_{sri} + \sum_k \delta_{tk} + \delta_u + \delta_b + \delta_{cd} \tag{1.2}$$

kde

δ_{cs} – zpoždění převodem do digitálního tvaru ve zdrojovém koncovém zařízení,
δ_p – paketizační zpoždění,
δ_w – zpoždění přípravy kompletní datové jednotky,
δ_a – zpoždění přístupu k přenosovému kanálu,
δ_{sr} – serializační zpoždění,
δ_{sw} – zpoždění přepojováním v uzlech sítě,
δ_t – zpoždění šířením elektromagnetického signálu po vedeních a v elektrických obvodech přenosových a spojovacích zařízení,
δ_u – depaketizační zpoždění,
δ_b – zpoždění ukládáním do vyrovnávací paměti,
δ_{cd} – zpoždění převodem do zdrojového tvaru v cílovém koncovém zařízení.

Z výše uvedených skutečností vyplývá, že sítě s přepojováním datových jednotek vykazují větší a proměnlivější latenci přenosu datových jednotek. Proměnlivost zpoždění je způsobena především dynamickými změnami stavu vytížení síťových prostředků podél trasy, kudy jsou data v rámci trvání dané relace přenášena. To se odrazí především ve změně zpoždění zpracování datových jednotek v přepojovacích prvcích, ale může k tomu dojít i v samotných koncových uzlech s jedním aktivním přístupem k síti a provozující současně více výpočetně náročných, případně i síťově velmi aktivních aplikací. Dalším důvodem proměnlivosti zpoždění u datagramových služeb může být průchod datových jednotek různými trasami.

V datových sítích přepojujících datové jednotky bez ohledu na typ služby, jejichž data jsou v datové jednotce přenášena, se při vyšším zatížením některého z úseků podél trasy služby v síti může snadno stát, že pro služby citlivé na zpoždění (služby v reálném čase) může

celková hodnota zpoždění překročit akceptovatelnou hodnotu, což způsobí degradaci kvality služby. Pro zabránění či spíše pro minimalizaci tohoto jevu (stoprocentně tomu zamezit nelze) je zapotřebí implementovat klasifikační mechanizmy rozdělující tok dle tzv. tříd služeb do prioritních front a přednostně zpracovávat datové jednotky s vysokou prioritou.

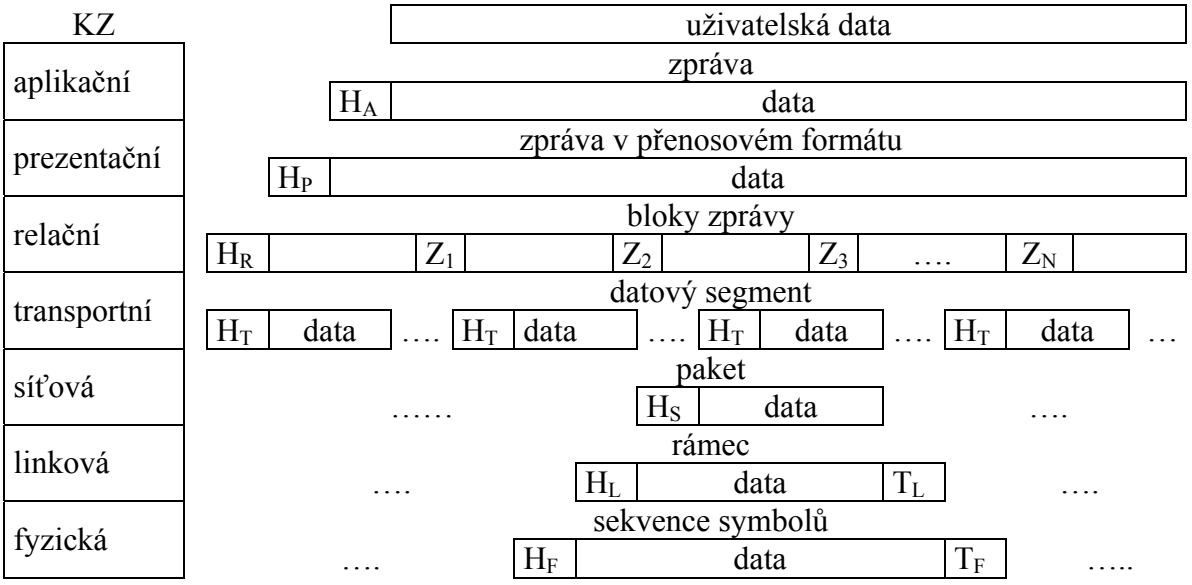
2 Vrstvová síťová architektura

Řešení problému komunikace mezi vzdálenými uzly ležící v různých sítích a používající různé architektury a způsoby zpracování informace je velice komplikovaný úkol, který nemůže být řešen jako jeden celek. Ani to není žádoucí z hlediska flexibility systému vůči implementaci změn v komunikačním systému (nové techniky, nové technologie, nové služby).

2.1 Vrstvy síťových architektur

Aby řešení komunikace v telekomunikačních sítích bylo snadnější a flexibilní, používá se architektura sestávající ze sady vrstev, kde každá vrstva řeší související sadu problémů. **Vrstvová architektura** nespecifikuje konkrétní řešení jednotlivých částí komunikačního řetězce, pouze definuje okruh funkcí každé vrstvy. Ve vrstvové architektuře platí, že **nižší vrstva poskytuje služby vrstvě vyšší**.

Obr. 2.1 ukazuje jednotlivé vrstvy referenčního modelu označovaného jako ISO/OSI (levá část obrázku) a průchod uživatelských (aplikačních) dat vrstvami (pravá část obrázku). Je zde znázorněno, jak jsou uživatelská data postupně kódována (komprimována, šifrována), doplňována režijními informacemi pro obnovení původního formátu dat v cílovém koncovém uzlu, informacemi pro správné směrování dat přes telekomunikační síť, informacemi pro zabezpečení dat proti chybám; a také jak jsou uživatelská data dělena na menší části, aby byl správně zajištěn princip sdílení síťových prostředků, tj. aby data jedné relace obsadila síťové prostředky pouze na krátkou dobu.



Obr. 2.1: Průchod uživatelských dat jednotlivými vrstvami vrstvového modelu koncového zařízení

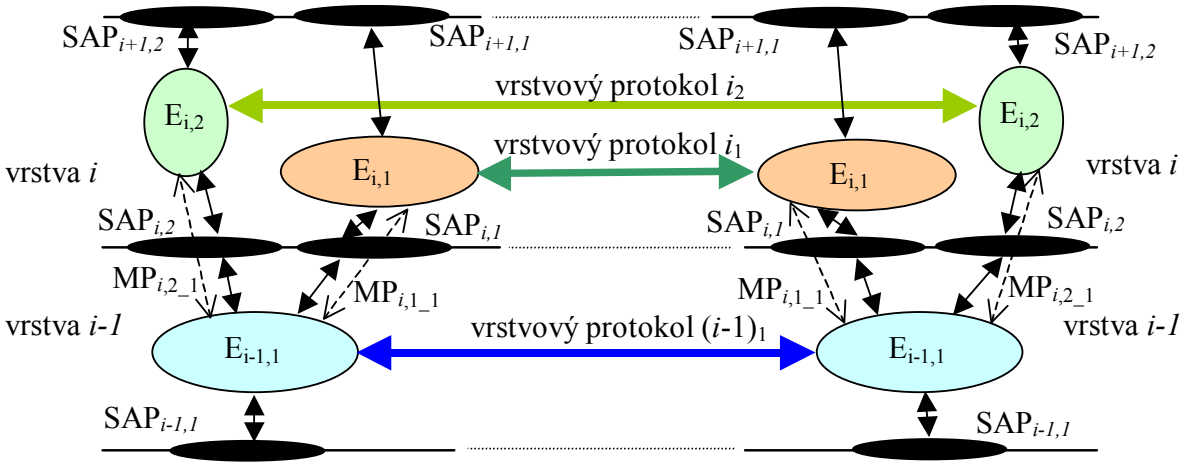
KZ – koncové zařízení,
H_X – záhlaví datové jednotky ve vrstvě X,
T_X – zakončení datové jednotky ve vrstvě X,
Z_i – značky v datech pro pokračování přenosu dat po obnově ztraceného spojení.

Funkce dané vrstvy jsou zajištěny pomocí funkčních jednotek, kterým se říká **entity**. Entita může mít buď softwarovou nebo hardwarovou podobu. V případě softwarové formy se jedná o instanci procesu nebo o jeho část (sdružuje-li proces více funkcí). Hardwarové řešení entity je voleno u nižších vrstev, nejčastěji u fyzické či linkové vrstvy. Na **Obr. 2.2** je zachycen příklad realizace architektury vrstev ve dvou vzájemně komunikujících uzlech a funkčních entit v těchto vrstvách a uzlech, a vztahy mezi nimi. Jak je ukázáno na obrázku, na jedné vrstvě se může vyskytovat více entit, pomocí nichž se funkce jedné vrstvy diferencují. Příkladem může být transportní vrstva TCP/IP, na které kralují dva protokoly TCP a UDP. Protokol TCP poskytuje spolehlivou spojově orientovanou transportní službu a protokol UDP zase nespojovanou a nespolehlivou transportní službu. Oba dva typy služeb jsou vhodné pro určitý okruh aplikací. Platí, že jedna entita určité vrstvy může nabízet služby více entitám vyšší vrstvy a naopak entita vyšší vrstvy může využívat služeb více entit nacházejících se ve vrstvě nižší. Rozdělení na vrstvy a specifikace komunikačního rozhraní mezi vrstvami pak umožňuje modifikaci entit dané vrstvy nezávisle na ostatních vrstvách.

Mezi entitami vrstvového systému probíhá komunikace, a to dvojího typu:

1. **mezi entitami sousedních vrstev** – komunikace je specifikována tzv. „***mezivrstvovým protokolem***“ a probíhá přes „***přístupový bod služby***“ (SAP – Service Access Point). Nejznámějším příkladem přístupového bodu je port v architektuře TCP/IP. Komunikace mezi entitami sousedních vrstev se řídí pomocí „***služebních primitiv***“ řadící se do několika skupin:
   a. žádosti,
   b. odpovědi,
   c. oznámení,
   d. potvrzení.

   Přenášené zprávy se označují jako „***služební datové jednotky***“ (SDU – Service Data Unit).
2. **mezi entitami odpovídajících vrstev** – komunikace je určena (***vrstvovými***) ***protokoly***. Předávané zprávy se označují jako „***protokolové datové jednotky***“ (PDU – Protocol Data Unit) a sestávají ze dvou či případně tří částí (viz Obr. 2.1):
   - **hlavička** – nese řídicí informace pro entitu stejné vrstvy protějšího systému
   - **vlastní data** – data předaná nadřazenou vrstvou, která se také skládají z těchto částí
   - **zakončení** – bývá přítomno pouze u datových jednotek některých vrstev, nejčastěji se jedná o linkovou vrstvu, kde zakončení nese například zabezpečovací informaci nebo informaci o převzetí jednotky cílovou stanicí apod.



Obr. 2.2**: Entity ve vrstvách a komunikace mezi nimi**

$E_{i,j}$ – entita *j* na *i*-té vrstvě,
$SAP_{i,j}$ – přístupový bod *j* služby mezi vrstvami *i* a *i*-1,
MP_{i,j_k} – mezivrstvový protokol mezi entitou *j* v *i*-té vrstvě a entitou *k* v *i*-1vrstvě.

2.2 Protokol

Protokol je sada komunikačních pravidel mezi entitami sousedních vrstev či entitami odpovídajících vrstev (viz **Obr. 2.2**). Pravidla jsou specifikována:

- **formátem předávaných datových jednotek** – struktura datové jednotky a funkce jednotlivých polí,
- **funkčními procedurami** – procedury navazování, udržení či rušení spojení, sestavování a odesílání datových jednotek, příjmu, kontroly, potvrzování a předávání datových jednotek, řešení standardních i chybových situací, apod.
- **parametry komunikace** – maximální, minimální či konstantní hodnoty určitých veličin jako jsou časové limity, počet opakování, maximální délka datové jednotky, apod.

Stavový protokol – protokol, u kterého se dialog může nacházet ve více stavech komunikace. V případě výskytu události se mění stav výkonné jednotky (procesu). Tyto stavy vyjadřují situaci v rámci dané komunikace. Výhodou stavových protokolů je, že v případě přerušení spojení a uchování stavových informací a opětovném navázání spojení může komunikace pokračovat od bodu, kdy byla přerušena. Nevýhodou je složitější řízení, neboť se musí stavová data ukládat a v případě ztráty komunikace se musí určit, jak dlouho se tyto stavové informace mají ještě podržet, co udělat s otevřenou relací (například ukončit a návrat - „reset“ procesu do výchozího stavu) a co udělat v případě obnovení spojení.

Bezestavový protokol – protokol, který při příchodu události provede odpovídající akci a vrátí se do původního stavu. Výhodou je jednodušší implementace protokolu a bezproblémové řešení nestandardních stavů, naopak nevýhodou je v případě přerušení a následném obnovení spojení potřeba začít vše úplně znova, což je nevýhodné pro přenosy větších objemů dat.

Nejběžnějšími síťovými architekturami jsou:

- TCP/IP,
- SNA,
- ISO/OSI,
- XNS (IPX/SPX).

2.2.1 Služby z hlediska spolehlivosti a orientace na spojení

Služby poskytované entitami na dané vrstvě lze nehledě na vrstvu, ve které jsou umístěny, posuzovat podle dvou hledisek:

- spolehlivost přenosu informace,
- orientace na spojení.

Podle toho rozlišujeme služby na:

- spolehlivé a nespolehlivé,
- spojované a nespojované.

Nespolehlivé služby – služby, které nezajišťují spolehlivý přenos dat, tzn. že nejsou vybaveny mechanizmy na zajištění správnosti a úplnosti přijatých dat v případě výskytu chyby. Pokud jsou vybaveny určitým zabezpečovacím kódem, pak pouze pro rozpoznání

chybných datových jednotek a zabránění jejich dalšímu šíření, a tím zbytečnému obsazování síťových zdrojů. Výhodou je jednoduchost implementace služby, nevýhodou je přesun „odpovědnosti“ za správnost doručování do některé z nadřazených entit vyšších vrstev.

Spolehlivá služba – služba zaručující v rámci svých zabezpečovacích schopností bezchybnost přenosu svěřené informace. Výraz „v rámci svých zabezpečovacích schopností“ zde znamená, že pravděpodobnost úspěšného a bezchybného doručení nikdy není stoprocentní. Například, selže-li přípojné vedení cílového koncového zařízení v kabelové síti, žádná telekomunikační služba nic nezmůže. Zabezpečení se děje na úrovni:

- **bitové** – zajišťuje se, že jsou všechny bity datové jednotky správné (korekcí = FEC nebo opakováním přenosu = detekce + ARQ),
- **blokové** – datové jednotky jsou číslovány a obdařeny identifikátorem spojení, podle čehož se rozezná, zda jednotka chybí, zda stejná jednotka přišla vícekrát, či zda se jedná o jednotku jiného spojení,
- **zpráv** – zpráva musí mít určitý formát, aby její data mohla být správně interpretována.

Nespojovaná služba – služba, při které se pro přenos informace nevytváří spojení. Proces „odesílatel“ při odeslání zprávy neví, zda je proces „adresát“ vůbec dostupný. Datové jednotky, na které je zpráva rozdělena, musí být plně vybaveny směrovacími i přídavnými informacemi (doba života, kvalitativní parametry, pozice ve zprávě, apod.) pro cestu sítí. Výhodou je možnost hromadného rozesílání zpráv a vyšší rychlost služby. Nevýhodou pak menší pravděpodobnost bezchybného doručení zprávy.

Spojovaná služba – služba, při které se před přenosem uživatelské informace vytváří spojení a po přenosu se opět ruší. Celá komunikace tedy sestává ze tří fází:

- sestavení spojení,
- vlastní přenos a udržování spojení,
- ukončení spojení.

Fáze navazování spojení poskytuje řadu možností:

- zjistit dostupnost adresáta,
- autentizovat komunikující strany,
- sjednat parametry komunikace – režim komunikace, identifikace spojení, velikost datových jednotek, způsob zabezpečení přenášených dat, apod.

Fáze vlastního přenosu řeší vlastní přenos aplikačních dat a činnosti spojené s udržením spojení. Fáze poskytuje větší možnosti potvrzování a opravování dat, řízení komunikace, řešení nestandardních situací, udržování informací o stavu přenosu, apod.
Fáze ukončení spojení pak slouží k potvrzení přenosu celé zprávy a uvolnění síťových zdrojů.

Nevýhodou spojované služby je větší složitost (funkce navázání, udržování a ukončení spojení) a tedy nižší rychlost služby, a nemožnost jednoduchého hromadného rozesílání dat. Výhodu je větší pravděpodobnost doručení dat a lepší využití přenosové kapacity sítě.

Výše dvě uvedené skupiny bývají spojovány do kombinací:

- ***nespojovaná a nespolehlivá služba*** – služba nerealizuje spojení ani neřeší problém opravy chyb v uživatelských datech. Příkladem může být protokol IP (Internet Protocol) protokolové sady TCP/IP. Výhodou je velká rychlost a relativní jednoduchost služby.
- ***spojovaná a spolehlivá služba*** – služba řeší jak problematiku spojení, tak i opravu chybně přenesených dat. Příkladem může být protokol TCP (Transmission Control Protocol) protokolové sady TCP/IP

Při kombinaci spojované a spolehlivé služby se jako mechanizmy zabezpečení přenosu spojí zabezpečení proti chybám v datových jednotkách a jednak proti ztrátě spojení, což zvyšuje výslednou pravděpodobnost úspěšného transportu informace a úspěšnosti celé služby. tato kombinace je vhodná pro přenos většího objemu dat, kdy vyšší režie přenosu je vyvážena vysokou pravděpodobností úspěchu hned na první pokus.
Naopak kombinace nespojované a nespolehlivé služby se využívá především tam, kde je kladen důraz na rychlost.

2.2.2 Referenční model ISO/OSI

Referenční model ISO/OSI (International Organization for Standardization / Open System Interconnection) je nejznámější vrstvový model komplexně popisující síťovou architekturu. Představuje abstraktní model reálného otevřeného systému. Model je definován mezinárodní normou ISO IS 7498 (přijata v roce 1984) a řadou doporučení ITU-T X.200.

Jedná se o **sedmivrstvý** hierarchický model zachycený v levé části Obr. 2.1. Model umožňuje i vytváření podvrstev, což se využilo především u lokálních počítačových sítí. Pravá část obrázku zachycuje průchod zprávy jednotlivými vrstvami a označení datových jednotek na jednotlivých vrstvách. Referenční model sestává z následujících vrstev (od nejnižší až po nejvyšší):

- **fyzická vrstva** – řeší úkol jak efektivně a bezpečně přenést data pomocí elektromagnetického nosného signálu konkrétním fyzickým prostředím,
- **linková** (**spojová**) **vrstva** – řeší komunikaci mezi sousedními uzly v síti, doručování datových jednotek – rámců (adresaci), řídí průběh linkového spoje (jeho navazování, udržení, ukončení), multiprotokolovou podporu a zabezpečení dat,
- **síťová vrstva** – základní funkcí je doručování (směrování) datových jednotek (paketů) v heterogenním síťovém prostředí,
- **transportní vrstva** – řeší transparentní komunikaci mezi koncovými uzly (end-to-end komunikace), podporuje současný běh více síťových aplikací a případně řeší spojovaný a bezchybný charakter komunikace,
- **relační vrstva** – řeší průběh dialogů (navázání, udržení a ukončení) mezi aplikacemi,
- **prezentační vrstva** – řeší formát prvků zprávy (znaků, číslic, grafických prvků, zvuku) a připadnou kompresi či šifrování,
- **aplikační vrstva** – obsahuje entity implementující protokoly síťových aplikací (www, e-mail, přenos souborů, přenos hlasu a videa po datových sítích a mnoha dalších)

Fyzická a linková vrstva jsou technologicky závislé a společně specifikují konkrétní síťovou technologii, například Ethernet, ATM, Token Ring, a další.

2.2.3 Vrstvy, dílčí funkce a jejich podoba v různých typech sítích

2.2.3.1 Fyzická vrstva

Fyzická vrstva je nejnižší vrstvou modelu a zabývá se tedy vlastním přenosem informace fyzickým prostředím prostřednictvím elektromagnetického signálu. Je specifikována parametry:

- mechanickými,
- elektrickými,
- funkčními,

- procedurálními.

- **Mechanické parametry** – určují mechanické vlastnosti fyzického prostředí, kterým se šíří elektromagnetický signál. Patří sem:
  - typ přenosového prostředí
    - vlnovodné (kabelové) – metalické, optické kabely, vlnovody
    - bezdrátové (rádiové, optické)
  - vlastnosti přenosového prostředí
    - typ kabelu, materiál kabelu, počet a průměr vodičů, ochrana kabelu, pravidla pokládky kabelů, konstrukční prvky pro rozvody kabelové sítě,
    - nároky na strukturu bezdrátového prostředí – nutnost přímé viditelnosti, prostupnost přes překážky
    - maximální délka kabelu, či maximální dosah bezdrátového spoje
  - vlastnosti rozhraní - tvar, materiál, velikost
    - kabelové - konektory a zapojení jednotlivých vodičů,
    - rádiové - antény a jejich typ,
    - optické - optické vysílače a detektory.

- **Elektrické (optické) parametry** – určují vlastnosti elektromagnetického signálu jako nosiče dat.
  - přenosové prostředí
    - primární parametry - permitivita, permeabilita prostředí, měrný odpor či vodivost, v případě metalických kabelů měrný svod, měrná kapacita, měrná indukčnost,
    - sekundární parametry – charakteristická impedance, fázová rychlost šíření signálu médiem, skupinové zpoždění,
    - směrovost spoje, vícecestné šíření, vidy
  - přenosové pásmo – parametry kanálu
    - v základním pásmu
      - bez potlačení ss složky,
      - s potlačením ss složky,
    - v přeneseném pásmu,
    - kmitočtová šířka kanálu,
    - kmitočtová charakteristika kanálu,
    - šumové poměry v kanálu,
    - způsob šíření signálu,
  - parametry signálu
    - typ signálu – analogový nebo digitální,
    - výkonové úrovně,
    - skramblování, prokládání
    - kódování a modulace – analogová a digitální,
    - polarizace,
    - zajištění bitové a blokové synchronizace,
    - přenosová rychlost.

- **Funkční parametry**
  - význam signálů jednotlivých vodičů, párů, vláken, případně určitých symbolů ve fyzickém rámci - datové a řídicí kanály, symboly pro řízení fyzického spojení (pro bitovou a rámcovou synchronizaci, aktivaci, a deaktivaci fyzického spoje, apod.),
  - typ přenosu

    - synchronní,
    - asynchronní – vkládání synchronizační směsi (preambule), zajištění minimální mezery mezi rámci
- způsob řešení duplexního provozu – oddělený prostorově, kmitočtově, časově, pomocí vidlice a potlačovače ozvěn,
- řešení multiplexů datových toků (Data Flow Multiplexing) pro efektivní využití dostupné přenosové kapacity daného spoje, po kterém je třeba přenášet více toků od více přispěvatelů (zdrojů). Tento problém na fyzické vrstvě řeší **multiplexní zařízení** (multiplexor) mající více vstupů a jeden vysokorychlostní výstup, do jehož přenosové kapacity jsou jednotlivé toky sdružovány.
    - **prostorový** multiplex
        - ***na kabelových spojích*** – každému dílčímu toku je přidělen jeden vodič (dvojice vodičů v případě symetrického přenosu) či jedno optické vlákno.
        - ***v bezdrátovém prostředí*** – pomocí technologie **MIMO** (Multiple Input Multiple Output) – pomocí více vysílacích a přijímacích rádiových řetězců (antén) lze za předpokladu statistické nezávislosti (nekorelovanosti) jednotlivých kanálů šíření pomocí kódování přenášet současně ve stejném pásmu více paralelních toků, které lze na straně přijímače od sebe oddělit. Efektivitu prostorového multiplexu lze vyjádřit veličinou označovanou jako multiplexní zisk.
    - **kmitočtový** multiplex (FDM – Frequency Division Multiplex),
    - **časový** multiplex (TDM –Time Division Multiplex),
    - **statistický** časový multiplex (STDM – Statistical Time Division Multiplex),
    - **kódový** multiplex (CDM – Code Division Multiplex),
    - **ortogonální** kmitočtový multiplex (OFDM – Orthogonal Frequency Division Multiplex).
- funkce zabezpečení, kódování, skramblování, prokládání a detekce symbolů a bitů, modulace, synchronizace.

- **Procedurální parametry**
    - identifikace obsazenosti fyzického spoje = tzv. detekce nosné (u sdíleného prostředí),
    - aktivace fyzického spoje – nastavení parametrů přenosu – přenosová rychlost (u systémů umožňující více rychlostí přenosu), nastavení ekvalizérů kanálu, nastolení bitové a rámcové synchronizace,
    - udržení fyzického spoje – udržení synchronizace, přenos značek signalizujících aktivitu fyzického spoje,
    - deaktivace fyzického spoje – pro úsporu energie v době, kdy se nic nepřenáší,
    - regenerace a rozbočení signálu – v zesilovačích, ekvalizérech, opakovačích, rozbočovačích.

Fyzická vrstva někdy bývá rozdělována do podvrstev řešících dílčí úkoly, jako kódování, modulace, koncový vysílač/přijímač signálu. Příklady specifikací fyzických vrstev jsou V.24, RS-232, RS-449, X.21, G.703, V.35, V.10, V.11, Ethernet 100Base-Tx, a další.

Mezi síťové prvky pracující pouze na fyzické vrstvě patří například opakovače, koncentrátory a muldexy.

2.2.3.2 Linková (spojová) vrstva

Linková vrstva zajišťuje služby řešící komunikaci mezi sousedními uzly sítě, propojenými prvky pracujícími pouze na fyzické vrstvě (kabely, zesilovače, opakovače, rozbočovače, koncentrátory, multiplexory, apod.).

Vrstva se zabývá přenosem datových jednotek označovaných jako „**rámec**“. V počítačových sítích bývá vrstva rozdělena do dvou podvrstev:

- podvrstva **řízení logického spoje** – LLC (Logical Link Control),
- podvrstva **řízení přístupu ke komunikačnímu kanálu** – MAC (Medium Access Control).

Obecná struktura datové jednotky na úrovni spojové vrstvy (rámce) je zachycena na **Obr. 2.3**.

Obr. 2.3: **Struktura datové jednotky na úrovni podvrstvy MAC**

V současnosti se v datových sítích preferuje nespojovaný charakter komunikace, takže LLC záhlaví obsahující informace pro řízení linkového spoje u jednotlivých technologií většinou chybí.

Na linkové vrstvě se řeší problematika:

- **typ spoje**
  - ***dvoubodový*** (P-to-P),
  - ***mnohabodový*** (MP),
- **vztah mezi linkovými entitami**
  - ***rovný s rovným*** (Peer-to-Peer),
  - ***hlavní versus podřízené stanice*** (P-to-MP, Master-to-Slave/-s),
- **fyzická adresace** - v případě mnohabodového spoje na linkové úrovni, tj. část sítě, kdy se mezi komunikačními uzly obsahující i vyšší vrstvy než linková nacházejí zařízení pracující maximálně na MAC podvrstvě (například přepínač),
- **přepojování rámců -** na úrovni MAC podvrstvy pomocí přepínačů,
- **zabezpečení datových jednotek** – například zabezpečení cyklickým kódem, potvrzování a případná oprava znovuvysláním datové jednotky,
- **řízení vícenásobného přístupu ke sdílenému médiu,**
- **možnost multiprotokolové podpory** pro protokoly na linkové a síťové vrstvě,
- **řízení komunikace** – aktivace a deaktivace linkové komunikace, potvrzování, číslování datových jednotek, řízení datového toku,
- **podpora kvalitativních požadavků služeb**.

Příklady protokolů linkové vrstvy mohou být:

- BSC (Binary Synchronous Control) – znakově orientovaný protokol,
- SDLC (Synchronous Data Link Control) – bitově orientovaný protokol,
- HDLC (High level Data Link Control) – bitově orientovaný protokol,
- LLC (Logical Link Control) – IEEE 802.2,
- LAPB (Link Access Procedure Balanced) – protokol ze specifikace sítí X.25,
- LAPD (Link Access Procedure on the D-channel) – mnohonásobný přístup k D-kanálu sítí ISDN.

2.2.3.3 Síťová vrstva

Síťová vrstva řeší problematiku směrování (transportu) datových jednotek (paketů) rozsáhlou heterogenní sítí složenou z mnoha různých typů sítí dílčích. To znamená, že zavedením jednotného způsobu směrování sjednocuje různé sítě do jediné tzv. „intersítě“ (internet).

Základní službou síťové vrstvy je poskytnout transportním entitám transparentní přenos datových segmentů sítí.

Nejčastěji se jedná o datagramovou službu. Vrstva realizuje následující úkoly:
- multiplex/demultiplex transportních či síťových datových toků,
- logická adresace na síťové úrovni,
- překlad mezi síťovými a fyzickými adresami,
- směrování paketů na základě údajů ve směrové tabulce,
- prioritizace datových toků (zajištění podpory QoS) – upřednostnění směrování paketů služeb s vyšší prioritou,
- spojovaný/ nespojovaný charakter (CONS – Connection Oriented Network Service, CLNS – ConnectionLess Network Service),
- řízení toku dat,
- filtrování paketů pro zavedení zabezpečení proti útokům,
- překlad adres pro odstínění struktury privátní sítě , tzv. „intrasítě“,
- poskytování informací o stavu komunikace na síťové úrovni – dosažitelnost uzlu, doba odezvy (zpoždění ve smyčce), nedoručitelnost paketu,
- fragmentace paketů pro přenos pomalejšími kanály,

Prvky pracující na síťové vrstvě (jejich nejvyšší vrstva), směrovače, oddělují dílčí sítě a zamezují tak všesměrovému šíření oběžníků. Příklady protokolů pracujících na síťové vrstvě mohou být protokol IP a IPX.

2.2.3.4 Transportní vrstva

Transportní vrstva je první vrstvou nad úrovní sítě. Komunikace mezi entitami koncových zařízení. Vrstva řeší řadu úkolů:
- transport dat jednotlivých relací,
- multiplex/demultiplex datových toků,
- segmentace/skládání zprávy, skládání segmentů ve správném pořadí, odstranění zdvojených a nesprávně doručených segmentů zprávy,
- určení optimální délky segmentů dat pro hladký průchod sítí,
- zajištění bezchybnosti a úplnosti přenosu zprávy – kontrola chyb a potvrzování,
- konverze nespojované služby na spojovanou – budování, udržení a rozpad spojení,
- řízení datového toku – řízení intenzity vysílání zdrojového koncového uzlu,
- upřednostnění urgentních dat – přednostní zpracování důležitých dat.

RM ISO/OSI definuje 5 tříd transportních služeb označených jako TP0 až TP4.
Příklady transportních protokolů jsou TCP a UDP v sadě TCP/IP a SPX v sadě IPX/SPX.
Vrstvy fyzická až transportní jsou nejčastěji součástí síťové podpory zabudované v operačním systému. Následující tři vrstvy vesměs bývají součástí určitých aplikací.

2.2.3.5 Relační vrstva

Protokoly relační vrstvy řeší problematiku zajištění korektního vedení dialogů (relací – sessions) komunikujících aplikačních procesů. Vrstva realizuje navazování, udržování a rušení relací. Definuje typ komunikace na úrovni relace (simplex, poloduplex, duplex), zavádí synchronizační body do přenášené zprávy pro možné pokračování v přenosu v případě rozpadu a následné obnovy relace. Nejčastěji existuje u zobrazení relace na transportní spojení poměr jedna k jednomu, ale může to být i více k jednomu a jedna k více transportním spojením. Vrstva tak například zajišťuje i možnost předání existujícího transportního spojení

jiné aplikaci. Další možností je identifikace komunikujících subjektů pro zajištění bezpečnosti přístupu k informacím.
Příkladem může být protokol RPC (Remote Procedure Call) v sadě TCP/IP.

2.2.3.6 Prezentační vrstva

Prezentační vrstva zahrnuje několik typů služeb - kódování, kompresi a šifrování. Cílem je především upravit formát zprávy do tvaru známého oběma komunikujícím aplikačním entitám. Společné formáty textu, čísel, statických obrázků, audia a videa umožňují komunikovat aplikacím různých systémů s různou vlastní prezentací datových typů. Komprese zvyšuje přenosovou rychlost z pohledu aplikační vrstvy. Šifrování poskytne přenos důvěrných dat nedůvěryhodným prostředím zabezpečený proti odposlechu a modifikaci obsahu.

2.2.3.7 Aplikační vrstva

Aplikační vrstva implementuje protokoly tvořící výkonná jádra konkrétních síťových služeb a jim odpovídajících aplikací, například pro přístup k webovým stránkám (HTTP – Hyper Text Transfer Protocol), přenos souborů (FTP – File Transfer Protocol), elektronická pošta (SMTP – Simple Mail Transfer Protocol, IMAP, POP3), aj. Aplikační vrstva řeší problematiku identifikace uživatelů, síťových zdrojů a synchronizace aplikací).

Tato vrstva nespecifikuje konkrétní podobu aplikace.

3 Datové sítě

Datové sítě jsou sítě tvořené skupinou výpočetních systémů propojených přenosovými a spojovacími prostředky za účelem vzájemné komunikace.

3.1 Vlastnosti datových sítí

3.1.1 Aspekty datových sítí

Datové (počítačové) sítě poskytují celou řadu možností pro různé lidské aktivity a tyto možnosti lze rozdělit do základních dvou kategorií:

- přínosy,
- negativní důsledky.

Mezi přínosy patří:

- komunikační prostředek – zjednodušení a zrychlení komunikace mezi lidmi i na značnou vzdálenost (e-mail, instant messaging, IP telefonie, videotelefonie, atd.),
- elektronická forma přenosu dat mezi počítačovými systémy,
- sdílení výpočetní a paměťové kapacity,
- sdílení drahých periférií – tiskárny,
- centrální řízení procesů,
- centrální dohled nad monitorovanými objekty,
- přístup k rozsáhlým informačním zdrojům,
- centralizace a zjednodušení správy počítačových systémů – mnoho úprav a změn lze provádět vzdáleně,
- prostředek vzdělávání,
- prostředek zábavy,
- vzdálená spolupráce při řešení úkolů,
- prostředek pro reklamu výrobků a služeb,
- elektronické obchodování – elektronické obchody,
- elektronické bankovní služby,
- zvýšení spolehlivosti systémů a bezpečnosti dat (clustery)
- aj.

Mezi negativní důsledky lze zařadit:

- prostředek pro provozování nelegálních aktivit,
- porušování autorských práv,
- rychlé šíření počítačových virů,
- nebezpečí útoků na systémy a spravovaná data,
- možnost odposlouchávání či pozměnění přenášené informace,
- možnost šíření nepravdivých či poplašných zpráv,
- možnost šíření nevyžádané reklamy (spamming),
- změna psychiky a komunikativních schopností lidí,
- aj.

3.1.2 Způsob zpracování dat

Počítačové sítě vnáší nové možnosti sběru a zpracování dat:

1. **distribuované** – data jsou rozmístěna a zpracovávána v mnoha rovnocenných uzlech sítě a je vyřešen způsob přístupu ke všem zdrojům z jednoho místa. Pro vyšší stupeň zabezpečení a rychlejší přístup bývají data z určitého uzlu zálohována v jednom či několika dalších uzlech,
2. **hierarchické** – uzly tvoří hierarchii, kdy jsou data na nich uložená rozdělena na lokální a centrální, a při dotazu na informaci se pomocí vazeb mezi uzly v hierarchii zajistí směrování dotazu k uzlu, který zodpovídá za správu požadované informace (například DNS systém),
3. **centralizované** - v síti existuje centrální uzel, který sám sbírá data, zpracovává je a poskytuje informace.

3.1.3 Vztahy mezi uzly (procesy) v síti

- **terminál – hostitelský počítač**: terminál (či proces) je pouhým prodloužením přípojných kabelů monitoru, klávesnice a případně ovládacího prvku (myš, dotyková ploška, apod.) přes síť. Zadávané příkazy z terminálu jsou vykonávány procesy běžícími na hostitelském počítači a výsledky jsou posílány na terminál,
- **klient-server**: software realizující danou síťovou službu je rozdělen do dvou částí, klienta a serveru. Klient posílá požadavky a zobrazuje výsledky a server přijímá příkazy, kontroluje, zda je možno příkaz vykonat (správná syntaxe, patřičná oprávnění, atd.), vykonává příkaz a zasílá klientské části výsledky operace. Jedná se o nejčastější případ v internetu,
- **peer-to-peer**: komunikující aplikace jsou si rovnocenné, tzn., že daná aplikace žádá od protějšku služby a také je sama poskytuje.

3.1.4 Způsoby komunikace v počítačových sítích

V počítačových sítích existují různé typy komunikací:

- **dvoubodové** (P-to-P) – přenos se uskutečňuje mezi dvěma body,
- **mnohabodové** (MP)
  - ***skupinové*** - datová jednotka se šíří od jediného zdroje a obsahuje buď seznam adres konkrétních cílových stanic nebo tzv. skupinovou adresu,
  - ***konferenční*** – data (hlas, video) jsou od jednotlivých účastníků rozesílány všem ostatním,
  - ***všesměrové*** – pro zasílání dotazů od aplikace neznající adresu cíle, pro zasílání zpráv určené všem stanicím, pro odeslání zprávy bez znalosti adresy cíle.

3.1.5 Výbava datových (počítačových) sítí

Prostředky počítačových sítí lze rozdělit na část **technického vybavení,** neboli **hardware** (HW) a část **programového vybavení**, neboli software (SW). HW výbavu tvoří:

- koncové uzly:
  - osobní počítače,
  - pracovní stanice,
  - přenosné – notebooky, netbooky, PDA (Personal Digital Assistant), chytré telefony, tablety, elektronické čtečky dokumentů, a jakékoliv zařízení ovládané mikroprocesorem a připojitelné k síti,

  - servery, mainframy,
  - terminály – různě vybavená speciální rozhraní pro komunikaci se sálovým počítačem,
  - další koncové uzly – IP telefony (kabelové, bezdrátové), síťové tiskárny, IP kamery, čidla (senzory), aj.,
- ukončovací zařízení – tzv. modemy, umožňující připojovat koncové uzly k síti s jiným rozhraním a komunikačním protokolem,
- propojovací prvky
  - opakovače, rozbočovače,
  - mosty, přepínače,
  - směrovače,
  - brány,
- přenosové systémy – multiplexory, koncentrátory, PDH a SDH systémy,
- přenosová média - kabely, spojky, konektory, antény, optické vysílače, přijímače,
- prvky pro strukturovanou kabeláž (stojany, rozvaděče, …),
- záložní zdroje,
- velkokapacitní zařízení pro ukládání dat,
- aj.

Softwarová výbava zaměřená na sítě:

- **klientské stanice** - operační systém s podporou síťové komunikace a patřičné protokolové sady (Windows™, Linux, Mac OS, aj.), případně s klientskou aplikací pro přihlašování se do sítě (např.),
- **servery** – výkonný síťový operační systém, správa databáze síťových objektů (uživatelé, aplikace, HW), systém řízení přístupu k síťovým zdrojům a aplikacím (např. Windows xxx Server, Novell NetWare Server, Linux, BSD Unix, Unix System V, Solaris, HP UX, IBM AIX, atd.),
- **SW terminál** – aplikace pro vzdálený přístup do systému,
- **síťové aplikace** – nejčastěji typu klient – server (e-mail, instant messaging, www, ftp, atd.),
- **informační systémy, databáze, databázové aplikace**,
- software pro **dohled a správu sítě.**

3.1.6 Typy datových sítí

Datové sítě se nejčastěji rozlišují na:

- **PAN** (Personal Area Network) – osobní datové sítě vybudované většinou na některé z bezdrátových technologií krátkého dosahu – v současnosti nejčastěji na technologii Bluetooth
- **LAN** (Local Area Network) – lokální počítačové sítě s vysokou přenosovou rychlostí a propustností, pro propojení počítačů v rámci jedné či několika budov, se sdílením přenosové kapacity, s dosahem řádově stovky metrů až jednotky kilometrů, ve vlastnictví jedné organizace, koncové uzly lze vypínat bez ohrožení chodu zbytku sítě,
- **MAN** (Metropolitan Area Network) – metropolitní sítě, s relativně vysokou přenosovou rychlostí, avšak nižší propustností, s dosahem řádově desítky kilometrů, ve vlastnictví síťových operátorů, s nepřetržitým provozem síťových uzlů,
- **WAN** (Wide Area Network) – sítě často s nižší přenosovou rychlostí (až na vysokorychlostní optické páteře), avšak s ještě nižší propustností, s dosahem řádově stovky až tisíce kilometrů, ve vlastnictví jednoho i více síťových operátorů, s nepřetržitým provozem síťových uzlů.
- **GAN** (Global Area Network) = globální datová síť Internet

3.1.7 Struktura sítí

Propojené uzly sítě mohou vytvářet různé konfigurace, které jsou určeny typem dané sítě, přičemž struktura závisí na úrovni pohledu

- **fyzická** – jakou konfiguraci vytváří fyzické propojení počítačů,
- **vizuální** – jakou topologii síť vytváří z vizuálního hlediska,
- **logická** – jakou konfiguraci síť tvoří z pohledu linkové vrstvy (lépe řečeno z pohledu MAC podvrstvy)

Sítě tvoří následující struktury:

- **sběrnice** – stanice (uzly) sdílí fyzicky či logicky jeden přenosový kanál v každém směru. Stanice jsou k fyzické sběrnici (např. koaxiální kabel) připojeny vysokoimpednačně, takže vypnutí či výpadek stanice zpravidla neohrozí činnost sítě.
- **hvězda** – koncové stanice jsou propojeny přes centrální uzel, který je všemocným a pro chod sítě nejdůležitějším prvkem v síti. Funkčnost a bezchybná činnost centrálního uzlu je nezbytným předpokladem činnosti sítě.
- **kruh** – stanice jsou uspořádány do fyzického či logického kruhu, čímž je určena posloupnost přidělování práv k přístupu ke sdílenému médiu. Musí být vyřešena problematika odstoupení a přihlášení se stanice do sítě. Kruh může být buď
  - jednoduchý – narušení kruhu způsobí ukončení činnosti sítě,
  - dvojitý – druhý kruh může být využit pro:
    1. zálohu v případě výpadku primárního kruhu (např. u sítě FDDI),
    2. opačný směr přenosu (např. u sítě DQDB),

  Bylo vytvořeno několik architektur na bázi kruhové topologie:
  1. **Newhallův kruh** – sítí obíhá v daný okamžik pouze jediná zpráva (příkladem je síť Token Ring),
  2. **Piercův kruh** – kruh tvořený posuvnými registry a jeho bitová kapacita je rozdělena do minirámců obsahující informaci o naplnění rámce a o převzetí dat cílovou stanicí (příkladem je síť „Cambridge ring“),
  3. **Kruh s vkládáním rámců** – stanice mající data k odeslání si zprávu připraví do posuvného registru, který po ukončení průchodu právě obíhající zprávy připojí do kruhu a zpráva se odešle. Po převzetí zprávy cílovou stanicí a zpětném příchodu zprávy do vysílací stanice je registr ze sítě odpojen a zpráva je z registru odstraněna.
- **strom** – propojení počítačů tvoří stromovou hierarchickou strukturu. Typickým příkladem je síť Ethernet na bázi přepínačů.
- **polygon** – uzly sítě jsou navzájem propojeny tak, že mezi dvěma body existuje zpravidla více cest. Je to výhodné pro vyšší bezpečnost doručení dat. Tato architektura se používá tam, kde to princip přenosu datových jednotek umožňuje, a to nejčastěji na úrovni propojení směrovačů.

3.2 Přenosová média

Přenosová média slouží k fyzickému přenosu informace prostřednictvím elektromagnetického signálu. Důležitými parametry jednotlivých médií jsou:

- **kmitočtová charakteristika** – udává kmitočtovou oblast využitelnosti pro přenos informace. Ve vybrané oblasti (kanálu) požadujeme co nejnižší a pokud možno konstantní útlum a také lineární fázovou charakteristiku. Odchylky od těchto požadavků pak vyvolávají lineární amplitudové a fázové zkreslení, což způsobuje změnu tvaru vyslaného signálu a také nebezpečí mezisymbolové interference.

Využitelná šířka pásma je ovlivněna potřebným dosahem média bez použití zesilovačů či regenerátorů číslicového signálu. Platí, že čím je potřebná délka větší, tím je užší použitelné pásmo, a tedy menší kapacita kanálu. Často se kapacita udává jako součin šířky pásma (případně přenosové rychlosti) a délky média

Pozn. 1: Maximální délka vedení může být omezena i samotnou síťovou technologií a nikoli přenosovými charakteristikami vedení, jak je tomu např. u sítí Ethernet.

Pozn. 2: Segmenty vedení musí být řádně impedančně zakončeny, aby nedocházelo k odrazům na jejich koncích.

- **úroveň šumu (rušení)** – zdrojem může být samotné přenosové médium nebo vnější zdroje rušení, kdy se nežádoucí signál přenese do kanálu induktivní či kapacitní vazbou, způsobuje nízký odstup signálu od šumu (výkon užitečného signálu nelze libovolně zvyšovat) a tedy nízká výsledná kapacita kanálu pro přenos digitálních dat a nebo výrazné rušení přenášeného analogového signálu.

Existuje velmi široká řada přenosových médií, které lze rozdělit do několika kategorií:

- **Venkovní vedení** – používá se stále méně, neboť nevykazuje dobré přenosové vlastnosti, není odolné proti rušení a vlastnosti jsou silně ovlivňovány povětrnostními podmínkami. Také vykazuje vysoký stupeň poruchovosti (vítr, námraza, apod.)
  - klasické (pásmo do 150 kHz),
  - s širokým kmitočtovým pásmem (pásmo do 1,3 MHz),
  - vedení velmi vysokého napětí (pásmo do 500 kHz).
- **Kabelová vedení**
  - ***metalická***
    - *symetrická* – kroucené páry, kabely UTP (unshielded twisted pair) (kategorie 1 až 7), STP (shielded twisted pair), FTP (foilled twisted pair)
    - *nesymetrická koaxiální vedení* – využitelný až do kmitočtů řádově jednotky GHz, pro větší dosah však podstatně méně, impedance různých typů se pohybuje mezi 50 až 100 Ω. Používá se pro přenos jak v základním, tak především v přeneseném pásmu.
  - ***optická*** – využívají se tzv. optická okna, tj. oblasti kolem vlnových délek 850 nm, 1300 a 1550 nm. Vlákna vykazují vysokou přenosovou kapacitu, nízkou hmotnost a vysokou odolnost proti vnějšímu rušení
    - mnohovidová – větší průměr jádra, menší kapacita a dosah vlivem vidové disperze při průchodu signálu vláknem
      - se skokovou změnou indexu lomu,
      - s grandientní změnou indexu lomu,
    - jednovidová – velmi tenké jádro vlákna, obrovská přenosová kapacita, dosah řádově desítky až sto km bez regenerátoru signálu.
      - jednovlnová – současná kapacita až 40 Gb/s,
      - s vlnovým multiplexem (WDM technologie) – kapacita jednoho vlákna až jednotky Tb/s.
- **Bezdrátová vedení -** není zapotřebí kabeláž, což přináší možnost rychlé instalace systému a možnost mobility koncových uživatelů. Snadno se realizuje všesměrové vysílání, problémem je vyšší úroveň rušení a vícecestné šíření signálu.
  - ***pozemní v rádiovém pásmu***
    - < 1GHz – analogový rozhlas a TV, analogové bezdrátové telefony, digitální mobilní systémy,

    - >1GHz (mikrovlny) – bezšňůrové telefonní systémy DECT, Bluetooth, WLAN 2,4 a 5 GHz, FWA, digitální mobilní systémy,
  - ***družicové spoje*** – vhodné pro realizaci spojení v oblastech bez telekomunikační infrastruktury (neobydlené oblasti, vývojově zaostalé oblasti, moře, vzdušný prostor, apod.). Umožňuje také mobilitu účastníka.
  - ***v optickém pásmu***
    - infračervené spoje,
    - s laserovým vysílačem.
- **Vlnovody** (metalické) – různé tvary, kmitočty desítky až stovky GHz.

3.3 Kanálové kódování digitálního toku

Digitální informace musí být na nejnižší části fyzické vrstvy prezentována jako určitá forma průběhu elektromagnetického signálu s vlastnostmi vhodnými pro přenos daným komunikačním kanálem. Signál nesoucí informaci může být kmitočtově umístěn:

- v **základním pásmu** – moduluje se ***stejnosměrný***, nebo ***periodický*** (spektrum obsahuje kmitočty od ss složky až po maximální hodnotu danou přenosovým médiem) průběh elektromagnetického signálu
  - se stejnosměrnou (ss) složkou,
  - s potlačenou ss složkou,
- v **přeneseném pásmu** – moduluje se ***harmonický*** průběh elektromagnetického signálu, tzv. nosná
  - s modulací – tzv. klíčování - dvou a vícestavové (amplitudové, kmitočtové, fázové, kvadraturní klíčování),
  - s modulací a směšováním – pro přesun do vyšších kmitočtových pásem s nosnou podstatně kmitočtově výše než je kmitočtová šířka komunikačního kanálu.

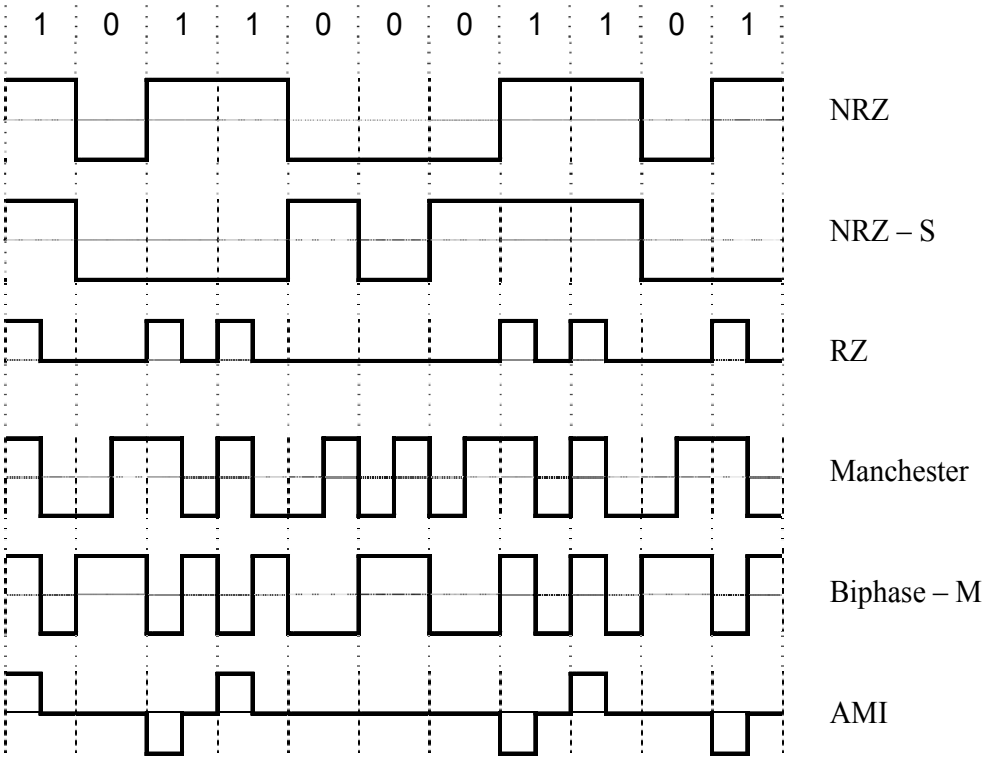
Vlastní kódování digitální informace na fyzické úrovni se často skládá z několika úprav původního sledu informačních bitů a ještě níže ve vrstvové struktuře i elektromagnetického signálu, které slouží ke zlepšení parametrů pro přenos daným typem komunikačního kanálu. Patří sem:

- **skramblování** – úprava posloupnosti bitů za účelem:
  - pro zrovnoměrnění kmitočtového spektra signálu,
  - zabránění vzniku přeslechů a intermodulačních produktů mezi kanály a vedeními a k
  - zajištění přenosu synchronizační informace do přijímače,
- **šifrování** na fyzické vrstvě – zabezpečení proti odposlechu při přenosu po fyzickém segmentu (nejčastěji po rádiovém kanálu),
- **rozdělení toku bitů do skupin** za účelem
  - vícestavového kódování (např. 2B1Q, 4B3T, QAM),
  - rozdělení toku pro přenos několika kanály oddělenými kmitočtově (pro potlačení vlivu vícecestného šíření signálu u bezdrátových sítí) či prostorově (přenos po více párech pro možnost využití méně kvalitních kabelážních systémů pro vysokorychlostní přenosy),
  - prokládání – zmenšení dopadu při vzniku shluku chyb,
  - překódování do vícebitových skupin
    - pro potlačení ss složky a zajištění synchronizace pro určitý typ následného fyzického kódování (např. 4B5B či 8B10B pro kódování NRZ – Non-Return to Zero),

- pro přenos více datových toků jedním kanálem (kódové oddělení – DSSS CDMA – Direct Sequence Spread Spectrum Code Division Multiple Access),

- **ochrana proti chybám s autokorekcí** - vkládání zabezpečovací informace pro autokorekci chyb v přijímači (nejčastěji konvoluční kódování),
- **filtrace** – pro kmitočtové omezení obdélníkového průběhu signálu reprezentujícího digitální signál a pro následující analogovou modulaci.

U datových sítí LAN s metalickými propojovacími kabely se nejčastěji používá přenos v základním pásmu. Některé z kódovacích mechanizmů jsou zachyceny na **Obr. 3.1**. Úrovně signálu jsou buď napěťové či proudové. Před vlastním vysláním signálu na kanál však signál bývá ještě dále upraven (nejčastěji kmitočtově omezen).



Obr. 3.1**: Příklady linkového kódování v sítích LAN**

NRZ (non-return-to-zero) – binární kód se dvěma úrovněmi, kde jedna logická hodnota má v průběhu bitového intervalu jednu úroveň signálu a druhá má opačnou úroveň signálu,
NRZ – S (NRZ – space) - binární kód se dvěma úrovněmi, kde logická nula mění polaritu signálu a logická jednička ponechává předchozí úroveň,
unipolar RZ – (return -to-zero) – unipolární signál s pulzem v logické jedničce a návratem k nule uprostřed bitového intervalu a nulovou úrovní v logické nule po celou dobu bitového intervalu,
AMI – Alternate Mark Inversion – polární signál s pulzy střídající se polarity v logické jedničce a nulovými úrovněmi v logické nule.

Kromě dvoustavových kódů existují i vícestavové, kde jeden symbol reprezentuje skupinu bitů, například 8-stavový symbol reprezentuje trojici bitů. Výstupem kanálového kódování je sekvence symbolů, které buď nesou informaci z vyšší vrstvy či podvrstvy nebo slouží k synchronizaci či označují zahájení či ukončení sekvence datových symbolů.

3.3.1 Adresování v datových sítích

3.3.1.1 Funkce a typy adres

Adresa má za úkol jednoznačně specifikovat objekt v počítačové síti na určité úrovni komunikace. Adresace má význam, pokud na dané úrovni komunikace existují více než dvě funkční jednotky (entity). Výraz „na určité úrovni" je myšlen tak, že je adresa vázána na určitou úroveň či vrstvu referenčního modelu. Nejčastěji se tím myslí adresování na úrovni:

- **spojové** (**linkové**) **vrstvy** – fyzická, hardwarová (HW), MAC adresa,
- **síťové vrstvy** – síťová adresa,
- **transportní vrstvy** – adresa přístupového bodu služby v rámci jednoho uzlu, na který je navázána určitá ***aplikace*** (tam očekává příchod dat ze sítě a odevzdává tam data k odeslání),
- **relační vrstvy** – jednoznačně definuje danou relaci mezi dvěma komunikujícími aplikačními entitami.
- **služby** – služba prezentovaná koncovými a řídicími uzly a vztahy mezi nimi vytváří nad intersítí tzv. překryvnou síť (overlay network), ve které jsou koncové uzly adresované pomocí logických adres. Příkladem je hovorová služba v sítích IP (VoIP), telefonní překryvná síť a adresace pomocí telefonních čísel nebo identifikátoru URI, např. sip: username:password@host:port.

Informace o adrese jsou typicky vkládány do záhlaví datových jednotek. Obsahem nejčastěji bývají zdrojová (kdo datovou jednotku odesílá) a cílová adresa (kam má být datová jednotka předána), případně pak i adresy některých či všech mezilehlých objektů stejné úrovně (specifikace cesty, existuje-li více cest).

Adresy mohou mít určitý rozsah platnosti a jedinečnosti:

I. **lokální** – daná adresa má platnost omezenou na určitou lokalitu, například uzel (čísla portů – přístupových bodů aplikací) či lokální síť,
II. **globáln**í – platnost a jedinečnost adresy má globální charakter. Globální platnost může být požadována ze dvou základních důvodů:
    1. na dané úrovni adresace jsou propojené všechny uzly rozlehlé (celosvětové) sítě – případ síťových adres v rámci Internetu,
    2. adresy jsou pevně definované již výrobcem síťového rozhraní a chceme zajistit možnost použít produkty různých výrobců v jedné oblasti sítě na dané úrovni – případ MAC adres lokálních počítačových sítí typu Ethernet, Token Ring, apod.

Dále, adresa na dané úrovni komunikačního modelu může mít několik forem a tedy významů:

- **unicast adresa** – definuje jediný objekt na dané úrovni,
- **multicast adresa** – definuje skupinu objektů na dané úrovni,
- **broadcast adresa** – definuje všechny objekty dosažitelné na dané úrovni,
- **anycast adresa** – definuje kterýkoli jeden objekt ze skupiny objektů.

Adresy mohou být:

- **jednoúrovňové** – objekty tvoří plochou strukturu, ty mívají spíše lokální charakter,
- **víceúrovňové** (**hierarchické**) – objekty jsou uspořádány do stromové struktury a části adresy pak postupně blíže a blíže specifikují daný objekt v této stromové struktuře objektů.

Vyjádření adres může být:

- **číselné** – adresa je specifikována bitovým slovem, který může být pro větší srozumitelnost pro člověka ve tvaru několika dekadických či hexadecimálních čísel.
- **jmenné** – daný objekt má specifikovanou adresu nejčastěji v podobě hierarchické struktury textových řetězců. Jmenná vyjádření jsou tvary „stravitelnější" a

zapamatovatelnější pro člověka. V případě takovéto adresace objektů v rámci větší oblasti je zapotřebí zajistit jednoznačnost jmen a implementovat službu (systém objektů v síti), která zajistí konverzi jmenného vyjádření na číselné, které pak používají výpočetní systémy (přepínače, směrovače) pro doručování.

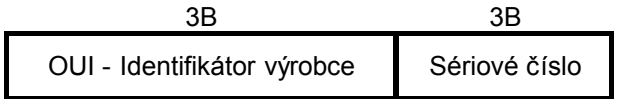
3.3.1.2 Adresace v LAN sítích

LAN sítě specifikované skupinou IEEE 802.x mají společné adresovací schéma. Délka fyzických (MAC) adres může být:

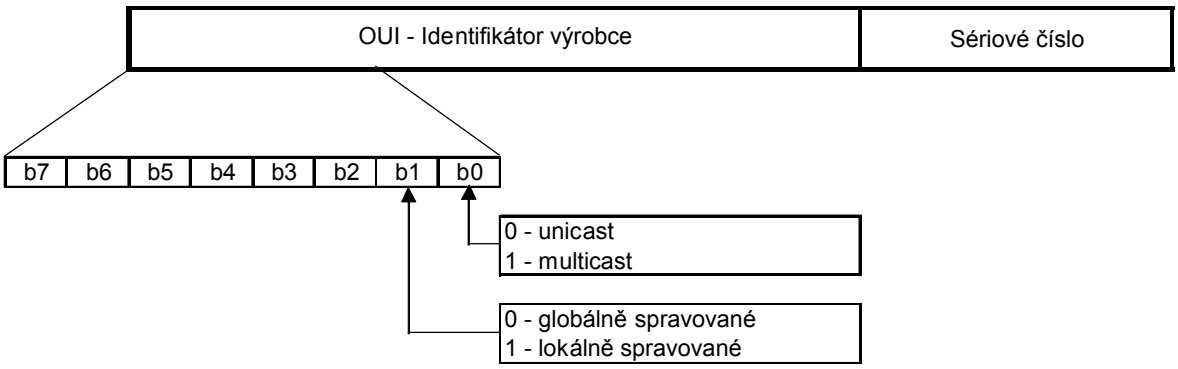
- **16 bitů** – pro lokální přidělování,
- rozšířené fyzické adresování (EUI – Extended Unique Identifier)
  - **48 bitů** (EUI-48) – pro lokální i globální adresování. Již hrozí vyčerpání!
  - **64 bitů** (EUI-64) – pro budoucí alokaci fyzických adres

Nejméně významným bitem (LSB bitem) nejvýznamnějšího bajtu adresy se rozlišuje, zda je adresa individuální (unicast) - log. 0 nebo skupinová (multicast) či všesměrová (broadcast) - log. 1 (u všesměrové adresy jsou pak v hodnotě log. 1 i všechny ostatní bity). Druhý bit před LSB bitem určuje, zda je adresa lokální (log. 1) nebo globální (log. 0).

Globální adresa je rozdělena na dvě části, kde první 3 oktety udávají kód výrobce síťového rozhraní (kódy jsou přidělovány organizací IEEE) a zbývající část tvoří sériové číslo, které si výrobce spravuje sám, tak aby byla zajištěna jedinečnost adresy v rámci celého světa.



Obr. 3.2: **Struktura globálních MAC adres**



Obr. 3.3: **Typy MAC adres**

3.4 Vícenásobný přístup k přenosovému kanálu

Signál nesoucí informaci se přenáší určitým komunikačním kanálem, který musí být v okamžiku vysílání volný, aby nedocházelo k znehodnocení vyslané informace. Často se totiž stává, že na daný kanál chce přistupovat více zdrojů toku, tedy, že kanál je sdílen. Pokud je vysílání více toků řešeno jedním uzlem, jedná se o určitý typ multiplexu toků, viz kap. 2.2.3.1.

Metody přidělování kapacity komunikačního kanálu lze rozdělit dle několika hledisek:

1. stálost přidělení

   a. ***permanentní*** – kanál je neustále k dispozici danému zdroji (např. analogové telefonní vedení, přímý přípoj k přepínači sítě Ethernet),
   b. ***relačně statické*** na dobu relace/spojení (realizace služby) – komunikační kanál je přiřazen zdroji toku (nejčastěji na žádost) a k dispozici po celou dobu realizace služby, po jejímž ukončení dojde k uvolnění kanálu pro ostatní přispěvatele (například B-kanály u přípojky ISDN, kmitočtový kanál a časový slot v rádiového rozhraní sítě GSM)
   c. ***dynamické*** – zdroje realizují nespojitý datový tok (po datových jednotkách) s proměnlivou četností generování
2. způsob rozdělení kapacity spoje
   a. ***prostorově*** dělená
   b. ***kmitočtově*** dělená,
   c. ***časově*** dělená,
   d. ***kódově*** dělená,
   e. ***statisticky*** dělená
3. způsob řízení přidělování kapacity spoje
   a. ***centralizované*** – existuje centrální autorita, jenž rozhoduje komu přidělí síťové zdroje,
   b. ***distribuované*** – celý algoritmus pro rozhodování, zda zdroj může či nemůže vysílat po komunikačním kanálu, včetně řešení možných situací, je implementován v každém zdroji.
4. časová určitost získání přístupu
   a. ***deterministické***,
   b. ***stochastické*** (náhodné).

3.4.1 Statické přístupové metody

Princip statických přístupových metod spočívá v tom, že danému přenosu je po celou dobu komunikace (komutované spoje) či dokonce stále (pevné spoje) vyhrazena určitá přenosová kapacita. Princip odpovídá spojování okruhů. Existuje řada způsobů:

   a. **SDMA** (Space Division Multiple Access) – více přispěvatelů může vysílat svá data ve stejném kmitočtovém pásmu a čase, ale je zajištěno jejich prostorové oddělení.
      - každý přispěvatel má své vedení – sadu metalických vodičů či optických vláken (příkladem mohou být účastnická telefonní vedení připojená k jedné telefonní ústředně, nebo segmenty kabelů UTP připojující jednotlivé koncové uzly k přepínači sítě Ethernet), přičemž je zajištěno, že v případě souběžného vedení nedochází vlivem přeslechů k vzájemnému významnému rušení hlavního signálu na vedení,
      - každý přispěvatel vysílá rádiový signál s takovým výkonem a v takovém prostoru, kdy je zajištěno, že se jejich rádiové signály setkávají v místě přijímače v takovém výkonovém poměru, který nezpůsobuje významné rušení signálu hlavního přispěvatele, je to řešeno dostatečnou vzdáleností v prostoru vzhledem k charakteru prostředí a vysílacímu výkonu, případně úzkou směrovou charakteristikou vysílacích a přijímacích antén se zajištěním přímé viditelnosti mezi komunikujícími uzly.
      - technika MU-MIMO-SDMA (MultiUser – Multiple Input Multiple Output – Space Division Multiple Access) – za pomocí „chytrých“ (smart) antén lze pomocí technik fázovacích polí anténu nasměrovat tak, aby se zajistil co největší zisk antén ve směru nejlepšího šíření signálu, a pomocí kódování se zajistí další zvýšení zisku, a tedy odstupu hlavního signálu od interferujících

signálů. Na straně přijímače se pro další vylepšení implementuje technika detekce současně vysílajících účastníků (multi-user detection nebo joint detection). Tento typ je tak spíše kombinací prostorově a kodově odděleného přístupu

b. **FDMA** (Frequency Division Multiple Access) – kmitočtově oddělený vícenásobný přístup, každé spojení je realizováno v jiném kmitočtovém pásmu.
c. **TDMA** (Time Division Multiple Access) – **časově** oddělený vícenásobný přístup, signál je sdružen se signály ostatních spojů do jednoho vysokorychlostního spoje. Vzniká tak rámec, kde každému spoji je přidělen určitý časový slot.
d. **CDMA** (Code Division Multiple Access) - kódový násobný přístup, přenos s rozprostřeným spektrem, kdy každému spoji je přidělena určitá posloupnost, která řídí způsob vysílání:
   - FHSS (Frequency Hopping Spread Spectrum) - s přeskakováním kmitočtů,
   - THSS (Time Hopping Spread Spectrum) - s přeskakování časových slotů,
   - DSSS (Direct Sequence Spread Spectrum) - s přímým rozprostřením spektra,
e. **OFDMA** (Orthogonal Frequency Division Multiple Access) - ortogonální kmitočtový násobný přístup,

Řada aplikací využívá kombinace několika výše uvedených metod. Například systém GSM pracuje na bázi kombinace FDMA, SDMA a TDMA.

3.4.2 Dynamické přístupové metody

Naproti tomu u dynamických metod je celá přenosová kapacita sdílena i v rámci průběhu jednotlivých relací, a tedy k dispozici všem přispěvatelům a jednotlivé zdroje se musí o přidělení možnosti vysílat určitým způsobem ucházet. Tento princip je vlastní sítím se spojováním datových jednotek a řeší přístup koncového uzlu ke sdílenému médiu (v sítích LAN).

Přístupové metody pro přístup koncových uzlů ke sdílenému médiu v sítích LAN řeší podvrstva MAC (Medium Access Control). Jedná se o metody dynamické a lze je rozdělit do několika skupin:

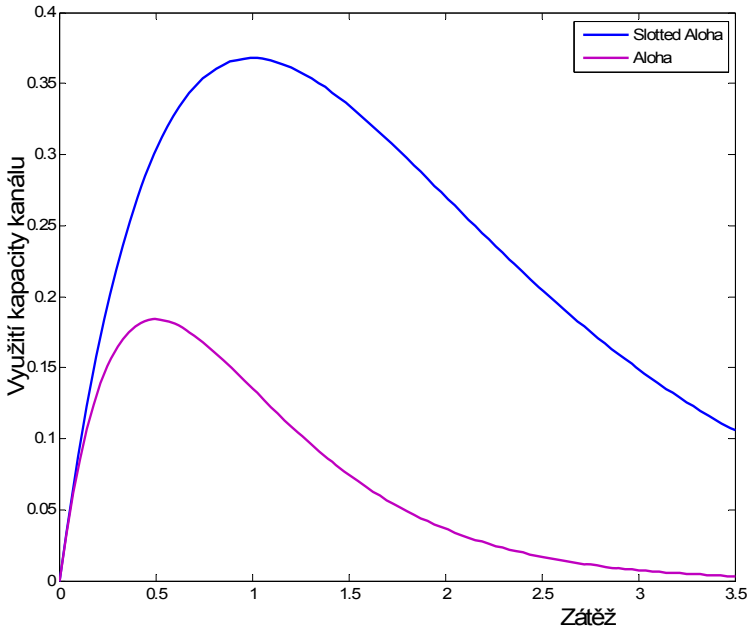
- **deterministické –** metody garantují maximální zdržení, než se stanice dostane k vysílání a umožňují implementaci priorit
  - ***s centrálním přidělováním*** – v síti existuje centrální uzel, který uděluje koncovým stanicím oprávnění k vysílání
    - na žádost – koncová stanice žádá centrální uzel o právo vysílat, jedná se o nejčastější případ, používá se v mobilních přístupových sítích,
    - na výzvu – centrální stanice se dotazuje koncových stanic, zda nechtějí vysílat
  - ***distribuované***
    - fyzický kruh – stanice spojené do fyzického kruhu si mezi sebou po směru vysílání předávají pověřovací rámec, kterým se stanici, která tento rámce obdrží, na určitou dobu pronajímá přenosová kapacita kruhu, pokud ji stanice nepotřebuje, předává pověření dál (např. síť Token Ring),
    - logický kruh – stanice jsou fyzicky spojeny do jiné topologie (sběrnice, hvězda), avšak z hlediska řízení přístupu tvoří logický kruh, kdy si stanice opět předávají pověření opravňující přístup ke sdílenému přenosovému kanálu,
    - synchronní – stanice jsou připojeny do fyzického kruhu tvořeného posuvnými registry. Přenosová kapacita je rozdělena do několika po sobě jdoucích rámců, které jsou vybaveny bity o naplnění daty a o převzetí dat

cílovou stanicí. Stanice může naplnit rámec vlastními daty pouze tehdy, indikuje-li stavový bit, že rámec je prázdný (např. síť Cambridge ring).

- s dvojitou frontou – síť je tvořena dvěma kanály pro opačné směry přenosu, kde přístup k oběma směrům je řízen pomocí dvou distribuovaných přístupových front (viz popis sítě DQDB – Distributed Queue Dual Bus).

➢ **stochastické (náhodné)** – přístup ke sdílenému kanálu je náhodný proces

- Pure Aloha – koncová stanice zahájí vysílání v kterýkoliv okamžik, když má připravená data, bez toho, aniž by si ověřila, zda již nevysílá jiná stanice a zda její data nebyla znehodnocena vysíláním jiné stanice. Tato metoda vykazuje velmi nízké procento celkové kapacity kanálu asi 18,4 % (pokud samozřejmě nevysílá pouze jedna a ta samá stanice velké množství dat a ostatní nemají nic k vysílání, ale dochází k soupeření mezi více stanicemi),
- Slotted Aloha – koncová stanice může zahájit vysílání pouze v pevně stanovených okamžicích (čas je rozdělen do slotů, stanice musí být synchronizovány). Maximální dosažitelné využití kapacity se tak zdvojnásobí na 36,8 %.



Obr. 3.4: **Využití kapacity sdíleného kanálu při nasazení metod (Pure) Aloha a Slotted Aloha**

Metody Aloha se využívaly u satelitních sítí a typ Slotted Aloha je i přístupovou metodou pro počáteční přístup mobilních stanic k síti.

- CSMA (Carrier Sense Multiple Access) – koncová stanice před vlastním vysíláním kontroluje obsazení kanálu. Pokud je kanál obsazený, stanice čeká a kontroluje jeho stav. Je-li volný, pak záleží na podtypu metody CSMA
  - naléhající (1-persistent),
  - *p*-naléhající (*p*-persistent),
  - nenaléhající (0-persistent),

  zda se ihned zahájí vysílání, či s nějakou pravděpodobností *p*, a nebo s pravděpodobností (1-*p*) se rozhodne čekat a pak čeká po náhodně vygenerovanou dobu, která se snižuje pouze, když je kanál volný, a teprve po

jejím uplynutí, je-li kanál volný, se začne vysílat. Metoda typu nenaléhající se s určitými úpravami využívá u bezdrátových datových sítí WLAN dle IEEE 802.11 a označuje se jako CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).

- CSMA/CD (Carrier Sense Multiple Access with Collision Detection) – metoda se používá u sítě Ethernet a v přístupové části sítě ISDN (vícenásobný přístup ke kanálu D). Jedná se o naléhající metodu CSMA (1-persistentní) avšak s detekcí kolizí (to není u bezdrátových sítí možné). U sdíleného Ethernetu stanice, která chce vysílat, nejprve po dobu kolizního slotu (ten je dán rychlostí sítě a minimální délkou rámce, např. pro 10 Mb/s a 512 bitů je to doba 51,2 μs) monitoruje obsazení kanálu. Je-li detekován provoz, stanice musí čekat, dokud není provoz ukončen. Zjistí-li, že je kanál po výše uvedenou dobu volný, začne ihned vysílat (1-persistent CSMA) a během vysílání současně kontroluje, zda odeslaná data nebyla narušena vysíláním jiné stanice. Způsob kontroly závisí na typu fyzické vrstvy, tj. jiná je pro Ethernet využívající koaxiální kabel, a jiná, je-li použit rozvod pomocí kabelů typu UTP a prvků typu rozbočovač. Pokud je narušení dat detekováno, nastala tzv. kolize, a první stanice, která kolizi zjistí, přeruší vysílání dat a zahájí vysílání signálu JAM (zpráva o délce 32 bitů), což způsobí, že všechny stanice účastnící se kolize přestanou vysílat. Každá stanice si pak vygeneruje náhodné číslo z intervalu $(0, 2^k)$, kde k závisí na počtu n předchozích neúspěšných pokusů o přenos ($k = \min(n, 16)$). Toto náhodné číslo vynásobené dobou časového slotu udává, jak dlouho bude stanice čekat, než se znovu pokusí o přístup na sdílený kanál. Cílem náhodného výběru doby čekání je rozprostření okamžiků přístupu k médiu v čase a zabránění tak dalším kolizím. S nárůstem provozu v tzv. kolizní doméně pravděpodobnost kolizí narůstá. Výhodou je relativní jednoduchost metody, nevýhodou pak je, že nezaručuje maximální dobu, za jakou se stanice dostane k úspěšnému odeslání datového rámce. Využití sítě nejdříve narůstá se zátěží v síti. Se zvyšováním zatížení sítě se však kolize stávají stále častějšími a nárůst využití sítě se zvolňuje až po překročení určité zátěže začne pozvolna klesat. Maximální využití kapacity je přibližně 80 % (důvodem je také nutnost dodržet alespoň minimální časové odstupy mezi následujícími rámci). V případě, že se provoz ve sdílené doméně častěji vyskytuje v okolí kritické úrovně zátěže či dokonce za ní, je nutné najít vhodné řešení situace. Řešení tohoto problému jsou dvě:
  - *zvýšení kapacity (přenosové rychlosti) sdíleného kanálu* – zvýšením přenosové kapacity kanálu (například z 10 Mb/s na 100 Mb/s dostaneme zátěž sítě pod kritickou úroveň(tzv. „řešení hrubou silou“), je však vybavit síť novými prvky, které podporují rychlejší technologii,
  - *rozdělení kolizní domény na několik menších* – zmenšení úrovně provozu pod kritickou úroveň vložením prvku oddělující kolizní domény (přepínače či dokonce směrovače)

3.5 Propojovací prvky a mechanizmy

Propojovací prvky vytvářející různé konfigurace sítí LAN a spojující je do větších celků (tzv. internetu, pozn. s malým „i“) mají dvě základní funkce:

- **spojovací** – pro zajištění komunikace mezi dílčími sítěmi či jejich částmi, tj. funkce přepojování

- **rozdělovací** – za účelem:
  - ***obejití limitů*** – například maximální délka segmentu, maximální počet uzlů (viz popis sítě Ethernet), možnost použití staršího i novějšího vybavení (například propojení segmentů s různou přenosovou rychlostí pomocí přepínačů), maximální počet přidělených adres,
  - ***zvýšení funkčnosti sítě***
    - zvětšení propustnosti – například rozdělení kolizních domén, případně umožnění duplexního provozu,
    - zvýšení spolehlivosti – vytvoření redundantních spojů,
  - ***zvýšení úrovně bezpečnosti*** – oddělení provozu od provozu, kde se přenášejí citlivé informace

3.5.1 Koncentrátory rozvodů

Koncentrátory vedení jsou pouze pasivní prvky umožňující vytvářet určitou schématickou topologii, například vytvoření schématu hvězda u kruhové sítě Token Ring, nebo poskytují napájení, či zajišťují překlenutí neaktivního portu v síti s kruhovou topologií.

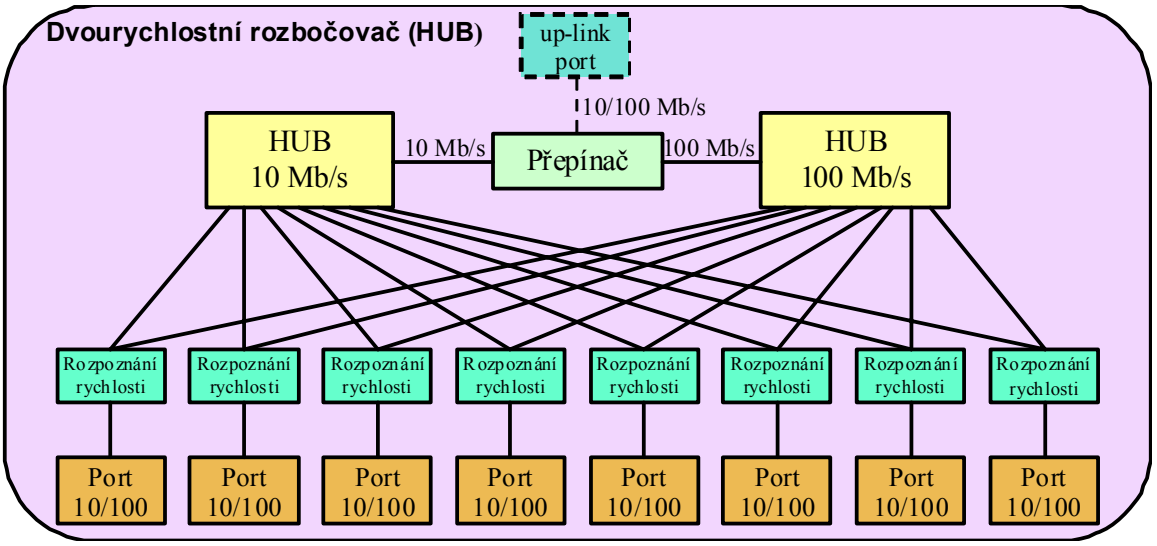
3.5.2 Opakovače a rozbočovače

Opakovače (repeaters) a rozbočovače (HUBs) jsou prvky pracující na fyzické úrovni vrstvového modelu sítě. Jejich hlavním úkolem je obnova (regenerace) signálu, tedy obnovení tvaru, časové polohy pulzů a doplnění bitové informace přidané na fyzické vrstvě (synchronizační směsi) tak, aby mohl být rámec správně přijat cílovou stanicí. Tato zařízení nerozlišují přenášený obsah, pracují se symboly. **Opakovač** je zařízení **se dvěma porty** a **rozbočovač** je zařízení **s mnoha porty**. **Signál přijatý** na jednom portu je regenerován a **odeslán na všechny ostatní porty** (nikoliv na port původní!). Jedná se o zařízení bez vyrovnávacích pamětí, zařízení **na všech portech** musí přenášet data **se stejnou rychlostí**! Do přenosové cesty tak prvek vkládá určité, byť malé, zpoždění. Pro vytvoření rozsáhlejších sdílených domén lze propojit více rozbočovačů. Pro správnou funkci je však **nutná striktní stromová struktura** (podobně jak je tomu u přepínačů, zde však neexistuje řešení pro vytváření záložních spojů, tudíž výpadek spoje či celého uzlu znemožní přístup řadě stanic do zbytku sítě). Je-li síť citlivá na zpoždění (například z důvodu přístupové metody, např. u sdíleného Ethernetu), je počet opakovačů v kaskádě (a tak i počet propojených segmentů) mezi libovolnými dvěma koncovými uzly (nebo koncovým uzlem a přepínačem či směrovačem) sdílené domény omezen. Všechny části propojené pouze opakovači (rozbočovači) tvoří jeden fyzický sdílený kanál (jednu kolizní doménu u sdíleného Ethernetu). Všechny porty pracují se stejnou rychlostí. Pokud to síťová technologie dovoluje, lze tyto prvky řadit do kaskády (pro propojení se použije buď překřížený kabel, nebo je vyhrazen speciální port s možností přepnout přijímací a vysílací pár), případně stohovat (propojit krátkým rychlým spojem, takže se více rozbočovačů chová jako rozbočovač jediný). Některé prvky tohoto typu umožňují propojit segmenty realizované odlišnými typy vedení, například koaxiální kabel a kabel UTP, tzn. že se jednotlivé porty liší ve spodní podvrstvě fyzické vrstvy (PMD – Physical Media Dependent). Opakovače a rozbočovače se používají u LAN sítí v případě Ethernetu, neboť u kruhové topologie se regenerace signálu provádí v přijímací části jednotlivých stanic (použití by bylo možné, pokud by jednotlivé stanice byly od sebe dál, než stanovuje limit pro daný typ sítě). Opakovače a rozbočovače jsou pro stanice i směrovače transparentní, tj., že nemají ani fyzickou a ani síťovou adresu (neobsahují-li dohledový modul) a stanice tudíž o jejich přítomnosti neví.

Vyšší třídy rozbočovačů jsou vybaveny modulem pro dohled (SNMP modul), případně možností rozpoznat a odpojit vadný port, či dokonce možností zálohovat port dalším portem, který se uvede v činnost až při selhání prvotního portu.
Vlastnosti rozbočovačů lze tedy shrnout do několika bodů:

- operace na fyzické vrstvě,
- obnova a rozbočení sledu symbolů z jednoho portu do všech ostatních portů
- počet portů,
- shodná přenosová rychlost na všech portech,
- typy fyzických rozhraní (koaxiální kabel, UTP, optický kabel),
- stohovatelnost, kaskádování,
- modul vzdálené správy,
- záložní napájecí zdroj,
- možnost zálohy portů.

V době začátku nástupu přepínačů (polovina devadesátých let dvacátého století) se objevil prvek nazývaný jako „dvourychlostní rozbočovač“. Z charakteristiky klasického rozbočovače vyplývá, že všechny porty musí pracovat se stejnou rychlostí, takže dvourychlostní rozbočovač nemůže být „čistým“ rozbočovačem, ale musí v sobě obsahovat jednak dvou či tříportový přepínač s vyrovnávacími pamětmi a obvod pro automatické vyhodnocení nejvyšší podporované rychlosti připojeného zařízení a přepojení portu na odpovídající deseti- či stomegabitový rozbočovač, viz **Obr. 3.5**.



Obr. 3.5: **Architektura „dvourychlostního rozbočovače“**

V současnosti se používání rozbočovačů, a tedy vytváření sdílených domén, v Ethernetu nedoporučuje, protože jednak to snižuje propustnost sítě, protože povolují pouze poloduplexní typ komunikace, a dále není garantovaná doba úspěšného odeslání datové jednotky - náhodná přístupová metoda s kolizemi a bez prioritizace provozu citlivého na zpoždění.

3.5.3 Mosty a přepínače

Mosty (bridges) a přepínače (switches) jsou spojovací prvky, které svoji činnost rozšiřují oproti opakovačům a rozbočovačům o spojovou (linkovou) vrstvu, konkrétně o její spodní část - podvrstvu označovanou jako MAC (Medium Access Control). Slouží k propojení/oddělení částí sítě mající vlastní přenosový kanál:

- **Ethernet** – vytvářejí stromovou strukturu sítě, podporují agregaci a redundanci spojů, podporují vytváření virtuálních sítí LAN, případně oddělují/propojují tzv. kolizní domény,
- **Token Ring** - oddělují/propojují nezávislé kruhy,
- **Frame relay** – přepínají rámce podle identifikátorů virtuálních okruhů (DLCI – Data Link Connection Identifier),
- **ATM** – přepínají buňky podle tzv. virtuálních kanálů (VCI – Virtual Channel Identifier) a virtuálních cest (VPI – Virtual Path Identifier), implementují třídy QoS.

V této kapitole se však budeme věnovat především mostům a přepínačům v sítích LAN (Ethernet, Token Ring).

3.5.3.1 Vlastnosti přepínačů a mostů

Hlavní funkcí přepínačů je **přepínání rámců** na základě informací uložených v přepínací tabulce, která obsahuje vazbu mezi hardwarovou (fyzickou, MAC) adresou a odpovídajícím portem, kam je stanice buď přímo, nebo přes opakovač(-e) či přes další přepínač(-e) připojena. **Budování tabulky je automatický proces**, tedy bez zásahu člověka. Přepínač (most) si z příchozích rámců čte nejenom cílovou fyzickou adresu určující, kam se bude rámec přepínat, ale také zdrojovou adresu, a tu si spolu s číslem portu zaznamená do tabulky (pokud již tento záznam v tabulce není z dřívější doby). Přijde-li pak rámec na tuto adresu, přepínač záznam vyhledá a přepojí rámec na příslušný port. Není-li záznam s cílovou adresou v tabulce nalezen, nebo je-li cílová adresa všesměrovou adresou, je rámec rozeslán podobně jako u rozbočovače na všechny ostatní porty.

Most je prvek se dvěma porty (byl používán dříve pro připojení segmentů k páteřní síti), přepínač je mnohaportový prvek.

Výhodnou vlastností mostů a přepínačů je možnost propojení segmentů **pracujících s různou přenosovou rychlostí**, samozřejmostí je dnes podpora více rychlostí na jednom portu (u sítě Ethernet např. 10/100/1000 Mb/s) a jejich **automatické rozpoznání (auto negotiation)**. Přepínač je za tímto účelem a pro vyrovnávání krátkodobých špiček v zatížení vybaven vyrovnávacími pamětmi.

Při úplném zahlcení přijímacích vyrovnávacích pamětí by hrozilo, že další rámce určené k přepnutí budou ztraceny. Většina moderních přepínačů však umí řídit provoz tak, aby k tomu nedošlo. Řeší se to dvěma základními způsoby:

- vytváření stavů kolize na zahlceném portu pracujícím v režimu poloduplexu (používající metodu CSMA/CD), a to tak dlouho, dokud se přijímací paměti opět neuvolní.
- pomocí zpráv PAUSE (systém XON/XOFF) - jsou-li kolizní domény odstraněny a na port přepínače sítě Ethernet je připojena pouze jediná stanice nebo se jedná o propojení mezi dvěma přepínači či mezi přepínačem a směrovačem, pak rozhraní umožňují přejít od poloduplexního režimu s metodou CSMA/CD na **plně duplexní provoz**, kdy nehrozí kolize, proto je metoda CSMA/CD vypnuta. Tím se podstatně zvýší propustnost sítě. Tento režim však znemožňuje řízení toků pomocí umělého generování kolizí a vyžaduje jiný způsob řešení problému zahlcení jedné z komunikujících stran, a to pomocí speciální zprávy PAUSE (XON/XOFF) udávající dobu pozastavení vysílání v násobcích trvání odeslání bloku 512 bitů. Tato zpráva je odeslána na „well known“ multicast MAC adresu 01-80-C2-00-00-01

Mosty dělíme do dvou typů:

1. **lokální** – propojují dva segmenty sítí LAN

nacházející se v jedné lokalitě,
2. **vzdálené** – propojují vzdálené segmenty LAN přes transportní síť pevným či komutovaným spojem (např. ISDN). Především komutované propojení pomocí mostů je však nevýhodné, protože mosty nefiltrují všesměrové rámce a tudíž je často spojení udržováno (a placeno) zbytečně jen kvůli přenosu mnohdy nepotřebných dat.

Z hlediska činnosti přepínačů rozlišujeme několik typů:
1. **Cut-through** (On the fly) – přepínač načte z přicházejícího rámce cílovou fyzickou adresu a ihned zahájí vyhledávání cílového portu a posléze přepínání rámce. Jedná se o nejrychlejší způsob přepínání, který však skrývá dosti podstatnou nevýhodu, a to, že přepíná i neúplné a chybné rámce, které pak zbytečně zatěžují síť.
2. **S kontrolou minimální délky rámce** – v síti Ethernet je specifikována minimální délka rámce, která je nutná pro správnou funkčnost přístupové metody CSMA/CD (např. 512 bitů pro Ethernet 10/100 Mb/s). Přepínač tedy nejprve čeká, než přijme tuto minimální délku rámce a pak teprve, není-li detekována kolize, či jinak není vysílání rámce narušeno, začne s přepínáním rámce. Tak se zamezí přepínání fragmentů rámců, které byly poškozeny kolizemi. Ani tato technika neprovádí kontrolu bezchybnosti celého rámce.
3. **Store and Forward** – celý rámec se nejprve načte do vyrovnávací paměti, pak se zkontroluje jeho bezchybnost a teprve, je-li v pořádku, dojde k jeho přepnutí. Tento režim je nejpomalejší, avšak zamezí předávání jak neúplných, tak i chybných rámců.
4. **Adaptive switching** - některé přepínače umožňují vyhodnocování kvality připojených spojů, režim činnosti portu (poloviční či plný duplex), případně i četnosti kolizí, a přepínají mezi režimy tak, aby efektivní propustnost přepínače byla co nejlepší a síť se příliš nezatěžovala neúplnými či chybnými rámci.

Přepínače lze vzájemně propojovat do stromové struktury pomocí překříženého kabelu, speciálního portu s možností přepnutí vstupního a výstupního páru či pomocí automatického rozpoznání protějšího prvku a přepnutí úlohy párů v konektoru – technika „Auto – MDIX“.

Požadavkem pro správnou funkci sítě s přepínači v síti Ethernet je **stromová struktura sítě** uzlů (v případě sítě Ethernet) či stromová struktura kruhů (v případě sítě Token Ring). Pokud by to nebylo dodrženo, došlo by po prvním všesměrovém či neznámém rámci k zahlcení a zhroucení sítě („Broadcast storm“)! Čistá stromová struktura má však slabinu, a to existenci pouze jediné cesty mezi dvěma uzly sítě, tedy nebezpečí odpojení větve sítě od zbývající části sítě v případě výpadku spoje či uzlu. Proto pro zvýšení bezpečnosti se záložní cesty budují, ty je však za normální činnosti zapotřebí vypnout tak, aby byla funkční pouze čistá stromová struktura. O to se stará protokol označovaný jako **STP** (Spannig Tree Protocol – součást specifikace IEEE 802.1D) řešící problematiku vytyčení logické stromové struktury pomocí algoritmu **STA** (Spanning Tree Algorithm), viz kap. 4.4. Mosty si pravidelně (každé 1 - 4 sekundy) vyměňují zprávy (**BPDU** – Bridge Protocol Data Unit) o konfiguraci. V případě výpadku aktivního spoje algoritmus do určité doby (řádově jednotky až desítky sekund) zajistí obnovení konektivity stromu aktivací náhradního spoje. Standard 802.1w vylepšuje rychlost obnovy konektivity a stromové struktury na jednotky sekund specifikací protokolu **RSTP** (Rapid STP). Ten byl v roce 2004 zapracován i do původního standardu IEEE 802.1D, kde nahradil původní protokol STP, jenž byl odstraněn.

Činnost mostů a přepínačů při příchodu rámce můžeme popsat takto:
- rámec je zahozen,

    - ♦ je-li rámec neúplný či chybný a je-li zvolen režim s kontrolou minimální délky či s úplnou kontrolou,
    - ♦ je-li určen stanici, která je připojena ke stejnému segmentu, odkud rámec přišel (není třeba nic přepínat),
    - ♦ je-li přijímací vyrovnávací paměť plná,
- rámec je přepnut na odpovídající jiný port, byl-li v přepínací tabulce nalezen patřičný záznam
- rámec je poslán na všechny ostatní porty,
    - ♦ je-li umístění cílové stanice neznámé (není záznam v přepínací tabulce),
    - ♦ je-li rámec zaslán všesměrově.

Je nutné zdůraznit, že všechny segmenty propojené přepínači (a rozbočovači) tvoří jedinou síť, což znamená, že se celou sítí šíří všesměrové rámce s dotazy a odpověďmi (viz popis činnosti přepínače). To může při větší velikosti sítě, množství poskytovaných služeb a větším provozu dosti velkou měrou zatěžovat síť. Snaha o zachování výkonnosti přepínání a o zavedení filtrace všesměrového šíření vedla k návrhu **virtuálních sítí LAN** označovaných zkráceně **VLAN** (Virtual LAN – **IEEE 802.1Q**), podrobněji viz kap. 4.3. Stanice připojené k přepínačům jsou podle určitého klíče přidělené k určité síti VLAN a všesměrové rámce se šíří pouze uvnitř dané sítě VLAN. Pro každou VLAN může existovat separátní instance protokolu STP.

Most/přepínač je přepojovací prvek, kde dochází ke zpoždění průchodu rámce, které je navíc silně ovlivněno provozem. Zavedení služeb pracujících v reálném čase (telefonie, video, atd.) vyžaduje implementaci podpory pro přednostní zpracování rámců těchto služeb. Toto opatření je představováno zavedením priorit podle normy **IEEE 802.1p/Q**. Informace o prioritě jsou součástí 4B značky (Tag) přidávané do rámce za účelem rozlišení sítí VLAN (viz kap. 4.3).

Dnešní komunikace ve velké míře v síti směřuje od koncového uzlu do vyšších úrovní, často do globální sítě Internet. Dochází tak směrem k vyšším úrovním k nárůstu zátěže. Pro zamezení zahlcení a ztrát rámců bývají přepínače vybaveny 2 až 4 porty s vyšší rychlostí (například 100-megabitové přepínače mají 2 gigabitové porty), které je vhodné použít tam, kde se soustřeďuje vyšší provoz, například jako příčka k dalšímu přepínači či jako přípoj ke směrovači (do Internetu – je-li zajištěna vysoká propustnost dále do Internetu) a nebo jako připojení k silně využívanému serveru. Navýšení propustnosti lze však vyřešit i pomocí tzv. **Agregace portů** (Port Trunking nebo také Link Aggregation) – sdružování portů do tzv. trunku za účelem zvyšování přenosové kapacity v určitém směru, kdy je nejčastěji možno sdružit od 4 až do 8 portů do 1 trunku. Tak například u 100 Mb/s portů je možno vytvořit spoj s kapacitou až 400 Mb/s nebo i až 800 Mb/s. V přepínačích může být implementováno **proprietární** řešení či **staticky** a nebo řešení dle standardu IEEE **802.1AX-2008** (dříve pouze pro kabelový Ethernet a označovaný jako IEEE **802.3ad** – Link Aggregation Control Protocol) – protokol nezávislý na fyzickém médiu. Zařízení pracující s protokolem LACP zasílají po sdružených portech datové jednotky označované jako LACPDU, jenž slouží k identifikaci agregovaného spoje a k detekci výpadku některého z linek spoje.

Doplňkovými funkcemi přepínačů mohou být:

1. **Bezpečnost** – omezení možnosti připojování nových zařízení na daný port – režimy normal/limited/secure = bez omezení/s omezením počtu MAC adres na daný port s aktivním stárnutím záznamů/s, možnost **uzamčení aktuálního stavu přepojovací tabulky** s deaktivovaným stárnutím záznamů.

2. **Dohled nad všesměrovým vysíláním** – omezení počtu všesměrových rámců za sekundu, které mohou daným portem projít (nejčastěji udávané jako několik úrovní, např. Low/Medium/High).
3. **Monitorování portů** – odbočení toku z monitorovaného portu na monitorovací port za účelem sledování a analýzy toku.
4. **Statistika provozu** na portech.
5. Podpora **napájení nízkopříkonových zařízení po kabeláži UTP**, tzv. PoE (Power over Ethernet) buď dle **IEEE 802.3af** (do 15,4 W), nebo **IEEE 802.3at** (až 25,5 W).

Přepínače vyšší třídy mohou být dále vybaveny **dohledovým modulem SNMP** (se sériovým portem pro konfiguraci síťového rozhraní – vlastní IP adresa, maska podsítě, adresa směrovače, …), mohou umožňovat **stohování** a vytvářet tak přepínač s *n*-násobným počtem portů (např. až 4x48 = 192 portů).

Vlastnosti přepínačů lze shrnout do několika bodů:

- určitý počet portů (4, 8, 12, 24, 48),
- podporované rychlosti, možnost automatického rozpoznání rychlosti (auto-negotiation),
- podpora duplexního provozu,
- způsob propojení s dalším přepínačem či rozbočovačem, automatické rozpoznání párů (auto-MDIX),
- celková propustnost spojovacího pole, s blokováním, nebo bez blokování - tzv. „wirespeed“ ,
- velikost vyrovnávacích pamětí a způsob řešení zahlcení,
- velikost paměti pro záznamy (adresy),
- způsob přepínání či možnost automatického výběru typu na základě parametrů provozu,
- možnost zálohování či agregace portů,
- podpora protokolu STP, počet STP instancí,
- možnost vytváření VLAN – počet, způsob rozlišení příslušnosti k dané VLAN,
- podpora QoS,
- přítomnost záložního zdroje,
- modul (SNMP, RMON) pro vzdálenou správu.

Pozn. Existují i přepínače, které pracují až na podvrstvě LLC, tzn., že jednotlivé porty mohou mít i odlišnou MAC podvrstvu. Takovéto přepínače pak umožňují propojit sítě se shodnou LLC podvrstvou, např. Token Ring a Ethernet.

3.5.3.2 Zdrojové přepínání (Source Route Bridging)

Zdrojové přepojování je způsob propojení kruhů Token Ring na linkové úrovni. Nejvhodnější cestu k cíli si zjišťuje zdrojový uzel sám a tuto cestu vkládá do záhlaví rámců (pole RIF – Routing Information Field) nesoucích data pro cílovou stanici. Tento způsob umožňuje existenci více cest na linkové úrovni. Zdrojová stanice vyšle průzkumný rámec, který prochází všemi mosty a kruhy směrem k cíli. Mosty do průzkumného rámce zaznamenávají informace (identifikátor mostu, identifikátor kruhu, kam bude rámec odeslán, a velikost MTU – Maximum Transfer Unit), čímž se zaznamená cesta a zamezí se vzniku smyček. Cílový uzel pak vrátí rámec stejnou cestou zpět. Zdrojová stanice pak vyhodnotí

vrácené rámce podle určitých kritérií (rychlost návratu, počet mezilehlých mostů, velikost MTU) a vybere nejvhodnější cestu.

3.5.4 Směrovače

Směrovače jsou síťové prvky zahrnující vrstvy fyzickou, linkovou a síťovou. Jejich hlavním úkolem je směrování paketů jednotlivými sítěmi ležícími na cestě mezi zdrojovou a cílovou sítí. Používají se pro oddělení/propojení LAN sítí, připojení sítě LAN k síti WAN a propojení částí sítí WAN. Směrovače tak oddělují dílčí sítě a tak filtrují všesměrové pakety určené pro danou síť. Existují však i nesměrovatelné protokoly (např. NetBios). Takové protokoly pak směrovač distribuuje všesměrově, pokud jejich šíření podporuje. Většinou je omezena vzdálenost (počet směrovačů), na kterou se daný nesměrovatelný protokol šíří. Znalost struktury paketů také směrovače předurčuje k možnosti implementace bezpečnostních mechanizmů (firewall).

Směrovače umožňují vytvářet složité síťové konfigurace polygonálního charakteru, které dovolují existenci více cest k danému cíli a tak zajišťují vysoký stupeň zabezpečení konektivity.

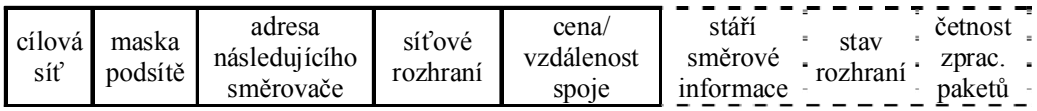
Směrovače pracují podle určitého směrovacího mechanizmu, nejčastěji se jedná o distribuovaný způsob směrování, kdy si každý směrovač buduje na základě komunikace s ostatními směrovači podle určitého **směrového protokolu** vlastní **směrovou tabulku** (častěji označovanou jako **směrovací tabulku**). Ta obsahuje záznamy určující, kam mají být pakety s určitou cílovou sítí předány. Pakety (mluvíme o datagramové službě) nesou informace o **síťové adrese** zdroje a cíle. Síťová adresa se nejčastěji rozděluje na dvě, případně tři základní části (adresa sítě, adresa síťového rozhraní a případně adresa podsítě). Směrovací tabulka nese záznamy pouze o cílové síti, případně o podsíti a také běžně obsahuje záznam o implicitním směru pro směrování do sítí, pro které v tabulce neexistuje záznam. Směrové tabulky mohou být:

- **statické** - směrovací informace jsou uloženy do tabulky ručně při konfiguraci směrovače. Změny musí být také prováděny ručně nebo pomocí řídicího protokolu síťové vrstvy (např. protokol ICMP sady TCP/IP). Je to vhodný způsob pouze pro jednoduché a stálé sítě. Záznam ve statické směrovací tabulce nejčastěji obsahuje tyto základní údaje:

cílová síť	maska podsítě	adresa následujícího směrovače	síťové rozhraní	stav rozhraní	četnost zprac. paketů

  Cílová síť – IP adresa cílové sítě,
  Maska podsítě – určuje jaká část IP adresy je adresa podsítě. Slouží při prohledávání směrovací tabulky k určení rozhraní kterým se bude paket posílat. Cílová IP adresa se vynásobí s maskou a výsledek se porovná s hodnotou cílové sítě. Je-li více kladných výsledků, vybere se ten směr, pro který byla maska podsítě nejdelší (nejdelší sled jedniček),
  Adresa následujícího směrovače – pokud cílová síť není připojena přímo k danému rozhraní, posílá se paket dalšímu směrovači ležícímu na cestě k síti,
  Síťové rozhraní – určuje kterým rozhraním směrovače se bude paket posílat směrem k cíli,
  Stav rozhraní – informace o stavu rozhraní (zapnuto/vypnuto).
- **dynamické** – směrovací uzly si mezi sebou vyměňují pravidelně směrové informace, čímž získávají informace o struktuře a stavu sítě, ze kterých si budují směrové tabulky výběrem nejlepšího směru pro danou cílovou síť. To oproti statickému směrování částečně zatěžuje síť. Výměny jsou zajišťovány směrovými protokoly. V síti TCP/IP to

jsou především protokoly RIP (Routing Information Protocol) a OSPF (Open Shortest Path First) a v sítích IPX/SPX pak IPX/RIP a NLSP (NetWare Link State Protocol). Tento způsob je vhodný pro rozsáhlejší a často se měnící sítě. Záznam dynamické směrovací tabulky obsahuje tyto základní údaje informace:



Cena/vzdálenost spoje – určuje, jak výhodné je poslat paket danou cestou. Vhodnost spoje může být určena „vzdáleností“ (počet mezilehlých směrovačů) či jeho cenou, což je hodnota vypočtená z řady parametrů dané cesty (počet mezilehlých směrovačů, přenosové rychlosti jednotlivých úseků, hodnoty MTU = Maximum Transfer Unit pro jednotlivé úseky, momentální stav úseků, apod.),

Stáří směrové informace – u dynamického směrování je zapotřebí informace pravidelně aktualizovat. To znamená, že pokud informace není obnovena do určité doby, je považována za starou, a tedy neplatnou.

Většinou pro daný cíl existuje pouze jediný záznam, a tedy jediná cesta. Novější směrové protokoly (OSPF) však umožňují existenci více stejně vhodných cest, a tedy možnost rozložení zátěže do více cest.

Směrové protokoly se rozdělují na:

- **vnitřní** (IGP – Interior Gateway Protocol) – protokoly používané uvnitř autonomního systému (oblast s jednotnou směrovací politikou), například RIP, OSPF.
- **vnější** (EGP – Exterior Gateway Protocol) – protokoly mezi hraničními směrovači odlišných autonomních systémů. Příkladem může být protokol BGP (Border Gateway Protocol).

Dalším úkolem směrovačů je realizovat překlad abstraktních (logických) síťových adres na konkrétní fyzické adresy sítě, která je připojena na rozhraní, kam má být paket směrován. Například v sadě TCP/IP existuje protokol ARP (Address Resolution Protocol).

Směrovač bývá často připojen k různým typům rozhraní s různou přenosovou rychlostí a také s různou hodnotou MTU (Maximum transfer unit) udávající maximální délku datové jednotky (rámce) přenášené daným spojem. Proto se může stát, že směrovač musí směrovaný paket rozdělit do několika menších tak, aby byla podmínka MTU splněna.

Může se stát, že jsou směrovací informace v tabulce některého ze směrovačů chybné. Pak může dojít k tomu, že paket nemůže být doručen a bloudí sítí. I tuto situaci směrovač musí řešit, a to kontrolou tzv. „doby života“ paketu. Době života odpovídá číslo v záhlaví paketu, které se s každým průchodem směrovačem snižuje, dokud není paket doručen, nebo dokud hodnota čísla neklesne na nulu. Pak je paket zahozen, aby nezatěžoval zbytečně síť.
S touto činností je spojen také přenos různých zpráv (nejčastěji chybových) týkající se stavu síťové vrstvy. Patří sem zprávy o nedosažitelnosti cíle, o zahození paketu, o existenci vhodnější cesty (přes jiný směrovač), časové informace udávající zpoždění mezi zdrojovou a cílovou stanicí, apod.

Pro integraci služeb do paketových sítí je vyžadováno, aby všechny přepojovací prvky sítě podporovaly různé třídy kvality služeb, tzv. QoS. K tomu se používá na síťové vrstvě dvou mechanizmů:

- IntServ (Integrated Services),
- DiffServ (Differentiated Services).

3.5.5 Smíšené propojovací prvky

Pro pružnější vytváření různých topologií a zachování možnosti použití starší (a pomalejší) techniky a díky vývoji technologie vznikly kombinované propojovací prvky, kam patří:

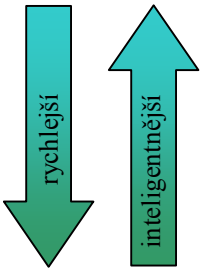
- **dvourychlostní rozbočovače** (HUBs) – kombinují vlastnosti fyzické a linkové vrstvy. Zařízení existuje v podobách
  - ***oddělené skupiny portů s různými rychlostmi*** **(**10 nebo 100 Mb/s) – tyto porty jsou uvnitř propojeny nízkoportovým přepínačem,
  - ***libovolný z portů může pracovat s různými rychlostmi*** (10 i 100 Mb/s) – port automaticky rozpozná rychlost komunikující strany a přes odpovídající transceiver port připojí do patřičné skupiny portů sdílející danou přenosovou kapacitu. Tyto skupiny jsou pak propojeny a navenek připojeny přes přepínač.
- **integrované přepínače/směrovače** – Směrovač je integrován do přepínače za účelem propojení sítí VLAN a pro vytvoření hraničního prvku sítě LAN, který se směrem do sítě WAN (či jiné LAN) chová jako směrovač a směrem do sítě LAN jako přepínač.
- **přepínače na 3. vrstvě OSI** (Layer 3 Switching). Jedná se o vlastně o směrování prováděné hardwarově. Důvod pro zavádění této technologie je následující - před řadou let se pro rozdělení sítí do více skupin používaly směrovače (tzv. colapsed backbone architektura). Při stále narůstajícím zatížení sítí přestaly směrovače vyhovovat (nízký výkon za vysoké ceny, velké zpoždění paketů při průchodu směrovačem – viz. tabulka). V té době přišly na svět výkonné přepínače. Začaly jimi být nahrazovány centrální směrovače, ale správci sítí si společně s dodavateli velice záhy ověřili slabinu přepínačů – přenášejí broadcast pakety a tudíž se sítě s vysokým počtem stanic začínají zahlcovat. Směrovače proto znovu našly uplatnění v propojování segmentů sítí oddělených pomocí VLAN postavených na přepínačích. Protože jsou však směrovače drahé a technologický rozvoj postoupil značně dopředu, začali výrobci hledat cesty jak řešení maximálně zlevnit. Jako jedna z nejschůdnějších se ukázala cesta integrace směrování do přepínačů, tedy tzv. Layer 3 Switching. V podstatě se jedná o obdobu přepínání na druhé vrstvě – zde je přepínání na základě tabulky MAC adres; na třetí vrstvě je přepínání také řešeno hardwarově a rozhodovací algoritmy jsou rozšířeny o další tabulku – tabulku logických adres (převážně IP). Definice směrovacího přepínače (Routing Switch), tak jak jej zavedla firma, která tento pojem začala používat jako první, tedy Bay Networks, hovoří o několika základních atributech:
  - přepínání na 3. vrstvě je implementováno v hardware,
  - směrování a přepínání jsou stejně rychlé,
  - zařízení zajišťuje libovolnou kombinaci přepínání i směrování na každém portu,
  - výborná průchodnost při zvýšeném zatížení, implementaci filtrů nebo použití QoS zůstane zachována,
  - zařízení rozhoduje o každém paketu,
  - zařízení umožňuje provozování standardních směrovacích protokolů (RIP, OSPF).

3.5.6 Přepojování na vyšších vrstvách

Přepojování na vyšších vrstvách je též nazýváno jako „Layer/4-7 Switching“ či „Content (Web) Switching“, neboť inteligentní přepojování a rozhodování je založeno na informacích ve 4-7 vrstvě OSI modelu.

Tab. 3.1: Přepojování na různých vrstvách modelu ISO/OSI

Vrstvy modelu ISO/OSI	Princip přepojování



aplikační	http přepojování založené na URL
prezentační	pro přepojování se nevyužívá
relační	pro přepojování se nevyužívá
transportní	TCP/UDP přepojování založené na číslech portů
síťová	přepojování založené na IP adresách
spojová (linková)	přepojování založené na HW (MAC) adresách
fyzická	pro přepojování se nevyužívá

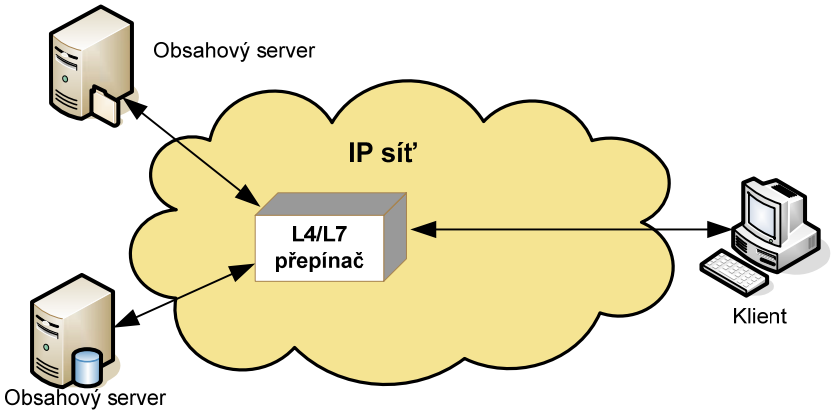
Na úrovni transportní vrstvy se pracuje s přístupovými body aplikací (porty), informací na páté a šesté vrstvě modelu OSI se nevyužívá, obsah zprávy se využívá pro přepojování na úrovni vrstvy aplikační.

V případě protokolu TCP/IP se jedná pouze o sedmou, aplikační vrstvu. Na základě znalosti

- obsahu paketu (http cookie),
- tabulky vytížení serverů,
- mechanismů pro zjišťování stavu serverů (FireWallů) atd.,

se tato technologie využívá nejen k přepojování podle umístnění požadovaného obsahu, ale také na:

- mnohem efektivnější využití webových zrcadel (web cache). Prohlédnutím obsahu URL požadavku, mohou být směrovány statické stránky z webových zrcadel (web cache), zatímco dynamické stránky jsou obslouženy přímo web serverem.
- Server load balancing (rozkládání zátěže na jednotlivé servery ve skupině);
- Global server load balancing – geografické rozkládání zátěže s optimalizací ISP prostředí (rozložení serverů do několika geograficky vzdálených lokalit s přesměrováním podle místa, odkud se klient dostává na server);
- FireWall load balancing – možnost zapojení redundantních systémů FireWall s rozložením zátěže;
- zvýšení bezpečnosti omezením pásma pro určité aplikace – ochrana proti DoS - (např. otevírání portů s neznámým portem);
- řízení pásma pro jednotlivé aplikace a adresy;
- Cache redirection (tedy přesunutí cache blíž k uživatelům, a tím i zvýšení rychlosti přenosu dat).



Obr. 3.6**: Příklad přepínání podle obsahu (content switching)**

Příklad inteligentního přepojování je ukázán na **Obr. 3.6**. Požadavek klienta je obsloužen inteligentním přepínačem, který s ním sestaví relaci. Přepínač funguje jako proxy pro více

serverů použitím techniky Virtual IP (VIP). Jestliže, požadavek obsahuje více objektů, je postupně vyřizován přepínačem a jednotlivými servery. Pro klienta zůstávají servery neviditelné, komunikuje přímo pouze s přepínačem.

3.5.7 Brány

Brány jsou propojovací prvky zajišťující komunikaci mezi sítěmi s odlišnými síťovými a vyššími protokoly. Brány tedy zajišťují konverzi mezi protokoly na všech vrstvách síťového modelu. Příkladem může být propojení poštovních systémů sady TCP/IP (SMTP – Simple Mail Transfer Protocol) a ISO/OSI (ITU X.400), tzv. e-mailová brána, nebo propojení sítě ISDN a TCP/IP sítě pro realizaci telefonního spojení (datová a signalizační brána – medium and signalling gateway).

4 Datové sítě LAN a MAN

Sítě LAN a MAN jsou počítačové sítě o dosahu stovek metrů až desítek kilometrů. Hlavním požadavkem je dostatečná propustnost sítě pro rychlý přenos dat a případně podpora služeb v reálném čase, jako jsou hlasová služba, přenos videa, apod.

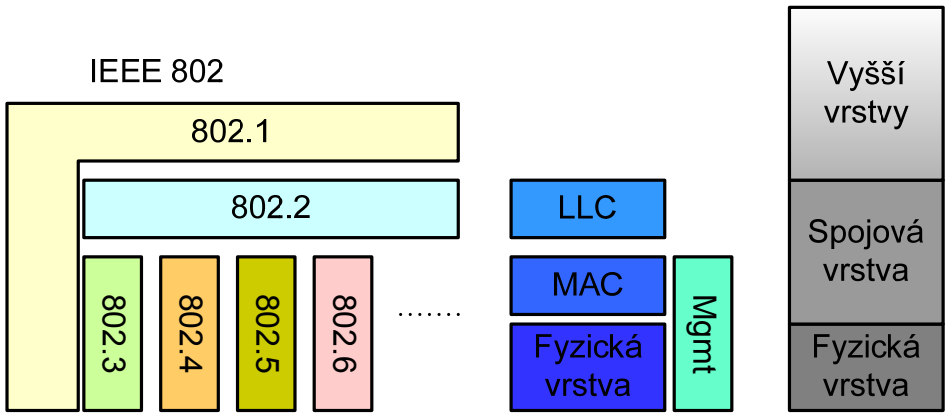
4.1 Standardizace datových sítí LAN a MAN

O rozvoj technologií datových sítí typu LAN a MAN se stará organizace **IEEE**, konkrétně její oddělení (projekt) **802**, které je dále děleno na pracovní skupiny, zabývající se standardizací jednotlivých síťových technologií, dále řízením komunikace, propojováním sítí do větších celků, mobilitou a správou daného typu sítí, viz **Obr. 4.1**.

Tab. 4.1: Oblast působnosti projektu IEEE 802 (kompletní výpis – stav 01/2012)

Název	Popis	Info
IEEE 802.1	Bridging (networking) and Network Management	
IEEE 802.2	LLC	neaktivní
IEEE 802.3	Ethernet	
IEEE 802.4	Token bus	skupina rozpuštěna
IEEE 802.5	Defines the MAC layer for a Token Ring	neaktivní
IEEE 802.6	MANs	skupina rozpuštěna
IEEE 802.7	Broadband LAN using Coaxial Cable	skupina rozpuštěna
IEEE 802.8	Fibre Optic TAG	skupina rozpuštěna
IEEE 802.9	Integrated Services LAN	skupina rozpuštěna
IEEE 802.10	Interoperable LAN Security	skupina rozpuštěna
IEEE 802.11 a/b/g/n	Wireless LAN (WLAN) & Mesh (Wi-Fi certification)	
IEEE 802.12	100BaseVG	skupina rozpuštěna
IEEE 802.13	CSMA/CD CSMA/CA	
IEEE 802.14	Cable modems	skupina rozpuštěna
IEEE 802.15	Wireless PAN	
IEEE 802.15.1	Bluetooth certification	
IEEE 802.15.2	IEEE 802.15 and IEEE 802.11 coexistence	
IEEE 802.15.3	High-Rate wireless PAN	
IEEE 802.15.4	Low-Rate wireless PAN (ZigBee, WirelessHART, MiWi, atd.)	
IEEE 802.15.5	Mesh networking for WPAN	
IEEE 802.16	Broadband Wireless Access (WiMAX certification)	
IEEE 802.16.1	Local Multipoint Distribution Service	
IEEE 802.17	Resilient packet ring	
IEEE 802.18	Radio Regulatory TAG (Technical Advisory Group)	
IEEE 802.19	Coexistence TAG	
IEEE 802.20	Mobile Broadband Wireless Access	
IEEE 802.21	Media Independent Handoff	
IEEE 802.22	Wireless Regional Area Network	
IEEE 802.23	Emergency Services Working Group	Nová skupina (03/2010)

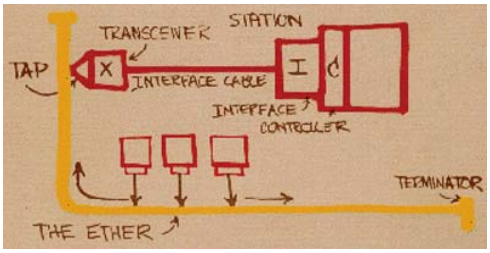
Název	Popis	Info
IEEE 802.1	Bridging (networking) and Network Management	
IEEE 802.2	LLC	neaktivní
IEEE 802.3	Ethernet	
IEEE 802.4	Token bus	skupina rozpuštěna
IEEE 802.5	Defines the MAC layer for a Token Ring	neaktivní
IEEE 802.6	MANs	skupina rozpuštěna
IEEE 802.7	Broadband LAN using Coaxial Cable	skupina rozpuštěna
IEEE 802.8	Fibre Optic TAG	skupina rozpuštěna
IEEE 802.9	Integrated Services LAN	skupina rozpuštěna
IEEE 802.10	Interoperable LAN Security	skupina rozpuštěna
IEEE 802.11 a/b/g/n	Wireless LAN (WLAN) & Mesh (Wi-Fi certification)	
IEEE 802.12	100BaseVG	skupina rozpuštěna
IEEE 802.13	CSMA/CD CSMA/CA	
IEEE 802.14	Cable modems	skupina rozpuštěna
IEEE 802.15	Wireless PAN	
IEEE 802.15.1	Bluetooth certification	
IEEE 802.15.2	IEEE 802.15 and IEEE 802.11 coexistence	
IEEE 802.15.3	High-Rate wireless PAN	
IEEE 802.15.4	Low-Rate wireless PAN (ZigBee, WirelessHART, MiWi, atd.)	
IEEE 802.15.5	Mesh networking for WPAN	
IEEE 802.16	Broadband Wireless Access (WiMAX certification)	
IEEE 802.16.1	Local Multipoint Distribution Service	
IEEE 802.17	Resilient packet ring	
IEEE 802.18	Radio Regulatory TAG (Technical Advisory Group)	
IEEE 802.19	Coexistence TAG	
IEEE 802.20	Mobile Broadband Wireless Access	
IEEE 802.21	Media Independent Handoff	
IEEE 802.22	Wireless Regional Area Network	
IEEE 802.23	Emergency Services Working Group	Nová skupina (03/2010)



Obr. 4.1: **Oblast standardizace v rámci projektu IEEE 802 (uvedeno pouze několik typů standardů)**

4.2 Ethernet

Síť Ethernet je nejpoužívanější typ lokálních počítačových sítí. Vznikl v roce 1973 ve výzkumném ústavu PARC (Palo Alto Research Center) společnosti Xerox s počáteční přenosovou rychlostí 2,94 Mb/s. Od doby zrodu však Ethernet prošel bouřlivým vývojem:



- **1973** – Robert Metcalfe z firmy Xerox podává první návrh (2,94 Mb/s po koaxiálním kabelu), [3]
- **1976** – první specifikace,
- **1979** – Bob Metcalfe přechází k firmě 3COM a publikuje standard pro 10 Mb/s,
- **1985** – standardizace Ethernetu převzata organizací IEEE,
- **1986** – jako médium je použit „tlustý žlutý“ koaxiální kabel,
- **1989** – návrh prvního přepínače pro Ethernet firmou Kalpana (nyní součást Cisca),
- **1991** – poprvé použit UTP kabel 3.kat. pro 10Base-T,
- **1994** – použití optického kabelu,
- **1995** – specifikace Fast Ethernet
- **1998** – gigabitový Ethernet 1000Base-X,
- **2000** – gigabitový Ethernet 1000Base-T
- **2002** – desetigigabitový Ethernet (po optice),
- **2006** – desetigigabitový Ethernet (po UTP),
- **2. pol. 2009** – pre-standard 40/100 Gb/s, 40 Gb/s pro konektivitu serverů, 100 Gb/s pro páteřní spoje,
- **2. pol. 2010** – standard 40/100 Gb/s (IEEE 802.3ba),
- **2015** (?) – terabitový Ethernet.

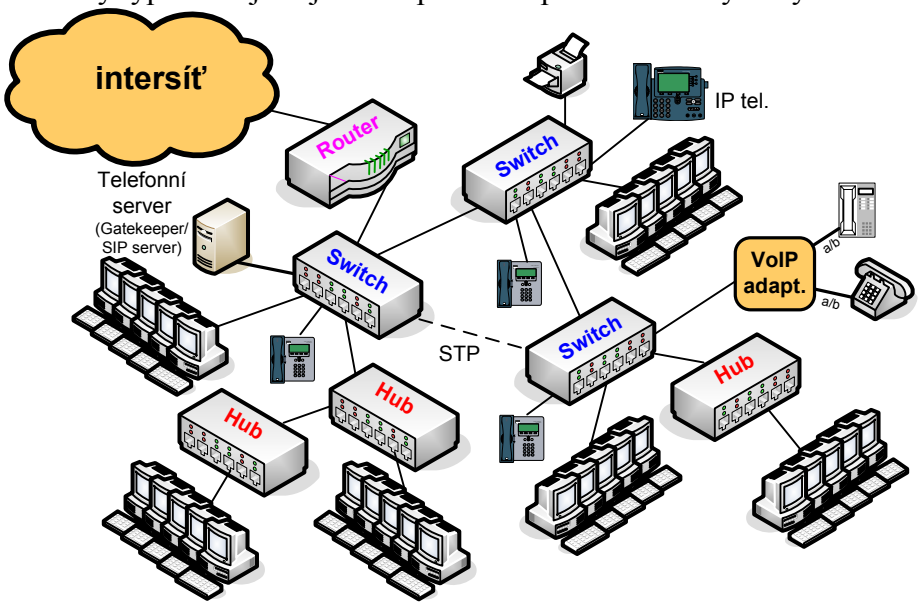
Dnes se odhaduje, že drtivá většina sítí LAN je vybudována na tomto typu sítě. V současnosti se však Ethernet (ve verzích gigabitových rychlostí) uplatňuje i na poli **metropolitních** i **rozsáhlých sítí**. Je standardizován skupinou standardů IEEE 802.3*, (* rozlišuje specifikace pro různé rychlosti a typy fyzické vrstvy), viz Tab. 4.2.

Tab. 4.2: Rychlosti, standardy a typy sítí Ethernet

Rychlost sítě	Standard	Označení typů
10 Mb/s	IEEE 802.3	10Base-2, 10Base-5, 10Base-T, 10Base-FL, 10Base-FB, 10Base-FP, 10Broad-36 (**1979 – 1993**)
100 Mb/s	IEEE 802.3u	100Base-TX, 100Base-T4, 100Base-FX (**1995**)
	IEEE 802.3xy	100Base-T2 (**1997**)
1000 Mb/s	IEEE 802.3z	1000Base-LX, 1000Base-SX, 1000Base-CX (**1998**)
	IEEE 802.3ab	1000Base-T (**2000**)
10 Gb/s	IEEE 802.3ae	10GBase-SR, 10GBase-SW, 10GBase-LX4, 10GBase-LR, 10GBase-LW, 10GBase-ER, 10GBase-EW (**2002**)
	IEEE 802.3ak	10GBase-CX4 (**2003**)
	IEEE 802.3an	10GBase-T (**2006**)
	IEEE 802.3ap	10GBase-KR, 10GBase-KX4 (**2007**)
40 Gb/s : 100 Gb/s	IEEE 802.3ba	40GBASE-KR4, 40GBASE-CR4, 40GBASE-SR4, 40GBASE-LR4, 100GBASE-CR10, 100GBASE-SR10, 100GBASE-LR4, 100GBASE-ER4 (**2010**)

Hlavními přednostmi sítě Ethernet jsou:

- široká podpora, nízká cena,
- jednoduchost technologie, snadné nasazení sítě, správa i údržba,
- možnost vytvářet rozmanité konfigurace,
- standardizovaný typ sítě zajišťující kompatibilitu produktů různých výrobců.



Obr. 4.2**: Příklad síťové topologie podle technologie Ethernet**

4.2.1 Desetimegabitový Ethernet

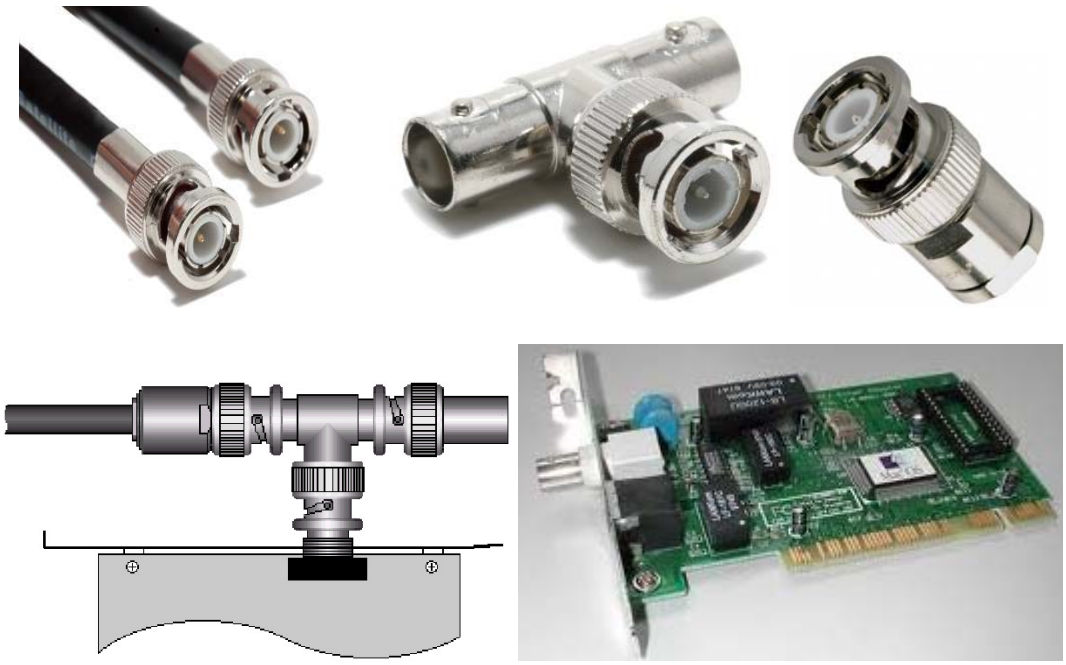
Síť Ethernet s přenosovou rychlostí 10 Mb/s je prvním standardem v řadě, který byl schválen již v roce 1983 jako standard IEEE 802.3. Síť se vyznačuje následujícími parametry:

- přenosová rychlost 10 Mb/s, kódování Manchester ±0,85 V,
- maximální počet segmentů – 5, maximálně 3 segmenty obsazeny stanicemi,
- propojení segmentů pomocí opakovačů či rozbočovačů (maximálně 4 v kaskádě),
- přístupová metoda CSMA/CD, Back-off algoritmus, náhodné zpoždění mezi $2^0 – 2^{16}$ x 9,6 μs,
- minimální délka rámce = 512 bitů (64 B) + preambule (7 B) + SFD (Start Frame Delimiter – 1 B), maximální délka rámce = 1518 B,
- mezirámcová mezera = 9,6 μs (IPG – Inter-Packet Gap), odpovídá době vyslání 96 bitů,
- maximální zpoždění ve smyčce = 51,2 μs (RTD – Round Trip Delay), odpovídá době vyslání 512 bitů, tato doba je důležitá pro včasné rozpoznání kolize na segmentu,
- fyzická adresace 48 bitů,

Bylo navrženo několik specifikací, 10Base-2, 10Base-5, 10Base-FL, 10Base-T, 10Broad-36.

4.2.1.1 10Base-2

Typ 10Base-2 je označován jako Thin Ethernet (v jednodušší verzi Cheap Ethernet), používá jako přenosové médium dvakrát stíněný koaxiální kabel RG 58 s impedancí 50 Ω.



Obr. 4.3**: Koaxiální kabel a konektory BNC , T-BNC, terminátor, síťová karta**

- fyzická vrstva se skládá ze dvou podvrstev
  - **PLS** (Physical Layer Signalling) – kóduje sériový tok bitů do podoby elektrického signálu a naopak (Manchester), zajišťuje synchronizaci, zjišťuje ukončení příjmu rámce podle detekce nosné, detekuje obsazení kanálu, kolize, vysílá kolizní signál (Jam)
  - **PMA** (Physical Medium Attachment) – zajišťuje vysílání a příjem bitů, detekce nosné, detekce kolize
- délka segmentu kabelu může být maximálně 185 m (i když existují i varianty karet umožňující délku až 300 m),

- na jednom segmentu může být maximálně 30 stanic,
- maximální celkový počet stanic v síti je 1024,
- napojení stanice – pomocí konektoru T-BNC (Bayonet Neill Concelman) s minimálním odstupem 0,5 m mezi sousedními stanicemi,
- zvětšení dosahu - propojení segmentů pomocí opakovačů, maximálně 4 opakovače, 5 segmentů, z toho maximálně 3 obsazené stanicemi,
- maximální dosah: 5 segmentů x 185 m = 925 m,
- segment musí být na obou koncích impedančně přizpůsoben pomocí tzv. terminátorů 50 Ω a jeden konec by měl být uzemněn.

4.2.1.2 10Base-5

Pro standard 10BASE-5 se vžil název Thick Ethernet, neboť se používá jako přenosové médium stíněný koaxiální kabel RG-8 neboli Yellow Cable s impedancí 50 Ω.

- délka segmentu může být maximálně 500 m; na kabel jsou připevňovány MAU (Medium Attachments Units) = transceivery (vampires),
- stanice jsou připojovány přes AUI konektor (DB 15), může být max. 50 m od transceiveru,
- transceivery musí být připevňovány ve vzdálenostech násobku 2,5 m (na kabelech bývá označení),
- segment musí také být na obou koncích ukončen pomocí tzv. terminátorů.

4.2.1.3 10Base-T

Standard 10-Base-T díky větším možnostem vytvářet rozmanité fyzické topologie brzy nahradil předchozí standardy využívající koaxiálních kabelů. Charakterizují ho následující vlastnosti:

- jako přenosové médium používá kroucený dvoudrát (stíněný nebo nestíněný) s impedancí 100 ohm (min. kategorie 3), konektor RJ 45,
- ze 4 dostupných párů jsou využity 2 páry (jeden pro vysílání a druhý pro příjem),
- pro poloduplexní i duplexní přenos,
- délka kabelu mezi uzlem a aktivním prvkem může být max. 100 m,
- zavádí testování integrity linky – pomocí NLP (Normal Link Pulse), který je vysílán ihned po zapnutí zařízení pro aktivaci a testování funkčnosti fyzického spojení. Nepovinným avšak vesměs využívaným doplňkem je signalizace aktivity spoje pomocí LED diody. Zařízení na opačné straně je:
  - aktivní – odpoví vysláním vlastního NLP,
  - vypnuté – aktivní zařízení periodicky každých 16 ms vysílá NLP dokud neobdrží odpověď.

4.2.1.4 10Broad-36

Specifikace 10Broad-36 je určena pro přenos po koaxiálních kabelových rozvodech, např. TKR (televizní kabelové rozvody). Pro každý směr přenosu jsou zapotřebí 3 kanály po 6 MHz šířky pásma, celkově tedy 36 MHz. Segmenty kabeláže mohou být dlouhé až 1800 m a maximální vzdálenost mezi stanicemi až 3600 m.

4.2.1.5 10BASE-FX

Specifikace 10Base-FX používají jako přenosové médium mnohavidová optická vlákna. Byly standardizovány 3 typy, 10Base-FL, 10Base-FB a 10Base-FP. Síť se skládá z optických segmentů, optických opakovačů a rozbočovačů.
Pro **10Base-FL** platí, že

- délka kabelu mezi uzly může být max. 2 km,
- délka kabelu mezi optickými opakovači může být max. 1 km

Specifikace **10Base-FB** byla vytvořena pro optické páteřní sítě. Slouží pouze pro propojení opakovačů a rozbočovačů a používá se synchronní způsob přenosu. Umožňuje propojení až 20 opakovačů s maximální délkou segmentu 2 km.
Specifikace **10Base-FP** definuje použití pasivního optického rozbočovače s maximálním dosahem 500 m a maximálním počtem propojených uzlů 30.
V současnosti existuje i modifikace používající jednovidový optický kabel, pro který je maximální vzdálenost mezi propojovacími prvky až 5 km.

4.2.2 Ethernet pro vyšší rychlosti

4.2.2.1 Podpůrné prostředky systémů s vyšší přenosovou rychlostí

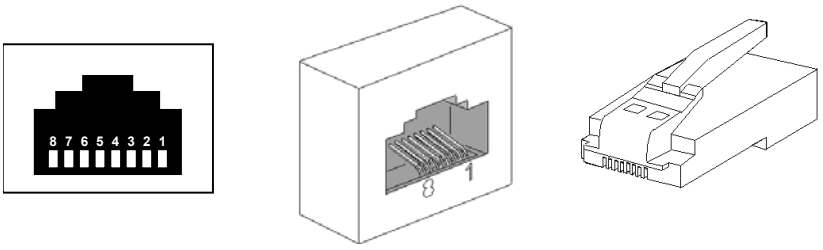
4.2.2.1.1 Vhodná kabeláž

Pro vyšší rychlosti sítí Ethernet se doporučuje mít kvalitně provedenou kabeláž. Jako metalické vedení je vhodný kabel UTP kategorie 5 (pro 100Base-TX), i když existují normy i pro kategorii 3 (100Base-T4 a 100Base-T2) a byla definována i varianta s kabelem STP o impedanci 150 Ω a konektorem DB9. Jako konektory zakončující kabeláž UTP byly vybrány 8-pinové konektory RJ45.

Tab. 4.3**: Kategorie kabelů UTP (Unshielded Twisted Pair) a jejich použití**

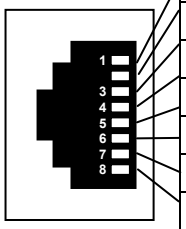
Kategorie	Typ	Šířka pásma	Dosah	LAN aplikace	Poznámky
Cat3	UTP	16 MHz	100m	10Base-T, 4Mbps	standardní telefonní kabel
Cat4	UTP	20 MHz	100m	16Mbps	vyskytuje se zřídka
Cat5	UTP	100MHz	100m	100Base-Tx, ATM, CDDI	běžně používaný v LAN
Cat5e	UTP	100MHz	100m	1000Base-T	běžně používaný v LAN
Cat6	UTP	250MHz	100m	1000Base-T	stále častěji používaný
Cat7	ScTP	600MHz	100m	10GBase-T	teprve nastupující

Pro propojení terminálů s propojovacími prvky se používají přímé kabely, viz **Obr. 4.4**. Tyto kabely mohou být použity i pro vzájemné propojení přepojovacích prvků, pokud jsou tyto prvky vybaveny speciálním vstupem umožňujícím manuální přepnutí vysílacích pinů na přijímací a naopak či pokud zařízení umožňují automatické rozpoznání párů a elektronické přepnutí pinů na patřičný typ (vysílací/přijímací) - auto. Pro propojení dvou terminálů či pro propojení propojovacích prvků bez výše uvedených schopností je zapotřebí překřížený kabel, viz. **Tab. 4.5**.



Obr. 4.4**: Zásuvka, zástrčka a číslování pinů pro konektor RJ-45**

Tab. 4.4**: Zapojení přímého kabelu UTP-5 pro přenos po dvou párech**

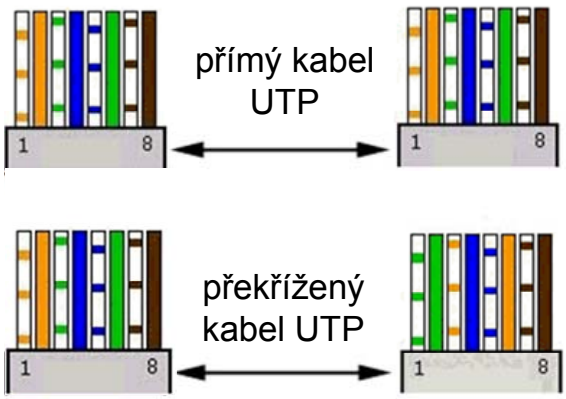


Datový terminál		Barvy vodičů	Propojovací prvek	
Význam pinů	Čísla pinů		Čísla pinů	Význam pinů
TX+	1	oranžová/bílá	1	RX+
TX-	2	oranžová	2	RX-
RX+	3	zelená/bílá	3	TX+
	4	modrá	4	
	5	modrá/bílá	5	
RX-	6	zelená	6	TX-
	7	hnědá/bílá	7	
	8	hnědá	8	

TX – vysílání,
RX – příjem.

Tab. 4.5**: Zapojení překříženého kabelu UTP-5 pro přenos po dvou párech**

Propojovací prvek/Datový terminál		Barvy vodičů	Propojovací prvek/ Datový terminál	
Význam pinů	Čísla pinů		Čísla pinů	Význam pinů
RX+/TX+	1	oranžová/bílá	3	TX+/RX+
RX-/TX-	2	oranžová	6	TX-/RX-
TX+/RX+	3	zelená/bílá	1	RX+/TX+
	4	modrá	4	
	5	modrá/bílá	5	
TX-/RX-	6	zelená	2	RX-/TX-
	7	hnědá/bílá	7	
	8	hnědá	8	



Obr. 4.5**: Barvy vodičů kabelu UTP pro zapojení přímého a překříženého kabelu dle TIA/EIA-568B**

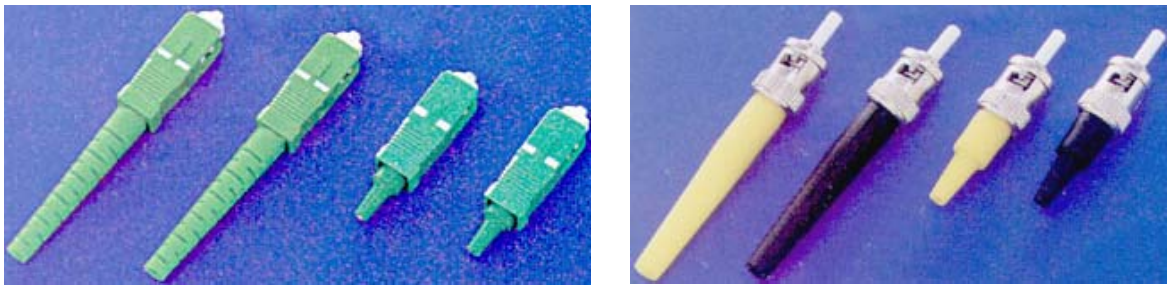
U standardu 100Base-T4 jsou využity všechny 4 páry kabelu UTP kategorie 3 či 4 (viz **Tab. 4.6**). Maximální délka segmentu UTP je 100 m.

Tab. 4.6**: Zapojení a význam vodičů přímého kabelu sítě 100Base-T4**

Datový terminál		Barvy vodičů	Propojovací prvek	
Význam pinů	Čísla pinů		Čísla pinů	Význam pinů
TX_1+	1	oranžová/bílá	1	RX_1+
TX_1-	2	oranžová	2	RX_1-
RX_1+	3	zelená/bílá	3	TX_1+
BI_2+	4	modrá	4	BI_2+
BI_2-	5	modrá/bílá	5	BI_2-
RX_1-	6	zelená	2	TX_1-
BI_3+	7	hnědá/bílá	7	BI_3+
BI_3-	8	hnědá	8	BI_3-

BI (bidirectional) - vodiče pro obousměrný přenos.

Pro připojení optických kabelů dle standardu 100Base-FX 802.3u jsou preferovány konektory typu SC, ale je možné použít i konektory typu MIC a bajonetové ST. Konektory SC pro vlákna 62,5/125 mikronů musí splňovat specifikaci TIA-5678SC.



SC ST

Obr. 4.6**: Konektory pro optické kabely počítačových sítí**

Jako na mediu nezávislá specifikace je definováno rozhraní MII (Media Independent Interface, 40-pinový konektor), kde se předpokládá použití transceiverů, stejně jako u rozhraní AUI standardu 10Base-T.

4.2.2.1.2 Propojovací prvky

Jako propojovací prvky sítí Ethernet se používají rozbočovače a přepínače. Směrovače již rozdělují části do samostatných sítí. Přepínače rozdělují kolizní domény a podporují různé přenosové rychlosti, často s porty podporující více rychlostí a jejich automatické nastavení (viz kap. 3.5.3.

Naproti tomu rozbočovače jsou zařízení, která slouží k regeneraci signálu a k vytváření sběrnicové struktury na logické (linkové) úrovni, podrobněji viz kap. 3.5.2). Všechny prvky jimi propojené jsou součástí jedné kolizní domény. Svou činností způsobují určité zpoždění v průchodu signálu, zvláště pokud propojují segmenty s odlišnými specifikacemi (způsobem kódování), např. 100Base-TX a 100Base-T4. U vyšších přenosových rychlostí je to pak obzvlášť citelné. Zatímco u desetimegabitového Ethernetu bylo možno zapojit do kaskády až 4 rozbočovače (opakovače), pak pro stomegabitovou síť už je to pouze 1 či maximálně dva a pro gigabitový Ethernet lze použít pouze jeden. Pro rychlost 100 Mb/s jsou definovány 2 skupiny rozbočovačů:

a) **Class I** – rozbočovač se schopností propojit segmenty 100Base-TX a 100Base-T4. Tento typ se smí v kolizní doméně vyskytovat pouze jeden.
b) **Class II** - rozbočovač se schopností propojit segmenty se stejným typem kódování, tedy například 100Base-TX a 100Base-TX či 100Base-TX a 100Base-FX. Rozbočovače tohoto typu způsobují menší zpoždění a mohou se vyskytovat v jedné kolizní doméně maximálně dva s maximální vzájemnou vzdáleností 5 m. Jejich přínos ve srovnání s typem Class I je zanedbatelný.

Tab. 4.7 ukazuje maximální vzdálenosti, které lze dosáhnout ve stomegabitové síti Ethernet různé specifikace a s použitím různého typu kabeláže. Označení HD a FD znamená poloviční a plný duplex.

Tab. 4.7**: Maximální dosahy kabeláže bez a s použitím opakovačů v sítích Ethernet 100 Mb/s, údaje jsou v metrech.**

	UTP (TX+TX)/ (T4+T4)	UTP (TX+T4)	Optika	UTP + Optika (T4 + FX)	UTP + Optika (TX + FX)
DTE - DTE	100	100(10Mb/s)	412-HD/2000-FD	-	-
opakovač Class I	200	200	272	231	260,8
opakovač Class II	200	-	320	-	308,8
2 x opakovač Class II	205	-	228	-	216,2

4.2.2.1.3 Symbolové kódování

Vhodné symbolové kódování napomáhá zajištění synchronizace, omezení potřebné šířky pásma, odstranění ss složky. V síti Ethernet 10Mb/s se používá kódování Manchester, které je však pro vyšší rychlosti nevhodné (velké nároky na šířku pásma). Řešením může být:

- skramblování dat(pro každý směr přenosu podle jiného schématu),
- rozšíření kódového prostoru (vícestavové kódování nebo zvýšení počtu dvoustavových symbolů a výběr vhodných kódových kombinací, možnost využít nedatové symboly pro ohraničení rámce, synchronizační výplň, detekce chyb, či řízení toku dat při duplexním přenosu),
- korekční zabezpečení – u 1000BASE-T.

4.2.2.1.4 Automatické rozpoznání komunikačního režimu

Používá se pro automatický výběr režimu u zařízení umožňující činnost ve více režimech, např. 1000/100/10 Mb/s. Tuto schopnost mohou mít na vedení obě či pouze jedno z obou zařízení. Děje se to pomocí systému autosensing (autonegotiation) – namísto NLP se posílají shluky [FLP (Fast Link Pulse) burst] 17 až 33 krátkých 16 b slov. Slovo se označuje jako LCW (Link Code Word) obsahující typ zprávy, schopnosti, chybu komunikace, potvrzení příjmu. Je-li odpověď na FLP shluk signál NLP, nastaví se 10Mb/s poloduplex.

4.2.2.1.5 Duplexní přenos

Řízení toku dat je zajištěno posláním pozdržovacím rámcem (Pause frame) generovaným MAC podvrstvou, který způsobí pozdržení vysílání na definovanou dobu. Je-li přijímač schopen přijímat data před uplynutím stanovené doby je vyslán další rámec s nastavením nulové doby čekání, čímž se vysílání ihned obnoví.

4.2.2.2 Fast Ethernet

Fast Ethernet je v principu standardní Ethernet, jen 10x rychlejší. Zachovává přístupovou metodu CSMA/CD (Carrier Sense Multiple Access/Collision Detection), strukturu i minimální délku rámce 64 B. Standard 100Base-T může být snadno implementován do většiny 10 Mb/s Ethernet sítí bez nutnosti podstatných změn v kabeláži, navíc se schopností koexistence se stávající standardní sítí Ethernet 10 Mb/s.
Bylo vyvinuto několik standardů, a to 100Base-TX, 100Base-FX, 100Base-T4 a 100 Base-T2, které poskytují řadu možností při přechodu z 10 Mb/s Ethernetu. Ve funkci kabeláže mohou být použity metalické kabely UTP kategorií 3 a vyšší a optické kabely.

4.2.2.2.1 100BASE-X (802.3u)

Specifikace 100Base-X zahrnuje standardy 100Base-TX a 100Base-FX. Oba typy používají kódování 4B/5B. 100Base-TX pak využívá kód MLT-3 (Multi-Level Transition), který je úsporný vůči potřebné šířce pásma. Technologie 100Base-FX pak přidává linkový kód NRZI (jednička provádí změnu polarity signálu, nula ji nemění).

- 16 kombinací (kódových skupin – code groups - CG) je pro přenos dat,
- 4 kódové kombinace se používají v párech a tvoří značky:
  - SSD (Start-of-Stream Delimiter) – tvoří první bajt preambule a je vyjádřen pomocí dvou kódových skupin CG (pětic bitů),
  - ESD (End-of-Stream Delimiter) – tvoří závěr rámce a je vložen za poslední bajt FCS,

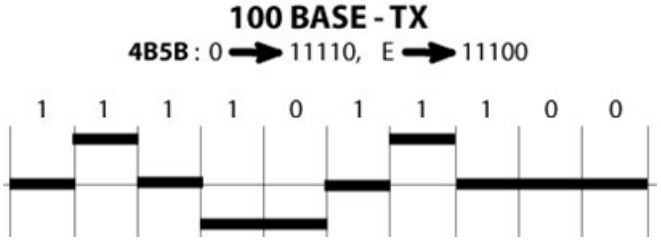
SSD (1B) (2CG)	PREAMBLE (6B)	SFD (1B)	MAC rámec	ESD (2CG)

PREAMBLE – preambule,
SFD – start-of-frame delimiter.

- 1 kódová značka IDLE – pro udržení synchronizace stanic i v mezirámcové mezeře IPG – neexistuje tedy klid v kanálu,
- 11 neplatných kombinací - příjem některé z těchto kombinací znamená chybu, a tedy neplatný rámec.

4.2.2.2.1.1 100Base-TX

Specifikace 100Base-TX podporuje 100 Mb/s Ethernet po UTP kabeláži Cat. 5 a STP Type 1 s využitím dvou párů. Tato specifikace je založena na stejném základě jako TP-PMD (Twisted-Pair Physical Medium Dependent) specifikace u technologie CDDI, vyvinutém výborem X3T9.5 organizace ANSI (American National Standards Institute). Stejně jako u CDDI je nosná frekvence 125 MHz a data jsou kódována metodou 4B5B/MLT-3.

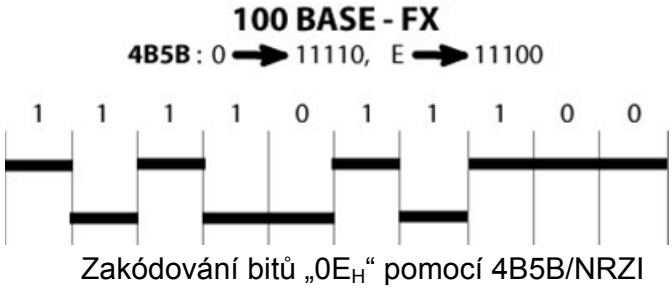


Zakódování bitů „$0E_H$“ pomocí 4B5B/MLT-3

Obr. 4.7: Použití kódu 4B5B/MLT-3 u technologie 100BASE-TX

4.2.2.2.1.2 100Base-FX

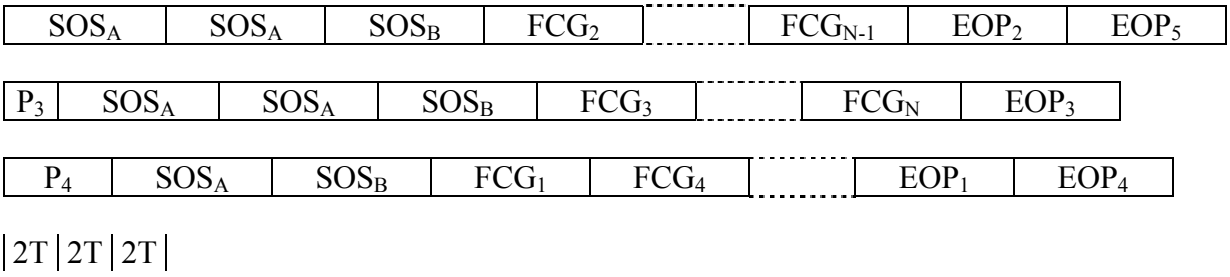
Specifikace 100Base-FX používá dvě multimodová optická vlákna a fyzická vrstva je založena na specifikaci sítě FDDI (podvrstvy PCS – Physical Coding Sublayer a PMD - Physical Medium Dependent).



Obr. 4.8: Použití kódu 4B5B/NRZI u technologie 100BASE-FX

4.2.2.2.2 100Base-T4

Specifikace 100Base-T4 vychází vstříc stávajícím instalacím s UTP kabely kategorie 3 a 4. Všechny 4 páry, protože jsou všechny využity pro přenos. Signál se přenáší třemi páry s modulační rychlostí 25 Mbaud s kódováním 8B6T a čtvrtý je využit pro detekci kolizí. Tím je umožněno využití i starších, méně kvalitních kabelů. Datový rámec z linkové vrstvy se vybaví preambulí a rozdělí se do oktetů, které jsou zakódovány do šestic ternárních symbolů (6T kódových skupin – code groups – CG) a střídavě posílány po všech 3 párech kabelu. Symboly pro data jsou vybrány tak, aby se minimalizovala stejnosměrná složka. Začátky i konce úseků všech párů nesoucí rámec jsou ohraničeny nedatovými skupinami symbolů (SOS - Start of Stream – dvě skupiny SOS_A a SOS_B, EOP - End of Packet – pět skupin EOP_1 až EOP_5). Způsob přenosu datového rámce po třech párech je zachycen na Obr. 4.9. Nedatová kombinace je také použita pro vyjádření klidu ve sdíleném kanálu, tedy v kolizní doméně (signál IDLE). Tento typ nepodporuje duplexní provoz.



Obr. 4.9: Struktura úseků dat na jednotlivých vysílacích párech nesoucí data jednoho rámce

SOS_A – šestice ternárních symbolů (1,-1,1,-1,1,-1),
SOS_B – šestice ternárních symbolů (1,-1,1,-1,-1,1),
P_3 – dvojice ternárních symbolů (1,-1),
P_4 – čtveřice ternárních symbolů (1,-1,1,-1),
EOP_1 - šestice ternárních symbolů (1,1,1,1,1,1),
EOP_2 - šestice ternárních symbolů (1,1,1,1,-1,-1),
EOP_3 - šestice ternárních symbolů (1,1,-1,-1,0,0),
EOP_4 - šestice ternárních symbolů (-1,-1,-1,-1,-1,-1),
EOP_5 - šestice ternárních symbolů (-1,-1,0,0,0,0),

FCG_i (Frame Code Group) - šestice ternárních symbolů odpovídající *i*-tému oktetu datového rámce.

4.2.2.2.3 100Base-T2

Standard 100Base-T2 nese označení IEEE 802.3xy a byl uvolněn v roce 1997. Je specifikován následujícími parametry:

- přenos po dvou párech UTP kabelu kategorie 3 a 4 sloužících pro oba směry přenosu,
- maximální délka kabelu je 100 m
- podporuje jak poloviční, tak i plný duplex pomocí vidlice a potlačovače ozvěn,
- pro plný duplex musí být jedna stanice zvolena jako Master (zdroj časování) a druhá jako Slave (odvozuje časování z přijímaného signálu) pomocí automatické identifikace (autonegotiation)
- data jsou nejdříve skramblována (pro každý směr je použitý jiný generační polynom, aby byla data obou směrů nekorelována) a rozdělena do čtveřic bitů kódovaných po dvojicích pomocí PAM 5x5 (1 pětkový symbol pro každý pár UTP a dvojici bitů) modulační rychlostí 25 Mbaud,
- MAC rámec je při přenosu ohraničen dvěma páry nedatových symbolů (SSD a ESD) a v mezirámcové mezeře jsou vysílány IDLE symboly

4.2.3 Gigabitový Ethernet

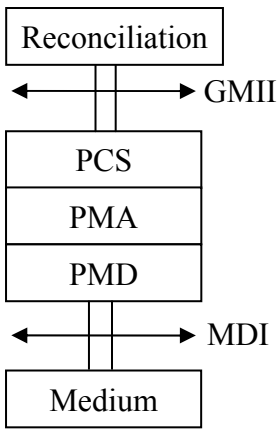
Gigabitový Ethernet byl dalším krokem ke zvýšení přenosové rychlosti. Pro základ fyzické vrstvy se vycházelo ze standardu Fibre Channel (vrstva FC-1 a FC-0). První skupina standardů byla schválena roku 1998 standardem IEEE 802.3z pod označením 1000Base-X. Další specifikací (v roce 2000) pak byl standard IEEE 802.3ab s označením 1000Base-T podporující nasazení na UTP kategorie 5 s využitím všech 4 párů a zajištěním dosahu až 100m. Gigabitový Ethernet se vyznačuje následujícími vlastnostmi:

- přenosová rychlost 1 Gb/s,
- doporučení a varianty:
  - **IEEE 802.3z**:
    - kódování 8B/10B, modulační rychlost 1025 Mbaud,
    - metalika
      - 1000 Base-CX – pro speciální stíněný kabel,
    - optika
      - 1000 Base-SX – na vlnové délce 850 nm,
      - 1000 Base-LX – na vlnové délce 1310 nm
  - **IEEE 802.3ab**:
      - 1000Base-T – všechny 4 páry UTP 5. kategorie, dosah až 100 m

4.2.3.1 1000Base-X

Varianty 1000 Base-CX, 1000 Base-SX, 1000 Base-LX jsou označovány jako 1000 Base-X a specifikace jejich fyzických vrstev vychází z fyzické vrstvy sítě Fibre Channel. Fyzická vrstva se skládá ze 3 hlavních podvrstev:

- **PCS** – Physical Coding Sublayer – kódování a dekódování (8B/10B), řeší proces automatického nastavení komunikační rychlosti (auto-sensing, auto-negotiation), zajišťuje synchronizaci,
- **PMA** – Physical Medium Attachment – provádí převod mezi paralelním a sériovým tokem dat a obnovuje signál při příjmu, bufferováním celé desetibitové kódové skupiny při příjmu zavádí zpoždění odpovídající době přenosu 10 bitů



- **PMD** – Physical Medium Dependent – popisuje konkrétní vlastnosti vysílače a přijímače signálů (výkonové úrovně signálů).

K tomu přísluší ještě vyrovnávací podvrstva (Reconciliation sublayer) a 2 rozhraní:

1. **GMII** – Gigabit Medium Independent Interface – zajišťuje paralelní přenos 8 bitů s taktovacím kmitočtem 125 Mbaud. Kromě toho obsahuje další řídicí signály – časovací signál, detekce nosné, chyba přenosu, apod. Nespecifikuje však typ konektoru pro připojení gigabitového tranceiveru kabelem, jak to bylo u rozhraní AUI pro desetimegabitový Ethernet a MII pro stomegabitový Ethernet.
2. **MDI** – Medium Dependent Interface – definuje konektory, pro 1000 Base-SX a 1000 Base-LX jsou definovány duplexní konektory typu SC

Specifikace 1000 Base-X je dále charakterizována vlastnostmi:

- přístupová metoda CSMA/CD,
- kódování 8B/10B,
- minimální délka slotu 520 B (u 10BASE-X to bylo 64 B) – při kódování 8B/10B vychází minimální délka MAC rámce čtyři pětiny, tedy 416B,
- řešením minimální délky je buď přidat výplň k malému rámci (=> zmenšení efektivní přenosové rychlosti) nebo vyslat shluk rámců, a to až do celkové délky 8192 B (= burst limit). Mezery mezi rámci ve vysílaném shluku jsou vyplněny bity „rozšíření rámce“, což ostatní stanice vnímají jako kontinuální přenos a nesnaží se tedy vysílat,
- maximální délka rámce 1518 B,
- desetkrát menší časová mezera mezi rámci než u 100 Mb/s (0,096 μs),
- doba sledování činnosti na lince před zahájením vysílání (0,512 μs).

Tab. 4.8: Typy vláken a jejich dosahy pro standardy 1000Base-LX a 1000Base-SX

Standard	typ vlákna	průměr [mikrometr]	modální šířka vlákna [MHz*km]	dosah [m]
1000BASE-SX 850 nm	MM	62,5	160	2 až 220
		62,5	200	275HD/275FD
		50	400	316HD/500FD
		50	500	316HD/550FD
1000BASE-LX 1310 nm	MM	62,5	500	316HD/550FD
		50	400	316HD/550FD
		50	500	316HD/550FD
	SM	9	N/A	316HD/5000FD

MM – multimode,
SM – singlemode,
HD – half-duplex,
FD – full-duplex.

4.2.3.1.1 1000Base-CX

Standard 1000Base-CX používá dva páry STP (150 Ω), maximální dosah je pouze do 25 m, jsou definovány 2 typy konektorů, „style-1“ (9-pinový miniaturní konektor D9, podobný jako DB9) a „style-2“ (8-pinový konektor ANSI Fibre Channel).

4.2.3.1.2 1000Base-SX

Standard 1000Base-SX používá vícevidová vlákna 62,5 a 50 μm na vlnové délce 850 nm, dosah až 550m, viz Tab. 4.8.

4.2.3.1.3 1000Base-LX

Standard 1000Base-LX používá vícevidová (62,5 a 50 μm) i jednovidová (9 μm) vlákna na vlnové délce 1310 nm, dosah i více než 5 km (pro plný duplex), viz Tab. 4.8.

4.2.3.2 1000Base-T

Specifikace 1000Base-T byla uvolněna v roce 2000 jako standard IEEE 802.3ab. Charakterizují ho následující vlastnosti:

- přenos po 4 párech UTP 5. kategorie,
- maximální vzdálenost mezi dvěma uzly ve sdílené (kolizní) doméně je 200 metrů,
- podporuje jak poloviční, tak i plný duplex,
- minimální délka MAC rámce je **520 B**,
- jedna z komunikujících stran je Master (switch, hub) a druhá Slave (terminál),
- z technologie 100Base-T4 je převzaté využití všech čtyřech párů,
- ze 100Base-TX je vzato řešení pro 125 Mbaud a zpracování signálovým procesorem,
- z řešení 100Base-T2 se použila kompenzace echa a přeslechů,
- kódování se děje po bajtech, kde 1B je překódován na slovo délky 12 bitů, které je rozděleno po trojicích na každý pár, kde trojice bitů je prezentována jako 1 pětkový symbol pro každý pár UTP (4-dimenzionální PAM 5) s modulační rychlostí 125 Mbaud,
- vyšší nároky na poměr odstup signálu od šumu o 6dB – řešeno zlepšenou opravou chyb – Forward Error Correction (data jsou skramblována a pak zabezpečena 8-stavovým Trellis kódováním),
- bajty jsou mapovány na čtveřice pětkových symbolů,
- v neaktivním (idle) stavu a při navazování spojení se používají třístavové symboly.

4.2.3.3 Standardy 1000BASE-TX, 1000BASE-LX10, 1000BASE-BX10 a 1000BASE-ZX

Standard 1000 BASE-TX byl navržen s cílem přenášet data gigabitovou rychlostí po jednom páru pro jeden směr, tedy principiálně stejně jako u standardů 10- nebo 100BASE-TX. Standard však vyžadoval kabeláž UTP minimálně kategorie 6, což ho odsoudilo k nezdaru.

Standardy 1000Base-LX10 a 1000 BASE-BX10 byly ratifikovány v roce 2004 pro využití v přístupových optických sítích – „First Mile“. Standard 1000Base-LX10 umožňuje dosáhnout gigabitové rychlosti na vzdálenost až 10 km a pár jednovidových vláken v pásmu 1310 nm. Standard 1000 BASE-BX10 pak umožňuje na stejnou vzdálenost přenášet gigabitovou rychlostí Ethernet rámce po jednom vláknu v obou směrech současně s využitím vlnového oddělení směrů – 1490 nm downlink a 1310 nm uplink.

Technologie 1000BASE-ZX není standard, avšak je široce využívána především v sítích MAN a WAN, neboť její nasazení umožňuje v pásmu 1550 nm po jednovidových vláknech dosáhnout vzdáleností kolem 100 km (více než 70 km).

4.2.4 10 Gb/s Ethernet

Desetigigabitový Ethernet je opět dalším krokem ke zvýšení propustnosti datových sítí této skupiny. V současnosti je zastoupen několika standardy: IEEE 802.3ae-2002 (fiber -SR, -LR, -ER and -LX4 PMDs), IEEE 802.3ak-2004 (CX4 copper twin-ax InfiniBand type cable), IEEE 802.3an-2006 (10GBASE-T copper twisted pair), IEEE 802.3ap-2007 (copper backplane -KR and -KX4 PMDs) a IEEE 802.3aq-2006 (fiber -LRM PMD with enhanced equalization).

4.2.4.1 Standard IEEE 802.3ae

Standard IEEE 802.3ae charakterizují následující rysy:

- schválení proběhlo v roce 2002,
- je navržen pouze pro plně duplexní provoz => dosah omezen pouze použitou technologií (je odstraněna jak fyzická tak i logická sběrnice, přístup na linku je možný kdykoliv, odpadá CSMA/CD),
- standard zahrnuje specifikace 10GBase-SR, 10GBase-SW, 10GBase-LX4, 10GBase-LR, 10GBase-LW, 10GBase-ER, 10GBase-EW, viz Tab. 4.10,
- pro přenos se využívají optická vlákna na vlnových délkách 850, 1310, 1550 nm s dosahy uvedenými v Tab. 4.9,

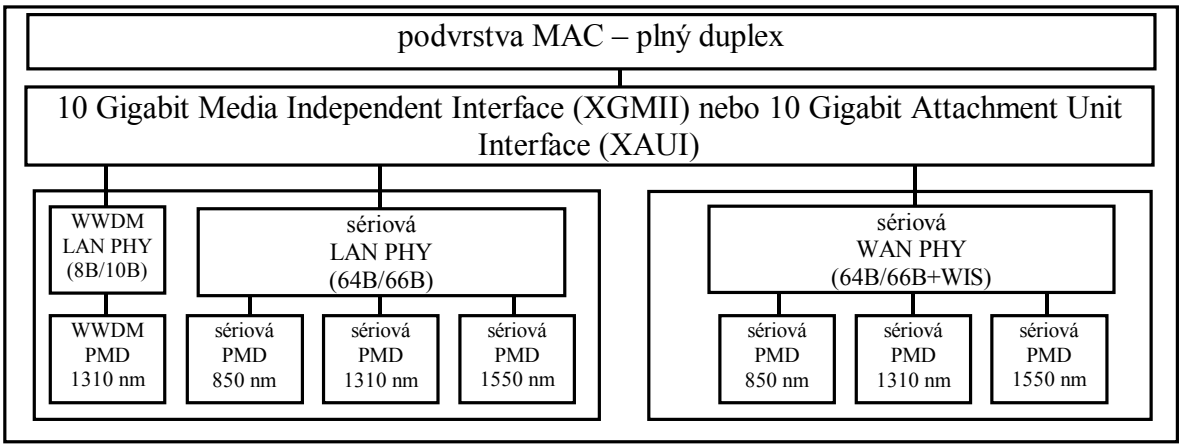
Tab. 4.9: Specifikace jednotlivých druhů vláken, vlnových délek a jejich dosahy

vlnová délka	850 nm	1310 nm		1550 nm
typ vlákna	multimode, 50/125 μm, 500 MHz*km	multimode 62.5 /125 μm 160 MHz*km	singlemode	singlemode
minimální dosah	65 m	300 m	10 km	40 km

Tab. 4.10: Jednotlivé specifikace standardu IEEE 802.3ae

Specifikace	Kódování	Podvrstva pro WAN (WIS)	Vlákno
10GBase-SR	64B/66B	ne	850 nm, sériově
10GBase-SW	64B/66B	ano	850 nm, sériově
10GBase-LX4	8B/10B	ne	1310 nm, WWDM
10GBase-LR	64B/66B	ne	1310 nm, sériově
10GBase-LW	64B/66B	ano	1310 nm, sériově
10GBase-ER	64B/66B	ne	1550 nm, sériově
10GBase-EW	64B/66B	ano	1550 nm, sériově

- počítá se s využitím jak v LAN tak i pro WAN sítě a jsou tedy definovány 2 typy fyzických vrstev LAN PHY a WAN PHY (podpora rychlostí SONET OC-192/SDH STM-64), viz Obr. 4.10.

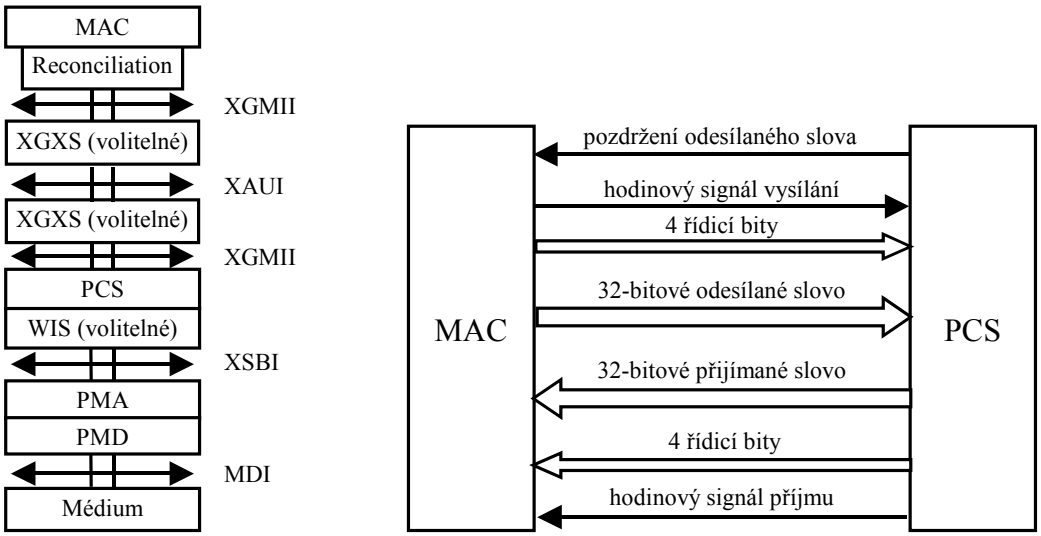


Obr. 4.10: Architektura standardu IEEE 802.3ae

Fyzická vrstva je rozdělena do:

- **PCS** (Physical Coding Sublayer) – kódování 64B/66B a převod do sériového toku, nebo několika paralelních toků pro přenos daným přenosovým prostředím,
- **PMA** (Physical Medium Attachment) – vzájemný převod mezi sériovou a paralelní podobou dat, obnova časování,
- **PMD** (Physical Medium Dependent) – vysílač/přijímač pro dané přenosové médium a vlnovou délku.

Napojení fyzické vrstvy na MAC vrstvu může být řešeno buď paralelním rozhraním XGMII (10 Gigabit Media Independent Interface), viz Obr. 4.11, nebo pomocí sériového rozhraní XAUI (10 Gigabit Attachment Unit Interface) specifikující pro každý směr přenosu 4 datové vodiče s rychlostmi 2,5 Gb/s, hodinový signál a další.



Obr. 4.11: Podvrstvy a rozhraní fyzické vrstvy desetigigabitového Ethernetu a podrobnější specifikace rozhraní XGMII

MDI – Medium Dependent Interface,
XSBI – 10 Gigabit Sixteen Biot Interface,
WIS – WAN Interface Sublayer.

Další využití desetigigabitového Ethernetu je v datových centrech, úložných sítích (SAN) či v tzv. „backplanech“ skříní (RACKů) se zásuvnými deskami.

4.2.4.2 Standard IEEE 802.3an

V roce 2006 byl schválen standard **IEEE 802.3an** pod označením **10GBase-T** využívající pro přenos desetigigabitového Ethernetu kabel UTP kat. 6a a 7, s nimiž je možné dosáhnout standardní vzdálenosti 100 m. Jsou povoleny i nižší kategorie 6 a 5e, ale dosah je 55 m respektive 45 m.

4.2.5 40G/100G Ethernet

Technologii 40G/100G Ethernet definuje standard IEEE 802.3ba, jehož ratifikace proběhla v červnu roku 2010. Technologie má v současnosti následující možnosti použití:

- 40 Gb/s - propojení datových center,
- 100 Gb/s – propojení přepojovacích prvků.

Stejně jako 10 GE nepodporuje sdílený Ethernet, tedy pouze plný duplex. Standard zachovává formát rámce, včetně velikostních limitů (min/max), je implementována podpora FEC se zajištěním maximální chybovosti 10^{-12}. Je zajištěna podpora pro optické transportní sítě (OTN).

Tab. 4.11: Typy a možnosti technologie 40G/100G Ethernet

dosah	40 Gigabit Ethernet	100 Gigabit Ethernet
nejméně 1 m po backplanu	40GBASE-KR4	
nejméně 10 m po copper cable	40GBASE-CR4	100GBASE-CR10
nejméně 100 m po OM3 MMF	40GBASE-SR4	100GBASE-SR10
nejméně 125 m po OM4 MMF	40GBASE-SR4	100GBASE-SR10
nejméně 10 km po SMF	40GBASE-LR4	100GBASE-LR4
nejméně 40 km po SMF		100GBASE-ER4

Přenosových rychlostí 40 Gb/s a 100 Gb/s se dosahuje pomocí technik WDM (Wavelength Division Multiplexing):

- 100 Gb/s
  - 10 vlnových délek s kapacitou 10 Gb/s,
  - 4 vlnové délky s kapacitou 25 Gb/s,
  - 5 vlnových délek s kapacitou 20 Gb/s,
- 40 Gb/s pro krátký dosah (do 100m – datová centra) pomocí QSFP (Quad Small Form-factor Pluggable) vysílačů/přijímačů a MM vláken
  - *x* spojů s kapacitami 5, 8 či 10 Gb/s pro dosažení kapacity až 40 Gb/s,

PCS (Physical Coding Sublayer) podvrstva řeší kódování, skramblování dat a kódování řídicích datových bloků 64/66B, **FEC** podvrstva řeší zabezpečení dat pro dopřednou opravu chyb (je volitelná).

4.2.6 Rámce sítě ETHERNET

Základní částí rámce je hlavička linkové vrstvy, která je následována daty (včetně hlaviček vyšších vrstev) a zakončen zabezpečením. Hlavičky jsou principielně 4 typů a jsou vzájemně nekompatibilní. Tyto typy jsou:

- Ethernet_II,
- Ethernet_802.3,
- Ethernet_802.2 LLC,
- Ethernet_SNAP.

Nejjednodušším a také nejpoužívanějším formátem rámce je Ethernet_II, označovaný také jako DIX, viz Obr. 4.12.

7 B	1B	6 B	6 B	2 B	46 až 1500 B	4 B
Preambule	SFD	adresa určení (DA)	zdrojová adresa (SA)	typ paketu	data	CRC

Obr. 4.12: Rámec Ethernet_II sítí Ethernet

Preambule - 7 oktetů střídajících se log.1 a log.0 (začíná se log.1), slouží k synchronizaci přijímající stanice,

SFD - (Start-of-Frame Delimiter) – 10101011, označení počátku rámce,

DA - (Destination Address) – HW adresa cílového síťového rozhraní v rámci lokální sítě,

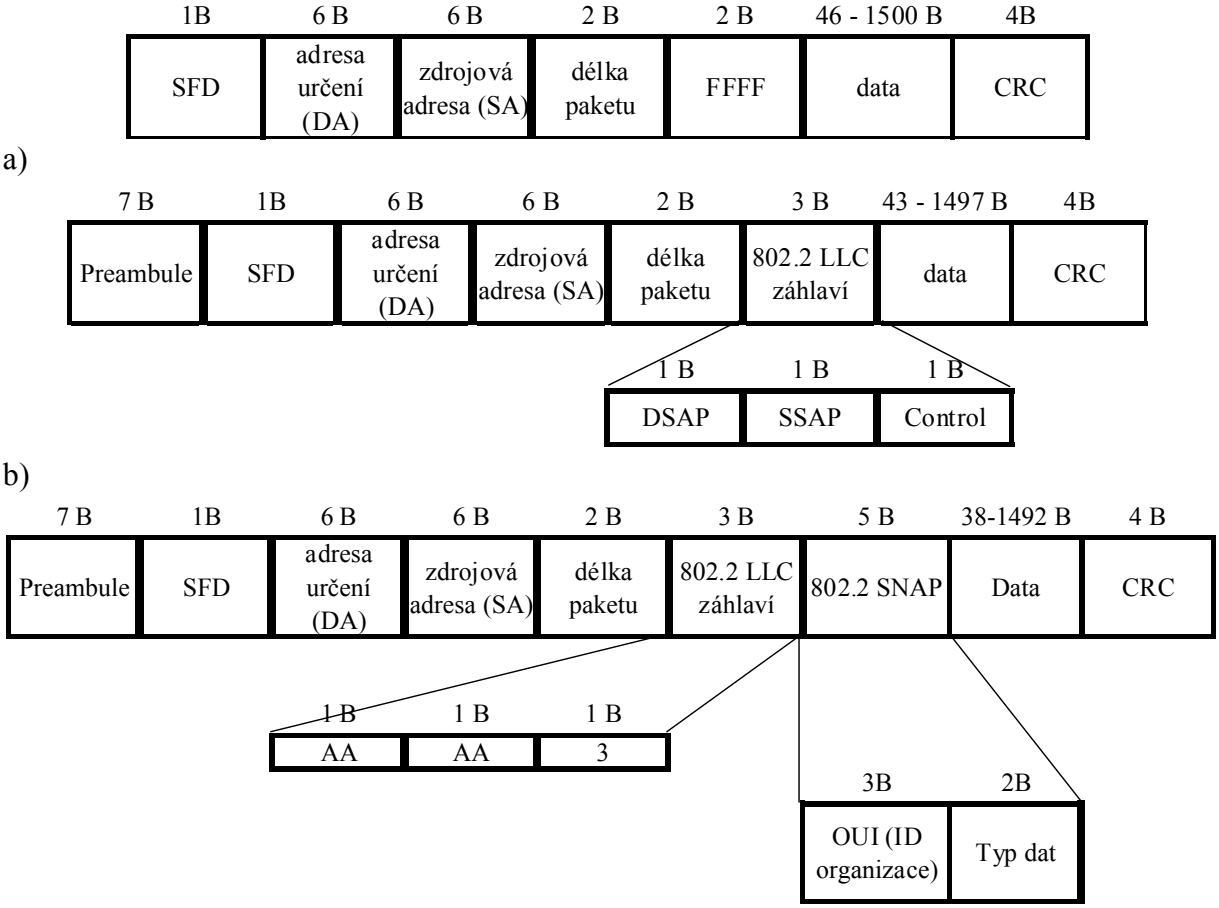
SA - (Source Address) - HW adresa zdrojového síťového rozhraní v rámci lokální sítě,

Typ paketu - určuje přístupový bod (SAP- Service Access Point), kam se mají data předat. Obsahuje číslo větší než 0x05DC. Menší čísla jsou využívána pro informaci o **délce rámce** u typu **802.3_raw**. Data mohou být určena buď entitě na stejné vrstvě (například entitě managementu linkové vrstvy) a nebo entitě představující protokol vyšší vrstvy. Například číslo **0x0800** označuje, že data jsou **IP paket** a budou předána entitě IP; **0x0806** představuje data pro protokol **ARP**, nebo **0x8137** označuje **Novell IPX paket**. Ostatní čísla lze najít v dokumentech RFC, např. RFC 1700.

CRC - (Cyclic Redundancy Check) – zabezpečení, 32 bitů, pomocí cyklického kódu definovaného generačním polynomem

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

Formáty dalších rámců (v sítích s protokolovou sadou TCP/IP nepoužívaných) jsou zachyceny na Obr. 4.13.



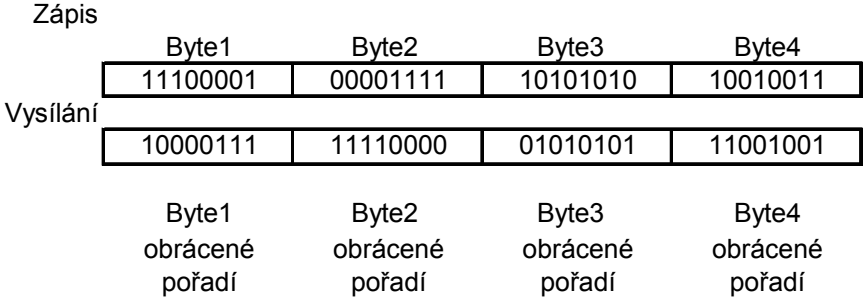
Obr. 4.13: Rámce používané v sítích Ethernet, a) Ethernet 802.3_Raw, b) Ethernet 802.3_LLC, c) Ethernet 802.3_SNAP

DSAP - Destination Service Access Point – cílový přístupový bod, 7 bitů ID + 1bit individuální/skupinový identifikátor,

SSAP - Source Service Access Point – zdrojový přístupový bod, 7 bitů ID + 1bit C/R (Command / Response),

Control - řízení, stejný formát jako má protokol HDLC.

Důležitý je také vztah mezi zápisem, přenosem a zpracováním bitů rámce sítě Ethernet. Co se týče přenosu oktetů (bajtů), tak je to vzhledem k zápisu rámce „zleva do prava“. Co se však týče pořadí bitů v rámci bajtu při přenosu, tak se nejdříve přenáší nejméně významný bit (LSB), neboli pořadí označované jako „little-endian“, viz Obr. 4.14.



Obr. 4.14: Zápis a přenos bajtů a jejich bitů rámce Ethernet

4.2.7 Ethernet v přístupových sítích (Ethernet in the First Mile – EFM)

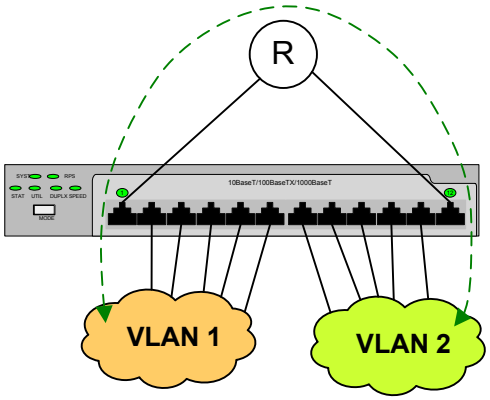
Použití technologie Ethernet v přístupových sítích definuje standard IEEE 802.3ah, jehož ratifikace proběhla v roce 2004. Standard definuje následující specifikace pro různé typy kabeláží:

- po měděných párech
  - **2BASE-TL** – duplexní provoz bod-bod po UTP kat. 3/4 s rychlostí od 2 do 5,69 Mb/s až na vzdálenost 2700 m po jednom páru,
  - **10PASS-TS** – duplexní provoz bod-bod po UTP kat. 3/4 s rychlostí 10Mb/s do vzdálenosti 750m po jednom páru
- po jednovidových optických vláknech
  - **100BASE-LX10** - point-to-point spoj, 100 Mb/s po páru vláken na vzdálenost alespoň 10 km.
  - **100BASE-BX10** - point-to-point spoj, 100 Mb/s po jendom vláknu na vzdálenost alespoň 10 km
  - **1000BASE-LX10** - po páru vláken, 1310 nm
  - **1000BASE-BX10** - optika, jedno vlákno, směry kmitočtově (barevně) odděleny, 1490 nm downstrem, 1310 nm upstream,
- po pasivních optických sítích (PON)
  - **1000BASE-PX10** - 1000 Mb/s Ethernet po sítích PON (EPON) na vzdálenost alespoň 10 km.
  - **1000BASE-PX20** - 1000 Mb/s Ethernet po sítích PON (EPON) na vzdálenost alespoň 20 km.

4.3 Virtuální sítě LAN (VLAN)

Pojem Virtuální síť LAN znamená označení logického seskupení koncových uzlů do samostatné skupiny, vytvořené dle určitého klíče (viz níže), nezávisle na fyzickém umístění koncových uzlů, se zajištěním vzájemné komunikace, jako by byly uzly v jedné fyzické síti LAN a se zajištěním oddělení od ostatních skupin na úrovni sítí LAN (na úrovni spojové vrstvy) a propojení přes zařízení pracující na síťové vrstvě (směrovač). Virtuální sítě LAN jsou tedy seskupení počítačů do samostatných celků vybudovaných na základě speciálních vlastností moderních přepínačů.
Nutnou podmínkou je existence přepínačů s podporou sítí VLAN a přídavných protokolů.
Důvody vzniku virtuálních sítí byly:

- obyčejný přepínač umí omezit velikost kolizních domén až na úroveň 1 počítače, ale nefiltruje všesměrové vysílání, nerozděluje tedy tzv. všesměrovou (broadcast) doménu (to umí klasické směrovače, ale ty jsou drahé a relativně pomalé),
- vznik přepínačů umožňujících rozdělení portů do oddělených skupin, omezujících všesměrové šíření, které jsou pro vzájemnou komunikaci propojeny přes směrovač = základ VLAN sítí
- vyšší stupeň bezpečnosti oddělením toků různých aplikací.



Obr. 4.15: Základní forma tvorby sítí VLAN na jednom přepínači

VLAN síť je tedy logická síť nezávislá na fyzickém rozmístění, dovoluje pružnou a efektivní segmentaci sítě, což umožňuje, aby uživatelé a síťové zdroje byli sdružovány logicky bez ohledu na jejich fyzické umístění. Změna konfigurace je pak podstatně snadnější a rychlejší, a také se zvyšuje celková propustnost sítě.

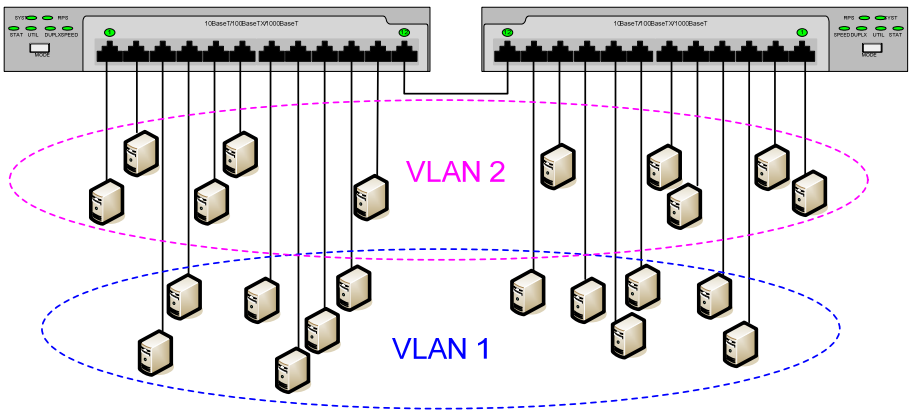
4.3.1 Způsoby vytváření VLAN sítí:

VLAN sítě lze vytvářet podle několika síťových znaků:

a) podle portů – nejčastější typ,
b) podle fyzické adresy,
c) podle síťové adresy,
d) podle skupinové adresy (multicast).

4.3.1.1 VLAN podle portů

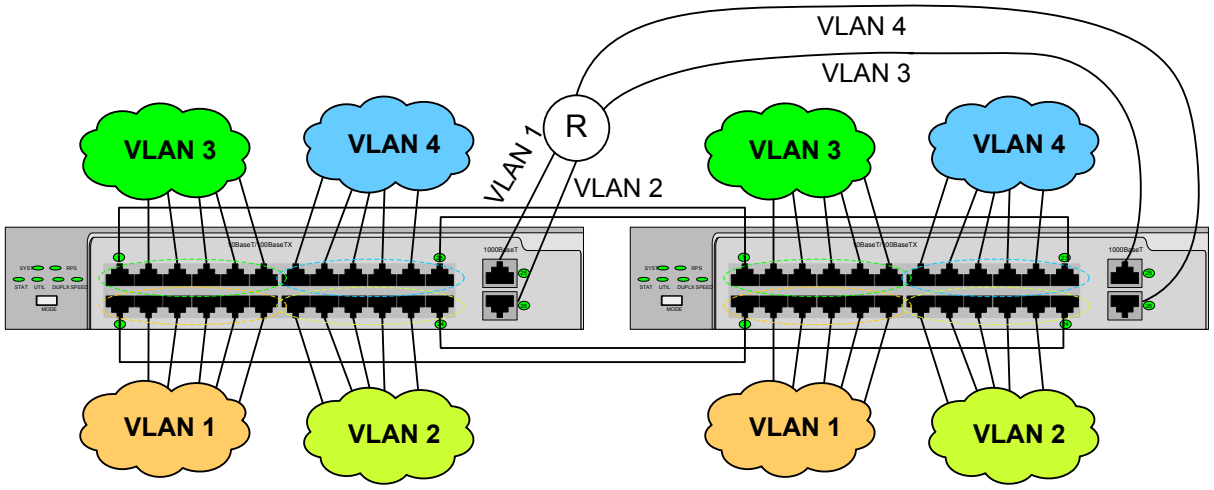
Tento historicky první typ virtuálních sítí definuje členství v síti pro jednotlivé porty přepínače (skupiny portů). První implementace těchto VLAN neumožňovaly rozšíření virtuální sítě přes více přepínačů, byly omezeny pouze na jeden přepínač. Druhá generace to již dovoluje, příklad takto definované sítě je na Obr. 4.16.



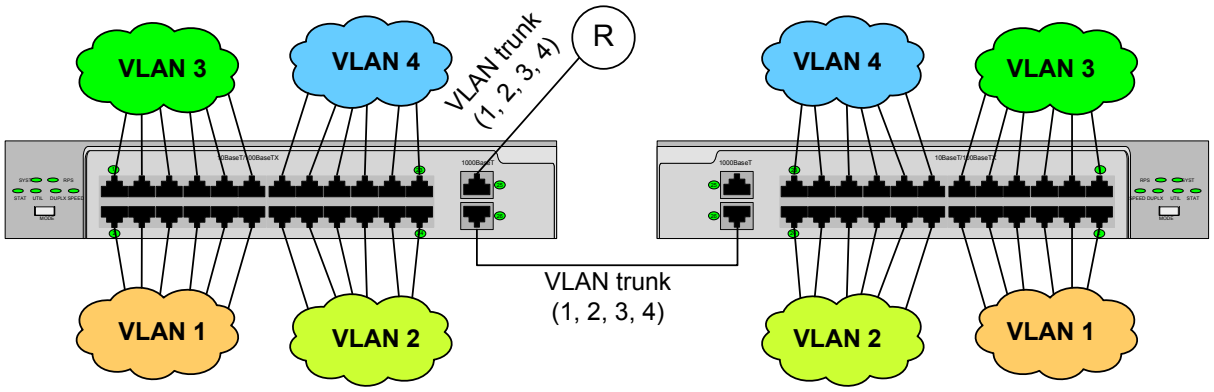
Obr. 4.16: VLAN se členstvím podle portů

Problém vznikne, jak identifikovat u rámců příslušnost k jednotlivým VLAN sítím. První, a pro větší počet naprosto nevhodná metoda je mít tolik propojení mezi přepínači a mezi přepínači a směrovačem, kolik je sítí VLAN, viz Obr. 4.17. Druhým a používaným způsobem je značkování rámců, kde značka nese identifikátor příslušnosti rámce k určité síti VLAN. Pak stačí pro celou skupinu sítí VLAN jediný spoj, tzv. „trunk“ vytvořený mezi značkovacími

porty, které vkládají a na druhé straně zase odstraňují značku s identifikátorem VLAN, viz Obr. 4.18.



Obr. 4.17: Těžkopádný způsob rozšíření sítí VLAN přes více přepínačů



Obr. 4.18: Tvorba sítí VLAN přes více přepínačů pomocí „trunkování“

Seskupování portů je stále nejpoužívanější metodou při vytváření virtuálních sítí. Je sice velmi jednoduchá a názorná, její základní omezení ale spočívá v nutnosti předefinování členství při jakémkoliv přesunu uživatelské stanice mezi jednotlivými porty přepínače (tedy přesněji řečeno takové změně portu, při které by došlo ke změně členství ve virtuální síti).

4.3.1.2 VLAN podle MAC adresy

MAC adresa je "natvrdo zadrátovaná" v obvodech síťového adaptéru, takže na takto definované virtuální sítě lze pohlížet jako na VLAN podle uživatelů. Změní-li totiž uživatel svoje připojení (přemístí se se svojí stanicí na jiný segment/port přepínače), jeho členství ve VLAN se nezmění.

Při této metodě je nutností prvotní manuální definice členství pro všechny stanice sítě. Jinou nevýhodou je možnost podstatného snížení výkonu v případě, že na portu přepínače je připojen sdílený segment se stanicemi v různých VLAN. Dalším, spíše ale jen okrajovým problémem může být situace, kdy uživatelé s mobilními notebooky mění svoji pozici a připojují se pomocí stabilně připojených docking stations. Tím se jím definiční MAC adresa s lokalitou mění (síťový adaptér je většinou součástí docku). Ačkoliv je to minoritní problém, dobře ilustruje jistá omezení VLAN, založených na členství podle MAC adresy.

4.3.1.3 VLAN podle protokolu nebo adres

Takto definované virtuální sítě jsou založeny na informacích ze třetí, tedy síťové vrstvy podle OSI modelu. V multiprotokolových sítích mohou být přiřazeny uzly do jednotlivých VLAN podle provozovaných síťových protokolů nebo např. v sítích s protokolem TCP/IP podle adresy podsítě.

Ačkoliv se zde pracuje s informacemi síťové vrstvy, je důležité si uvědomit, že se nejedná o jejich využití pro směrování. I když přepínač musí prohlédnout paket k určení IP adresy a tím členství ve VLAN, neprovádí žádné směrovací výpočty. Přepínač nevyužívá směrovací protokoly (jako jsou RIP, OSPF) a i na VLAN definovanou podle informací ze třetí, síťové vrstvy se musíme dívat jako na síť s plochou topologií, propojenou přepínači či můstky.

Dnešní rozmach přepínání i na třetí, síťové vrstvě a existence přepínačů se zabudovanými schopnostmi směrovačů tento problém při prvním pohledu trochu zamlžuje. Jedná se ale o odlišné funkce - pouhé určení členství ve VLAN na základě síťové adresy v jednom případě a plné využití směrovacích schopností na základě směrovacích protokolů a výpočtů na straně druhé. Zde je nutné podotknout, že komunikace mezi jednotlivými VLAN vyžaduje použití směrovačů - ať už klasických nebo právě těchto zabudovaných v nových přepínačích se směrovacími funkcemi.

Způsob definice VLAN podle síťové vrstvy má své zřejmé výhody. Patří mezi ně mobilita uživatelů či přesněji řečeno jejich stanic bez nutnosti překonfigurování členství ve VLAN, možnost vytváření skupin specifických pro jistou službu nebo aplikaci a eliminaci potřeby značkování paketů informací o členství ve VLAN při vzájemné komunikaci přepínačů (viz dále).

4.3.1.4 VLAN podle skupinového vysílání

Skupinové vysílání v IP sítích (IP multicast) pracuje tak, že paket, určený ke skupinovému vysílání je poslán na speciální adresu, která funguje jako proxy pro explicitně definovanou skupinu uzlů (IP adres). Paket je pak doručen všem uzlům, které jsou členy dané skupiny. Ta se sestavuje dynamicky, uzly se do této skupiny průběžně přihlašují a odhlašují.

Na všechny stanice takovéto skupiny můžeme tedy pohlížet jako na členy jedné virtuální LAN, protože skupina tvoří jednu doménu všesměrového vysílání. Od předchozích uvedených typů se liší ve dvou podstatných rysech - je vytvářena dynamicky jen na určitou dobu, takže je velmi flexibilní a její rozsah není omezen směrovači, tzn., že se může rozprostírat např. i po rozlehlé síti WAN.

4.3.2 Hlediska vytváření VLAN

4.3.2.1 Rozhodovací kritéria

- ***Podle organizační struktury firmy***

  Samostatná VLAN je vytvořena pro každou organizační jednotku podniku (konstrukce, výroba, obchod odděl., atd.). Předpokládáme, že většina komunikace probíhá v rámci jednotky - se specializovanými lokálními servery jednotlivých oddělení, tiskárnami atd. Pouze celopodnikově sdílené zdroje (např. e-mail brána) jsou členy všech virtuálních sítí. Tento přístup je administrativně poměrně nenáročný a je vhodný pro organizace s jasně definovanou plochou strukturou.

- ***Podle poskytovaných služeb***

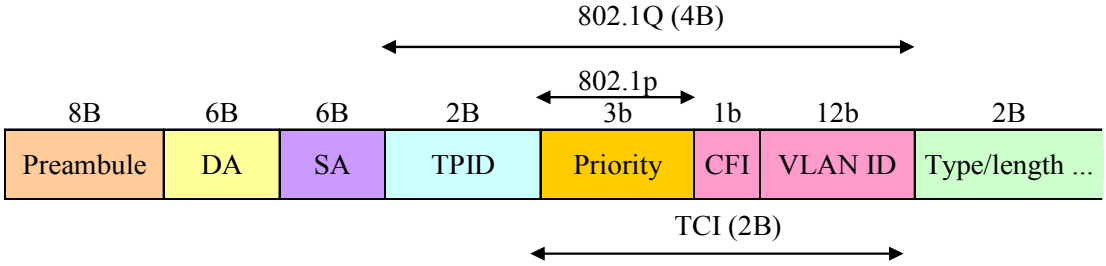
Tento přístup nekopíruje organizační strukturu firmy, ale je založen na přístupu uživatelů k jednotlivým poskytovaným síťovým službám. Tzn., že každá VLAN odpovídá jedné službě (související skupině služeb) sítě. Např. členy VLAN, odpovídající službě e-mail, budou asi všichni uživatelé, členy VLAN, odpovídající databázového serveru s ekonomickými agendami, budou jen členové ekonomického oddělení atd. Tento přístup je sice administrativně mnohem náročnější než předchozí způsob, lépe ale odpovídá dnešní, mnohem méně rigidní organizaci moderních firem.

4.3.2.2 Konfigurace VLAN

a) **ruční** s využitím různých programových prostředků
b) **zautomatizovaná** – podle kritérií definovaných správcem, např. podle využívaných aplikací, s využitím informací na DHCP serveru, apod.

4.3.3 Identifikace VLAN sítí

Nemá-li být VLAN omezena na jeden samostatný přepínač, musí si být přepínače schopny navzájem předat informace o členství jednotlivých uzlů (který uzel patří do které VLAN). V současnosti se používá technika značkování rámců (***Frame tagging***), kdy jednotlivé rámce jsou při přenosu mezi přepínači opatřeny speciální hlavičkou, nesoucí informaci o členství ve VLAN. Tento způsob byl vybrán a specifikován jako standard IEEE 802.1Q. Značkování se provádí pomocí 4 přídavných oktetů mezi pole SA (Source Address) a Length/Type, viz Obr. 4.19.



Obr. 4.19: Záhlaví rámce sítě Ethernet se značkováním

TPID (Tag Protocol Identifier) – identifikátor značky, pro IEEE 802.1Q má hodnotu **0x8100**
TCI (Tag Control Information) – řídicí pole značky,
Priority – priorita dat v rámci, 8 úrovní dle IEEE 802.1p, (0-7, 7 nejvyšší priorita),
CFI (Cannonical Format Indicator) – 0 značí, že adresy v rámci jsou v kanonické formě,
VLAN ID – identifikátor konkrétní sítě VLAN (12 bitů, 1-4094, 0 označuje prioritní rámec, 4095 je rezervováno).

ID typu VLAN – dvouoktetová hodnota vyjadřující, že se jedná o rámec sítě VLAN
Značkovací řídicí informace (Tag control information) –

- ***identifikace VLAN*** (VID) – číslo VLAN,
- ***priorita přenosu*** – 3 bity,
- ***CFI*** – identifikace pořadí bitů adresy (různé u Ethernetu, Token ringu a FDDI).

Nevýhodou standardu je, že definuje vytváření VLAN jen na základě první a druhé vrstvy (dle portů a MAC adres), neumožňuje vyváření VLAN na základě třetí vrstvy.

4.3.4 Protokol STP (Spanning Tree Protocol) v sítích VLAN

STP zajišťuje čistou stromovou strukturu sítě výběrem nejlepšího stromu a vypínáním redundantních spojů tvořících smyčky. Vytváření záložních spojů a tím i smyček je záměrné pro řešení přesměrování toku dat v případě výpadku jednoho spoje, existuje-li spoj záložní.

Protokol existuje ve dvou verzích, STP a RSTP (Rapid STP, specifikovaný standardem IEEE 802.1w). Verze RSTP umožňuje v Ethernetových metropolitních sítích zotavení v případě výpadku páteřní linky za 2 až 3 vteřiny, což je řádový rozdíl proti standardnímu STP, kdy tato doba činí 30 až 40 vteřin.

Původní technologie VLAN s přepínáním na 2. vrstvě, vyžaduje standardně separátní instanci protokolu STP pro každou VLAN. Některé přepínače (např. IronWare) implementují proprietární metodu pro spojování skupin uživatelů metropolitní sítě do tzv. spanning tree domén, založených na VLAN značkování. Tato metoda zvaná Superspan kombinuje více virtuálních sítí VLAN do jednotlivých instancí RSTP. Každý přepínač pak může být nakonfigurován pro 2 až 16 takových domén. Výsledným efektem těchto domén je omezení počtu STP map, které musí provozovatel sítě spravovat a zvýšení počtu virtuálních sítí, které přepínač zvládne.

4.3.5 Přínosy VLAN

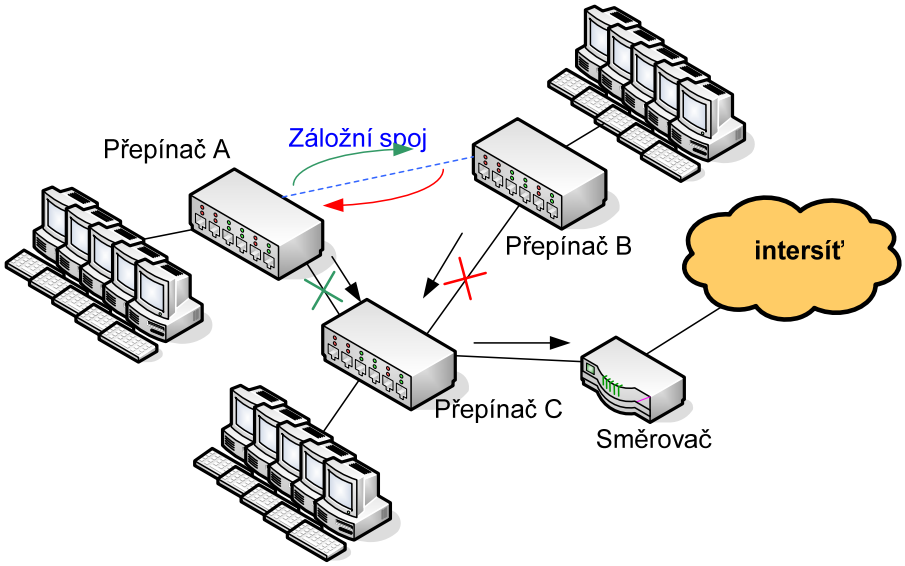
Mezi přínosy virtuálních sítí LAN (VLAN) patří především:

- vyšší výkonnost sítě
  - omezení všesměrového a vícesměrového šíření zpráv,
  - přebírá část zátěže od směrovačů,
  - větší rychlost,
- mobilita stanic (v některých případech),
- pružné seskupování stanic do VLAN sítí - není třeba fyzických přesunů,
- jednodušší správa sítí,
- úspora finančních prostředků,
- zvýšení bezpečnosti přístupu k citlivým datům (možnost implementace Firewallu).

Nevýhodou sítí VLAN je nezbytnost směrovače pro propojení různých VLAN.

4.4 Techniky zajištění čisté stromové struktury v sítích Ethernet - Spanning Tree Protocol

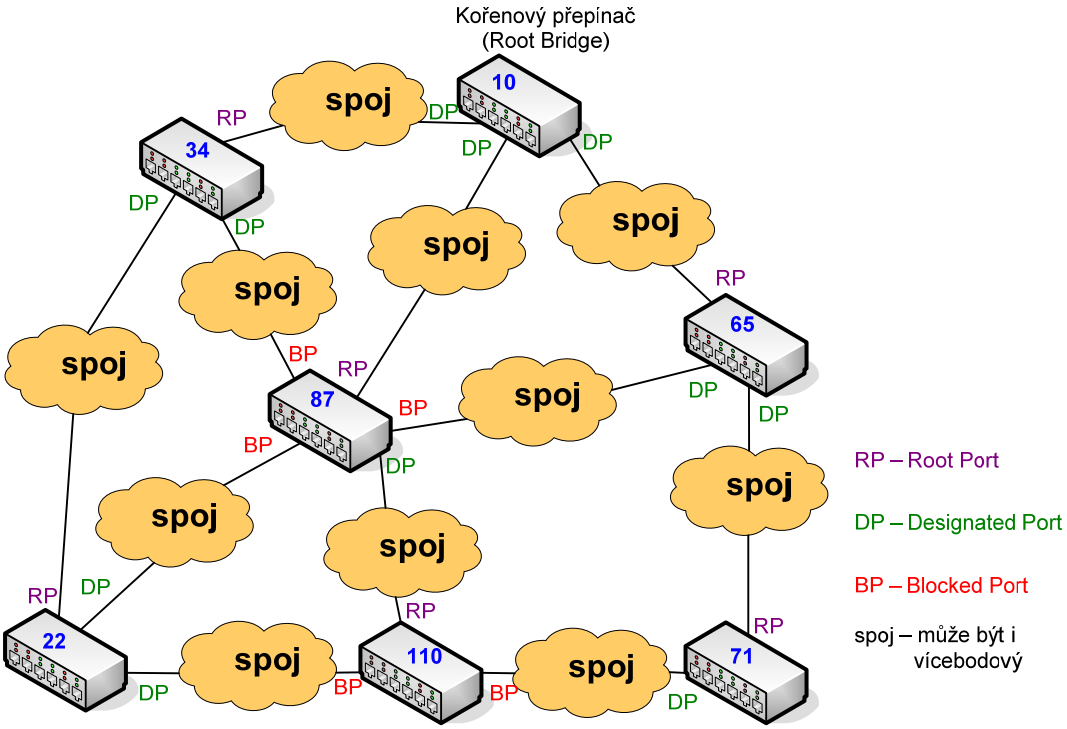
Pro bezproblémovou činnost sítí Ethernet je čistá stromová topologie spojů na úrovni MAC podvrstvy. To lze jednoduše zajistit stromovou fyzickou topologií sítě, což však s sebou přináší zásadní nevýhodu, a to nebezpečí odpojení části sítě při výpadku spoje či uzlu. Cílem rodiny protokolů označovaných jako **Spanning Tree Protocol** (**STP**) je udržovat v rozsáhlé síti s redundantní fyzickou topologií, a tedy obsahující smyčky, čistě stromovou logickou topologii pro MAC podvrstvu, tedy bez smyček a bez nebezpečí zhroucení sítě vlivem jevu „broadcast storm“.



Obr. 4.20: Princip zálohování spojů

4.4.1 Protokol STP

Přepínač podporující STP odesílá pravidelně (tzv. „Hello time interval“) zprávu **Bridge Protocol Data Unit** (**BPDU**). Tento rámec je odesílán implicitně každé 2 sekundy (lze nakonfigurovat) na všechny porty na rezervovanou skupinovou MAC adresu 01-80-C2-00-00-00. Struktura rámce je zobrazena na Obr. 4.22. Na základě priority přepínače (v případě shodných priorit i identifikátoru přepínače/mostu rozhoduje nejnižší MAC adresa) se nejdříve určí **kořenový přepínač** (kořen stromu – **root bridge**).



Obr. 4.21: Volba stromu

Ostatní si od něj na základě cen spojů (implicitně dle propustnosti spoje, ale může být administrátorem ručně definováno) odvodí cenu cesty. V případě, že mu přijde zpráva BPDU o stejném přepínači na více portů, **port s nejnižší cenou cesty** nechá zapojený a uvede do role

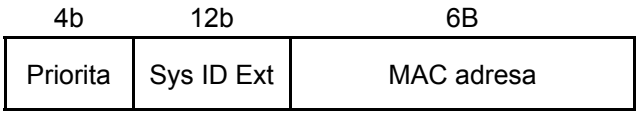
root port RP (port přepínače, přes který vede nejlevnější cesta ke kořenovému přepínači). Ostatní porty se uvedou do softwarově odpojeného stavu – Blocked port a je mu přidělena role označovaná jako *Alternate*. Porty přepínače, do kterých vstupuje tok, jenž má směřovat ke kořenovému přepínači jsou označeny jako Designated ports DP (ustanovené porty).

Celý proces je poměrně časově náročný, trvá v rozmezí 30 – 50 sekund. Všechny porty musí projít čtyřmi z pěti stavů: *Blocking, Listening, Learning, Forwarding* a *Disabled* (manuální zablokování), než začnou vysílat rámce. Po zvolení root přepínače jeho všechny porty přejdou do role *Designated* a stavu *Forwarding* a začnou vysílat BPDU rámce na své porty. Na základě ceny cesty si ostatní přepínače nastaví své porty do role *Root Port* (mají nižší cenu k *root* přepínači), *Designated* (pro ostatní přepínače je přes ně k root přepínači nejnižší cena), nebo *Alternate* (mají větší cenu cesty k *root* přepínači) – tento port rovnou uvedou do stavu *Blocking*, ve kterém zůstane. *Root* a *Designated* porty pak přejdou do stavu *Blocking*, kdy přijímají pouze BPDU rámce od root přepínače, ostatní komunikaci zahazují. V tomto stavu setrvají 20 sekund (hodnota Max-Age v BPDU rámci). Poté přejdou do stavu *Listening*. V tuto chvíli přijímají a vysílají BPDU rámce, žádnou další komunikaci nepřipouští. V tomto stavu setrvají 15 sekund (Forward Delay). Dále pokračují do stavu *Learning*, kdy posílají a přijímají BPDU rámce a zároveň se učí MAC adresy. V tomto stavu setrvají 15 sekund (Forward Delay). Následně přejdou do stavu *Forwarding*, kdy již přijímají a posílají vše.

Pole	Velikost [B]
Protocol ID	2
Version	1
BPDU Type	1
Flags	1
Root Bridge ID	8
Root Path Cost	2
Sender Bridge ID	8
Port ID	2
Message Age	2
Maximum Age	2
Hello Time	2
Forward Delay	2

Obr. 4.22: Struktura datové jednotky BPDU

Parametr **Bridge ID** má délku 8 B, a skládá se ze tří částí:



Priorita – nastavitelný parametr pro možnost ovlivnění výběru kořene STP
Sys ID Ext – další parametr, implicitně VLAN ID,
MAC adresa – fyzická adresa přepínače/mostu.

4.4.2 Protokol RSTP

Protokol RSTP (Rapid Spanning Tree Protocol) je definován standardem 802.1w. Byl vylepšen hlavně v rychlosti konvergence celé sítě. V praxi bylo zjištěno, že 30 - 50 sekundová

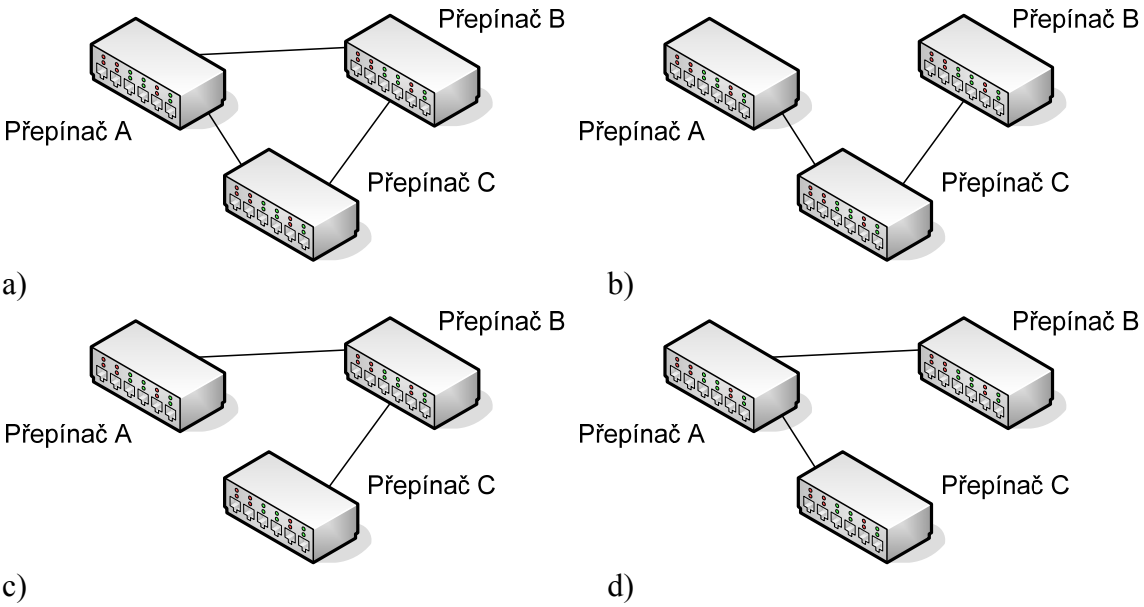
prodleva po startu nebo změně topologie u protokolu STP je moc dlouhá. Protokol byl vylepšen. Lze dopředu označit porty jako tzv. Edge. Takovým způsobem se označí porty ke kterým se budou připojovat koncové stanice, a ne další síťové prvky. Ty pak hned po rozběhnutí RSTP přejdou do stavu *Forwarding* a jsou připraveny na komunikaci. Další změnou je, že port neprochází stavy *Listening* a *Learning*, ale jen stavy – *Discarding*, *Forwarding* a *Disabled*. Během tří vyměněných BPDU rámců, je schopen protokol RSTP síť zprovoznit. Důležitá je i zpětná kompatibilita se standardem 802.1D (STP) – RSTP se degraduje na STP a celý proces konvergence znovu probíhá 30-50 sekund.

PVST

Protokol PVST (Per-VLAN Spanning Tree) je podpora více instancí STP pro síť LAN, ve které je vytvořeno více sítí VLAN, přičemž z hlediska bezpečnosti a možnosti rozložení zátěže je vhodné, aby každá VLAN mohla mít svou logickou stromovou strukturu a tudíž instanci STP. Spolu s PVST+ se jedná o proprietární řešení společnosti Cisco.

4.4.3 Multiple STP

Máme-li v síti implementováno více virtuálních sítí VLAN, pak každá VLAN by mohla provozovat samostatnou instanci protokolu STP. Při velkém počtu VLAN by to bylo výpočetně náročné, přičemž v síti může existovat jen několik logických topologií (podstatně méně než může být sítí VLAN), které jednotlivé VLAN opakovaně využívají, viz Obr. 4.23.

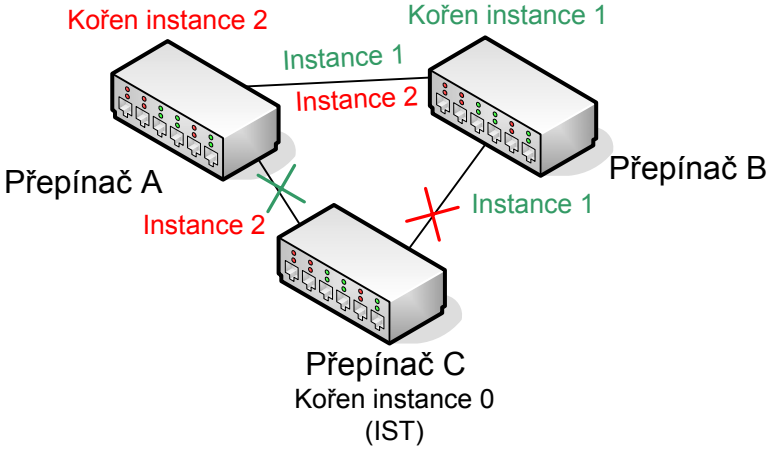


Obr. 4.23: Problematika instancí STP pro více VLAN: a) fyzická toplogie, b) logický strom 1, c) logický strom 2, d) logický strom 3

Protokol MSTP (Multiple Spanning Tree Protocol) umožňuje provozovat více STP instancí, a to jednu instanci pro každou jednotlivou logickou topologii. Tyto instance jsou nezávislé na VLAN. Konkrétní síti VLAN se pak přiřadí konkrétní instance MSTP. Původně byl tento standard v samotné normě **IEEE 802.1s**, od roku 2005 byl přidán do standardu **IEEE 802.1Q**, se kterým úzce souvisí.

Vystupuje zde nový parametr – **Region**, pod který všechny přepínače podporující MSTP musí patřit. Region je oblast zahrnující v. Po spuštění MSTP jsou všechny VLAN sítě zahrnuty do jedné instance STP označované jako IST (Internal Spanning Tree) a mající číslo 0. Kromě IST instance v síti existují další instance označované jako MSTI*n*, které kromě

jiného čísla se mohou lišit jinými prioritami přidělenými přepínačům, jinými hodnotami cen jednotlivých spojů i jinými hodnotami priorit jednotlivých portů přepínačů. Přepínače, na kterých běží MSTP, musí mít stejné rozdělení instancí pro VLAN. Tímto jednoduchým způsobem můžeme ovlivnit, kterou cestou bude procházet tok patřící např. Voice VLAN, jíž je přiřazena instance 1, a jejíž datové jednotky se tak nemusí potkat s ostatními rámci jiných VLAN, kterým je přiřazena instance 2. Schéma možného zapojení je na Obr. 4.24.



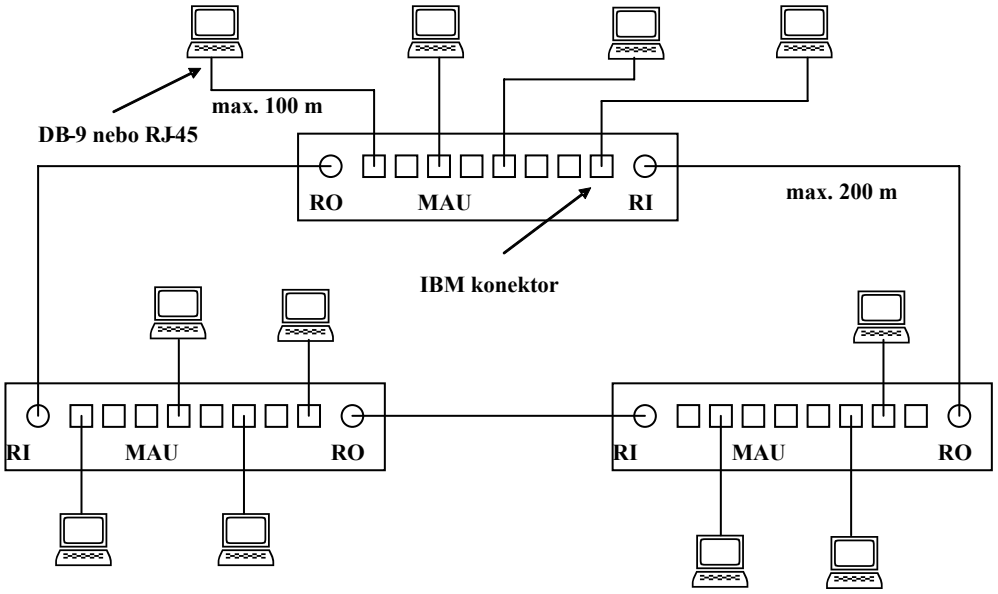
Obr. 4.24: Vytvoření dvou instancí pro oddělení VLAN pro hlasovou službu (Voice VLAN) od ostatních VLAN

Protokol MSTP je zpětně kompatibilní s RSTP, a přepínače podporující pouze RSTP vidí celý region jako jeden virtuální přepínač RSTP.

4.5 Síťová technologie Token Ring

4.5.1 Charakteristika sítě Token Ring

Token Ring (TR) je síť LAN s fyzickou kruhovou topologií, která byla navržena firmou IBM v 70. letech. Z návrhu pak vychází výsledný standard vypracovaný skupinou IEEE pod označením IEEE 802.5. V současnosti existuje v několika verzích – 4 Mb/s (Token Ring - TR), 16 Mb/s (Early Token Ring - ETR), 100 Mb/s (HSTR – High Speed Token Ring (802.5t) a ve stádiu návrhu byla vypracována i varianta 1000 Mb/s (802.5v). Vizuální topologie sítě je hvězda, která je vytvářena pomocí rozbočovacích zařízení označovaných jako MSAU (MultiStation Access Unit). Propojeno může být několik těchto zařízení pro vytvoření většího kruhu. Kruh je jednosměrný a může být i dvojitý, kdy druhý kruh je záložní. Každá jednotka MSAU obsahuje n portů obsahující vstup a výstup a přemosťovací relé, které se sepne a přemostí port, je-li stanice mimo provoz. MSAU může být také inteligentnější zařízení, které sleduje provoz v síti a napomáhá s rekonfigurací sítě v případě havárie. Stanice jsou k MSAU jednotce připojeny buď pomocí UTP, STP, koaxiálního či optického kabelu (multimode). Na fyzické vrstvě se pro rychlosti 4 a 16 Mb/s používá kódování diferenciální Manchester plus nedatové symboly J (High) a K (Low), pro 100 a 1000 Mb se používá fyzická vrstva Ethernetu (tj. 4B5B, 8B10B).



Obr. 4.25: Organizace sítě Token Ring

4.5.2 Přístupová metoda sítě Token Ring

Pro přístup ke sdílenému přenosovému kanálu se používá deterministická metoda předávání pověření (token passing). Princip metody spočívá v tom, že vysílat zprávu může pouze ta stanice, která přijala pověření. Toto pověření si stanice předávají ve směru toku dat, buď ihned, pokud stanice nemá data k vysílání, nebo po odeslání vlastních dat a případném ověření doručení dat. Navíc jsou do sítě TR implementovány ještě priority (8 úrovní), takže kromě vlastnictví pověření (tzv. peška) je zapotřebí patřičná priorita dat. Aby doba oběhu peška byla relativně krátká, je pro danou přenosovou rychlost stanoven maximální počet stanic v kruhu (např. 250 pro 4 a 16 Mb/s pro optiku a STP a 72 stanic pro UTP), maximální vzdálenost stanice od MSAU (a tedy max. vzdálenost mezi sousedními stanicemi, do 200 m pro UTP, pro optiku více), maximální vzdálenost mezi jednotkami MSAU (350 m pro UTP a až 10 km pro optiku) a maximální doba, po kterou si může stanice pověření (právo k vysílání) ponechat (pro 4 Mb/s je to max. 10 ms).
Implementace priorit je řešena pomocí dvou prioritních ukazatelů:

- aktuální priorita,
- rezervovaná priorita.

Pouze stanice se stejnou či vyšší prioritou, než ta, co je uvedena v přijatém pověření, smí vysílat data. Stanice vysílající datový rámec začlení pověřovací rámec (token) do datového rámce, ale s pozměněným bitem T (viz Obr. 4.26). Když datový rámec prochází stanicemi, mohou si stanice s prioritou vyšší než má vysílací stanice rezervovat vysílání v příštím kole uložením priority v poli RRR při zapamatování původní hodnoty rezervované priority. Po zrušení převzatého rámce vysílací stanicí je uvolněn token, který má nastavenu aktuální prioritu podle dříve rezervované priority. Token tak rychle projde stanicemi s daty s nižší prioritou a dříve se dostane k stanici, která si vysílání rezervovala. Po odvysílání stanice vyšle token, kde nastaví aktuální hodnotu priority podle rezervované priority.
V okruhu sítě je vždy jeden uzel označován jako aktivní monitor, který vykonává speciální řídicí a kontrolní funkce. Ostatní uzly jsou schopny převzít při výpadku monitoru tyto funkce automaticky. Jedná se o:

1. funkce generování hodinového signálu,

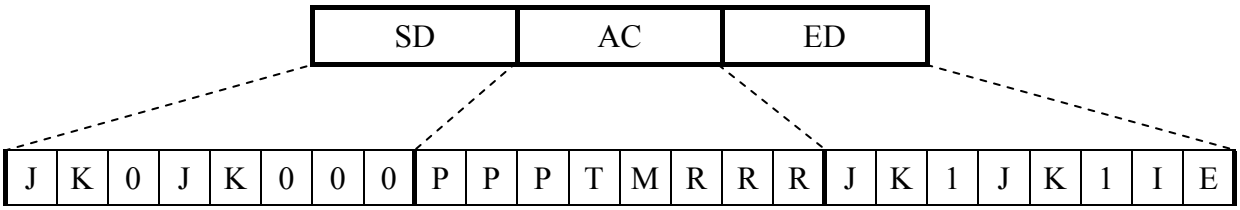
2. sledování ztráty pověření (stanice při ztrátě vynuluje okruh) a vygenerování nového token rámce,
3. odstraňování bloudících rámců,
4. vyrovnávaní frekvenčních odchylek,
5. pravidelná informace o přítomnosti monitoru ostatním uzlům.
6. inicializuje zjišťování sousedů v kruhu – důležité pro zjištění případného viníka rozpadu kruhu. Stanice, která od svého souseda neobdržela dlouho pověření, vyšle speciální zprávu (beacon) ostatním stanicím v kruhu. Stanice, která to pravděpodobně způsobila, se musí odpojit z kruhu a pak, je-li v pořádku, se opět připojit.

Při každém odstoupení či přistoupení stanice se předešlá konfigurace kruhu ruší a vyvolá se proces rekonfigurace.

4.5.3 Rámce sítě Token Ring

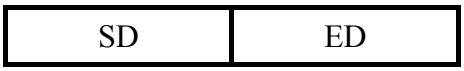
V síti TR se vysílají 3 druhy rámců:

- **Token** – pověření (pešek), délka 3 oktety, viz Obr. 4.26.



Obr. 4.26: Struktura pověřovacího rámce (token)

  - **SD** – Start Delimiter – úvodní sekvence sestavená z bitů 0 a nedatových symbolů J a K, jejichž tvar je závislý na typu kódování,
  - **AC** – Access Control – řízení přístupu k právu vysílat. Tvoří ho jeden oktet, který je rozdělen do 4 částí:
    - PPP – tři bity představující aktuální prioritu dat,
    - RRR – tři bity představující rezervovanou prioritu,
    - T – jeden bit vyjadřující, zda se jedná o pověřovací (0) či datový rámec (1),
    - M – jeden bit, tzv. monitorovací, využívá se pro odstranění cirkulujících rámců. Vysílací stanice jej nastaví na 0 a monitorovací stanice ho změní na 1. Přijde-li rámec ještě jednou, tzn., že nebyl vysílací stanicí zrušen, je monitorovací stanicí odstraněn.
  - **ED** – End Delimiter – jeden oktet, ukončovací znak,
    - I – Intermediate Symbol – hodnota je 1, jedná-li se o průběžný rámec zprávy (má význam pro datový rámec), 0, jedná-li se o poslední rámec,
    - E – Error bit – chybový bit vyjadřuje, zda při přenosu kruhem došlo k chybě. Kontrolu provádí každá stanice.
- **Abort Sequence** – zrušení platnosti právě vyslaného rámce vysílací stanicí, viz Obr. 4.27



Obr. 4.27: Rušicí rámec

- **Data Frame** – datový rámec nesoucí uživatelská (aplikační) data, viz Obr. 4.28.

SD	AC	FC	DA	SA	RI	DATA	FCS	ED	FS	IFG

Obr. 4.28: Datový rámec sítě Token Ring

- **FC** – Frame Control – udává, zda se jedná o MAC (management MAC podvrstvy) či LLC (datový) rámec
- **DA** – Destination Address – cílová adresa, 16 nebo 48 bitů dlouhá. Význam prvního bitu adresy závisí na způsobu přepínání. Používá-li se Source Route Bridging pak hodnota 1 prvního bitu specifikuje, že je cíl v jiném kruhu a že cesta k cíli povede přes mosty specifikované v RI (routing information). Jinak první bit značí, zda je adresa individuální či skupinová. Druhý bit v obou případech značí lokální (1) či celosvětovou jedinečnost (0) adresy.
- **RI** – Routing Information – informace určující cestu rámce přes mosty či přepínače, je-li nastaven první bit adresy na 1. Pole RI obsahuje typ rámce vzhledem k přepínání (datový rámec se zadanou cestou, průzkumný rámec, rámec protokolu STP), délku pole RI, délku rámce a seznam identifikátorů cesty - identifikátor kruhu (12 bitů) a identifikátor mostu (4 bity)
- **DATA** – informace LLC vrstvy (SNAP, řízení – HDLC, typ vyššího protokolu) a aplikační data
- **FCS** – Frame Check Sequence – 32 pole pro zabezpečení rámce pomocí cyklického kódu.
- **FS** – Frame Status – jeden oktet, prakticky obsahuje dvakrát opakovanou dvojici bitů A,C, které jsou po odeslání nastaveny na 00. Rozpozná-li cílová stanice data a zkopíruje-li si je, nastaví AC na 11, což je informace pro odesílatele, že data byla správně doručena.
- **IFG** – InterFrame Gap – jeden oktet pro 4 Mb/s, 5 oktetů pro 16 Mb/s.

Maximální délky datových rámců jsou 4 a 18 kB pro rychlosti 4 a 16 Mb/s.
Podvrstva LLC podporuje dva typy služeb:

- bez spojení,
- spojově orientovanou.

Mosty a přepínače sítě TokenRing mohou realizovat dva druhy přepínání:

- **transparentní** – jako přepínače u Ethernetu, avšak s principem přijímání a značení rámců v síti Token Ring,
- **zdrojové přepínání** (Source Route Bridging) – viz kap. 3.5.3.2. Síť pak nemusí být striktně stromová. Určení cesty je práce koncových uzlů. Problémem je podpora všesměrového šíření, kdy by mohlo vlivem existence smyček dojít k zahlcení (kolapsu) sítě (broadcast storm).

4.5.4 Fast Token Ring

Fast Token Ring (FTR) je síť Token Ring s přenosovou rychlostí 100 Mb/s. Standard je specifikován pod označením IEEE 802.5t. Fyzická vrstva je převzata z Fast Ethernetu (IEEE 802.3u) a upravena pro potřeby sítě Token Ring. Přenosovými médii jsou xTP a optické vlákno.

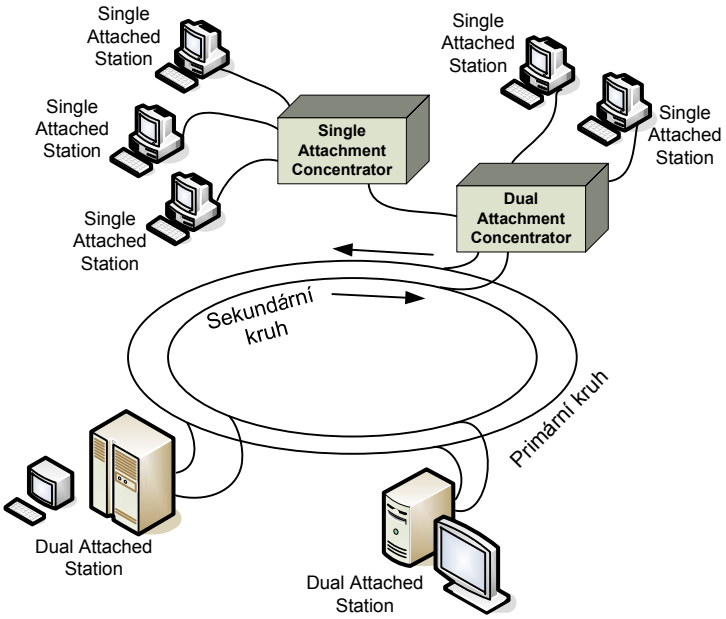
4.5.5 Gigabit Token Ring

Gigabit Token Ring (GTR - 802.5v 1000Mbit/s) přebírá fyzickou vrstvu od Gb Ethernetu (802.3z) pro optiku (jednovidová i mnohavidová vlákna) i kroucený dvoudrát. Linková vrstva zůstává stejná, tj. přístupová metoda a struktura rámce, ale s implementací standardů IEEE 802.1q a 802.1d.

4.6 FDDI

4.6.1 FDDI-I

Síť **FDDI** (Fibre Distributed Data Interface) je síť s kruhovou topologií. Byla to první síť s přenosovou rychlostí 100 Mb/s a byla navržena pro sítě MAN. Byla vyvinuta v 80. letech institutem ANSI pod označením X3T9.5 a mezinárodně standardizována organizací ISO pod číslem 9314. Kruhová struktura je tvořena dvěma kruhy pro opačné směry přenosu, z nichž jeden je záložní pro případ možnosti obnovy kruhu při jeho přerušení. Obnova kruhu je řešena automaticky uzavřením smyčky v sousedních uzlech, mezi nimiž došlo k přerušení kruhu. Délka kruhu se tak téměř zdvojnásobí, a taktéž počet uzlů. FDDI byla navržena pro použití optických kabelů, a to vícevidových (max. vzdálenost mezi stanicemi je 2 km) i jednovidových (větší dosažitelná vzdálenost – i desítky km). V současnosti však existuje standard i pro kroucený pár označovaný jako CDDI (Copper DDI).

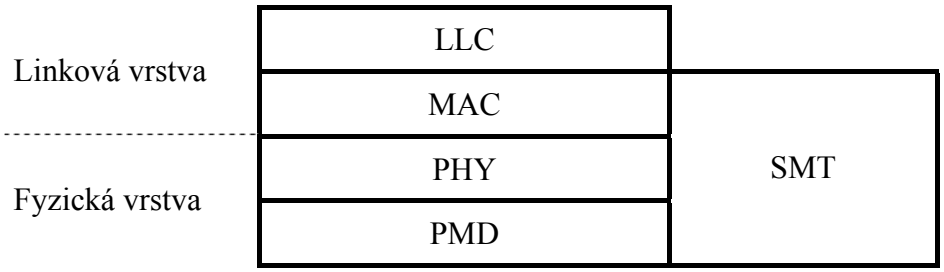


Obr. 4.29: Struktura sítě FDDI

FDDI je definována čtyřmi specifikacemi:

- protokol fyzické vrstvy **PHY**,
- specifikace vrstvy **PMD** (Physical Medium Dependent) – nejspodnější část fyzické vrstvy,
- protokol přístupu k médiu **MAC**,
- protokol správy stanice a kruhu **SMT** (Station Management),

Protokol řízení linkového spoje využívá specifikaci **LLC** podle IEEE 802.2.



Obr. 4.30: Vrstvová architektura FDDI

Maximální délka kruhu může být až 200 km a maximální počet stanic je 1000. Tento limit se však snižuje téměř na polovinu, chceme-li využívat výhod dvojitého kruhu. Stanice či koncentrátory mohou být připojeny ke kruhu dvěma způsoby:

- k hlavnímu i záložnímu kruhu se schopností obnovit kruh v případě rozpadu hlavního kruhu – **Dual Attached Stations** (DAS), **Dual Attachment Concentrator** (DAC),
- pouze k hlavnímu kruhu – **Single Attached Stations** (SAS), **Single Attachment Concentrator** (SAC).

Použité symbolové kódování je 4B/5B ve spojení s NRZI (Non-Return to Zero Inverted – logická nula polaritu signálu nemění, logická jednička ano). Vybrané pětice bitů obsahují maximálně 3 nuly za sebou, pravidlo však platí i pro přechody mezi pěticemi. Nedatové symboly se používají pro rámcové značky ohraničující rámce.
Přístupová metoda je stejně jako u sítě Token Ring deterministická metoda předávání pověření „token passing“ ovšem se spěšným uvolněním rámce token (obdoba ETR).

Délka rámce se pohybuje v rozmezí 9 až 4500 oktetů s minimální mezirámcovou mezerou 8 oktetů. Používají se dva základní typy, které jsou podobné rámcům sítě Token Ring:

- **pověřovací rámec** (token), viz Obr. 4.31,

Obr. 4.31: Pověřovací rámec sítě FDDI

  - **Preambule** – alespoň 16 pětic bitů pro synchronizaci přijímače,
  - **SD** – Start Delimiter – počáteční omezovač obsahující nedatové kombinace,
  - **FC** – Frame Control – 1octet udávající typ rámce (datový či řídicí, případně konkrétní druh řídicí zprávy), typ provozu (synchronní – pravidelné vysílání, např. pro toky ISDN či PCM; asynchronní – klasický paketový přenos) a typ adresy (16-bitová či 48-bitová),
  - **ED** – End Delimiter – zakončovací omezovač obsahující nedatové kombinace
- **datový rámec či rámec managementu** – viz Obr. 4.32.

Obr. 4.32: Datový či managementový rámec sítě FDDI

DA – Destination Address – cílová adresa, 16 nebo 48 bitů dlouhá. První bit značí, zda je adresa individuální či skupinová. Druhý bit v obou případech značí lokální (1) či celosvětovou jedinečnost (0) adresy,
DATA – informace LLC vrstvy (SNAP, řízení – HDLC, typ vyššího protokolu) a aplikační data nebo data pro management (SMT),
FCS – Frame Check Sequence – 32 pole pro zabezpečení rámce pomocí cyklického kódu,
FS – Frame Status – jeden oktet, obsahuje dvojici bitů které jsou po odeslání nastaveny na 00. Rozpozná-li cílová stanice data a zkopíruje-li si je, nastaví AC na 11, což je informace pro odesílatele, že data byla správně doručena. Pokud je hodnota jiná došlo k chybě.

K řízení vysílání a předávání pověřování se využívá několik časovačů:

- **TTRT** – Target Token Rotation Time,
- **TRT** – Token Rotation Time,

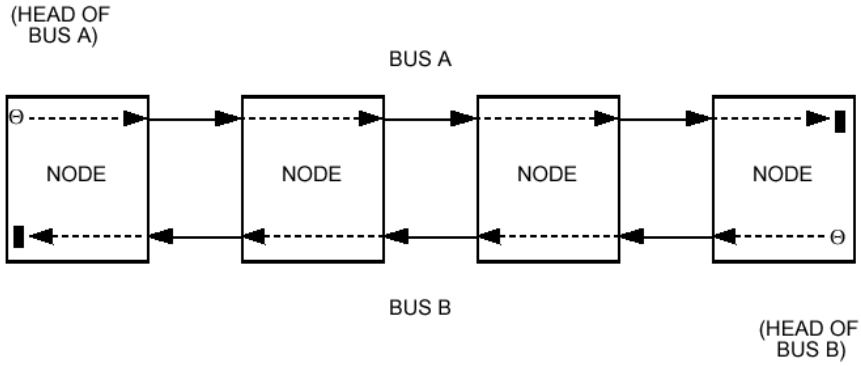
- **THT** – Token Hold Time.

4.6.2 FDDI-II

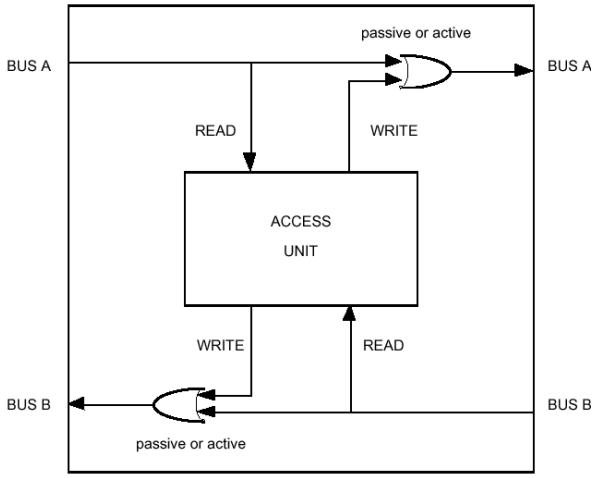
Možnosti sítě FDDI byly rozšířeny v podobě specifikace FDDI-II, která podporuje izochronní služby, tedy například přenos multiplexů telefonních kanálů jako PCM, E1 a podobně. Je to řešeno rozdělením kapacity 100 Mb/s na 16 izochronních kanálů s přenosovou rychlostí 6,144 Mb/s a paketový kanál 768 kb/s. Každý izochronní kanál může být rozdělen na 3 subkanály s rychlostí 2,048 Mb/s nebo 4 subkanály s rychlostí 1,536 Mb/s a ty dále na 32 nebo 24 kanálových intervalů pro rychlost 64 kb/s. Jeden rámec trvá 125 μs a slot pro každý kanál 6,144 Mb/s obsahuje 96 oktetů, slot pro paketový přenos 12 oktetů. Nevyužité izochronní kanály jsou použity pro rozšíření kapacity pro paketový přenos.

4.7 DQDB

Síť DQDB (Distributed Queue Dual Bus) je tvořena dvojitou sběrnicí s opačnými směry přenosu. Je specifikovaná normou IEEE 802.6, která byla schválena v roce 1989. Je řazena především mezi sítě MAN, neboť může pokrýt oblast na vzdálenost až 100 km až s 500 uzly se vzdáleností mezi sousedy až 2 km. Hodí se pro propojování sítí LAN. Důležitou vlastností je nespecifikovaná a pouze úrovní technologie omezená přenosová rychlost. Zavedením různých způsobů přístupu (viz níže) umožňuje poskytování jak datových služeb, tak i služeb v reálném čase (hlas, video).



Obr. 4.33: Otevřená topologie sítě DQDB

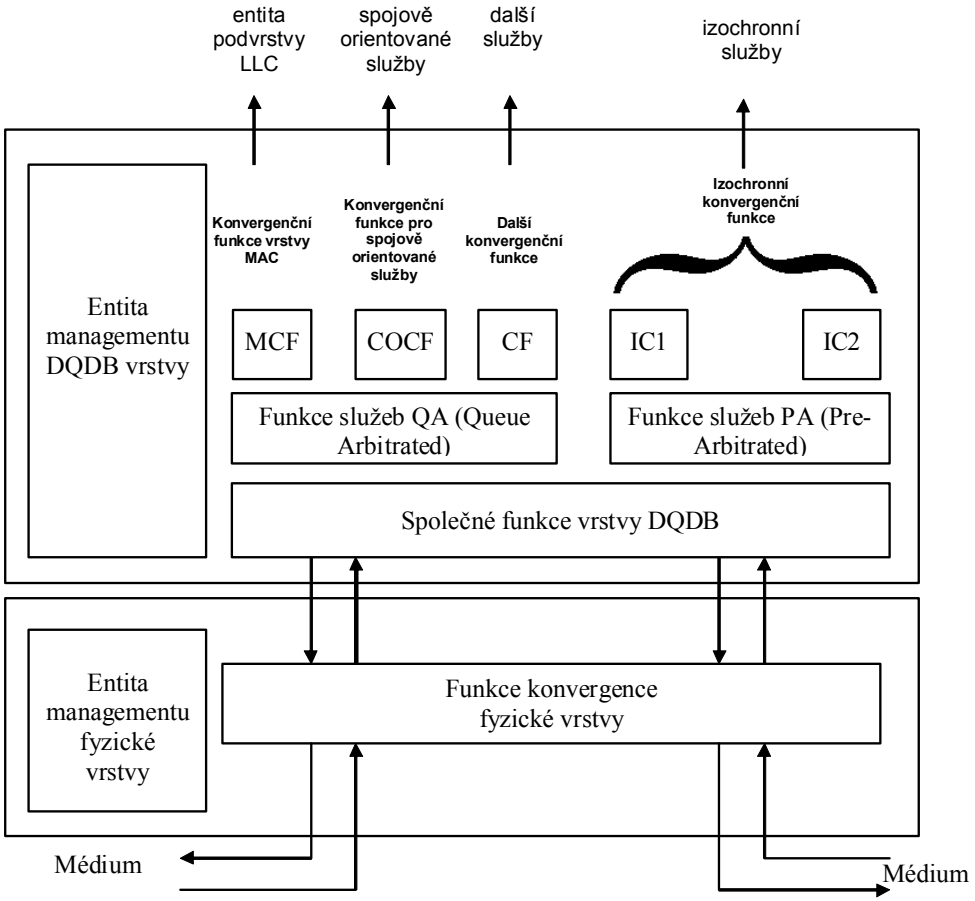


Obr. 4.34: Příklad připojení přístupové jednotky ke sběrnicím

Jako přenosového média se využívají buď koaxiální kabely ale stále častěji spíše optická vlákna. Přenosová kapacita je rozdělena do stejně dlouhých časových slotů (rámců) o délce 53B (souhlasí s délkou buňky v ATM). Sběrnice začíná generátorem rámců a končí terminátorem. Je-li rámcový generátor i terminátor pro oba směry v jedné stanici, vzniká **kruhová topologie**, avšak stále se sběrnicovou architekturou. Výhodou této topologie je, že v případě poruchy sběrnice v určitém místě, lze zaručit funkčnost sítě, a to tím, že původní stanice, která byla generátorem rámců a koncovým bodem pro obě sběrnice, se stane průchozí stanicí a funkci generátorů a koncových bodů převezmou stanice, mezi kterými byly sběrnice přerušeny.
Vrstvová architektura sítě DQDB (fyzická vrstva a podvrstva MAC) je zachycena na Obr. 4.35, podrobněji pak na Obr. 4.36, který zachycuje možnost podpory různých typů služeb – nespojově orientovaných, spojově orientovaných a izochronních.

konvergenční entity vrstvy DQDB (DQDB Layer Convergence Entities)	entita managementu vrstvy DQDB (DQDB LME - Layer Management Entity)
konvergence fyzické vrstvy (Physical Layer Convergence)	entita managementu fyzické vrstvy (Physical LME - Layer Management Entity)

Obr. 4.35: Vrstvová architektura sítě DQDB



Obr. 4.36: Podrobnější znázornění vrstvové struktury sítě DQDB

Pro přístup k médiu jsou definovány dva mechanizmy:

- **PA** (**Prearbitrated Access**) – mechanizmus pro přidělení konstantní přenosové rychlosti pro poskytování služeb v reálném čase (hlas, video, …). Slotům je po ustanovení spojení přidělen identifikátor cesty VCI (Virtual Channel Identifier), který je vložen do hlavičky rámců nesoucí data, přičemž datové pole daného slotu je složeno z několika skupin oktetů, které mohou být obsazovány a nebo čteny různými stanicemi. Každá stanice musí znát ofset (počáteční oktet skupiny oktetů) a délku skupiny oktetů, které má obsazovat daty nebo je naopak číst. O vysílání slotů označených jako PA se stará generátor rámců (počáteční stanice ve směru vysílání).
- **QA** (**Queue Arbitrated Access**) - metoda distribuovaných front pro každý směr (sběrnici). Je-li k tomu přidána ještě sada priorit, pak se musí udržovat dvojice front pro každou prioritu. Při neuvažování prioritního mechanizmu každá stanice má pro každý směr dva čítače, čítač žádostí o vysílání ***RC*** (***Request Counter***) a čítač pozice ve frontě ***CD*** (**Count Down**). Chce-li stanice vyslat data v určitém směru, překopíruje si hodnotu RC do CD a v opačném směru vyšle požadavek na vysílání (nastavení určitého bitu v rámci). Požadavek je zaznamenán ve stanicích, které se nacházejí ve směru k generátoru rámců. Pak stanice počítá prošlé prázdné rámce v požadovaném směru a za každý sníží čítač CD o jedničku. Dosáhne-li CD hodnoty nula, může stanice příští prázdný rámec naplnit vyslanými daty.

Datové rámce v podobě **IMPDU** (Initial MAC Protocol Data Unit) jsou odesílány po částech (segmentech) v několika slotech v podobě **DMPDU** (Derived MAC Protocol Data Unit).

IMPDU záhlaví			IMPDU data			
Všeobecné záhlaví PDU	MCP záhlaví	Rozšíření záhlaví	INFO	PAD	CRC 32	Všeobecné zakončení PDU
(4B)	(20B)	k*4B	≤ 9188B	1,2,3 B	0 nebo 4B	(4B)

Obr. 4.37: Struktura datového rámce IMPDU

Všeobecné záhlaví PDU

1B	1B	2B
Rezervováno	BEtag	BAsize

Obr. 4.38: Struktura všeobecného záhlaví PDU

- ***BEtag*** (Begin_End Tag) – číslo pro označení začátku IMPDU jednotky. Musí souhlasit s BEtag ve Všeobecném zakončení PDU.
- ***BAsize*** (Buffer Allocation Size) – požadavek na velikost bufferu pro příjem jednotky IMPDU. Musí souhlasit s položkou délka (Length) ve Všeobecném zakončení PDU.

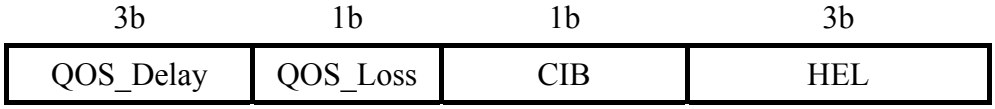
Záhlaví MCP (MAC Convergence Protocol)

8B	8B	1B	1B	2B
DA	SA	PI/PL	QOS/CIB/HEL	Bridging

Obr. 4.39: Formát záhlaví MCP

- ***DA*** (Destination Address) / ***SA*** (Source Address) – cílová a zdrojová adresa, první 4 bity specifikují délku adresy, individuální či skupinovou povahu adresy a globální či lokální platnost. Délka adresy může být 16, 48 a 60 bitů.

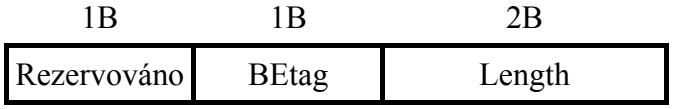
- ***PI/PL*** (Protocol Identifier – 6b/PAD Length-2b) – PI identifikuje data (pro LLC podvrstvu, lokální administraci a rezervované hodnoty), PL definuje délku výplně, která může nabývat hodnoty 1, 2 a 3 oktety na doplnění délky na celistvý násobek 4 oktetů.
- ***QOS/CIB/HEL*** (QoS/CRC Indicator Bit/ Header Extension Length) – má následující strukturu:



Obr. 4.40: Formát pole QOS/CIB/HEL

  - *QoS_Delay* – požadavek na zpoždění, 8 úrovní,
  - *QoS_Loss* – možnost zahodit jednotku, většinou má hodnotu 0 (nesmí se zahodit),
  - *CIB* – indikuje přítomnost či nepřítomnost CRC32,
  - *HEL* – definuje délku rozšíření záhlaví (v násobcích 4 oktetů), max. 5,
- ***Bridging*** – pro budoucí využití mostů pro propojení mezi dvojitými sběrnicemi, např. specifikace počtu mostů, přes které může jednotka,

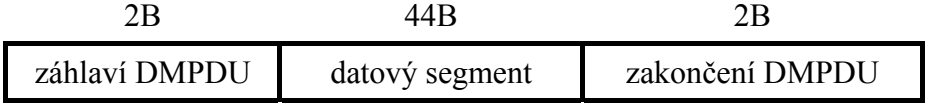
Rozšíření záhlaví – pro budoucí využití pro přenos dalších typů datových jednotek,
INFO – obsahuje datovou jednotku MSDU (MAC Service Data Unit) – nejčastěji se jedná o datovou jednotku LLC (PI = 1),
PAD – výplň na celistvý násobek 4 oktetů,
CRC 32 – zabezpečení dat, buď je přítomno (CIB = 1) a má délku 4 oktety a nebo chybí (CIB = 0).
Všeobecné zakončení jednotky PDU



Obr. 4.41: Struktura Všeobecného zakončení jednotky PDU

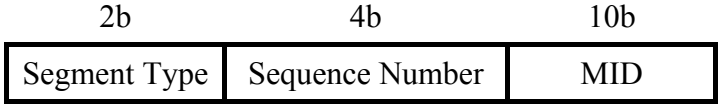
- ***BEtag*** – značka konce datové jednotky, hodnota je shodná se značkou začátku datové jednotky v poli Všeobecné záhlaví jednotky PDU,
- ***Length*** – udává celkovou délku (v oktetech) polí MCP, Rozšíření záhlaví, Info, PAD a CRC 32. Hodnota se musí shodovat s hodnotou pole BAsize v poli Všeobecné záhlaví jednotky PDU.

Datová jednotka IMPDU se segmentuje na části (**Segmentation unit**) dlouhé 44 oktetů (poslední se vyplní do této délky) a přidá se k tomu záhlaví a zakončení, čímž vznikne 48 oktetová jednotka **DMPDU** (Derived MAC Protocol Data Unit).



Obr. 4.42: Struktura DMPDU

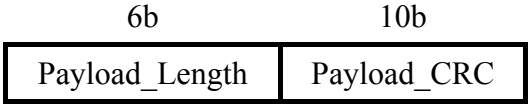
DMPDU záhlaví



Obr. 4.43: Struktura záhlaví DMPDU

- **Segment_Type** – definuje zda se jedná o počáteční, průběžný, závěrečný segment jednotky IMPDU, nebo segment tvoří celou jednotku IMPDU,
- **Sequence Number** - číslo segmentu modulo 16,
- **MID** (Message Identifier) – číslo jednoznačně identifikující zprávu, slouží k opětovnému složení zprávy v přijímací stanici.

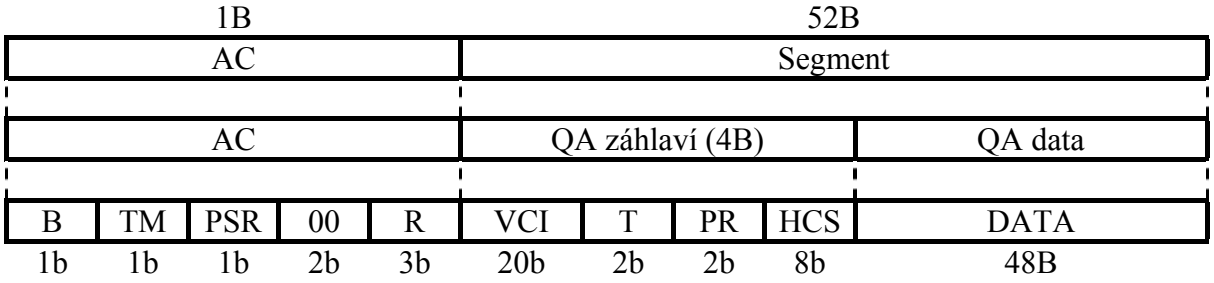
DMPDU zakončení



Obr. 4.44: Struktura zakončení DMPDU

- **Payload_Length** – udává počet oktetů z jednotky IMPDU, nabývá hodnot 4, 8, ..., 44,
- **Payload_CRC** – 10-bitové zabezpečení.

Jednotky DMPDU jsou pak doplněny o 4 oktety záhlaví a oktet pro řízení přístup, čímž vznikne konečná podoba 53 B rámců (buněk) přenášených fyzickou vrstvou, viz Obr. 4.45.



Obr. 4.45: Struktura rámce sítě DQDB

- **B** – obsazenost segmentu,
- **TM** – typ segmentu (PA/QA),
- **PSR** (Previous Segment Received) - možnost zahodit předešlý slot (při nastavení na log. 1),
- **00** – nevyužité bity,
- **R** (Request) – definice úrovně požadavku na vysílání (3 priority),
- **VCI** – identifikátor virtuální cesty,
- **T** – typ přenášených dat, pro uživatelská data má hodnotu 00, ostatní kombinace jsou rezervovány,
- **PR** – priorita segmentu při nasazení víceportových můstků, jinak nastaveno na 00,
- **HCS** (Header Check Sequence) – kontrolní pole záhlaví $x^8 + x^2 + x + 1$ (pro opravu jednobitových chyb).

4.8 Ostatní sítě LAN a MAN

V průběhu vývoje sítí vznikla řada dalších typů, kam patří především sítě Token Bus, Arcnet, Fibre Channel a 100VG-AnyLan. Většina z nich se až na technologii Fibre Channel již používá pouze výjimečně.

4.8.1 Fibre Channel

Fibre Channel je typ sítě s relativně malým dosahem a vysokou propustností (stovky Mb/s až jednotky Gb/s), která byla navržena pro propojení procesorových systémů například za

účelem zvýšení bezpečnosti výpočetních systémů (clustering). Komunikace mezi dvěma uzly sítě je buď přímá (přímé propojení kabelem) nebo přepínaná a nebo do kruhu.
Vrstvový model se skládá z pěti podvrstev (viz Tab. 4.12).

Tab. 4.12: Vrstvy sítě Fibre Channel

Vrstva	úloha vrstev
FC-4	mapování rozhraní IPI, SCSI, HIPPI, SBCCS, 802.2, IP, ATM
FC-3	konvergenční vrstva
FC-2	signalizační vrstva
FC-1	přenosová vrstva
FC-0	fyzická vrstva

IPI – Intelligent Peripheral Interface,
HIPPI - High Performance Parallel Interface,
SCSI – Small Computer System Interface,
SBCCS – Single-Byte Command Code Set.

Síť Fibre Channel definuje uzly sítě, které mohou mít obecně jeden i více portů (N_port = Node_port) a mohou jimi být pracovní stanice (počítač) či vstupně-výstupní zařízení. Propojovací prvek (Fabric) může mít teoreticky až téměř 2^{24} tzv. F_portů (Fabric_ports).
Základním přenosovým médiem v FC-0 je optické vlákno (více- nebo jednovidové), ale jsou specifikovány i další typy kabelů – koaxiální a stíněný symetrický kabel. Podporované jsou přenosové rychlosti 132,8, 265,6, 531,25 a 1062 Mb/s.

- **Podvrstva FC-1** řeší problematiku kódování (8B10B),
- **Podvrstva FC-2** plní některé úkoly spojové vrstvy (řízení spoje, řízení toku dat, vytváření rámců, zabezpečení a kontrola rámců, multiplex a demultiplex datových jednotek vyšší vrstvy. Podvrstva FC-2 také poskytuje několik tříd služeb (přepojování okruhů, přepojování rámců, datagramovou službu), které mohou být v kanále poskytovány buď samostatně nebo i současně (režim Intermix). Rámec může nést až 2112 oktetů dat, ke kterým se přidá záhlaví dlouhé 24 oktetů a z druhé strany zabezpečení dlouhé 4 oktety. Fyzická vrstva k rámci přidává ještě počáteční a koncový omezovač, viz Obr. 4.46.

4 B	24 B	70-2112 B	4 B	4 B
Počáteční omezovač	Záhlaví	Data	Kontrolní součet	Koncový omezovač

Obr. 4.46: Rámec sítě Fibre Channel

  Řízení toku dat umožňuje předcházet zahlcení příjemce pomocí systému kreditů, kdy příjemce zasílá vysílači tzv. kredity umožňující odeslat pouze limitované množství dat.
- **Podvrstva FC-3** je podvrstvou, která plní konvergenční funkce, tzn. že umožňuje různým službám (protokolům vyšší vrstvy) využívat společné spodní vrstvy architektury Fibre Channel. Příklady mohou být služby spojování portů do skupin s možností adresace skupiny a přenosu dat jedním z volných portů.
- **Podvrstva FC-4** provádí mapování různých komunikačních rozhraní na společné sériové rozhraní sítě Fibre Channel, což umožňuje propojit zařízení s odlišnými rozhraními a komunikačními protokoly s protějším zařízením přes síť Fibre Channel. Je definováno mapování pro systémy IPI-3, SCSI, HIPPI, SBCCS, 802.2, IP/ARP, ATM.

Síť Fibre Channel není omezená fyzickou topologií a umožňuje vytvářet spoje:

- ***dvoubodové*** – možnost plného duplexu a dosahu až 10 km pro nejvyšší rychlost a jednovidové vlákno,

- ***přepínané*** – využívá jeden či více přepínačů s neblokujícím spojovacím polem,
- ***ve smyčce*** – kruhová topologie nevyžadující rozbočovač či přepínač, s možností propojení zařízení s celkovým počtem až 126 portů, přenosový kanál je sdílený, metoda přístupu je podobná metodě předávání pověření, kdy pořadí je dáno vzestupnou posloupností čísel portů.

5 Protokolová architektura TCP/IP

V současnosti je s drtivou převahou nejpoužívanější sada TCP/IP. V minulých letech například firma Novell používala ve svých produktech sadu IPX/SPX, která se však ukázala pro globálním počítačovou síť jako neperspektivní.

5.1 Úvodní charakteristika protokolové sady TCP/IP

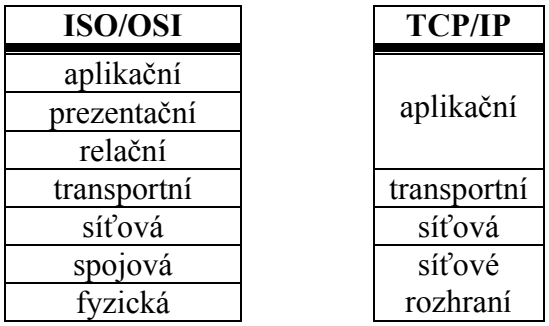
Celosvětová síť Internet je v současnosti založena protokolové sadě TCP/IP (Transmission Control Protocol/ Internet Protocol). Její vývoj probíhá od počátku 70. let. Již od raných verzí byla architektura založena na těchto zásadách:

- vývoj TCP/IP směřuje od jednoduššího ke složitějšímu,
- síť nemusí být spolehlivá, musí však být co nejrychlejší. To znamená, že může docházet ke ztrátě paketů a spolehlivost si zajišťují až koncové uzly sítě, a to až na transportní či vyšší vrstvě, pokud je spolehlivost vyžadována. Pro zajištění spolehlivosti musí mít koncový uzel vyrovnávací paměti pro případ žádosti o opakování,
- upřednostňuje se nespojovaný charakter komunikace na úrovni sítě, tedy síť poskytuje nespojované a nespolehlivé služby. Spojovaný charakter komunikace si vytváří opět až koncový uzel sítě, je-li to nezbytné.
- vrstvový model TCP/IP neobsahuje vrstvy relační a presentační jako model OSI, neboť tyto služby těchto vrstev nejsou využívány všemi aplikacemi, a v takových případech zbytečně zvyšují režii přenosu a tedy užitečný přenosový výkon sítě. Aplikace, které tyto služby vyžadují si je samy musí implementovat.

5.2 Vrstvová struktura modelu TCP/IP

Problematika komunikace je z pohledu této sady rozdělena do 4 vrstev (na rozdíl od systému OSI, který je 7-vrstvý), viz Obr. 5.1:

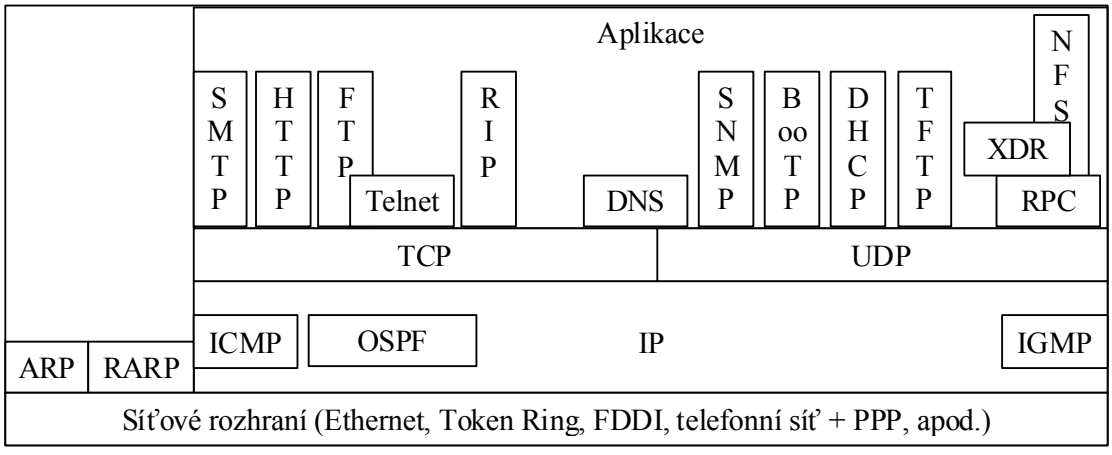
- aplikační,
- transportní,
- síťová,
- vrstva síťového rozhraní.



Obr. 5.1: Vrstvová struktura referenčního modelu TCP/IP a porovnání s modelem ISO/OSI

1. ***Vrstva síťového rozhraní*** – není blíže specifikována touto sadou, neboť je závislá na použité přenosové technologii (ETHERNET, TOKEN RING, ATM, dvoubodový spoj...). zajišťuje vysílání a příjem paketů do/ze sítě.
2. ***Síťová vrstva*** (často také IP vrstva) – zajišťuje směrování paketů po síti, sjednocuje různé typy sítí na úrovni směrování (struktura datové jednotky = IP paket a adresování = IP adresa). Poskytuje nespojovanou a nespolehlivou službu. Funkce vrstvy jsou realizovány protokoly IP, ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol) a RARP (Reverse ARP), OSPF (Open Shortest Path First) a IGMP (Internet Group Management Protocol).
3. ***Transportní vrstva*** (TCP vrstva) – realizuje a zajišťuje komunikaci koncových uzlů. Mulitplexuje (ve směru do sítě) a demultiplexuje (ve směru ze sítě) datový tok od/k jednotlivých /-ým aplikací/-ím. S entitami aplikační vrstvy komunikuje přes přístupové body, tzv. porty. Nabízí 2 služby z hlediska spojení:
   - ♦ spojově orientovanou – protokol TCP (Transmission Control Protocol) – ověří se existence, dostupnost a připravenost komunikujících uzlů, čímž se naváže spojení. Spojení je identifikováno pomocí dvojice **soketů** (soket = IP adresa + číslo portu) odesílatele a příjemce, což umožňuje současné využití jednoho portu jednoho počítače více spojeními. Po skončení komunikace se spojení rozpadá. Navíc je umožněno řízení toku dat pomocí řízení vysílajícího uzlu uzlem přijímacím.
   - ♦ nespojově orientovanou – protokol UDP (User Datagram Protocol) – pakety se vysílají příjemci bez ověření existence, dostupnosti a připravenosti cíle. Neexistuje potvrzování přijetí ani řízení toku dat.

   Nabízí následující služby z hlediska zajištění spolehlivosti:
   - ♦ spolehlivou – kontroluje úplnost přijatých dat, potvrzuje přijatá data odesílateli, který v případě nepotvrzení dat do určitého časového limitu zajistí znovuvyslání dat. Tato služba je zajišťována protokoly:
     - ♦ TCP (Transmission Control Protocol),
     - ♦ SCTP (Stream Control Transmission Protocol),
   - ♦ nespolehlivou – UDP – nezajišťuje bezchybnost přenosu dat.
4. ***Aplikační*** – obsahuje protokoly nejčastěji používaných služeb, např. SMTP (Simple Mail Transfer Protocol), FTP (File Transfer Protocol), TELNET (vzdálený přístup), DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol), BOOTP (BOOTstrap Protocol), ...

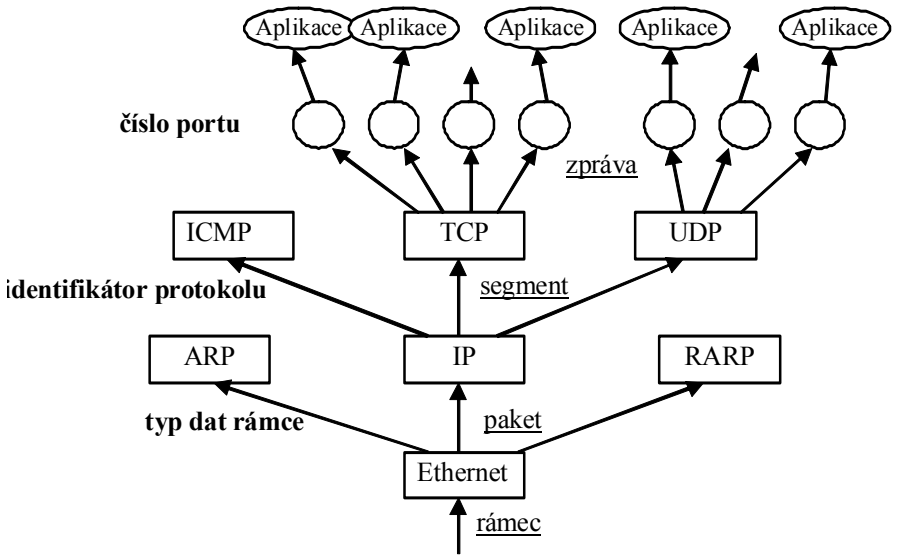


Obr. 5.2: **Nejdůležitější protokoly sady TCP/IP a jejich pozice v modelu TCP/IP**

Při srovnání modelů TCP/IP a ISO/OSI lze vidět, že v modelu TCP/IP chybí vrstva relační a prezentační, neboť služby poskytované těmito vrstvami potřebují pouze některé aplikace (např. NFS – Network File System). Takže aplikace, která tyto služby vyžaduje, si je musí implementovat sama. Výjimkou jsou protokoly

- **RPC** (Remote Procedure Call) – pro relační služby,
- **XDR** (eXternal Data Representation) – pro prezentační služby,

které jsou realizované jako samostatné moduly a mohou být využívány aplikacemi, takže jejich služby může aplikace využít a nemusí je zajišťovat sama.
Obr. 5.3 zachycuje předávání datových jednotek v daných vrstvách při příchodu bloku dat do uzlu.



Obr. 5.3: **Větvení datových jednotek v daných vrstvách pro protokolovou sadu TCP/IP**

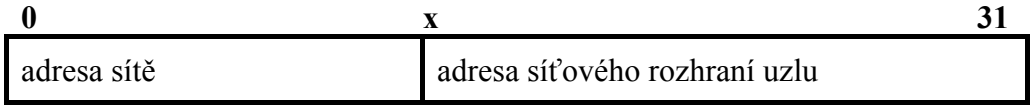
5.3 Adresování v prostředí IP sítí

Sada protokolů TCP/IP používá pro adresování konkrétního procesu v síti 2 čísla, která jsou však umístěna v protokolech různých vrstev:

1. **IP adresa** = adresa síťového rozhraní (nikoli uzlu, ten jich může mít i několik). Používá se na síťové vrstvě a v současně používané verzi protokolu IPv4 je 32-bitová
2. **Port** = přístupový bod na rozhraní transportní vrstva – aplikační vrstva. Je vázán na konkrétní transportní protokol (TCP nebo UDP), tj. stejné hodnoty portů, ale s rozdílným transportním protokolem jsou 2 různé přístupové body a nemají spolu nic společného.

IP adresa se skládá ze 2 částí (viz):

- adresa dílčí sítě,
- adresa síťového rozhraní uzlu,



Obr. 5.4: **Struktura adresy IP**

Jsou to abstraktní adresy používané pro sjednocení různých typů lokálních sítí a v konkrétní síti musí být přepočítány na fyzické adresy. Průběžné směrovače využívají pro směrování pouze adresu sítě, a až směrovač v cílové síti se rozhoduje podle 2. části

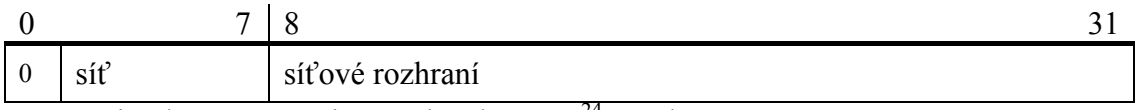
adresy. Adresy protokolu IPv4 se zapisují pomocí 4 dekadických čísel oddělených tečkami, např.

147.229.195.12

- IP adresa musí být v rámci celého Internetu jedinečná. Pro koordinaci přidělování IP adres existuje hierarchická struktura autorit (správců), která zajišťuje jejich jedinečnost.
- žádná část IP adresy (tzn. adresa sítě a adresa rozhraní) nesmí obsahovat samé jedničky či samé nuly
  - celá adresa je nulová – koncový uzel nezná svoji IP adresu,
  - adresa sítě není nulová, adresa síťového rozhraní (SR) je 0 = IP adresa představuje adresu sítě
  - adresa sítě je 0, adresa SR není nulová = koncový uzel nezná svou síťovou adresu,
  - adresa IP je samé jedničky (binárně), tedy 255.255.255.255 = všesměrová adresa pro danou LAN
  - adresa sítě není nulová ani samé jedničky, adresa síťového rozhraní (SR) je samé jedničky = všesměrové vysílání v rámci sítě určené síťovou částí IP adresy,
  - 127.x.x.x = vyhrazené adresy pro softwarovou místní smyčku pro meziprocesovou komunikaci v rámci jednoho počítače,

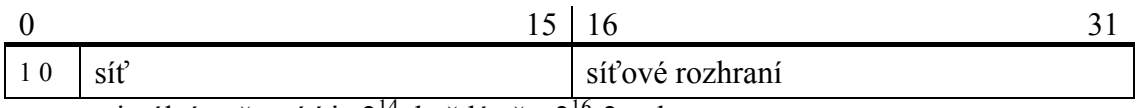
Bitové zastoupení obou částí v adrese není pevné, ale mění se, čímž lze definovat různý počet různě velkých sítí. Podle velikosti síťové a uzlové části adresy se prostor IP adres rozděluje do 5 tříd označených písmeny:

1) **třída A** – v dekadickém vyjádření adresy začíná čísly 1 až 127. Určena pro největší sítě.



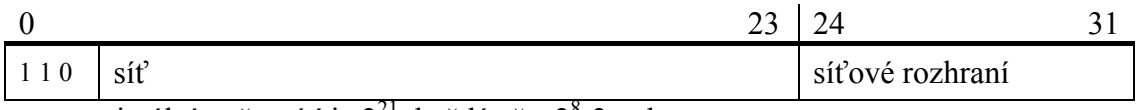
- maximální počet sítí je 126, každá až s 2^{24}-2 uzly

2) **třída B** – v dekadickém vyjádření adresy začíná čísly 128 až 191. Určena pro středně velké sítě.



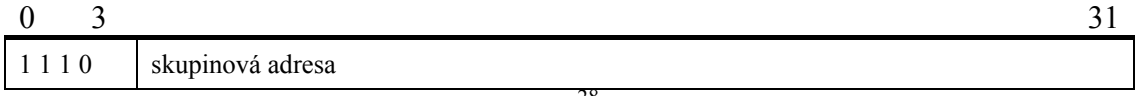
- maximální počet sítí je 2^{14}, každá až s 2^{16}-2 uzly

3) **třída C** – v dekadickém vyjádření adresy začíná čísly 192 až 223. Určena pro malé sítě.



- maximální počet sítí je 2^{21}, každá až s 2^{8}-2 uzly

4) **třída D** – v dekadickém vyjádření adresy začíná čísly 224 až 239. Určena pro adresování skupin počítačů (multicast).



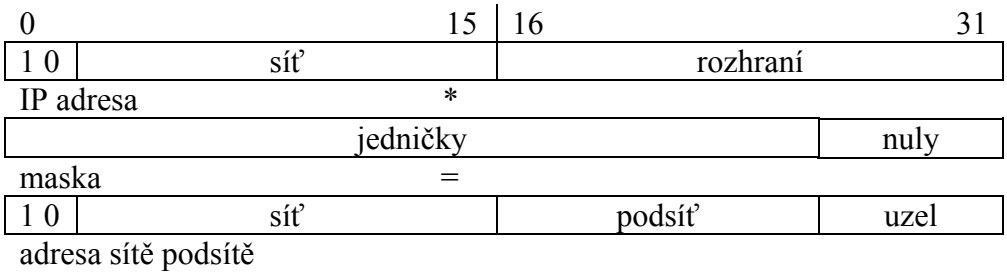
- maximální počet skupinových adres je 2^{28}- 2.

5) **třída E** – v dekadickém vyjádření adresy začíná čísly 240 až 255. Určena pro experimentální účely

Protože i rozdělení IP adresy na 2 části je dosti hrubé, byly zavedeny tzv. podsítě, a adresování bez tříd, kdy adresa síťového rozhraní byla dále rozdělena na 2 části:

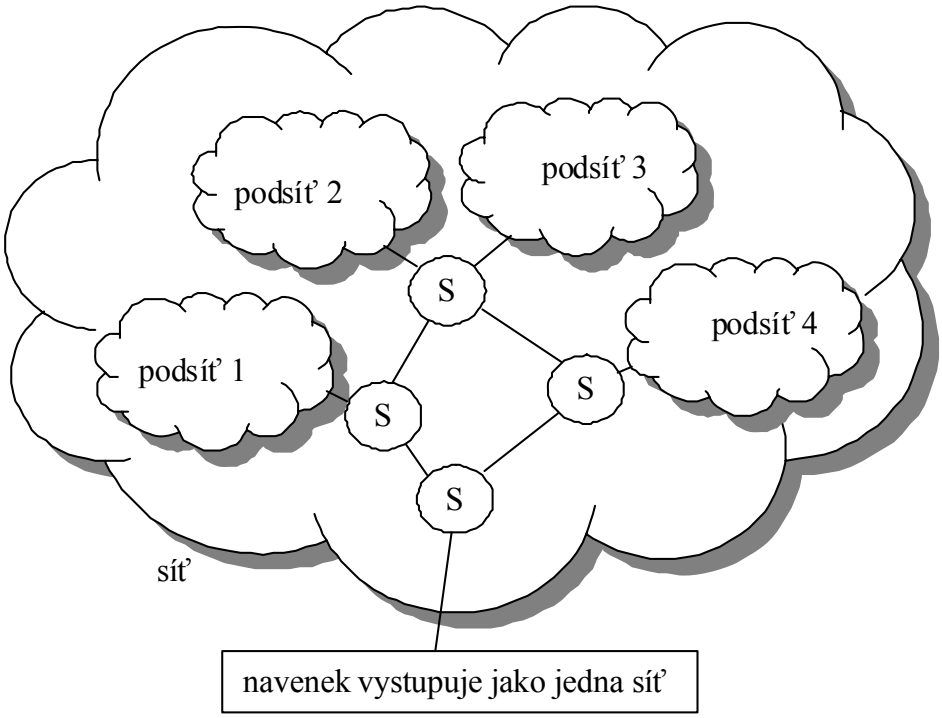
a) adresa podsítě (pro adresu podsítě platí stejná omezení jako pro adresu sítě),
b) adresa uzlu (rozhraní).

Jak velkou část která položka zabírá, definuje tzv. maska podsítě. Ta se skládá se souvislých posloupností jedniček a nul, kdy logickým součinem této masky s danou IP adresou získáme adresu podsítě (viz Obr. 5.5)



Obr. 5.5: **Výpočet adresy podsítě a adresy uzlu z IP adresy a masky podsítě**

Tato maska je součástí směrovacích tabulek a využívá se až směrovači uvnitř cílové sítě.



Obr. 5.6: Princip podsítí

Pro novější směrové protokoly (RIP II a OSPF) může být maska podsítí různě dlouhá i v rámci jedné sítě.

Každý uzel v intersíti musí být jednoznačně identifikovatelný, tzn., že IP adresa musí být v rámci celého Internetu jedinečná. Množství dostupných adres pro koncové uzly závisí na třídě přidělené adresy a na způsobu rozdělení na podsítě. Platí totiž, a to i pro podsítě, že žádná část IP adresy (tzn. adresa sítě a adresa rozhraní) nesmí obsahovat samé jedničky či samé nuly). Máme-li tedy například přidělenu adresu třídy C, která má pro adresu uzlu vyhrazeno 8 bitů (tj. 256 kombinací), můžeme mít v síti maximálně 253 počítačů, či obecně zařízení se síťovým rozhraním (síťové tiskárny, HW tiskové servery, IP telefony, VoIP brány, nepočítaje směrovač), nevytvoříme-li podsítě. Zbývající dvě kombinace jsou nepovolené (samé nuly a jedničky) a třetí bude přidělena směrovači pro odesílání dat ven ze sítě. Chceme-

li vytvořit podsítě, ztrácíme část adresního prostoru, a to tím větší, čím menší počet podsítí vytvoříme (viz Tab. 5.1).

Tab. 5.1: Využití adresových prostorů při vytváření podsítí

Třída IP adresy	Délka masky podsítě	Maximální počet podsítí	Počet adres pro koncové uzly	Ztráta adresového prostoru
C	24	1	253	0
	25 (nelze)	0	0	253
	26	2	2*61	131
	27	6	6*29	79
	28	14	14*13	71
B	16	1	65 533	0
	20	14	14*4093	8231
	24	254	254*253	1271

Opačný případ je seskupování dílčích sítí do větších celků, tzv. „supersítí“. Technika se používá pro zjednodušení směrovacích tabulek. Využívá se opět masek, avšak tentokrát s posloupností jedniček kratší než je délka pole vyhrazeného pro adresu sítě dané třídy. Pro vnější směrovač se pak tato skupina sítí jeví jako jedna supersíť a má pro tuto skupinu sítí buď jediný záznam (v případě protokolu RIP) nebo maximálně několik málo záznamů o případných více stejně oceněných cestách k supersíti (v případě používání protokolu OSPF).

Určitá část adresového prostoru je určena pro použití ve vnitřních sítích (intranetech), viz Tab. 5.2.

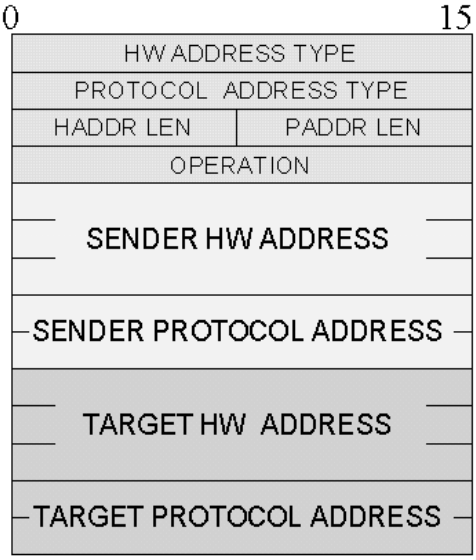
Tab. 5.2: Adresový prostor vyhrazený pro sítě intranet

Třída adres	počáteční adresa	koncová adresa
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

5.4 Protokol ARP (Address Resolution Protocol)

Na síťové úrovni se jako identifikátor cíle a zdroje používá IP adresa. Celý spoj se však skládá z linkových úseků, na kterých se používá adresace linkové vrstvy. U paketových WAN sítí (Frame Relay, ATM) to jsou identifikátory virtuálních cest. U LAN sítí se používají adresy označované jako fyzické, HW či MAC adresy zdroje a cíle, které však označují zdroj a cíl v rámci jedné lokální sítě, tedy například dvou směrovačů, přes které paket přechází. Každý paket se tedy musí vložit do rámce, který nese fyzickou adresu příjemce (pokud se nejedná o dvoubodový spoj) a odesílatele. Ve směrové tabulce má však uzel uvedenou IP adresu následujícího směrovače. Musí tedy docházet ke konverzi IP adresy na adresu fyzickou. K převodu hardwarově nezávislé IP adresy na adresu fyzickou (hardwarovou, MAC adresu), která je však závislá na typu sítě, slouží protokol ARP (Address Resolution Protocol).

Počítač, který chce zjistit fyzickou adresu na základě znalosti IP adresy, vyšle do lokální sítě všesměrový rámec (jako cílovou fyzickou adresu uvede samé jedničky) s typem rámce ARP (0806_H) a do datového pole umístí tělo ARP dotazu (viz. Obr. 5.7). Položka Target HW ADDRESS se vyplní nulami. Tento rámec je přijat všemi stanicemi v lokální síti, ale pouze ta s odpovídající IP adresou na dotaz odpoví uvedením své fyzické adresy. Tento převod se dočasně uloží do převodní tabulky, aby dotaz nemusel být vykonáván pokaždé.



HW ADDRESS TYPE – typ fyzické sítě (Ethernet = 1),
PROTOCOL ADDRESS TYPE – typ adresy nadřazeného síťového protokolu (IP = 0800H),
HADDR LEN – délka fyzické adresy v oktetech (Ethernet = 6)
PADDR LEN – délka adresy síťového protokolu (IP = 4)
OPERATION – dotaz /odpověď, ARP/RARP
ARP dotaz (1),
ARP odpověď (2),
RARP dotaz (3),
RARP odpověď (4),
SENDER HW ADDRESS – fyzická adresa odesílatele
SENDER PROTOCOL ADDRESS – síťová (IP) adresa odesílatele,
TARGET HW ADDRESS – fyzická adresa cíle,
TARGET PROTOCOL ADDRESS – síťová (IP) adresa cíle

Obr. 5.7: **Struktura a popis ARP zprávy (platí i pro RARP)**

Zvláštním typem je **PROXY ARP**, která bývá implementována na směrovači. Směrovač má u sebe uloženou tabulku záznamů IP adresa – HW adresa pro počítače připojené na jedno jeho rozhraní (např. pomalé rozhraní). Na ARP dotazy z jiného rozhraní (rychlého) odpovídá sám směrovač a posílá dotazujícímu svoji fyzickou adresu, takže vystupuje jménem ostatních počítačů a přijímá rámce a obstarává jejich rozesílání. Tímto způsobem virtuálně včleňuje uvedené počítače do jiné sítě. Pro tyto počítače se směrovač chová jako prostředník pro komunikaci s vnějším světem.

5.5 Protokol RARP (Reverse ARP)

Protokol RARP (Reverse Address Resolution Protocol) slouží k opačnému převodu, tedy k získání IP adresy na základě znalosti HW adresy, neboť každý uzel, aby mohl komunikovat v síti TCP/IP, musí znát určité informace o sobě a síti, kde se nachází:

- svou IP adresu,
- masku podsítě, ve které se nachází,
- IP adresu implicitního směrovače,
- IP adresu DNS (Domain Name System) serveru,
- aj.

Pokud chce Host znát pouze svou IP adresu, je možno použít protokol RARP (Reverse ARP). Zašle se všesměrový dotaz, jehož cílem je RARP server poskytující požadované odpovědi nesoucí přidělenou IP adresu. Datová struktura dotazu je shodná se strukturou protokolu ARP. IP adresa je však pro komunikaci v prostředí TCP/IP nedostačující, a proto se protokol RARP k tomuto účelu nepoužívá. Existují komplexnější protokoly BootP a DHCP. Pro dynamické přidělování IP adres byl navržen protokol DRARP (Dynamic RARP).

5.6 Protokoly BootP a DHCP

5.6.1 Protokol BootP

Pouhá znalost IP adresy pro komunikaci po síti TCP/IP nestačí (viz. výše), a proto je zapotřebí komplexnějšího protokolu, kterým jsou protokoly BOOTP (Bootstrap Protocol) nebo DHCP (Dynamic Host Configuration Protocol). Dříve byl protokol BOOTP používán bezdiskovými stanicemi pro získání informace, kde získat soubor pro zavedení operačního systému. Dotaz vysílá stanice, která zná pouze svou fyzickou adresu, a to všesměrově (cílová IP adresa je 255.255.255.255). Bootp server by se tedy měl nacházet v lokální síti. Pokud ne, musí směrovač lokální sítě pracovat jako „Bootp forwarder“, který vyšle dotaz opět všesměrově do sousední sítě. Bootp server jako odpověď pošle informace (opět všesměrově), které jsou uloženy pro daný počítač (danou fyzickou adresu) v tzv. bootp tabulkách.

- je řešením na vyšší (aplikační) úrovni,
- vychází z modelu klient/server,
- k přenosu svých dat využívá UDP datagramy (a IP pakety)
  porty: server 67/udp,
  klient 68/udp,
- umožňuje poskytnout uzlu i další informace (až celý “boot image” = zaváděcí soubor),
- uzel je klientem, svůj dotaz posílá serveru, využívá možnosti všesměrového vysílání na úrovni protokolu IP (tj. vysílání na adresu 255.255.255.255) – nezná adresu serveru,
- server posílá odpověď také broadcastingem (bez své IP adresy by klient nepoznal, že odpověď patří jemu)

0	8	16	24
Opcode	Hardware type	Hardware address length	Hop count
Transaction ID			
Number of seconds		Flags	
Client IP address			
Your IP address			
Server IP address			
Gateway IP address			
Client hardware address :::			
Server host name :::			
Boot filename :::			
Vendor specific info :::			

Obr. 5.8: **Struktura BootP zprávy**

Opcode (8 bitů) - typ zprávy,

Hodnota	Popis
1	BOOTREQUEST - Boot žádost.
2	BOOTREPLY - Boot odpověď.

Hardware type (8 bitů) - typ fyzické sítě,

Hodnota	Popis
1	Ethernet.
6	IEEE 802.
7	ARCNET.
8	Hyperchannel.
11	LocalTalk.
12	LocalNet (IBM PCNet nebo SYTEK LocalNET).
14	SMDS.
15	Frame Relay.
16	ATM, Asynchronous Transmission Mode.
17	HDLC.
18	Fibre Channel.
19	ATM, Asynchronous Transmission Mode.
20	Serial Line.

Hardware address length, (8 bitů) – délka fyzické adresy,
Hop count (8 bitů) – počet mezilehlých směrovačů předávající Bootp zprávu,
Transaction ID (32 bitů) – identifikace dané komunikace,
Number of seconds (16 bitů) – čas v sekundách od vyslání dotazu klientem,
Flags (16 bitů) – příznaky definované doporučení RFC 1542,
Client IP address (32 bitů) – IP adresa klienta (nezná-li ji klient, je položka nulová),
Your IP address (32 bitů) – IP adresa klienta sdělená serverem v dopovědi,
Server IP address (32 bitů) – IP adresa serveru vrácená v odpovědi,
Gateway IP address (32 bitů) – IP adresa směrovače, přes který se bude zavádět ze serveru systém,
Client hardware address (16 bajtů) – fyzická adresa klienta,
Server host name (64 bajtů) – jméno serveru zakončené nulou, ze kterého se bude zavádět systém,
Boot filename (128 bajtů) – cesta k zaváděcímu souboru,
Vendor specific info (64 bajtů) – volitelné informace zaslané serverem klientovi. Jednotlivé položky mají strukturu

Type	Length	Value

Type – typ položky,
Length – délka informační části,
Value – informační část.
Položkami mohou být:

- maska podsítě,
- adresy DNS serverů,
- adresy směrovačů,
- apod.

5.6.2 Protokol DHCP

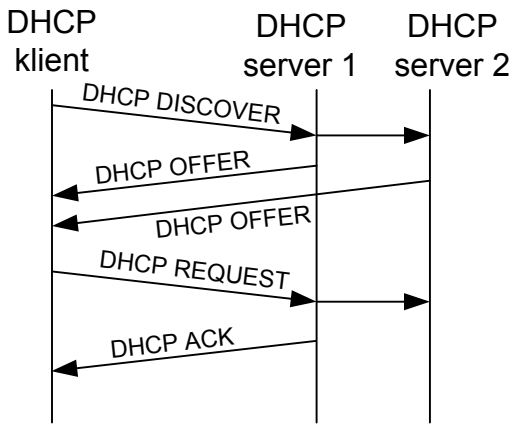
Protokol DHCP (Dynamic Host Configuration Protocol) slouží k dynamickému přidělování IP adres. V dnešní době protokol DHCP nahradil protokol Bootp. DHCP umožňuje celkem tyto typy přidělování:

1. statické – zasílání adres definovaných staticky správcem sítě = obdoba Bootp.
2. automatické – přidělování stálých adres,
3. dynamické – dočasné přidělování adres,

K přenosu svých dat využívá stejně jako protokol BootP UDP datagramy (a IP pakety)

porty: server 67/udp,
klient 68/udp.

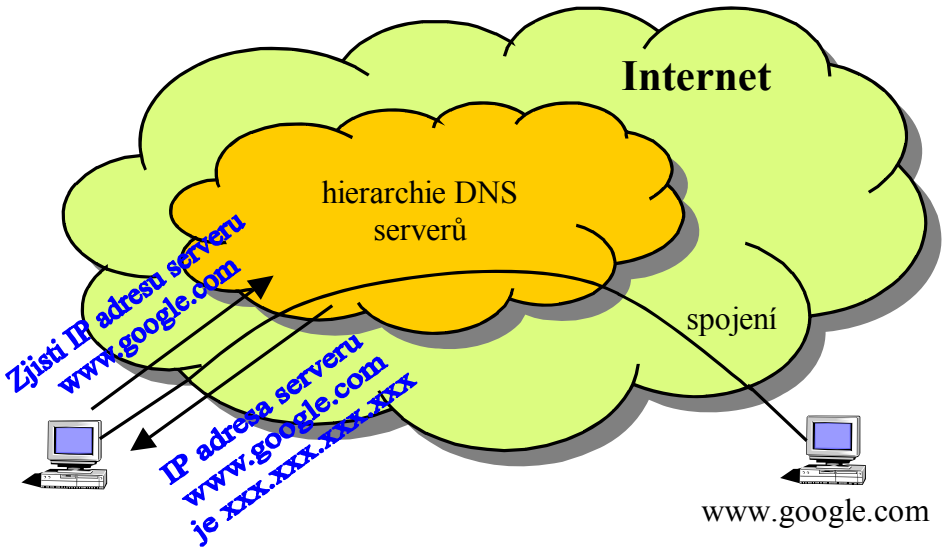
Datová struktura zprávy souhlasí se strukturou protokolu Bootp, je však doplněna o další parametry. Dynamický způsob přidělování umožňuje časově omezovat přidělení IP adresy. Před vypršením platnosti přidělení adresy musí stanice opět požádat o obnovení platnosti adresy, je-li to třeba. DHCP žádosti posílá stanice všesměrově. To by bez dalšího doplňku znamenalo, že se DHCP server musí nacházet v každé síti, protože všesměrové zprávy standardně končí na rozhraní směrovače. Aby nemusel být DHCP server pro každou síť, musí být směrovač schopen rozpoznat a přeposlat DHCP zprávy DISCOVER. Přeposlaná zpráva je však modifikována v poli Gateway IP address, kde směrovač vloží IP adresu rozhraní na kterém přijal zprávu DHCP DISCOVER. DHCP server se tak dozví, odkud přišla zpráva, a tedy z jakého intervalu IP adres (a pro jakou síť) má IP vybrat. Dotaz se může dostat k více DHCP serverům, které mohou klientovi poslat nabídku DHCP OFFER. Klient si vybere nejvhodnější z nich a odešle všesměrově zprávu DHCP REQUEST, kde uvede, co si vybral, takže se ostatní servery dozvědí, že jejich nabídka nebyla přijata, a že mohou navrátit na chvíli zablokovanou IP adresu zpět do seznamu volných adres. Server, jehož nabídky byla vyslyšena, potvrdí klientovi rezervaci zprávou DHCP ACK.



Obr. 5.9: **Průběh získání komunikačních parametrů prostřednictvím protokolu DHCP**

5.7 Jmenný systém (DNS)

V síti TCP/IP se adresuje podle IP adresy, což je nějaké číslo. Zapamatovat si několik IP adres je problematické. Pro lidi je přirozenější pracovat se jmény, tedy s řetězcovým označením cíle komunikace. Vzniká tu tedy problém mapování jméno-IP adresa. Řešením je decentralizovaný systém jmen s hierarchickou strukturou = DNS (Domain Name Service), který zajišťuje převod jmen na IP adresy a naopak. Je to systém založený na modelu klient-server.



Obr. 5.10: Podstata systému DNS

5.7.1 Struktura systému DNS

I pro jména platí zásada jedinečnosti jména v rámci celého Internetu. Proto byl zaveden hierarchický systém jmenných domén. Jméno určitého uzlu má pak strukturu:

jméno.doména$_k$.doména$_{k-1}$. .... .doména$_2$. doména$_1$

Jméno můžeme chápat jako rodné jméno člověka a sadu domén jako příjmení. Index u domén značí úroveň v hierarchii domén, tzn. index „1“ označuje nejvyšší doménu v hierarchii. Příkladem může být jméno webovského serveru www.seznam.cz.

Domény nejvyšší úrovně (Top Level Domains) mohou být dvojího typu:

1. generické domény – nadnárodní domény původně zavedené pouze v USA, nyní se téměř všechny (kromě 2: gov, mil) používají v celém Internetu. Jsou to:
   - com – komerční organizace,
   - edu – vzdělávací instituce,
   - gov – vládní instituce,
   - mil – armádní skupiny USA,
   - org – ostatní organizace,
   - net – síťové organizace,
   - int – mezinárodní organizace,
2. národní domény – dvoupísmenné zkratky jednotlivých států, např. cz, uk, sk, ru, at, de, pl, apod.

Vztah mezi IP adresou a jménem je velmi volný, takže doména není svázána s určitou sítí. Dále platí, že jedno jméno může být použito pro více IP adres (např. pro směrovač). Opačně pro jednu IP adresu může existovat více jmen, rozlišující nejčastěji typy služeb, které jsou uzlem poskytovány, např. www, ftp, apod. Jedno z těchto jmen však musí být to pravé (kanonické) a ostatní jsou přezdívky, které jsou uvedeny v datovém souboru pro danou doménu s typem CNAME (Canonical Name), např.

```
www        IN  CNAME    meloun.spol.cz
```

Mapování jméno-IP_adresa a jiné informace s tím související jsou uloženy v tzv. jmenných serverech, kdy pro každou doménu musí existovat takový server. Existují 3 typy serverů lišících se svou důležitostí a funkcí:

1. ***Primární*** - určuje obsah domény, je pouze 1 pro doménu a poskytuje autoritativní odpovědi. Je udržován v aktuálním stavu ručně.
2. ***Sekundární*** – je zálohou primárního serveru, poskytuje autoritativní odpovědi, automaticky je v určitých intervalech obnovován jeho obsah podle stavu primárního serveru (pracuje jako zrcadlo). Pro každou doménu musí existovat alespoň 1. Měl by být umístěn jinde než server primární, aby v případě poruchy kabeláže nebyly oba odpojeny.
3. ***Pomocný*** – pracuje jako vyrovnávací paměť pamatující si zodpovězené převody. Neposkytuje však autoritativní odpovědi. Každý z předcházejících serverů může současně pracovat jako pomocný.

Jeden uzel může zastávat funkci více primárních, sekundárních i pomocných serverů pro více domén a může být také primárním serverem pro reverzní doménu.

Kromě těchto serverů, které jsou definovány pro každou doménu, existují tzv. kořenové servery, kterých je v současnosti o něco více než 10 a které mají přehled o všech serverech domén nejvyšší úrovně. Tyto kořenové servery musí znát každý jmenný server ve všech doménách. Jejich jména jsou:

a.root-servers.net

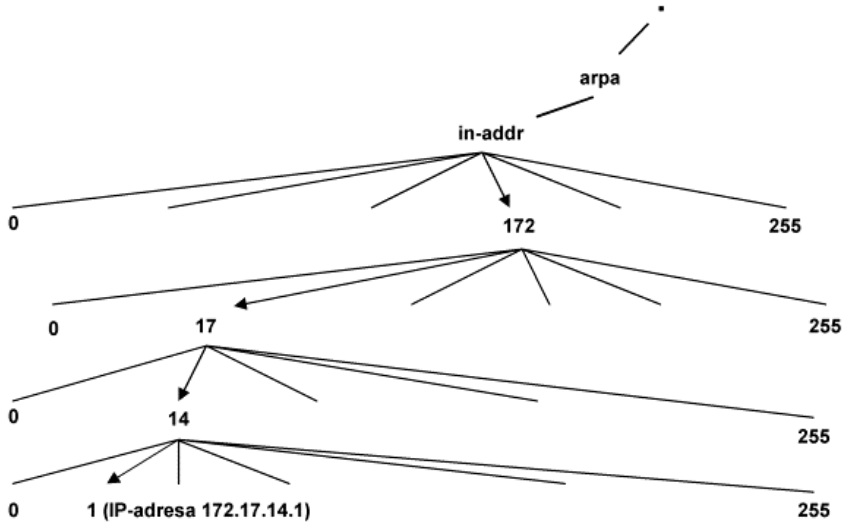
.

m. root-servers.net

Aktuální seznam kořenových serverů lze nalézt na adrese
ftp://rs.internic.net/netinfo/root-servers.txt

Vazby mezi servery jsou takové, že každý DNS server musí znát kořenové servery a všechny DNS servery nižší úrovně. Má-li stanice dotaz na převod, pošle dotaz místnímu jmennému serveru, jehož IP adresu má definovanou v nastavení sítě, nebo zjištěnou pomocí BOOTP či DHCP protokolu. Převod může probíhat 2 způsoby, které se často kombinují:

1. **nerekurzivní** (iterativní) – dotazy klade stále tazatelský uzel, tázaný uzel pouze vrací odkaz na další server, který by měl vědět víc.
2. **rekurzivní** – zjišťování převodu se postupně ujímají dotazované jmenné servery, a je-li zjištěna odpověď, je poslána přes všechny zainteresované servery, které si tuto informaci zapíší do vyrovnávací paměti.



Obr. 5.11: Struktura domén pro zpětný převod

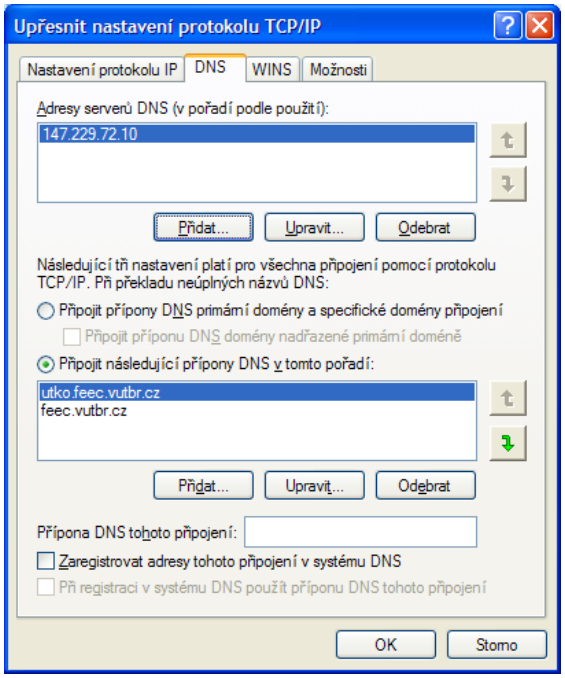
Většinou se používá kombinace obou metod, kdy uzly nejnižších úrovní používají rekurzivní způsob (mají méně požadavků, a proto se mohou samy zabývat zjišťováním IP adresy) a servery vyšších úrovní nerekurzivní způsob (aby nebyly zahlceny prací s převody).

5.7.2 Reverzní DNS

Pro zpětný převod IP adresa – jméno je vyhrazena doména in-addr.arpa, kde jednotlivé bajty IP adresy se objevují jako poddomény avšak v opačném sledu. Např. jméno pro počítač 147.229.195.56 se bude zjišťovat jako údaj pro jméno 56.195.229.147.in-addr.arpa.

5.7.3 Konfigurace systému DNS

Konfigurace systému DNS sestává z konfigurace klientů a serverů. Aby stanice mohla vznést požadavek na převod, musí být nakonfigurována jako DNS klient. Konfigurace spočívá v nastavení domény, kde se stanice nachází (to umožní zadávat dotazy se zkrácenými jmény) a v uvedení IP adresy (nikoli jména) alespoň jednoho serveru DNS (doporučují se 2). Správnou činnost klienta lze ověřit např. jednoduchým programem ping, kde se cíl zadá jménem cílového počítače.



Obr. 5.12: **Příklad konfigurace DNS klienta v systému Windows XP**

5.7.4 Konfigurace serverů DNS

Konfigurace závisí na typu serveru. V systémech unix se pro funkci DNS serveru používá například program **named**.

- ***Pomocný server*** – v konfiguračním souboru (např. pro linux a program named je to /etc/named.boot) se nastavuje umístění datových souborů pro DNS (adresář, např. /etc/dns), a umístění souboru s informacemi o kořenových serverech (jména a jejich IP adresy),
- ***Sekundární server*** – v konfigurační serveru se uvede, pro kterou doménu je server sekundárním a IP adresu primárního serveru dané domény,
- ***Primární server*** – v hlavním konfiguračním souboru se uvede pro které domény je server primární a jméno souboru s daty pro tuto doménu. Samozřejmě se nastaví i do role

pomocného serveru. Soubory obsahující informace o doménách a jménech počítačů jsou uloženy v textových souborech, jejichž obsah se skládá ze záznamů majících tvar

<doména> <platnost_informace> <třída> <typ> <data>,

doména – určuje, ke které doméně či konkrétnímu počítači se daný záznam vztahuje (jméno počítače se také považuje za doménu),
platnost – doba platnosti informace,
třída – třídí záznamy do skupin podle zaměření (např. IN = Internet),
typ – určuje typ informace (např. A = address, NS = name server, MX = poštovní server, PTR = reverzní převod, apod.) viz. následující tabulka,
data – jedna či více informací oddělených mezerami (např. IP adresa, jména DNS serverů pro poddomény, priorita a jméno uzlu, na kterém je spuštěn poštovní server, atd.),

Tab. 5.3: Některé typy záznamů v souboru s popisem domény

Typ	**Anglický název**	**Význam pole RDATA**
A	A host address	32 bitová IP adresa
NS	Authoritative name server	Doménové jméno name serveru, který je autoritou pro danou doménu.
CNAME	Canonical name for an alias	Doménové jméno specifikující alias (přezdívku) ke kanonickému (pravému) jménu NAME
SOA	Start Of Autority.	Právě jedna věta SOA uvozuje každou zónu. Obsahuje 7 polí. přesný popis viz. DNS databáze.
PTR	Domain name pointer	Doménové jméno. Věta se používá pro reverzní překlad.
HINFO	Host information	Obsahuje dva znakové řetězce. První obsahuje popis HW a druhý popis SW, které jsou používané na počítači NAME.
MX	Mail exchange	Obsahuje dvě pole. První 16 bitové pole bez znaménka obsahuje preferenci a druhé obsahuje doménové jméno mailového serveru.

Pro kontrolu systému DNS existuje řada nástrojů, např. v operačním systému Linux to je např. program nslookup.

V současných moderních operačních systémech, jako Novell Netware 5 či Windows 2000 se projevuje snaha zaintegrovat systém DNS do obecného systému adresářových služeb (directory services), který obecně řeší problematiku získávání různých informací v prostředí počítačových sítí. Např. Novell Netware 5 umožňuje integrovat systém DNS do vlastního adresářového systému Novell eDirectory.

5.8 Směrové protokoly

O směrování se v síti TCP/IP starají směrovače, které směřují pakety na základě směrovacích tabulek. Směrování může být řešeno dvojím způsobem:

1. **staticky** – směrovací informace jsou uloženy do tabulky ručně při konfiguraci směrovače. Změny musí být také prováděny ručně. Je to vhodný způsob pouze pro jednoduché a stálé sítě
2. **dynamicky** – směrovací uzly si mezi sebou vyměňují pravidelně směrovací informace, čímž získávají informace o struktuře a stavu sítě. Výměny jsou zajišťovány směrovými

protokoly. V současnosti v sítích TCP/IP jsou to především protokoly RIP (Routing Information Protocol) a OSPF (Open Shortest Path First)

Směrovací informace dynamické tabulky nejčastěji obsahuje tyto základní údaje

cílová síť	maska podsítě	adresa následujícího směrovače	síťové rozhraní	metrika	stáří směrové informace	stav rozhraní	četnost zprac. paketů

Obr. 5.13: Struktura dynamického záznamu ve směrovací tabulce

Cílová síť – adresa cílové sítě.

Maska podsítě – určuje jaká část síťové adresy je adresa podsítě. Slouží při prohledávání směrovací tabulky k určení rozhraní kterým se bude paket posílat. Cílová adresa se vynásobí s maskou a výsledek se porovná s hodnotou cílové sítě. Je-li více kladných výsledků, vybere se ten směr, pro který byla maska podsítě nejdelší (s nejdelším vyhovujícím prefixem).

Adresa následujícího směrovače – pokud cílová síť není připojena přímo k danému rozhraní, posílá se paket dalšímu směrovači ležícímu na cestě k síti.

Síťové rozhraní – určuje kterým rozhraním směrovače se bude paket posílat, může být určeno identifikátorem rozhraní či jeho síťovou adresou.

Stav rozhraní – informace o stavu rozhraní (zapnuto/vypnuto).

Metrika – určuje, jak výhodné je poslat paket danou cestou. Metrika spoje může být určena „vzdáleností“ (počet mezilehlých směrovačů mezi směrovačem a cílovou sítí) či jeho cenou, což je hodnota vypočtená z řady parametrů dané cesty (počet mezilehlých směrovačů, přenosové rychlosti jednotlivých úseků, hodnoty MTU = Maximum Transfer Unit pro jednotlivé úseky, momentální stav úseků, apod).

Stáří informace – u dynamického směrování je zapotřebí informace pravidelně aktualizovat. To znamená, že pokud informace není obnovena do určité doby, je považována za starou, a tedy neplatnou.

U **statické** směrovací informace chybí položky cena spoje a stáří informace, neboť záznamy mají statický charakter a výběr nejvhodnější cesty je volba správce sítě.

5.8.1 Směrový protokol RIP (Routing Information Protocol)

Směrovací protokol RIP existuje ve dvou verzích I a II. Jako měřítko dosažitelnosti sítě se bere počet mezilehlých směrovačů a maximální vzdálenost je 15. Směrovače posílají své směrovací tabulky sousedním směrovačům každých 30 s. Verze II se od první verze liší v tom, že v dané síti mohou existovat podsítě, a to různě velké (s různými maskami podsítě). Pro přenos tabulek se využívá transportní protokol UDP. Základním kriteriem dosažitelnosti sítě je vzdálenost k této síti. Vzdálenost je vyjádřena jako počet mezilehlých směrovačů mezi daným směrovačem a cílovou sítí (hop count). Již se nezohledňuje propustnost linek, tedy jejich rychlost, maximální velikost přepravovaných rámců, apod. K dané cíli z daného směrovače vede pouze jediná cesta. Nelze tedy využít možnosti rozložení zátěže mezi více stejně dlouhých cest. Je-li vzdálenost rovna 16, je síť chápána jako nedosažitelná. Rozšíření informace o změně mezi ostatní směrovače je dosti pomalá. Další nevýhodou je značné zatížení sítě, neboť si směrovače posílají celé tabulky, jejichž velikost závisí na celkovém počtu sítí.

5.8.2 Směrový protokol OSPF (Open Shortest Path First)

Směrovací protokol OSPF je složitější, ale dokonalejší než protokol RIP. Umožňuje lépe využít nabízených kapacit sítě, rychleji reagovat na změny v síti. Každý směrovač si shromažďuje informace o topologii celé oblasti. Směrovače si předávají informace o stavu přímých linek. Stav linek lépe odpovídá skutečné propustnosti sítě. Na základě stavů linek se pomocí Dijkstrova algoritmu vypočítá nejkratší cesta (s nejnižší cenou). V případě změny v síti se tato změna záplavovým mechanismem rozšíří velmi rychle po celé oblasti. Tento protokol také umožňuje rozdělit zatížení na více cest, existuje-li více cest se stejnou cenou. OSPF má menší režii než RIP (informace se posílají každých 30 minut) a je lépe škálovatelný, tj. jeho režie s růstem celé soustavy sítí neroste tak rychle, jak by rostla v případě protokolu RIP.

Metrika protokolu OSPF není omezena hodnotou 16 jako u protokolu RIP. Může nabývat hodnotu až 65535. OSPF autonomní systém je rozdělen do oblastí, z nichž jedna je zvolena jako páteřní (má číslo 0). Ostatní oblasti musí být s ní spojeny buď přímou nebo virtuální linkou. Oblasti jsou spojovány hraničními směrovači (Area Border Router – ABR). OSPF autonomní systém je s ostatními autonomními systémy (a případně používajícími jiný směrový protokol, např. RIP) spojen pomocí směrovačů ASBR (Autonomous System Boundary Router). Každý OSPF směrovač je identifikován 4-bajtovým číslem.

V současnosti existuje OSPF verze 2 specifikovaná v dokumentu RFC 2178, který nahrazuje verzi 1 z dokumentu RFC 1583.

5.9 Protokoly síťové vrstvy

Základním úkolem je přeprava paketů intersítí pomocí na konkrétní síti nezávislého mechanismu. Hlavním protokolem je protokol IP. K němu jsou pak přidruženy další protokoly, jednak, které protokol IP využívají, což jsou ICMP (Internet Control Message Protocol) a IGMP (Internet Group Management Protocol), a pak samostatné protokoly přistupující přímo k vrstvě síťového rozhraní, a to ARP (Address Resolution Protocol) a RARP (Reverse ARP), jenž zajišťují adaptaci mezi vrstvou síťového rozhraní (konkrétní sítí) a síťovou (IP) vrstvou. Protokoly zajišťují:

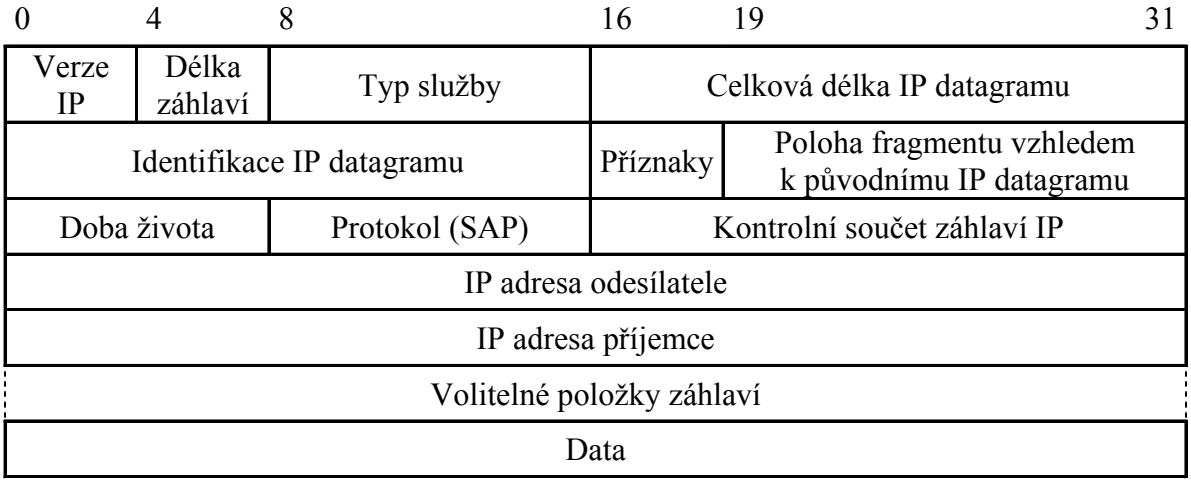
- způsob na síti nezávislého adresování (IP adresy), převod IP adres na adresy používané v konkrétní síti (ARP) na úrovni síťového rozhraní, případně naopak pro zjištění IP adresy (RARP),
- formát datových jednotek pro jednotlivé protokoly (IP paket, jednotky ARP,RARP, ICMP a IGMP),
- směrování (podle směrových tabulek – statické, dynamické),
- pravidla přenosu paketů (fragmentace, doba života),
- testování přenosové cesty a řešení nestandardních situací (ICMP)

5.9.1 IP (Internet Protocol) protokol

IP (Internet Protocol) je hlavní protokol síťové vrstvy zajišťující přenos datových jednotek (paketů) intersítí. V této kapitole je uveden popis verze 4 (IPv4). Tato verze protokolu IP se vyznačuje těmito rysy:

- poskytuje datagramovou službu (nespojovanou a nespolehlivou),
- paket protokolu IP je označován jako datagram (IP datagram),
- definuje formát IP paketů,
- zajišťuje směrování IP paketů,
- implementuje jednotné adresování (IP adresami),

- ošetřuje nestandardní situace (fragmentaci, zacyklení, ...),
- nezajišťuje vlastní fyzický přenos pouze předává paket k přenosu vrstvě síťového rozhraní.



Obr. 5.14: Struktura IP paketu

- **Verze (IP Version)** = verze IP-protokolu. V současnosti IP-protokol verze 4, (hodnota = 4).
- **Délka záhlaví (Header Length)** = délka záhlaví IP-datagramu v násobcích 4 bajtů. Délka záhlaví musí tak být i v případě použití volitelných položek násobkem čtyř. V případě, že by záhlaví nevyšlo na násobek čtyř, pak se na násobek čtyř doplní nevýznamnou výplní. Maximální délka záhlaví IP-datagramu je 60 B (=15x4). Povinné položky mají 20 B.
- **Typ služby (Type of Service – TOS)** – možnost označení datagramu pro přednostní zpracování. V praxi nenašla svého naplnění. Cílem bylo označit některé IP-datagramy tak, aby byly dopravovány přednostně či aby byla zaručena rychlá odezvat atp.
- **Celková délka IP-datagramu (Total Length)** – obsahuje celkovou délku IP-datagramu v bajtech. Maximální délka IP-datagramu je 65535 bajtů.
- **Identifikace IP-datagramu (Identification)** – obsahuje identifikaci IP-datagramu, kterou do IP-datagramu vkládá operační systém odesílatele. Identifikuje původní paket jako celek. Při následné fragmentaci mají všechny fragmenty stejnou identifikaci, což se využije při opětovném sestavování u příjemce.
- **Příznaky (Flags)** – týkají se fragmentace IP paketů

Příznaky		
0	DF	MF

Obr. 5.15: Příznaky v IP hlavičce (DF – Don't Fragment, MF – More Fragments)

Je-li DF = 1, je fragmentace zakázána. Je-li MF = 1, daný paket není posledním fragmentem původního paketu.

- **Offset fragmentu (Fragment Offset)** – určuje pozici počátku fragmentu vůči počátku v původnímu paketu v násobcích 8 B.
- **Doba života datagramu (Time To Live – TTL)** slouží k zamezení bloudění IP-datagramu Internetem. Každý směrovač kladnou položku TTL snižuje alespoň o jedničku. Je-li TTL = 0, IP-datagram se zahazuje a odesílateli IP-datagramu je tato situace signalizována protokolem ICMP.
- **Protokol vyšší vrstvy (Protocol)** – obsahuje identifikaci protokolu, který využívá IP-datagram ke svému transportu. Jsou to protokoly transportní vrstvy, TCP (6) nebo UDP

(17) nebo jeden ze služebních protokolů síťové vrstvy ICMP (1) či IGMP (2). Jako protokol vyšší vrstvy může být i protokol, který je tunelován přes Internet (encapsulation). Tunelovány mohou být např. protokoly, které Internet nepodporuje jako je např. protokol IPX (111), nebo může být tunelován sám protokol IP (IP over IP) (4) pro vytvoření virtuální privátní sítě.

- **Kontrolní součet z IP-záhlaví (header checksum)** – obsahuje kontrolní součet ze záhlaví IP-datagramu.
- **IP-adresa odesilatele a IP-adresa příjemce (source and destination address)** – obsahuje čtyřbajtovou IP-adresu odesílatele a příjemce IP-datagramu.
- **Volitelné položky (Options)** – jsou ojediněle využívány.
  – položky IP OPTIONS jsou určené především pro potřeby testování a ladění
  – zpracování IP OPTIONS je pro všechny implementace povinné

Patří sem položky:

- ***Záznam cesty (Record Route)*** – sledování, kudy datagram při cestě k příjemci procházel,
- ***Pevně předepsaná cesta (Strict route)*** – paket má pevně určenou cestu, kudy má jít,
- ***Volně předepsaná cesta (Loose Source Route)*** – paket má určeny pouze některé uzly, kudy má jít,
- ***Sledování doby přenosu (Timestamp)*** – záznam dob průchodu jednotlivými směrovači,

- **Výplň (Padding)** – zarovnání délky záhlaví na celistvý násobek 4 B.

Fragmentace paketů: Různě rychlé okruhy v síti mohou mít definované různé maximální délky datových jednotek (paketů) – MTU (Maximum Transfer Unit). To znamená, že když má být poslán na okruh delší paket než je povoleno parametrem MTU, existují 2 řešení:

1. zahodit paket a vyslat ICMP zprávu o nedoručitelnosti
2. rozdělit původní paket na menší jednotky, pokud je to povoleno (viz. příznak DF) = fragmentace paketu

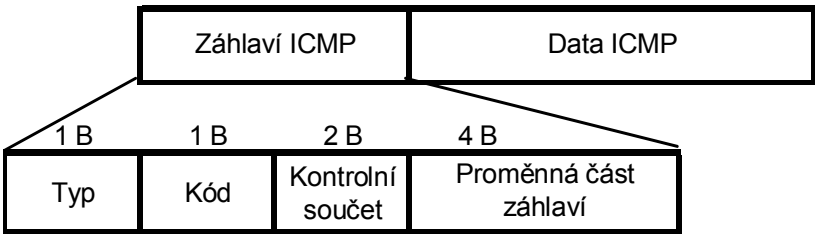
Je-li paket rozdělen na menší části, každá z nich se stává samostatným paketem, který cestuje zbytkem sítě nezávisle na ostatních částí. To že je to fragment původního paketu, je definováno identifikací paketu, dále jednobitovým příznakem fragmentace MF a ofsetem fragmentu, který udává posun počátku datové části fragmentu vůči počátku datové části původního paketu. Fragmentace může být i vícenásobná, tedy i fragmenty mohou být dále fragmentovány. Fragmenty jsou skládány do původního paketu až koncovou stanicí. Značí to tedy, že při ztrátě byť jediného fragmentu se musí opakovat vyslání celého původního paketu.

5.9.2 ICMP (Internet Control Message Protocol)

ICMP doplňuje činnost protokolu IP o přenos řídicích zpráv mezi směrovači navzájem nebo mezi směrovači a koncovými uzly (počítači). Tento protokol se používá pro:

1. **testování dosažitelnosti cílového uzlu** prostřednictvím protokolu IP (např. program PING),
2. **chybové zprávy** – nedosažitelnost adresáta, vypršení doby života, chybný parametr v záhlaví paketu, apod.,
3. **synchronizace času a odhad doby přenosu**,
4. **řízení přenosu** – upozornění na zahlcení mezilehlého nebo koncového uzlu,
5. **přesměrování trasy** – upozornění hosta směrovačem, že existuje vhodnější brána k danému cíli,

6. **získání přídavných informací** – např. síťové části IP adresy, nebo masku podsítě (zastaralé).



Obr. 5.16: Struktura ICMP zprávy

- Typ – určuje základní druh zprávy,
- Kód – detailněji specifikuje význam zprávy,
- Kontrolní součet - zabezpečení ICMP zprávy,
- Proměnná část záhlaví – využití závisí na typu zprávy, není-li využita je naplněna nulami,
- Data – v případě echo zprávy nese libovolná data, v případě chybových zpráv nese IP záhlaví a prvních 64 bitů datové části paketu, který chybu způsobil.

5.9.3 IGMP (Internet Group Management Protocol)

Protokol IGMP je podobně jako protokol ICMP služebním protokolem (podmnožinou) protokolu IP. Pakety IGMP-protokolu jsou baleny do IP-datagramů. Protokol IGMP slouží k šíření adresných oběžníků (multicasts) v rámci LAN, kdy cílová IP adresa vyjadřuje skupinovou adresu (třída D). Počítač, který chce odebírat oběžníky, se musí nejprve do skupiny přihlásit . Místní směrovače si udržují seznam skupin, a pokud skupina není prázdná zajistí rozeslání oběžníků všem jejím členům v rámci dané LAN. Protokol IGMP verze 2 je definován normou RFC-2236.

1B	1B	2B	4B
Typ	MRT	Kontrolní součet	IP adresa oběžníku

Obr. 5.17: Struktura datové jednotky IGMP verze 2

Typ – určuje typ IGMP zprávy nabývá hodnot:
Dotaz na existenci členů skupiny v dané LAN (Membership Query)
Žádost o členství ve skupině (Membership Report)
Opuštění skupiny (Leave Group)

MRT (Maximum Response Time) – doba v desetinách sekundy, během které musí všechny počítače odpovědět přihláškou do skupiny, pokud v ní chtějí nadále zůstat

Kontrolní součet - zabezpečení

IP adresa – samé nuly nebo konkrétní skupinová adresa. V případě samých nul je např. dotaz míněn na členství ve všech skupinách

Všechny IGMP pakety mají v IP-záhlaví nastavenu položku TTL=1.

IP-adresy adresných oběžníků jsou v intervalu 224.0.0.0 až 239.255.255.255. Interval 224.0.0.0 až 224.0.0.255 je určen pro vyhrazené účely na LAN. Jelikož jsou oběžníky s těmito adresami určeny pro šíření pouze v rámci dané LAN, mívají v položce TTL záhlaví IP paketu nastavenu hodnotu 1.

5.9.4 Protokol IPv6

Původní a dodnes používaný protokol IPv4 již v současnosti nevyhovuje novým potřebám stále rychleji se rozrůstající sítě Internet. Největším problémem je dosti omezený adresový prostor (32 bitů), který již začíná být pomalu zaplněný (zvlášť v oblasti adres pro větší sítě – třídy A a B). Dalším nedostatkem starší verze je neexistence bezpečnostních mechanizmů a chybějící podpora služeb citlivých na zpoždění a na změnu zpoždění. Proto se na začátku devadesátých let minulého století začalo pracovat na nové verzi označované jako IPv6 nebo také IPng (IP next generation).
Protokol IPv6 odstraňuje výše uvedené nedostatky původního protokolu IP verze 4, přičemž hlavní důraz je zaměřen na řešení problémů adresování uzlů, dynamické konfigurace, podpory multimediálních aplikací a bezpečnostní procedury při používání protokolu IP v síti Internet. Protokol IPv6 také zavádí obecný mechanismus rozšiřování nového protokolu, který umožní jej jednoduše obohatit i v budoucnu o takové vlastnosti a schopnosti, jaké budou zapotřebí. V současnosti nezanedbatelným přínosem nového protokolu je podpora mobility.
Protokol IPv6 byl také navrhován s tím, aby mohl být do intersítě včleňován postupně (překryvný způsob), tzn. aby umožňoval přenos i paketů přicházejících z částí sítě používající IPv4 nebo naopak paketů do nich směrovaných. Řeší se to buď tunelováním a nebo pomocí technologie MPLS (Multiprotocol Label Switching).
Hlavní změny protokolu IPv6 oproti IPv4 jsou následující:

1. ***Nový adresový prostor*** - IPv6 proto rozšiřuje adresní prostor z původních 32 bitů na 128 bitů. Adresy se zapisují v hexadecimálním tvaru po slovech (skupinách čtyřech hexadecimálních číslic) oddělených dvojtečkou (8 šestnáctibitových polí). Pro zápis adresy platí pravidla

(vzorový příklad FEDC:0000:0000:0000:3243:0000:0035:ABCD):

- lze vynechat počáteční nuly v každém slově,
- lze přeskočit jednu sekvenci nulových slov, např. FEDC::3243:0000:0000:ABCD,
- lze nechat posledních 32 bitů adresy zapsaných ve formátu adresy IPv4, např.::147.229.196.88,
- lze definovat délku prefixu adresy, např. 2345:BA23:7::/40

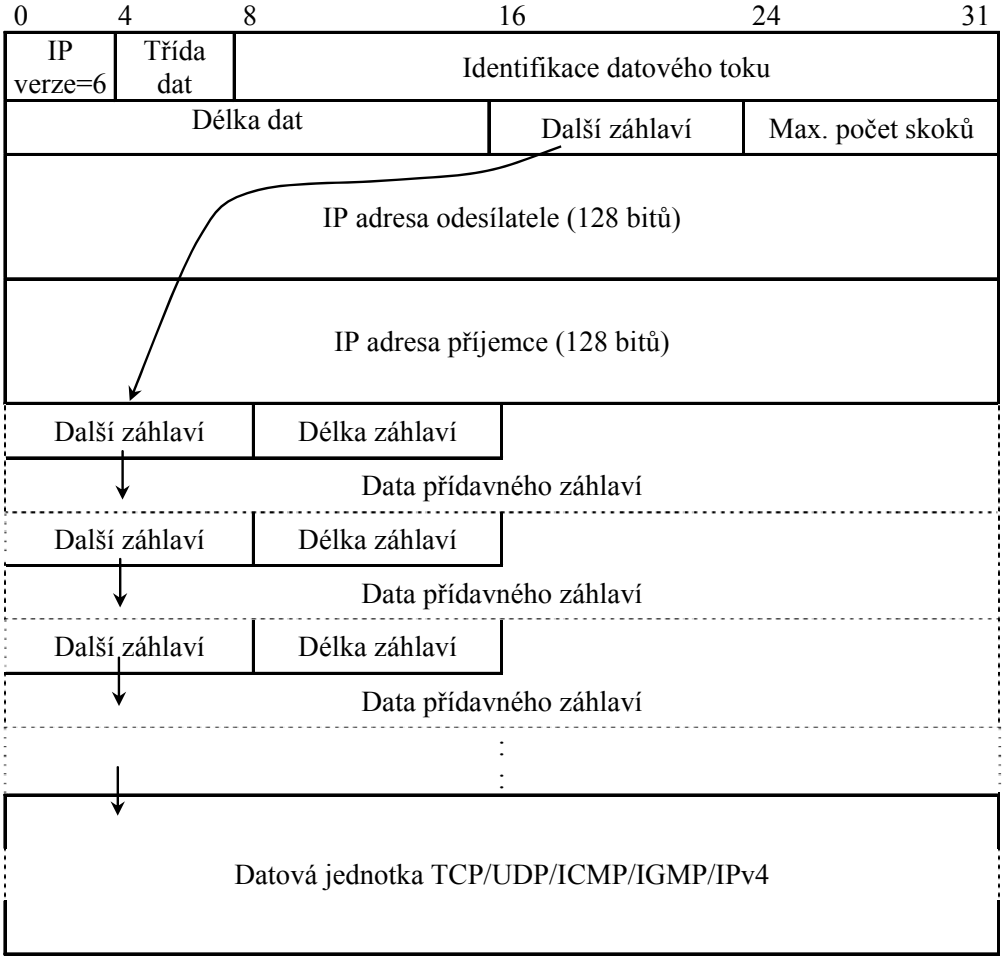
Další příklady adresace:

plný zápis	**zkrácený zápis**
F9A8:A28B:0000:0000:0000:0000:4A51:1022	F9A8:A28B::4A51:1022
0000:0000:0000:0000:0000:0000:147.229.169.6	:: 147.229.169.6

2. ***Změna a zjednodušení hlavičky protokolu*** - zjednodušuje původní hlavičku odstraněním přebytečných polí z povinné části záhlaví s možností jejich umístění do částí volitelných, které následují povinnou část hlavičky. Mimo základní hlavičky se používají volitelná záhlaví pro směrování, fragmentaci a ověřování přístupu. Jsou to např. položky rozšířeného záhlaví s názvem Hop-by-Hop Options, Routing, Fragment, Destination Options, Authentication, Encalupsulating Security Payload. Používají se jen v případě požadavku na danou funkci.
3. ***Automatická konfigurace uzlů*** - protokol má zapracované mechanismy automatického přidělování konfiguračních údajů sítě jeho jednotlivým uzlům pomocí protokolu DHCPng.

4. ***Bezpečnostní procedury*** - nový protokol má přímo zabudované bezpečnostní procedury ověřování přístupu a šifrování na úrovni IP komunikace. Bezpečnostní mechanizmy mohou být implementované prostřednictvím volitelných záhlaví AH (Authentication Head) a ESP (Encapsulating Security Payload). IPv6 umožňuje volitelný výběr bezpečnostních metod a parametrů. Implicitně se však používají metody autorizace přístupu MD5 a kódování podle DES (Data Encryption Standard).
5. ***Podpora multimediálních aplikací*** - nárůst aplikací požadujících komunikaci v reálném čase v síti Internet si vyžádal i zvýšení podpory tohoto druhu komunikace na straně IP protokolu. IP za tímto účelem používá metodu označení datových toků pomocí návěští (Flow Label). Přiřazením číselného návěští danému datovému toku prostřednictvím protokolu RSVP (Resource Reservation Protocol), může IP směrovač obsluhovat přenos paketů různých toků odlišným způsobem.

Paket (datagram) protokolu IPv6 včetně přídavných záhlaví má tvar zachycený na Obr. 5.18.



Obr. 5.18: Struktura datagramu protokolu IPv6

Povinné záhlaví má délku 40 oktetů a obsahuje tyto informace:

- **Verze IP** (IP Version) – 4 bity, má hodnotu 6 pro IPv6,
- **Třída dat** (Traffic Class) – 4-bitové pole, jehož množina hodnot je rozdělena na poloviny. První polovina hodnot (0-7) definuje různé typy provozu nesoucí klasická počítačová data. Druhá polovina hodnot je určena pro přenos dat služeb v reálném čase, přičemž nižší hodnota znamená nižší důležitost dat z hlediska chování směrovače při zahlcení.
- **Identifikace datového toku** (Flow Label) – 24 bitů – hodnota spolu s IP adresou jednoznačně identifikuje datový tok v rámci celého Internetu. Využití této položky je v základě dvojí:
  - **usnadnění směrování** – pakety jednoho datového toku jsou předávány na určitý výstup podle záznamu datový_tok-výstupní port-HW_adresa následujícího směrovače,
  - **zajištění patřičné šířky pásma** rezervované např. pomocí protokolu RSVP (Resource Reservation Protocol).
- **Délka dat** (Payload Length) – 16 bitů – definuje délku datagramu bez povinného záhlaví. Maximální hodnota je 65535, lze však definovat i delší datagram pomocí položky „Rozsáhlý datagram“ v přídavném záhlaví „Informace pro směrovače“.
- **Další záhlaví** – určuje typ dalšího záhlaví, kterým může být buď rozšíření záhlaví samotného protokolu IPv6 nebo již záhlaví dalších protokolů stejné či vyšší vrstvy, viz Tab. 5.4.

Tab. 5.4: Význam parametru „Další záhlaví“ (Next Header)

Hodnota pole „Další záhlaví“	**Typ následujícího záhlaví**
0	Informace pro směrovače (Hop-by-Hop Header)
4	Protokol IPv4
6	Protokol TCP
17	Protokol UDP
43	Směrovací informace (Routing Header)
44	Záhlaví fragmentu (Fragment Header)
45	Protokol IRP (Interior Routing Protocol)
46	Protokol RRP (Registry Registrar Protocol)
50	Bezpečnostní záhlaví (Encapsulating Security Payload)
51	Autentizační záhlaví (Authentication Header)
58	Protokol ICMPv6
59	Další záhlaví již nenásleduje
60	CLNP (ConnectionLess Network Protocol) – ISO/OSI
89	OSPF (Open Shortest Path First)

Další záhlaví mohou mít další členění na menší informační elementy, které se skládají zpravidla ze 3 částí, typu, délky a hodnoty informačního elementu.

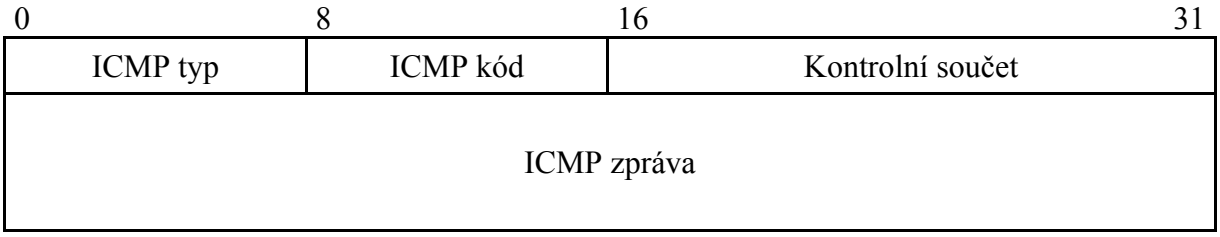
- **Maximální počet skoků** (Hop Limit) – maximální počet směrovačů, přes které může paket projít. Položka je obdobou doby života datagramu (TTL) v záhlaví datagramu protokolu IPv4. Pole lze využít pro odstraňování zbloudilých datagramů a k omezení dosahu šíření datagramu.

IPv6 vyžaduje změny u některých dalších protokolů, které mají co dočinění se směrováním, a s úkoly síťové vrstvy obecně. Ovlivněny jsou tak protokoly ICPMP a DNS a dále pak směrové protokoly (OSPF).

5.9.5 ICMPv6

Nový protokol IPv6 vyžaduje také nové funkce od pomocného protokolu ICMP. Proto byl navržen nový typ ICMPv6. Protokol je specifikován dokumentem RFC-2463. Pro přenos se využívá datagram protokolu IPv6, kde je v položce „další záhlaví“ uveden kód 58. Kromě standardních funkcí přenosu chybových hlášení a poskytování diagnostických služeb známých z verze pro protokol IPv4 zastupuje navíc činnost protokolu ARP. Umožňuje tedy získat fyzickou adresu dalšího uzlu na cestě (následujícího směrovače či cílové stanice) potřebnou pro sestavení rámce, viz Tab. 5.5.

Struktura zprávy ICMP je zachycena na Obr. 5.19, typy a kódy jsou uvedeny a vysvětleny v Tab. 5.5.



Obr. 5.19: Struktura zprávy ICMPv6

Tab. 5.5: Typy a kódy a význam ICMP zpráv

Typ	Kód	Popis
1		***Nedoručitelný IP-datagram*** (*Destination Unreachable*)
	0	Ve směrovací tabulce neexistuje směr pro tuto adresu (*No Route to Destination*)
	1	Spojení s adresátem je administrativně uzavřeno (*Communication with Destination Administratively Prohibited*)
	3	Nedosažitelná adresa (*Address Unreachable*)
	4	Nedosažitelný port (*Port Unreachable*)
2	0	Příliš velký datagram (*Packet Too Big*)
3		***Čas vypršel*** (*Time Exceeded*)
	0	Dosažen počet hopů (*Hop Limit Exceeded in Transit*)
	1	Vypršel čas na sestavení IP-datagramu z jeho fragmentů (*Fragment Reassembly Time Exceeded*)
4		***Chybný parametr*** (*Parameter Problem*)
	0	Chybné pole v záhlaví (*Erroneous Header Field Encountered*)
	1	Nepodporovaný typ v poli další hlavička (*Unrecognized Next Header Type Encountered*)
	2	Nepodporovaná volba (*Unrecognized IPv6 Option Encountered*)
128	0	Žádost o echo (*Echo Request)*
129	0	Echo (*Echo Reply*)
133	0	Žádost o směrování (*Router Solicitation*)
134	0	Oznámení o směrování (*Router Advertisement*)
135	0	Žádost o linkovou adresu (*Neighbor Solicitation*)
136	0	Oznámení o linkové adrese (*Neighbor Advertisement*)
137	0	Změň směrování (*Redirect Message*)

Typy ICMP zpráv se dělí na dvě skupiny:

- **chybové zprávy** - typ 0 až 127.
- **informativní zprávy** - typ 128 až 255.

5.10 Transportní protokoly

Na transportní vrstvě existují 3 základní protokoly: TCP, SCTP a UDP. Úkolem transportního protokolu je hlavně multiplex a demultiplex datových toků od jednotlivých procesů, které komunikují s transportní vrstvou přes speciální přístupové body (SAP – Service Access Point), tzv. porty. Jsou to místa v paměti, kterým je přiděleno 16-bitové číslo. Přitom stejné číslo může být přiděleno portu TCP a UDP. Označuje to však dva různé porty.

Protokoly UDP a TCP jsou využívány odlišnými aplikacemi (viz.Obr. 5.2). Protokol TCP je podstatně složitější než UDP, neboť nabízí více funkcí. Každý z nich nabízí různé služby.

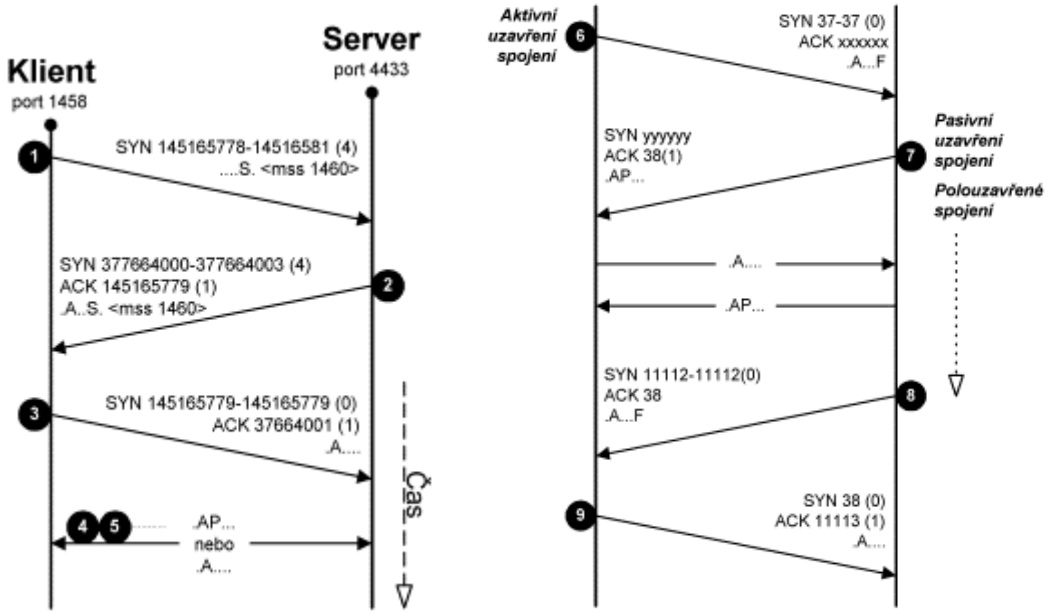
Tab. 5.6: Čísla některých „wellknown“ portů TCP

číslo „wellknown“ portu	navázaný protokol
21	FTP
23	Telnet
25	SMTP
42	DNS
67/68	BootP server/klient
80	HTTP
110	POP3

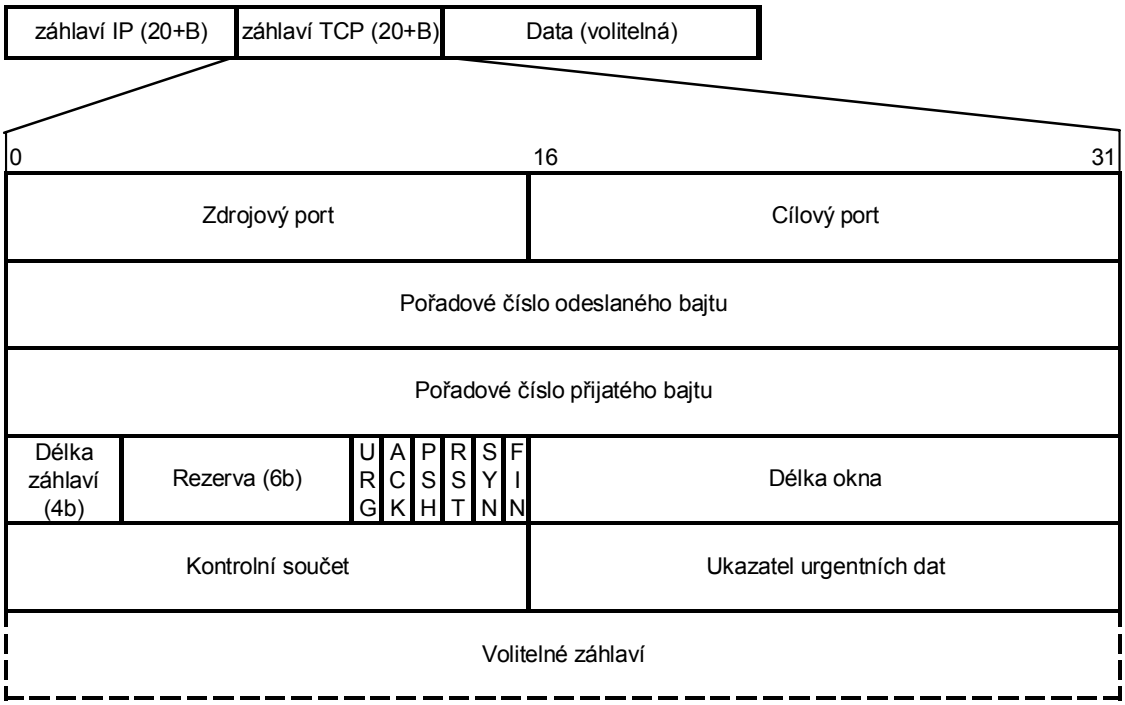
5.10.1 TCP (Transmission Control Protocol)

TCP poskytuje:

- **spojově orientovanou službu** - komunikace probíhá ve 3 fázích: navázání spojení, vlastní přenos dat, rozpad spojení (viz. Obr. 5.20)
- **spolehlivou službu** (tzv. bitová roura) – pomocí pořadových čísel, délky TCP segmentu, kontrolního součtu, časovače odpovědi a kladného potvrzování. Potvrzení posílá přijímač po příjmu paketu. Chyba je tedy indikována v případě, kdy potvrzení nepřijde do časového limitu vůbec, a nebo 3-krát po sobě přijde potvrzení se stejnou hodnotou pořadového čísla přijatého bajtu. Pak následuje procedura opakování. Příjemce si segmenty přišlé mimo pořadí uchovává, a je-li tedy přijat znovuvyslaný chybějící segment, pak se v potvrzení potvrdí všechna přijatá data tvořící souvislý tok bajtů. Není tedy třeba vysílat vše od původně ztraceného segmentu.
- **řízení toku dat** – pomocí 2 datových okének. Jedním si příjemce řídí vysílač tím, že sděluje vysílači pomocí velikosti tohoto okénka WIN, kolik dat je schopen přijmout. Druhé okénko CWND (Congestion window) je stanoveno na straně vysílače, aby nedošlo k zahlcení některého (nejpomalejšího) úseku sítě mezi odesílatelem a příjemcem. Velikost tohoto okénka je zjišťována postupně během zkoušení „co síť snese“. Přestanou-li docházet potvrzení, a přitom velikost prvního okénka definovaného příjemcem se nezmenšuje, znamená to, že došlo k zahlcení sítě a je nutné okénko CWND zmenšit. Výsledné množství vysílaných dat než přijde potvrzení je pak dáno jako min(WIN,CWND).



Obr. 5.20: Princip navazování a ukončení spojení



Obr. 5.21: Záhlaví TCP segmentu

Zdrojový port (*source port*) je port odesílatele TCP segmentu,
Cílový port (*destination port*) – TCP port adresáta TCP segmentu. Pětice: zdrojový port, cílový port, zdrojová IP-adresa, cílová IP-adresa a protokol (TCP) jednoznačně identifikuje v daném okamžiku spojení v Internetu.
Pořadové číslo odesílaného bajtu je pořadové číslo prvního bajtu TCP segmentu v rámci celé zprávy přenášené od odesílatele k příjemci. Tok dat v opačném směru má vlastní číslování svých dat. Jelikož pořadové číslo odesílaného bajtu je 32 bitů dlouhé, tak po dosažení hodnoty 2^{32}-1 nabude cyklicky opět hodnoty 0. Číslování obecně nezačíná od nuly (ani od nějaké určené konstanty), ale číslování by mělo začínat od náhodně zvoleného čísla. Vždy, když je nastaven příznak SYN, tak operační systém odesílatele začíná znovu číslovat,

tj. vygeneruje startovací pořadové číslo odesílaného bajtu, tzv. ISN (*Initial Sequence Number).*

Pořadové číslo přijatého bajtu – vyjadřuje číslo následujícího bajtu, který je příjemce připraven přijmout, tj. příjemce potvrzuje, že správně přijal vše až do pořadového čísla přijatého bajtu mínus jedna.

Délka záhlaví vyjadřuje délku záhlaví TCP segmentu v násobcích 4 B.

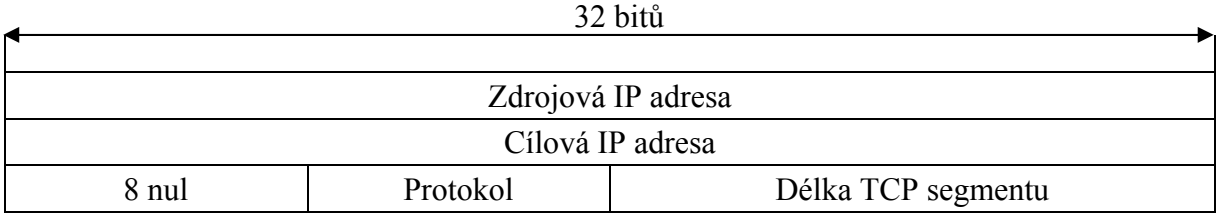
Délka okna vyjadřuje přírůstek pořadového čísla přijatého bajtu, který bude příjemcem ještě akceptován. Tento parametr slouží k řízení toku dat

Ukazatel naléhavých dat může být nastaven pouze v případě, že je nastaven příznak URG. Přičte-li se tento ukazatel k pořadovému číslu odesílaného bajtu, pak ukazuje na konec úseku naléhavý dat. Odesilatel si přeje, aby příjemce tato naléhavá data přednostně zpracoval. Tento mechanismus používá např. protokol Telnet.

V poli příznaků mohou být nastaveny následující příznaky:

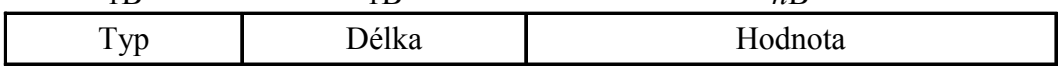
- **URG** – TCP segment nese naléhavá data.
- **ACK** – TCP segment má platné pole "Pořadové číslo přijatého bajtu" (nastaven ve všech segmentech, kromě prvního segmentu, kterým klient navazuje spojení).
- **PSH** – Zpravidla se používá k signalizaci, že TCP segment nese aplikační data, příjemce má tato data předávat aplikaci. Použití tohoto příznaku není ustáleno.
- **RST –** Odmítnutí TCP spojení.
- **SYN** – Odesílatel začíná s novou sekvencí číslování, tj. TCP segment nese pořadové číslo prvního odesílaného bajtu (ISN).
- **FIN** – odesilatel ukončil odesílání dat. Pokud bychom použili přirovnání k práci se souborem, pak příznak FIN odpovídá konci souboru (EOF). Přijetí TCP segmentu s příznakem FIN neznamená, že v opačném směru není dále možný přenos dat. Jelikož protokol TCP vytváří plně duplexní spojení, tak příznak FIN způsobí jen uzavření přenosu dat v jednom směru. V tomto směru už dále nebudou odesílány TCP segmenty obsahující příznak PSH (nepočítaje v to případné opakovaní přenosu).

Kontrolní součet – počítá se z celého TCP-segmentu (ze záhlaví i z přenášených dat) a pseudozáhlaví (viz. Obr. 5.22). Kontrolní součet vyžaduje sudý počet bajtů, proto v případě lichého počtu se data doplní jedním bajtem na konci.



Obr. 5.22: Pseudozáhlaví TCP segmentu

Volitelné položky – upřesňují či mění některé parametry komunikace. Jejich celková délka musí být < 40 B.



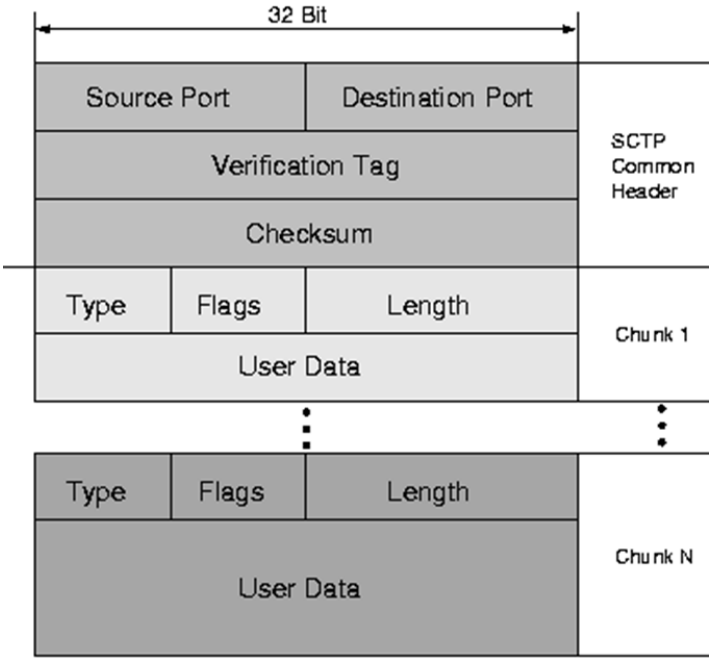
Obr. 5.23: Struktura volitelné položky

- ***Maximální velikost TCP segmentu*** (Maximum Receive Segment Size) – příjemce oznamuje největší velikost TCP segmentu, který je ochoten přijmout.
- ***Zvětšení příjmového okna*** (Window Scale) – hodnota *k* určuje zvětšení původního okna na pův. velikost*2^k.

- ***Selektivní potvrzování*** (SACK – Selective Acknowledgement) – žádost o selektivní potvrzování bloků dat. Pak je možné opakovat pouze nepotvrzený blok.
- ***Selektivní potvrzování povoleno*** (SACK Permitted) – posílá se při inicializaci spojení a určuje, zda je druhou stranou akceptováno selektivní potvrzování.
- ***TCP Echo*** – žádost k protější stanici o echo. Spolu s odpovědí to slouží k odhadu rychlosti obousměrného spoje a nastavení časovačů.
- ***Odpověď na TCP echo***
- ***Výplňová položka*** (No Operation) – doplňuje délku předchozí položky na celistvý násobek 4B, pokud to následující položka vyžaduje.
- ***Konec voleb*** (End of Option List) – ukončení bloku volitelných položek

5.10.2 Protokol SCTP

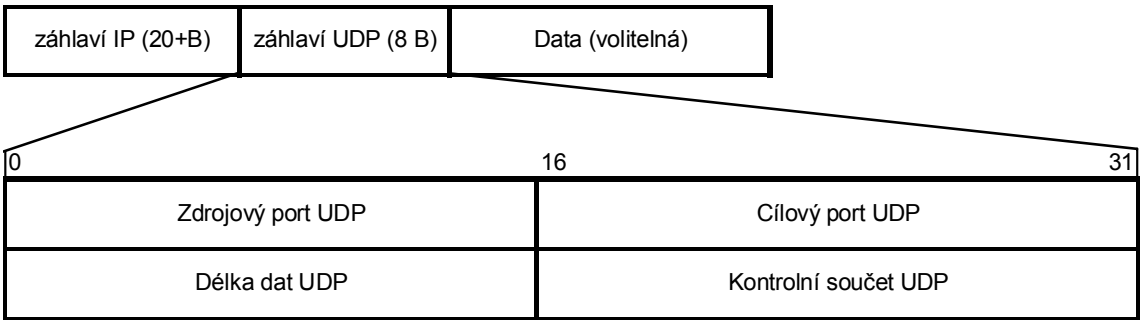
Protokol SCTP je spolehlivý transportní protokol, který je na rozdíl od TCP orientovaný na přenos zpráv. Původně byl navržen pro přenos signalizace SS7 přes IP síť. Protokol SCTP používá namísto spojení tzv. asociaci, která umožňuje přenos více dílčích datových toků v rámci jedné asociace. Protokol SCTP také odděluje spolehlivost přenosu od zajištění pořadí doručení, především co se týče různých dílčích datových toků v rámci jedné asociace. Datová jednotka SCTP obsahuje společné záhlaví a pak segmenty více jednotlivých dílčích toků označované jako „chunk“, viz Obr. 5.24. Každý dílčí segment (chunk) obsahuje čtyřbajtové záhlaví a datovou část. Stejně jako TCP i SCTP podobně řeší řízení datového toku a problém zahlcení sítě.



Obr. 5.24: Datová jednotka protokolu SCTP

5.10.3 Protokol UDP (User Datagram Protocol)

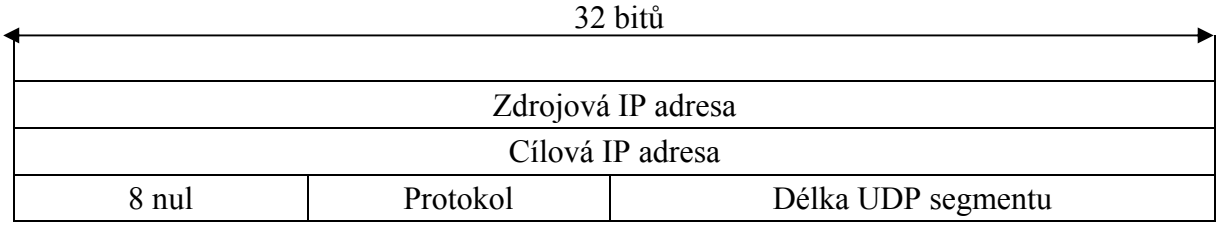
Protokol UDP zajišťuje minimální nádstavbu nad protokol IP. Zajišťuje multiplex a demultiplex mezi jednotlivé aplikace a provádí segmentaci dat. Na rozdíl od TCP nabízí nespojovanou a nespolehlivou službu, což umožňuje aby byl rychlejší, neboť vyžaduje minimum režie. Případné zabezpečení si musí zajistit aplikace sama.



Obr. 5.25: Záhlaví UDP segmentu

Zdrojový port – port protokolu UDP aplikace odesílatele. Je odlišný od TCP portů,
Cílový port – port protokolu UDP aplikace příjemce,
Délka dat – délka celého UDP segmentu,
Kontrolní součet – nepovinný, je-li 0, znamená to, že je nepoužit.

Při předávání mezi transportní a síťovou vrstvou se před vlastní záhlaví připojuje stejně jako u TCP ještě pseudozáhlaví (viz. Obr. 5.26).



Obr. 5.26: Formát pseudozáhlaví UDP segmentu

Tím, že je protokol UDP nespojovaný, je vhodný pro multicasting (hromadné rozesílání oběžníkových zpráv skupině počítačů).

5.11 Aplikační protokoly

Aplikační protokoly jsou nejširší skupinou protokolů sady TCP/IP a tvoří komunikační jádra aplikací pro různé služby jako vzdálený přístup (Telnet, SSH), přenos souborů (FTP), přístup k www stránkám (HTTP), a další.
Protokoly nižších vrstev až po vrstvu transportní (včetně) jsou implementovány jako součást operačního systému. V TCP/IP neexistuje samostatná prezentační a relační vrstva, a proto si aplikace příslušné mechanismy musí implementovat samy (pokud je potřebují). Teprve až v devadesátých letech se začínají zavádět prostředky pro sdílení takovýchto mechanismů (XDR, RPC)
Konkrétní forma rozhraní mezi aplikační a transportní vrstvou je závislá na implementaci (na použitém OS), např.

- BSD Unix: rozhraní socket interface (a implementováno pomocí ovladačů zařízení)
- AT&T Unix: rozhraní TLI (Transport Layer Interface) implementováno pomocí mechanismu “streams”
- MS Windows: rozhraní Windows Sockets, alias Winsock (podle BSD Unix)

Z pohledu ostatních uzlů musí mít přístup k aplikacím, a tedy rozhraní transportní-aplikační vrstva obecnou strukturu, která je na operačním systému nezávislá. Je to řešeno pomocí tzv. **portů**. Aplikační protokoly jsou nejčastěji založeny na modelu **klient/server**:

- aplikace typu **klient** žádá server o poskytnutí služby,
- **klient** je proces spuštěný uživatelem (např. prohlížeč webu), respektive automaticky operačním systémem po startu (např. DHCP klient) či na žádost od jiného klienta (např. DNS klient),
- **server** je obvykle proces, který je buď spuštěn a aktivován po startu systému, běží trvale a čeká na klientské požadavky, které jsou mu předávány operačním systémem a nebo je spouštěn až po příchodu požadavku operačním systémem nebo na popud jiného procesu,
- implementace serverů v různých OS:
  - MS Windows: úloha,
  - NetWare: modul NLM,
  - Unix: proces (typu démon, bez uživatelského rozhraní).

5.11.1 Telnet

Telnet je služba vzdáleného přihlašování, která vznikla již v roce 1969. Poskytuje možnost vzdáleného ovládání hostitelských počítačů prostřednictvím příkazového řádku. Avšak v současné době se od jejího používání ustupuje, neboť neposkytuje zabezpečovací mechanizmy chránící přenášená data před „odposloucháváním“ a doporučuje se ho nahradit zabezpečeným přístupem pomocí systému SSH (Secure SHell), využívajícího asymetrického šifrování (šifrování s veřejným klíčem).

Protokol Telnet je služba typu klient-server a vyznačuje se následujícími vlastnostmi:

- umožňuje přístup a komunikaci se vzdálenými serverovými procesy (např. s webovým serverem, SMTP serverem, apod.) pomocí uvedení portu při zahájení klienta,
- server čeká na portu 23,
- klient i server mohou stát na různých platformách (např. klient pod MS DOS či Windows, a server pod Unixem),
- klient dnes nejčastěji funguje na principu terminálové emulace (v roli terminálu vystupuje jiné zařízení, než jednoúčelový terminál),
- Telnet server je realizován na aplikační úrovni (jako systémová úloha - démon), a nikoli “uvnitř” OS,
- Telnet lze aktivovat příkazem:

  telnet adresa_vzdáleného_počítače [**číslo_portu**]
- Adresa vzdáleného počítače může být uvedena jak ve formě IP adresy, tak ve formě symbolického jména.

5.11.2 Protokol FTP (File Transfer Protocol)

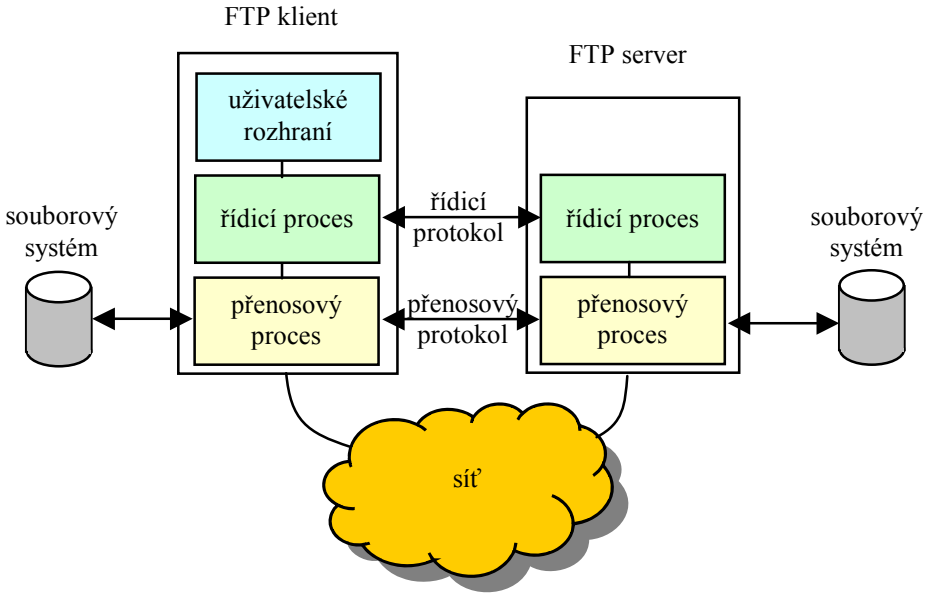
Protokol FTP řeší problematiku obousměrného přenosu datových souborů mezi dvěma počítači v konfiguracích:

místní počítač – vzdálený počítač - přenos řídicích informací i souborů,

- **místní počítač – vzdálený počítač 1 – vzdálený počítač 2** - přenos řídicích informací po spojích místní počítač – vzdálený počítač 1 a místní počítač – vzdálený počítač 2, přenos souborů po spoji vzdálený počítač 1 – vzdálený počítač 2.

Na rozdíl od NFS (Network File System – transparentní sdílení souborů v síti) FTP zajišťuje netransparentní způsob přenosu souborů (je jednodušší), tj. uživatel si uvědomuje existenci sítě a skutečnost, že různé soubory se nachází na různých počítačích a musí vědět, kde se vzdálené soubory nachází a jak se jmenují. Uživatel musí sám (explicitně) podnikat určité akce, aby získal přístup ke vzdáleným souborům (přihlášení ke vzdálenému systému, nastavení parametrů přenosu, vyhledání požadovaného souboru a zahájení přenosu). Protokol FTP je charakterizován následujícími vlastnostmi:

- vychází z modelu klient/server,
- klient je typicky aplikačním programem,
- server obvykle systémovým procesem (démonem, NLM souborem, službou, rezidentním programem apod.),
- návrh protokolu je uzpůsoben možnosti úsporné implementace (takové, která si nárokuje většinu systémových zdrojů až v okamžiku jejich skutečné potřeby),
- pro transport používá protokol TCP,
- server používá 2 porty: č. 20 pro data a č. 21 pro řízení,
- zajištění potřebných funkcí v rámci FTP je rozděleno mezi dva subjekty:
  - interpret protokolu (PI, Protocol Interpreter), realizuje řídicí spojení s protějším PI,
  - přenosový proces (DTP, Data Transfer Process) – realizuje spojení pro vlastní přenos souborů,
- interpret protokolu existuje trvale, přenosový proces vzniká až na základě konkrétního požadavku,



Obr. 5.27: Části klientské a serverové aplikace a typy spojení

- řídicí spojení iniciuje klient,
- server "poslouchá" na dobře známém portu (č. 21),
- datové spojení iniciuje server (jeho přenosový proces), a je realizováno přes dynamicky přidělený port,
- FTP zavádí jednotný formát dat pro potřeby přenosu a veškeré konverze z/do tohoto formátu ponechává na koncových uzlech,
- umožňuje ale oběma stranám dohodnout se v konkrétním případě na jiném formátu (kvůli větší efektivitě přenosu),
- FTP přenáší data 8-bitově,

- pro možnost konverzí z/do jiných specifických formátů je nutné vědět, zda jde o text či binární data, a proto se protokolu FTP musí explicitně říci, co se vlastně přenáší (implicitně se předpokládá, že jde o text),
- pro text používá FTP stejný formát, jako protokol Telnet:
  - jednotlivé znaky přenášeny v 8 bitech,
  - konec řádky = CR+LF,
  - kódování ASCII.
- alternativní možností je použití kódu EBCDIC, použití nestandardní velikosti bajtu atd.,
- Struktura souborů v FTP
  - FTP implicitně chápe soubor jako dále nestrukturovaný (bez vnitřní struktury) - označováno jako file structure,
  - alternativně je schopen se na něj dívat jako na posloupnost stejně velkých záznamů (records) - record structure,
  - nebo jako na množinu stránek (které mohou tvořit nespojitý soubor) - page structure.
- Režimy přenosu v FTP
  - implicitně je obsah souboru přenášen jako spojitý proud dat (tzv. stream mode),
  - alternativou je blokový režim (block mode), při kterém je možné vkládat mezi bloky "zarážky", a po přerušení a následné obnově spojení není nutné začít přenos od začátku, ale stačí pokračovat od poslední úspěšně přenesené zarážky,
  - z hlediska zahajování vlastního přenosu dat rozlišujeme:
    - **aktivní režim** – datový tok zahajuje server z portu TCP/20 na dynamický port TCP/>1024.
    - **pasivní režim** – datový spoj otevírá klient z dynamického portu na dynamický port TCP. Tento režim je vhodný, nachází-li se klient za směrovačem s překladem adres (NAT). Zde může být problém s vlastním přenosem dat při použití firewallu, protože není pevně dán žádný z portů pro datový tok.
  - další možností je komprimovaný režim, kdy je používána jednoduchá metoda komprese (eliminují se opakující se znaky).

5.11.3 Protokol TFTP

Existují situace, kdy protokol FTP není nejvýhodnější:

- např. pro tzv. bootstrap bezdiskových stanic je příliš složitý,
- pro některé jednoduché OS za účelem vzdáleného update firmware je problém jej implementovat.

V rámci sady TCP/IP existuje zjednodušená verze FTP pod názvem TFTP (Trivial FTP). Rozdíly mezi TFTP a FTP:

- TFTP využívá přenosových služeb protokolu UDP (FTP využívá TCP),
- TFTP si spolehlivost zajišťuje sám,
- TFTP využívá jednotlivé potvrzování,
- TFTP přenáší data po blocích velikosti 512 bytů,
- TFTP nezajišťuje na vzdáleném počítači žádné systémové akce typu ls, cwd, rm apod.
- TFTP nezná pojem aktuálního adresáře,
- uživatel musí explicitně zadat úplnou přístupovou cestu k souboru, který má na mysli (a musí jej znát),
- TFTP nezná pojem uživatele,
- TFTP nezajišťuje žádné přihlašování na vzdáleném počítači,

- definice TFTP ponechává na implementaci, jak se vyřeší přístupová práva,
- obvykle je pro TFTP dostupné to, co je dostupné pro všechny uživatele.

5.11.4 Elektronická pošta (e-mail)

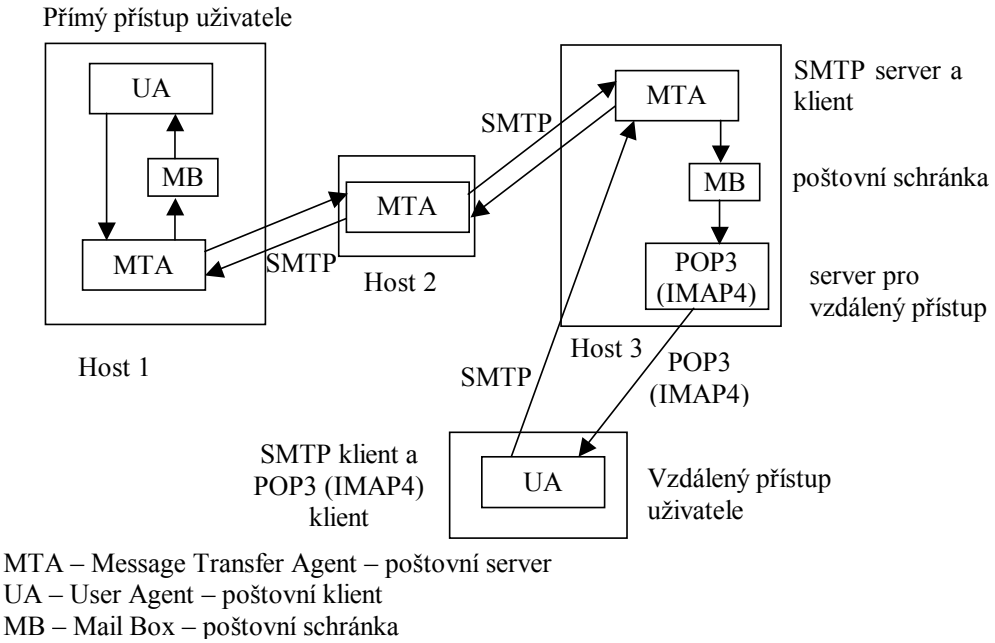
Elektronická pošta neboli e-mail je služba posílání obecně multimediálních dokumentů v elektronické podobě počítačovou sítí. Je to jedna ze základních služeb počítačových sítí.

Podstata elektronické pošty na bázi SMTP zahrnuje:
- přeprava elektronických dopisů Internetem,
- založena na bázi server/klient,
- využívá protokolů pro přihlašování a odesílání a transfer elektronické pošty (protokol SMTP – Simple Mail Transfer Protocol) a protokoly pro odběr elektronické pošty (protokoly POP3 nebo IMAP - Internet Message Access Protocol)
- SMTP server očekává požadavky na portu č. 25,
- původně měl obsah textovou povahu, dnes se používá i pro přenos multimediálních dokumentů,
- základním protokolem je aplikační protokol SMTP (Simple Mail Transfer Protocol).

5.11.4.1 Protokol SMTP

SMTP (Simple Mail Transfer Protocol) je komunikační prostředek mezi poštovními servery a zčásti i mezi klientem a serverem. Je specifikován dokumentem RFC 821. Formát zpráv je definován dokumentem RFC 822. Přenosové prostředí pro dopravu elektronické pošty v Internetu je tvořeno soustavou poštovních serverů (mail server). Server očekává požadavky na portu 25/TCP. Komunikace mezi SMTP servery či mezi SMTP serverem a SMTP klientem má textovou formu. Další možnosti a příkazy byly přidány uvedením rozšířeného protokolu ESMTP (Enhanced SMTP). Nejčastějšími příkazy jsou:

HELO EHLO MAIL RCPT DATA
RSET NOOP QUIT HELP VRFY
EXPN VERB ETRN DSN AUTH
STARTTLS



MTA – Message Transfer Agent – poštovní server
UA – User Agent – poštovní klient
MB – Mail Box – poštovní schránka

Obr. 5.28: Struktura, protokoly a přístup k elektronické poště

Komunikace probíhá podle následujícího vzoru:

```
-ksh-3.2$ telnet ant.feec.vutbr.cz 25
  Trying 147.229.144.10...
  Connected to ant.feec.vutbr.cz.
  Escape character is '^]'.
  220 ant.feec.vutbr.cz ESMTP Sendmail 8.14.5/8.14.4; Mon, 30 Jan 2011
  16:12:10 +0100 (CET)
  EHLO ant.feec.vutbr.cz
  250-ant.feec.vutbr.cz Hello ant.feec.vutbr.cz [147.229.144.10], pleased to
  meet you
  MAIL from:<novotnyv@feec.vutbr.cz>
  250 2.1.0 <novotnyv@feec.vutbr.cz>... Sender ok
  RCPT To:<novotnyv@feec.vutbr.cz>
  250 2.1.5 <novotnyv@feec.vutbr.cz>... Recipient ok
  DATA
  354 Enter mail, end with "." on a line by itself
  ahoj
  .
  250 2.0.0 q0UFCAbv052053 Message accepted for delivery
  QUIT
  221 2.0.0 ant.feec.vutbr.cz closing connection
  Connection closed by foreign host.
```

5.11.4.2 Přenos pošty

Protokol SMTP využívá transportní protokol TCP. SMTP server přijímá od SMTP klienta či jiného SMTP serveru požadavky, reaguje na ně a jako odpověď zasílá kódy s popisem charakterizující reakci serveru.
Pro vyhledání adresy cílového poštovního serveru slouží systém DNS. Ve jmenné databázi DNS serveru jsou také záznamy typu

<doména> IN MX <priorita > <jméno_poštovního_serveru >,

např. IN MX 0 ustav1.skola.cz
IN MX 50 ustav2.skola.cz

Na základě tohoto záznamu (ale většinou jich bývá více, aby se zvýšila pravděpodobnost doručení pošty) a dále převodního záznamu jméno-IP adresa se pošta pošle do poštovného uzlu s nejnižší hodnotou priority (takový uzel by měl být ten cílový). Pokud se spojení nepodaří, kontaktuje se server s druhou nejnižší hodnotou priority. Ten se pak snaží předat poštu tomu cílovému. Aby se zamezilo zacyklení pošty, daný server může předat poštu jenom serveru s nižší hodnotou priority. Cílový poštovní server pak uloží zprávu do schránky uživatele.

5.11.4.3 Uživatel elektronické pošty

Uživatel využívá elektronické pošty prostřednictvím poštovního klienta. Pošta je ukládána do poštovní schránky (adresář na domácím poštovním serveru).
- uživatel, jako účastník elektronické pošty, je specifikován elektronickou poštovní adresou (e-mailovou adresou)
- přístup uživatele k poště je buď

- lokální – není zapotřebí další protokol nebo
- vzdálený – je nutný komunikační protokol (a jemu odpovídající servery a klienti) pro příjem (POP3, IMAP4) a posílání pošty (SMTP, POP3).

5.11.4.4 E-mailová adresa

Emailová adresa je dána doporučením RFC 822 a nejčastěji má tvar

schránka@poštovní_doména

např. novotnyv@ feec.vutbr.cz nebo novotny.vit@feec.vutbr.cz či utko@fee.vutbr.cz
Může však nabývat i dalších tvarů:
- "text" <schránka@poštovní_doména> text je nejčastěji plné jméno uživatele,
- schránka@[IP_adresa_cílového_SMTP_serveru] např. novotnyv@[147.229.192.10]

Pro zasílání pošty více účastníkům lze buď jednotlivé adresy vypsat a oddělit je čárkou, nebo použít rozesílací seznamy.

Jako jméno schránky lze použít i jiná jména než uživatelské jméno, tzv. aliasy, avšak ty musí být uvedeny ve zvláštním souboru zvaném nejčastěji aliases.

5.11.4.5 Formát zpráv el. pošty

Každá zpráva elektronické pošty má dvě části:
- záhlaví,
- tělo.

Původní pošta v rámci TCP/IP definovaná dokumenty RFC 821 a 822 definovala pouze syntaxi a sémantiku záhlaví (v doporučení RFC 822), a tělo brala jako "černou skříňku". Dnes existuje rozšíření (standard MIME), které zčásti specifikuje i formát těla zprávy.

5.11.4.6 POP (Post Office Protocol)

POP (Post Office Protocol) je protokol definující pravidla pro vzdálený přístup k elektronické poště. Dnes se používá verze POP3 specifikovaná dokumentem RFC 1939. Protokol POP charakterizují následující vlastnosti:
- software typu klient-server,
- server čeká na požadavek na portu 110/TCP,
- pracuje v offline režimu, a je tedy určen ke stažení došlé pošty z poštovního serveru (pro download), pro upload se předpokládá použití SMTP, i když POP3 umí i upload,
- vždy stahuje všechnu poštu nebo nic, neumí selektivní výběr,
- POP3 server se může nacházet v v jednom ze tří stavů:
  - autorizační – ověření uživatele,
  - transakční – vlastní přenos zpráv,
  - aktualizační.
- protokoly POP mají jen minimální schopnosti, postačující pro:
  - identifikaci uživatele (vůči serveru),
  - přenos zpráv ze serveru ke klientovi,
  - smazání zpráv na serveru,
- protokoly POP neumožňují např. zjistit obsah zprávy (ani subject) před jejím stažením (pouze zjistí délku zprávy)

5.11.4.7 IMAP4 (Internet Message Access Protocol)

Protokol IMAP4 je specifikován v dokumentu RFC 2060. Dalšími dokumenty jsou RFC 2061, 2086, 2087, 2088, 2177, 2193, 2221, 2342, 2359.
Server očekává příkazy na portu 143, 993 (zabezpečený přenos přes TLS/SSL)
Poskytuje řadu vylepšení oproti protokolu POP3:

- umožňuje různé módy zpracování pošty:
  - offline,
  - online,
  - odpojený mód.
- umožňuje tedy jak stáhnout poštu, odpojit se a zpracovávat ji na svém počítači (jako POP3), tak i přímo zpracovávat poštu v poštovní schránce na vzdáleném poštovním serveru, či stáhnout si vybranou poštu, zpracovat ji a znovu se připojit a předat uvedené změny (odesílaná pošta, smazání zprávy, úprava seznamů e-mailových adres, apod.) poštovnímu serveru

Protokol SMTP podporuje pouze sedmibitové e-maily. Jak to řešit, je-li potřeba odeslat např. dopis psaný česky nebo snad program? Existuje protokol Extended SMTP, který podporuje 8-bitový mail, ale to opět není řešení, protože ne všude je k dispozici.

Nejčastější řešení je převod 8-bitových dat na 7-bitová. Problém je v převedení (zašifrování) 8-bitových dat do 7-bitových, protože existuje několik vzájemně nezaměnitelných algoritmů. Nejpoužívanější jsou uuencode, MIME a BinHex. Odesilatel i příjemce musí použít stejný algoritmus.

5.11.4.8 MIME (Multipurpose Internet Mail Extensions)

Standard MIME rozšiřuje původní specifikaci elektronických dopisů pomocí RFC 822 o schopnosti přenášet jiná data než ASCII text nebo zprávy složené z více částí.
Rozšíření MIME (Multipurpose Internet Mail Extension) se snaží řešit omezení původního standardu podle RFC822. MIME je standardem, který doplňuje RFC822 a zajišťuje zpětnou kompatibilitu. Je navrženo tak, aby mohly být posílány stávajícím poštovním systémem zprávy obsahující diakritiku, obrázky, zvuk atd.
Tento standard řeší dvě otázky:

1. Jak vytvořit ze zprávy obsahujícího např. binární data zprávu vyhovující RFC822 a tedy přepravitelnou používanými přenosovými protokoly. Tj. zavádí standard pro kódování.

2. Jak rozlišit jednotlivé druhy zpráv, tj. zavádí klasifikaci přenášených informací. Klasifikace přenášených informací se ukázala velmi užitečnou i mimo e-mail. Moderní služby Internetu ji přebírají a používají ke stejnému účelu. MIME zavádí další hlavičkové řádky do e-mailové zprávy, které specifikují typ posílaných dat a způsob jejich kódování.

5.11.4.9 MIME hlavička

MIME hlavička obsahuje:

- **MIME-Version** - přítomnost této hlavičky v mailu indikuje, že je zpráva sestavena podle RFC2045 až RFC2049,
- **Content-Type** - specifikuje typ a podtyp dat posílaných v těle zprávy (text, audio, video, virtuální realita),
- **Content-Transfer-Encoding** - specifikuje použité kódování, pomocí kterého je zpráva převedena do formátu vyhovujícímu přenosovému mechanismu (do ASCII),
- **Content-ID** - identifikace zprávy použitelná v možném odkazu,
- **Content-Description** - textový popis obsahu.

5.11.4.10 Typy dat kódovaných pomocí MIME

Typy dat kódovaných pomocí MIME jsou dvojího druhu:

- Typy popisující typ přenášených dat. Jedná se o typy:
  - text,

  - application,
  - image,
  - audio,
  - video,
  - model.
- Typy specifikující, že zpráva se skládá z několika částí. Jedná se zejména o:
  - message,
  - multipart.

Lze použít i experimentální typy, ty je však potřeba odlišit od standardních typů prefixem **x-** před jménem typu např. pro zprávu VRML se kdysi používalo x-world/x-vrml. Dnes však VRML (po ukončení experimentů) používá model/vrml.

5.11.4.11 Způsoby kódování MIME dat

Použitý typ kódování je uveden v této hlavičce zprávy. RFC2045 až RFC2049 definuje několik základních algoritmů kódování. Další algoritmy mohou být podle RFC2048 rovněž registrovány odesláním příslušného formuláře. Registrované algoritmy jsou vystaveny na: ftp://ftp.isi.edu/in-notes/iana/assignments/transfer-encodings
Nejčastější algoritmy kódování jsou:

- 7bit,
- quoted-printable,
- base64,
- 8bit,
- binary,
- x-rozšíření.

6 Správa sítí

Správa sítě zajišťuje hladký chod sítě, jehož udržování vyžaduje řadu činností:

- **správa techniky** - kontrola stavu techniky, odstraňování poruch a modernizace stávajícího zařízení, dále rozšiřování sítě, tedy instalace a konfigurace nových zařízení (počítačů, serverů, síťových tiskáren, faxových bran, směrovačů, přepínačů, rozbočovačů, rozvaděčů, kabeláže) a v neposlední řadě dohled nad úrovní provozu, ztrátami a poruchovostí a návrh konfiguračních změn pro zvýšení propustnosti a spolehlivosti sítě,
- **správa uživatelských účtů** - zavádění a rušení účtů, uživatelských skupin, přidělování přístupových práv, pracovního prostoru, přizpůsobení pracovního prostředí pro daného uživatele, dále řešení problémů uživatelů se sítí či programovým vybavením a také realizace konzultací a školení uživatelů pro práci v síťovém prostředí a se síťovými aplikacemi,
- **správa programového vybavení a dat** - instalace a konfigurace nového software, upgrade stávajícího programového vybavení, dále zálohování dat a v poslední době také ochrana dat před neautorizovaným přístupem (především z vnějších sítí) a virovými nákazami.

6.1 Úrovně správy

- snaha o centralizaci sledování stavu a provozu v síti, o umožnění centralizovaného zásahu do problematických oblastí = možnost vzdáleného testování funkčnosti a vzdálené konfigurace různých uzlů v síti. Pro dohled, kontrolu činnosti síťových prvků či softwarových modulů sítě lze použít různé prostředky:

1) **orientační kontrola funkčnosti** – používání standardních utilit, jako např. telnet, ping, nslookup, traceroute, apod.

2) **využití nesjednocených dohledových SW modulů** dodávaných s daným zařízením či síťovým operačním systémem, tzv. SW monitorů. Ty nám sbírají statistické údaje o své činnosti a o provozu i o problémech na jednotlivých rozhraních.

3) **využití síťových analyzátorů** - speciálních zařízení sledujících provoz na daném spoji a určitém spojovacím uzlu, které sebraná data třídí a vyhodnocují a poskytují výstupy v patřičném formátu. Takovéto analyzátory mohou vystupovat v různých úlohách, např. jen jako nezúčastněný monitor provozu, či jako jeden z prvků sítě (koncové zařízení, přijímací a vysílací část spojovacího uzlu, apod.).

4) **využití standardu** podporovaného širokou platformou výrobců síťových komponentů a komplexní řešení centralizovaného dohledu nad celou sítí - soubor HW a SW prostředků instalovaných v různých prvcích sítě (koncových zařízeních, rozbočovačích, přepínačích, směrovačích, síťových tiskárnách, serverech, a v centrální dohledové stanici). Příkladem může být podpora protokolu **SNMP** (Simple Network Management Protocol).

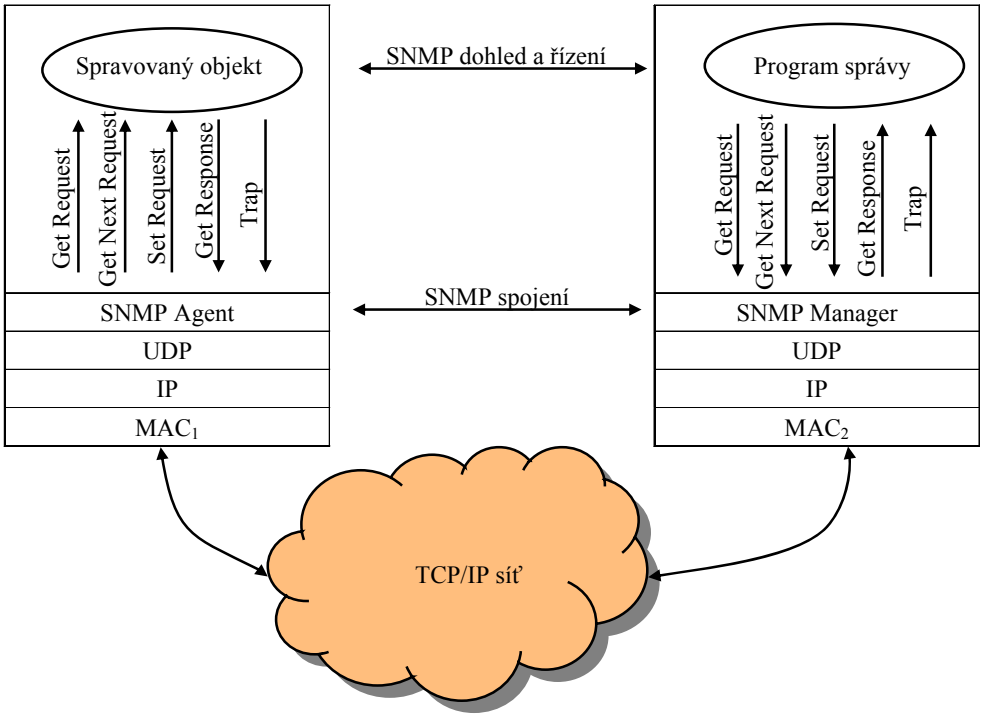
6.2 SNMP (Simple Network Management Protocol)

SNMP je nejčastěji používaným protokolem pro centralizovaný dohled nad většími sítěmi pracující s protokolovou sadou TCP/IP. Je specifikován doporučením RFC 1157, ke kterému se vážou další 2 doporučení RFC 1065 definující SMI (Structure of Management Information) a RFC 1213 popisující databázi objektů MIB-II (Management Information Base). Sestává ze 2 základních částí:

1) **SNMP Manažer** = SW modul pracující v dohledové stanici a shromažďující, třídící a vyhodnocující informace o síťových prvcích. Kromě těchto činností umožňuje i vzdálený zásah do konfigurace či vzdálené odstartování testovacích procedur na daném síťovém prvku.
2) **SNMP Agent** (někdy nazývaný SNMP server) = HW + SW modul implementovaný jako nadstandardní část daného síťového prvku. Tento modul sbírá informace o činnosti přidruženého síťového prvku, na žádost či při vzniku nestandardní události odesílá stavové informace a případně na žádost manažera může měnit i nastavení parametrů daného síťového prvku.
SNMP používá pro komunikaci UDP protokol.

6.2.1 SNMP operace

SNMP Manažer komunikuje s SNMP Agentem pomocí příkazů a odpovědí. Existuje celkem 5 typů zpráv:
1) **Get Request** (M-A) = žádost o zaslání hodnoty určité proměnné,
2) **Get Next Request** (M-A) = žádost o zaslání hodnoty proměnné následující po posledně zmíněné proměnné (nemusí být uvedeno její jméno(adresa)),
3) **Set Request** (M-A) = žádost o nastavení určité proměnné, tato zpráva tak umožňuje ovládat dané zařízení,
4) **Get Response** (A-M) = odpověď na zprávu Get Request,
5) **Trap** (A-M) = zaslání zprávy pro Manažera v případě výskytu nestandardní, případně chybové situace. Zpráva Trap je jediná možnost, jak se může Agent ozvat bez vyzvání Manažerem.



Obr. 6.1: Spojení mezi manažerem a agentem protokolu SNMP, typy zpráv

6.2.2 Bezpečnost SNMP

Aby nemohl každý zjišťovat informace uchovávané SNMP agenty, případně dokonce ovládat činnost síťových prvků, je přístup chráněn heslem. Případně lze nastavit, že informace jsou pouze pro čtení. Základní verze protokolu SNMP v současnosti nevyhovuje požadavkům na

bezpečnost komunikace po síti, a proto byla navržena propracovanější verze SNMP v2 a v roce 1999 SNMPv3.

6.2.3 MIB (Management Information Base)

Vlastnosti různých síťových prvků jsou uspřádány do hierarchické struktury objektů, kde umístění každého objektu je definováno jeho adresou sestávající z čísel oddělených tečkami, např. 5.12.3.1.11.3.0. Toto číselné vyjádření má také své textové vyjádření, např. adrese 1.3.6.1.2.1.4 odpovídá textový řetězec iso.org.dod.internet.mgmt.mib-2.ip. V současnosti se používá MIB-II, která je podstromem obecné databáze SMI (Structure of Management Information) rozděluje objekty pro sadu protokolů TCP/IP do 10 kategorií:
- system = operační systém SNMP Agenta,
- interfaces = jednotlivá síťová rozhraní,
- at = mapování síťových a fyzických adres (Address Translation),
- ip = IP protokol,
- icmp = ICMP protokol,
- tcp = TCP protokol,
- udp = UDP protokol,
- egp = EGP protokol,
- transmission = informace o přenosových médií jednotlivých rozhraní,
- snmp = statistické informace o provozu SNMP agenta.

Databáze MIB obsahuje nejenom parametry pro daný síťový prvek společné všem výrobcům, ale i vlastnosti, které se vyskytují pouze u prvku daného výrobce. Pak samozřejmě Manažer nemůže tyto parametry znát (tedy jejich adresy), takže jediná možnost pro Manažera, jak se k hodnotám těchto vlastností dostat, je příkaz Get Next Request.

Seznam použité literatury

Monografie

[1] PUŽMANOVA, R. *Moderní komunikační sítě od A do Z.* Computer Press, ISBN 80-251-1278-0, 2006, Brno, ČR.

[2] PUŽMANOVA, R. *TCP/IP v kostce.* Kopp, ISBN 978-80-7232-236-2, 620s, České Budějovice, ČR, 2004.

[3] METCALFE, R.M., BOGGS, D.R. Ethernet: Distributed Packet Switching for Local Computer Networks. *Communications of the ACM*, vol. 19, No. 7, 1976

[4] CHOWDBURY, DHINAM, D. *High Speed LAN Technology Handbook*. Springer Verlag, ISBN 3-54066597-8, 2001

[5] SEIFERT, R. *The Switch Book: The Complete Guide to LAN Switching Technology*. John Wiley & Sons, ISBN 0-471-34586-5, 2000, USA

[6] CHAO, H.J., LIU, B. High Performance Switches and Routers. John Wiley & Sons, ISBN 978-0-470-05367-6, USA, 2007.

[7] CISCO SYSTEMS Inc. *Internetworking Technologies Handbook*. Cisco Systems, třetí vydání, ISBN 1-58705-00-13, USA, 2001

[8] PERAHIA,E., STACEY,R. *Next Generation Wireless LANs: Throughput, Robustness, and Reliability in 802.11n*. Cambridge University Press, ISBN-13 978-0-511-43688-8, UK, 2008

[9] WANG, Z. *Internet QoS : Architectures and Mechanisms for Quality of Service*. Morgan Kaufman Publishers, 2001. 240 s. ISBN 1-55860-608-4.

[10] MARCHESE, M. *QoS over heterogenous network.* John Wiley & Sons, 2007. 307 s. ISBN 978-0-470-01752-4.

[11] SZIGETI, T., HATTINGH, CH., *End-to-End QoS Network Design*. Cisco Press, ISBN 1-58705-176-1, Indianapolis, USA

[12] BIGELOW, Stehen J. *Mistrovství v počítačových sítích*. Computer Press, ISBN: 80-251-0178-9, ČR, 2004

[13] KRETCHMAN, J.s M.- DOSTÁLEK, L. *Administrace a diagnostika sítí*. Computer Press, ISBN: 80-251-0345-5, ČR, 2005

[14] WALKE,B.H., MANGOLD,S., BERLEMANN,L. IEEE 802 Wireless Systems: Protocols, Multi-hop Mesh/relaying, Performance and Spectrum Coexistence. John Wiley & Sons, ISBN-10: 0-470-01439-3, UK, 2006

[15] CROWCROFT, J., PHILLIPS, I. *TCP/IP and Linux Protocol Implementation*. John Wiley Sons ltd., ISBN 0471408824, USA, 2001

[16] SANTAMARIA,A., LOPEZ-HERNANDEZ, F.J. *Wireless LAN; Standards and Applications*. Artech House, ISBN 0-89006-943-3, UK, 2001

[17] MIANO,G., MAFFUCCI,A. *Trasnsmission Lines and Lumped Circuits*. Academic Press, ISBN 0-12-189710-9, USA, 2001

[18] PUIJE,P.D. *Telecommunication Circuit Design.* John Wiley & Sons, ISBN 0-471-41542-1, SA, 2002

[19] COLLINS,D. *Carrier Grade: Voice over IP*. Mc Graw-Hill, ISBN 0-07-136326-2, USA, 2001

[20] ŠMRHA,P., RUDOLF,V. *Interworking pomocí TCP/IP.* Kopp, ISBN 80-85828-09-X, České Budějovice 1995.

[21] DOSTÁLEK,L., KABELOVÁ,A. *Velký průvodce protokoly TCP/IP a systémem DNS*. Computer Press, ISBN 80-7226-193-2, Praha 1999

[22] DOSTÁLEK,L. a kol. *Velký průvodce protokoly TCP/IP: Bezpečnost*. Computer Press, ISBN 80-7226-513-X, Praha, 2001

Elektronické dokumenty

[23] CASTLE ROCK *Dokumentace k produktu SNMPc Network Manager*. Castle Rock, 2008 Dostupné z: <http://www.castlerock.com/products/snmpc/default.php>

[24] DILHAC, J.-M. *From tele-communicare to Telecommunications*, 2004. [cit. 05.10.2011] Dostupné na Internetu:

<http://www.ieee.org/portal/cms_docs_iportals/iportals/aboutus/history_center/conferences/che2004/Dilhac.pdf >

[25] PETERKA,J *Archiv článků a přednášek.* [cit. 18.6.2011]. Dostupné na Internetu: http://www.earchiv.cz/i_prednasky.php3, 2011.

[26] IEEE 802: *Standardy pro kabelové a bezdrátové sítě LAN a MAN*, [cit. 3.6.2011] Dostupné na Internetu: http://www.ieee802.org

[27] ETSI - www.etsi.org - materiály evropské standardizační instituce ETSI, [cit. 15.9.2011] Dostupné na Internetu: http://www.etsi.org

[28] Cisco Systems: dokumenty společnosti Cisco Systems, [cit. 8.10.2011] Dostupné na Internetu: http://www.cisco.com