

Komunikačné technológie 1

Matilda Drozdová, Ľudovít Mikuš, Peter Palúch

Predhovor

Ak si dáte vo vyhľadávači kľúčové slovo komunikačné technológie, nájdete len veľmi málo odkazov, kde by toto spojenie bolo samostatné. V prevažnej väčšine je v spojení informačné a komunikačné technológie. V minulosti oddelené odvetvia vytvárajú informačno-komunikačnú infraštruktúru pre poskytovanie elektronických komunikačných služieb. Spojením týchto odvetví sa výrazne zmenil výsledný produkt poskytovaný informačno-komunikačnou infraštruktúrou, elektronické komunikačné služby. Vnímame ich ako prirodzenú súčasť nášho života a pritom prevažná väčšina používateľov nemá a ani nepotrebuje znalosti princípov, ktoré bolo potrebné vytvoriť pre ich realizáciu.

Študenti informatiky nepatria iba k používateľom elektronických služieb. Ich budúce profesie budú vždy v určitej miere spojené s informačno-komunikačnými technológiami. Považujeme preto za potrebné, naučiť študentov informatiky aj základné princípy elektronickej komunikácie, jej vývoj a v súčasnosti používané technológie. To je zámer vyučovania predmetu Komunikačné technológie 1 vyučovanom pre študijný program informatika a počítačové inžinierstvo na Fakulte riadenia a informatiky Žilinskej univerzity v Žiline.

Vysokoškolskú učebnicu sme koncipovali z dvoch uhlov pohľadu. Prvým sú princípy komunikácie podľa teoretického modelu otvorenej komunikácie systémov OSI (*Open System Interconnection*), druhou rovinou sú komunikačné siete a ich technológie, ktoré princípy OSI modelu vždy v určitej miere využívajú. Prvú rovinu považujeme za kľúčovú, tak ako je kľúčový jazyk a písmo pre iné formy komunikácie. Tomuto pohľadu sme venovali kapitoly 1 ž 9. Sú to princípy, ktoré sa nemenia. Elektronický prenos je stále realizovaný elektromagnetickým vlnením, v rôznych technológiách sa menia iba jeho vlnové dĺžky. Signál je stále nosičom informácie, mení sa len jeho tvar a spracovanie. Komunikačné systémy sú stále využívané na prepojenie dvoch alebo viacerých používateľov. Menia sa iba spôsoby prepojovania, rýchlosť prenosu a kvalita poskytovaných služieb. K tomu sú využívané ďalšie teoretické princípy, kódovanie, šifrovanie, komprimovanie,... Druhým uhlom pohľadu sú konkrétne elektronické komunikačné siete a ich technológie. Pojem technológia je tu chápaný ako produkt, využívaný pre splnenie požiadaviek konkrétneho typu elektronickej komunikačnej siete. Tejto časti venovaná kapitola 10. Pretože technologické zmeny sa uskutočňujú veľmi rýchlo, venovali sme sa aj v tejto kapitole viac princípom vybraných, v súčasnosti najviac používaných technológií. Aktuálne technológie a ich uplatnenie v praxi budú vždy tvoriť inovovanú časť prednášok z predmetu Komunikačné technológie.

Učebnica je dielom troch autorov. Kapitoly 1 – 6 a kapitolu 10 spracovali Matilda Drozdová a Ľudovít Mikuš, Kapitoly 7 – 9 spracoval Peter Palúch.

Autori ďakujú recenzentom, Stanislavovi Marchevskému a Františkovi Jakobovi za starostlivé posúdenie rukopisu a cenné rady a pripomienky.

1 Komunikačné technológie a služby

Ciele učenia

Po štúdiu tejto kapitoly by ste mali vedieť:

- Vysvetliť vývoj IKT a ich vplyv na vývoj spoločnosti.
- Poznať význam komunikačných sietí a ich služieb pre používateľov.
- Vedieť prezentovať a vyjadriť informáciu a spôsoby jej prenosu cez elektronické komunikačné siete (analogovým signálom, digitálnym signálom).
- Porozumieť základným funkciám prenosu (prenos, adresovanie, prepojovanie/spojovanie, signalizácia) a základným parametrom elektronických komunikačných sietí (prenosová rýchlosť, oneskorenie, chybovosť).
- Poznať názvy základných technológií elektronických komunikačných sietí.

1.1 Úvod

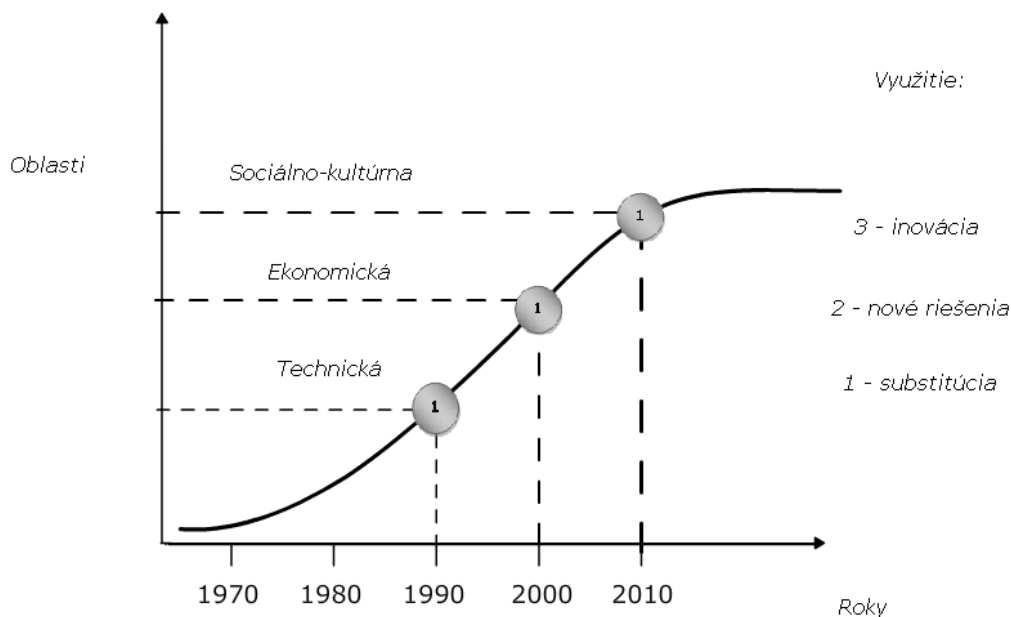
V historickom pohľade do minulosti sa rozlišujú významné vývojové tendencie rôznych časových období. V stredoveku to bol rozvoj remesiel, v 18. storočí rozvoj manufaktúr, 19. storočie je charakteristické industriálnym rozvojom, ktorý pokračoval aj v 20. storočí. Tieto zmeny boli v minulosti pravidelné a sú označované ako fázy rastu, alebo podľa ruského vedca Kondratieva ako Kondratievove cykly. V [1] sa označuje doteraz päť zásadných inovačných cyklov:

Kondratievove cykly	Približné trvanie
1. cyklus - parný stroj	1800-1850
2. cyklus - oceľ a železnica	1850-1900
3. cyklus - elektrotechnika a chémia	1900-1950
4. cyklus - petrochémia a automobil	1950-1990
5. cyklus - informačno-komunikačné technológie	1990-ca. 2010

Každá priemyselná revolúcia si okrem technologických zmien, podmieňujúcich hospodárske zmeny, vyžiadala aj zmeny spoločenské. Informačno-komunikačné technológie, ktoré najviac ovplyvňujú spoločnosť na začiatku 21. storočia nie sú výnimkou. Menia svet tak radikálne ako v minulosti parný stroj, či automobil. Sú fenoménom, ktorý svojimi možnosťami mení život našej planéty. Hovoríme o prechode zo spoločnosti industriálnej do **spoločnosti informačnej**.

1.1.1 Fázy vývoja informačno-komunikačných technológií

Vývoj informačno-komunikačných technológií z pohľadu ich uplatnenia v hospodárstve a spoločnosti možno posudzovať spôsobom, ktorý sa všeobecne používa pri difúzii nových produktov. Model S-krivky pre informačno-komunikačné technológie označuje podľa [2] tri fázy vývoja, znázornené na obr. 1.1.



Obr. 1.1 Fázy vývoja informačno-komunikačných technológií

Prvá fáza predstavuje široké nasadenie, ešte oddelených informačných a telekomunikačných technológií, vo všetkých sférach pracovného a spoločenského života. Vyznačuje sa predovšetkým použitím polovodičovej techniky a elektroniky, v spracovaní dát a automatizácii procesov. Informačné a telekomunikačné technológie substituujú buď priamo prácu človeka, alebo doterajší spôsob vykonávaných činností. Ich použitie má vplyv na zvyšovanie produktivity v procesoch produkcie a riadenia. V zmysle substitúcie sa zisťujú technické možnosti vo vzťahu k používateľskému rozhraniu.

Druhá fáza predstavuje integráciu informačnej a telekomunikačnej techniky. Výpočtové strediská sú prepájané počítačovými sieťami. Na trh sa dostávajú nové informačné a telekomunikačné technológie, ktoré rozširujú a zlepšujú využitie výpočtovej techniky a jej vzájomné využívanie na diaľku. Uskutočňujú sa experimenty ďalšieho využitia, ktoré majú aj ekonomickú dimenziu a vznikajú mnohé nové riešenia. Začína sa spoločné využívanie informačných a telekomunikačných technológií, ktoré sa označujú ako **informačno-komunikačné technológie**. V tejto fáze sa začínajú hľadať používateľsky potrebné riešenia a zabezpečenie informačného obsahu. Vedľa stúpajúcej produktivity sa zlepšuje kvalita, funkčnosť a spoľahlivosť technických systémov.

Tretia fáza sa vyznačuje okrem doterajších substitučných efektov a kvalitatívneho rastu aj inovačnými účinkami v hospodárstve a spoločnosti. Nové riešenia zasahujú do existujúcich činností a procesov tak, že ich búrajú a umožňujú nové doteraz nepoužívané riešenia a možnosti. Po zmenách v priemyselných produkčných systémoch nastávajú zmeny vo všetkých oblastiach života. Hospodársky rast a dopyt sa posúvajú od výrobkov ku informačno-komunikačným službám. Hodnota služby sa vytvára nielen využitím informačno-komunikačných technológií, ale vhodným uplatnením informačných zdrojov. Táto fáza vyžaduje okrem technického a ekonomického aspektu aj riešenie aspektu sociálno-kultúrneho. Okrem technických a implementačných problémov je to aj celková hospodárska

a politická situácia, právne aspekty umožňujúce voľný trh, jeho celkový vývoj a postoj spoločnosti k danému smerovaniu.

V poslednej fáze vývoja informačno-komunikačných technológií sa stáva najdôležitejším ich využitie v reálnom živote. To si vyžaduje poznať rovnako technológie ako aj používateľské prostredie, v ktorom sú technológie implementované.

1.2 Vývoj komunikačných technológií

Pojem komunikácia možno všeobecne chápať ako vzájomnú interaktívnu výmenu informácií medzi dvoma alebo viacerými objektmi.

Potreba komunikácie je tak stará ako ľudstvo samo. V dávnoveku to bol len ľudský hlas, neskôr v starom Sumeri asi 4 000 rokov pred našim letopočtom hlinené doštičky, v starom Egypte papyrusové zvitky, potom asi okolo roku 100 nášho letopočtu papier. Prenos takých informácií bol vždy viazaný na fyzický prenos ich nosičov. Na začiatku 21. storočia má ešte fyzický prenos nosičov informácie svoje miesto. Mení sa však forma nosičov na ktorých sú informácie prenášané. K tradičnému písanému alebo tlačenému textu na papieri pribudli elektromagnetické nosiče. V mnohých aplikáciách sú tieto nosiče veľmi obľúbené a pri ich používaní. Príkladom sú požičovne alebo predajne video kaziet a DVD. Je však pravdepodobné, že v budúcnosti bude ich používanie čoraz zriedkavejšie.

Pri pohľade do histórie zistíme, že ľudia si už dávno uvedomili možnosť prenosu informácie aj iným spôsobom ako len fyzickým prenosom nosičov, na ktorých je informácia zaznamenaná. V staroveku v niektorých situáciách sa ľudia dokázali dorozumieť pomocou optickej signalizácie zábleskami svetla, zapalovaním strážnych ohňov, dymovými signálmi apod.. Práve indiánske dymové signály predstavovali pomerne prepracovaný systém optickej komunikácie. Najvyššie vývojové štádium optických komunikačných systémov predstavoval optický Chappeov telegraf. Jeho princíp vytvorili bratia Chappeovci na jednoduchej myšlienke. Na dobre viditeľných miestach boli postavené stožiare so sústavou ramien a pák, ktoré sa mohli rôzne natáčať podľa vopred dohodnutého kľúča. Obmedzený dosah daný priamou viditeľnosťou bol riešený budovaním celého reťazca miest, kde sa informácie postupne odovzdávali. Dohodnutý kľúč umožňoval oznámenie jednoduchých správ z jedného miesta na ďalšie viditeľné miesto a postupne až k adresátovi. Takým spôsobom bol prepojený Paríž s mestom Lille vo vzdialenosti 230 km a doba prenosu správ medzi týmito dvoma mestami bol rádovo minúty. Tento systém bol najviac používaný v dobe napoleonských vojen a vydržal až do roku 1852, kedy bol nahradený telegrafom na elektrickom princípe. Princíp telegrafu bol založený na prenose elektricky, dnes skôr elektronicky spracovanej informácie, medzi dvoma alebo viacerými miestami prostredníctvom elektronickej komunikačnej siete.

Z uvedeného prehľadu vývoja v oblasti **výmeny informácií** je možné urobiť nasledovné zhrnutie elektronickej spracovanej informácie. Výmena informácií je dnes uskutočňovaná v princípe dvoma spôsobmi :

- fyzickým prenosom nosičov informácií, na ktorých je elektronicky spracovaná informácia uložená (**stand alone**),
- prenosom informácií prostredníctvom elektromagnetického signálu po elektronických komunikačných sieťach, ktorý označujeme pojmom **elektronická komunikácia**.

Fyzický prenos nosičov informácie má tieto nedostatky: samotný prenos je časovo zrovnateľný s prenosom klasickou poštou, informácie nie je možné jednoducho aktualizovať a využívať v reálnom čase. Preto sa pozornosť rozvoja prenosu informácie sústredila na prenos informácie prostredníctvom elektromagnetického signálu po rôznych typoch **elektronických komunikačných sietí**, poskytovaním rôznych informačných resp. informačno-komunikačných služieb.

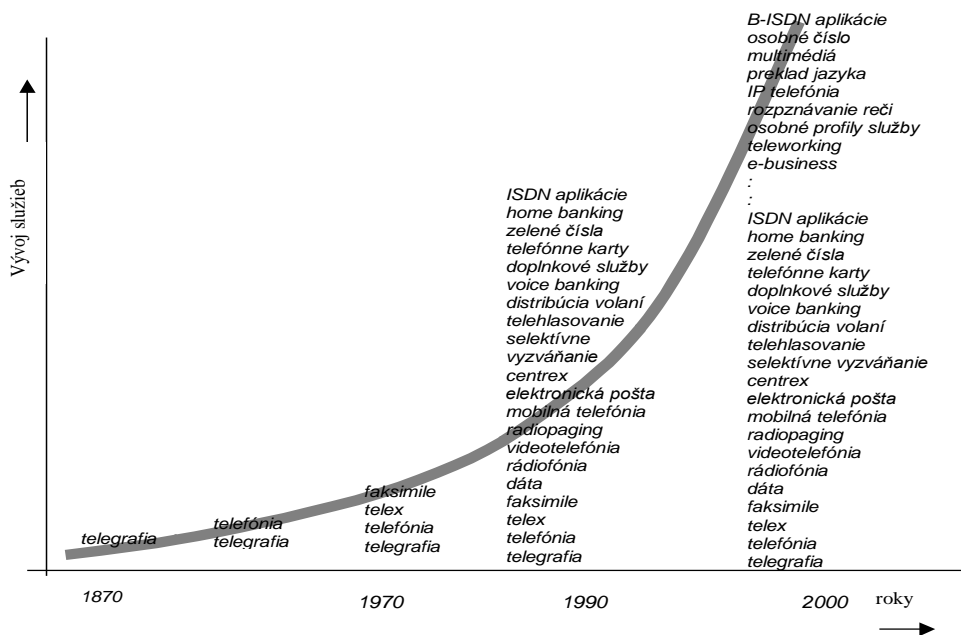
1.3 Informačno komunikačné služby

1.3.1 Vývoj informačno-komunikačných služieb

Začiatok vývoja informačno-komunikačných (IK) služieb je spojený s pojmi telekomunikačné a rádiokomunikačné služby, podľa názvov elektronických komunikačných sietí. K telekomunikačným službám patril telefón a telegraf prevádzkovaný po telefónnej a telegrafnej sieti, ku rádiokomunikačným službám rádiové a televízne vysielanie, prevádzkované po televíznych a rádiových sieťach. Takéto členenie vyplynulo zo skutočnosti, že sa jednalo o dva rozdielne princípy prenosu, po rôznych typoch komunikačných sietí. Telekomunikačné služby boli prevádzkované po drôtových sieťach, rádiokomunikačné služby po bezdrôtových sieťach.

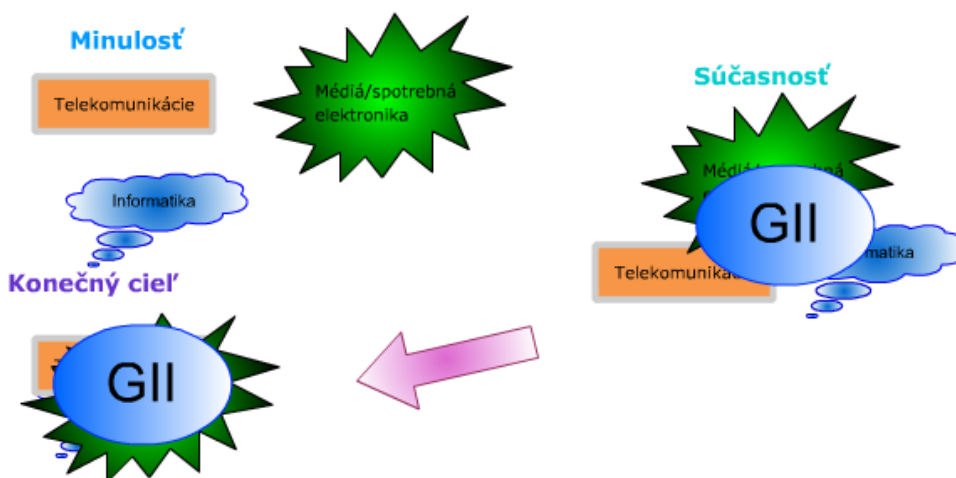
Rozvoj ďalších informačno-komunikačných služieb umožnili hlavne produkty výpočtovej techniky a informatiky, spolu so zvyšovaním prenosovej rýchlosti komunikačných sietí. Na základe možností integrácie informačných a telekomunikačných technológií špecifikuje štandardizačná organizácia CCITT (z francúzskeho *Comité Consultatif International Téléphonique et Télégraphique*) v roku 1980 pojem telematické služby. Týmto názvom označuje skupinu služieb Telex, Teletex, Telefax a Videotex. Neskôr sa do tejto kategórie služieb zaraďovali aj ďalšie služby, vytvárali sa rôzne iné kategórie služieb podľa rôznych kritérií a pre rôzne použitie. Dnes sa tieto služby všeobecne označujú ako **informačno-komunikačné služby**.

Vznik informačno-komunikačných služieb je výsledok výrazných technologických zmien v oblasti informačných a komunikačných technológií. Dochádza k rapídne spojovaniu a stieraniu rozdielnosti medzi zberom, prenosom, uložením a spracovaním informácie, ktoré umožňuje vytváranie rôznych služieb pre využívanie tak v privátnom živote, ako aj v podnikovej praxi. Ich počiatočný vývoj v časovom horizonte je znázornený na obr. 1.2 a označenia sú prevažne z používateľského hľadiska.



Obr. 1.2 Vývoj informačno-komunikačných služieb

Vznik **informačno-komunikačných služieb** je dôsledok konvergencie technológií troch odvetví, znázornených podľa [3] na obr. 1.3. Telekomunikácie, informatika/ výpočtová technika a médiá vrátane spotrebnej elektroniky, postupne vytvárajú jeden celok. Minulosť je prezentovaná oddelenou činnosťou jednotlivých odvetví, súčasnosť predstavuje čiastočné približovanie všetkých troch typov odvetví na začiatku 21. storočia, budúcnosť je vytvorená integráciou všetkých troch odvetví do Globálnej informačnej infraštruktúry (GII). Pojem GII pojem označuje infraštruktúru potrebnú k poskytovaniu služieb, ktoré vyžadujú elektronické spracovanie, uchovanie, prenos a prezentovanie informácie. **Informačná infraštruktúra** zahŕňa všetky technické produkty, potrebné na poskytovanie informačno-komunikačných služieb. Patria sem elektronické komunikačné siete, koncové zariadenia, hardvérové a softvérové produkty pre podporu služieb a spracovanie informácie a často je označovaná aj pojmom **informačno-komunikačná infraštruktúra**.



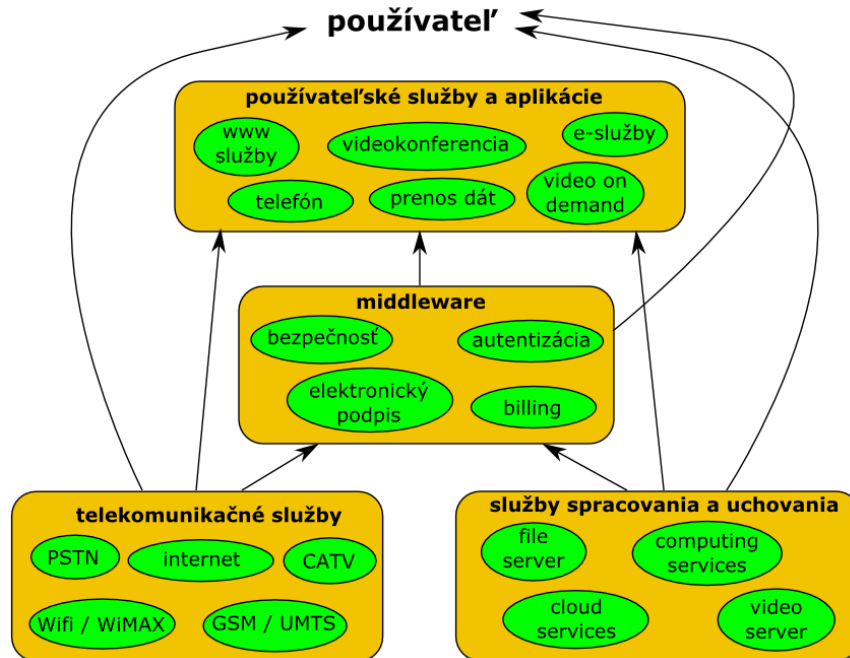
Obr. 1.3 Konvergencia odvetví telekomunikácie, informatika / výpočtová technika a médiá

Možnosti, ktoré bude v budúcnosti informačná infraštruktúra poskytovať sa dajú iba predpokladať. Sú prezentované hlavne novými multimediami službami poskytovanými po širokopásmových elektronických komunikačných sieťach. Oproti minulosti sa mení relatívna hodnota úloh tvorcov informačno-komunikačných služieb. Menia sa zásadne hodnoty jednotlivých tvorcov informačno-komunikačných služieb. Zdôraznená je úloha poskytovateľa informácie. Ten zaujíma podľa [3] v priemere 30% až 35% celkovej vytvorenej hodnoty, zatiaľ čo poskytovateľ služby prenosu dosahuje iba 6 - 8 % vytvorenej hodnoty a v budúcnosti sa bude tento rozdiel ešte zvyšovať. Tento fakt zdôrazňuje relatívnu hodnotu informačného obsahu verzus komunikácia.

1.3.2 Základné kategórie informačno-komunikačných služieb

Vybudovanie informačnej infraštruktúry je základným predpokladom poskytovania IK služieb. Koncový používateľ však nevníma informačnú infraštruktúru iba ako technický systém, ale ako prostriedok pre využitie určitej služby. K tomu si vyberá príslušnú komunikačnú sieť, príslušného operátora siete alebo poskytovateľa služby. Pojmom služba je označované mnoho rôznych produktov informačno-komunikačných technológií. Niektoré zo špecifikácií sú uvedené ďalej.

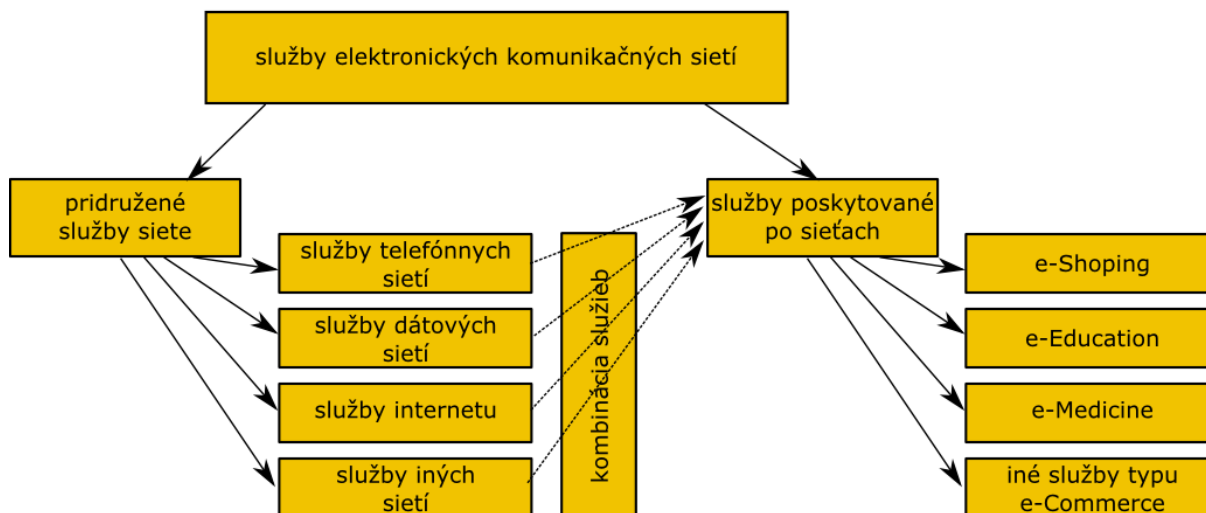
Štruktúrálny model služby podľa odporúčania Medzinárodnej telekomunikačnej únie (*International Telecommunication Union*) ITU Y.110, znázornený na obrázku 1.4., dáva vysvetlenie rôznych druhov informačno-komunikačných služieb a ich poskytovateľov.



Obr. 1.4 Štruktúrálny model informačno-komunikačných služieb

Konečným produktom informačnej infraštruktúry je vždy poskytovanie služby. Tvorcovia služieb hľadajú technické prostriedky pre jej uskutočnenie. Vzniká tak hodnotový reťazec, ktorý je čiastočne znázornený v štruktúrálnom modeli. V tomto hodnotovom reťazci však nie je zahrnutá hodnota prenášanej informácie a jej využitie. Práve tá je v poslednom

období spájaná s pojmom informačno-komunikačných služieb. Z tohto pohľadu sú služby podľa odporúčania Európskej komisie EK COM393 rozdelené do dvoch základných skupín: **služby pridružené ku elektronickej komunikačnej sieti a služby poskytované po sieti**. Ich rozlíšenie a príklady sú znázornené na obr. 1.5.



1.5. Základné členenie informačno-komunikačných služieb

Vytváranie uvedených dvoch typov služieb má inú koncepciu. V službách pridružených k sieti sa služby vytvárajú podľa možností technológie, nezávisle na potrebách používateľov. Takto vytvorené služby neboli v minulosti vždy úspešné. Niektoré zo služieb používatelia prijali a sú rozšírené, napríklad mobilná telefónna služba, iné ako služba videotexu, alebo teletexu sa v Slovenskej republike ani nikdy neprevádzkovali.

Služby poskytované po sieti sú služby odlišného typu a nevyhnutne súvisia s hodnotou prenášanej informácie a jej využitím pri tvorbe ďalšieho produktu (výrobku alebo služby). K tvorbe týchto služieb je nevyhnutná spolupráca odvetví informačno-komunikačných technológií a odvetvia v ktorom má byť služba implementovaná. Sú to dve rozdielne prostredia, ktoré musia spolupracovať, pokiaľ chcú byť obaja úspešní. Vytvárajú navzájom spoločný podnik, v ktorom je potrebné poznať jeho štruktúru a špecifikovať jednotlivé úlohy. Rozhrania jednotlivých častí je potrebné špecifikovať vytvorením pravidiel pre spoločný postup tvorby služieb, ktoré sú označované ako e-služby, alebo služby typu e-commerce či e-biznis.

1.4 Zmeny spoločnosti vyvolané informačno-komunikačnými technológiami

1.4.1 Trh informácií

Informačno-komunikačné technológie otvorili nový priestor pre trh informácií. Ten mení radikálne svoju predošlú podobu tým, že elektronicke spracovaná informácia sa stáva produktom pre obchodovanie. Produktom k distribúcii, vyhľadávaniu a výmene informácií sú informačno-komunikačné služby.

Aby sa dosiahol ekonomický pohyb elektronicky spracovaných informácií, je potrebný konkurenčný trh. Pre jeho vytvorenie bola ako prvá uskutočnená **liberalizácia** komunikačných sietí a koncových zariadení, v spojení s revíziou noriem a pravidiel, ktoré sú využívané v počítačovom a mediálnom odvetví. Rozvoj trhu informácií si následne vyžiadala liberalizáciu aj na úrovni informačno-komunikačných služieb.

Spolu s liberalizáciou bola potrebná aj **regulácia**, umožňujúca ochranu ovládnutia trhu informácií. Zrovnoprávnenie pravidiel medzi rozdielnymi časťami trhu informácií a rôznorodosť účastníkov, ktorí chcú v ňom participovať, vyžaduje však minimalizáciu regulácie, aby nedošlo k narušeniu prirodzeného vývoja trhu. Regulačné orgány kladú dôraz na zabezpečenie toho, aby zákazníci mali možnosť výberu a aby mali prospech z ekonomiky tohto nového trhu. Pre získanie dôvery k využívaniu nových informačno-komunikačných služieb je potrebné zabezpečiť ochranu súkromia ľudí, obchodných informácií, autorského práva publikovaného materiálu a iných práv intelektuálneho vlastníctva. Tieto skutočnosti však nesmú vyvolať obmedzovanie produkcie a manažmentu informácie a jej prenosu. Ďalej je potrebné **zabezpečenie informácie** pred jej neoprávneným získaním a zneužitím. Túto skutočnosť chráni zákon o elektronickom podpise, ktorý je prijatý vo väčšine vyspelých krajín.

Trh informácií nie je oddelený trh, ale je súčasťou viacerých spolupôsobiacich trhov. Vyváženie ponuky a dopytu prostredníctvom nových informačno-komunikačných služieb patrí medzi rozhodujúce faktory jeho úspešného rozvoja.

1.4.2 Zmena spoločnosti

Ako sa v budúcnosti zmení život ľudí vplyvom informačno-komunikačných technológií je dnes možné iba odhadovať. Všeobecne sa predpokladá, že aktivity v rozličných oblastiach života jednotlivca sa budú v budúcnosti meniť a mnohé tradičné rozdiely sa budú strácať. Spoločenské zmeny a rozvoj informačno-komunikačnej infraštruktúry sú previazané, pretože sa budú vzájomne podnecovať a navyše jedno sa nemôže uskutočňovať bez druhého.

Využívaním informačno-komunikačných technológií sa zmení napríklad rozdiel medzi vzdelávaním a prácou, rozdiel medzi prácou a odpočinkom. Doterajší oddelený spôsob, práca a domov, sa opäť zmení na spôsob pred priemyselnou revolúciou. Pracovný život sa stane viac rozmanitejší, pravdepodobne viac prepletený s domácim životom, práca profesionála doma sa stane viac všednou vecou. Rôzne experimenty on-line práce uvedené v [4] ukazujú na mnoho výhod. Najdôležitejšia je väčšia spokojnosť v zamestnaní a menšie stresy. V niektorých prípadoch sa uvádza zlepšenie nárastu produktivity až o 30 %. Ďalším prínosom je pružnosť pracovnej doby a zlepšenie životného prostredia tým, že sa zníži dochádzanie do zamestnania. Samozrejme sú tu aj isté nevýhody a to sú v súčasnosti veľké náklady na prenos informácie, nákup a údržbu potrebných koncových zariadení. Ďalším faktom je skutočnosť, že pracovanie na diaľku nenahradí blízkosť spolupracovníkov, ktorá je v niektorých prípadoch tvorivej práce nevyhnutná. A nakoniec dnes budované byty a domy málokedy rátajú pri architektonickom riešení s možnosťou práce doma.

Okrem zmien v práci sa zmení aj úroveň vzdelania požadovaná od všetkých typov obyvateľstva a zvýši sa časové obdobie nadobudnutia potrebného vzdelania. Potreby vzdelávania budú hrať kritickú úlohu vo vývoji informačnej spoločnosti, pretože potreby na pružnejšie učenie a učenie presne na mieru, k okamžitej potrebe v pracovných činnostiach vytvára pružnejší a efektívnejší pracovný život. V tom bude zohrávať čoraz významnejšiu úlohu e-vzdelávanie ako nástroj kontinuálneho celoživotného vzdelávania. Metódy e-vzdelávania musia však byť ekonomické a aj efektívne v porovnaní s existujúcimi vyučovacími metódami. Tieto dôvody vytvárajú doteraz najväčšie zábrany na široké využitie informačno-komunikačnej infraštruktúry pre vzdelávanie.

Ak predošlé dva príklady zmien spoločnosti uvedené v [4] nie sú ešte veľmi rozvinuté, ďalší príklad z predpokladov v roku 1999 je už prítomný hlavne vo vytváraní sociálnych sietí. Uvedený citát predpokladov je už realizovaný: *„Pre určité záujmy istých spoločenských skupín bude možné vytváranie virtuálnych spoločenstiev, či už v rámci riešenia osobných alebo kultúrnych a etnických záujmov. Ďalej bude možné ponúkať nové príležitosti pre lokálne skupiny/ komunity, hľadať špeciálne potreby spoločenských segmentov ako sú starší občania a invalidi a urobiť podľa potrieb špeciálne služby pre potrebu jednotlivcov v rámci týchto skupín. To umožní ľuďom obracať sa na radu k profesionálom z rôznych oblastí, od rady na podávanie liekov až po hľadanie ľudí s rovnakými záujmami. Pre tieto spoločenské skupiny je záujem druhých to najdôležitejšie aj keď je to len prostredníctvom elektronickej komunikácie.“*

1.5 Prenos informácie v elektronickej komunikácii

1.5.1 Správa

Informácia, ktorú chceme pri elektronickej komunikácii preniesť je spracovaná vo forme správy. Je to tvar, v ktorom chceme uskutočňovať prenos informácie. Každú správu možno posudzovať z troch aspektov:

1. vlastného informačného významu - sémantizmu,
2. formálnej skladby – syntaxe,
3. praktického využitia.

Pre prenos a spracovanie správy má najpodstatnejší význam formálny spôsob vyjadrenia správy - syntax. Správa je tvorená usporiadaným súborom prvkov správy. Zdroj správy obsahuje abecedu zdroja správy, z ktorej sa vytvára správa. Abeceda zdroja správy je napríklad slovenská abeceda vytvorená z daného počtu písmen a čísiel. Takýmto zdrojom je možné vyjadriť textovú správu, napríklad písaný list. Hudobná skladba pri audio správe je zaznamenaná z určitého počtu tónov. Iným príkladom je dvojprvková abeceda zdroja na vyjadrenie správy stavu určitého zariadenia (zapnuté – vypnuté).

Formu správy si volí odosielateľ informácie. Tým môže byť človek alebo stroj pre spracovanie informácií. Informácia zo zdroja je prenášaná k príjemcovi správy, ktorým rovnako môže byť človek, alebo stroj.

Prenášaná správa musí mať náhodný charakter prenášaných prvkov správy. Prenos by nemal zmysel, keby sa prenášali vždy rovnaké prvky správy. Príjemca správy musí však vopred poznať, aké typy a formy správ môžu byť vysielané zo zdroja. Nevie ale, ktorá podmnožina prvkov abecedy zdroja danú správu tvorí.

1.5.2 Informácia

Dôvodom všetkých spôsobov komunikácie je výmena informácií medzi komunikujúcimi subjektmi. Informácia umožňuje príjemcovi prechod zo stavu neviem do stavu viem. Prináša mu určitý nový poznatok. V tejto učebnici budeme uvažovať výmenu informácie prostredníctvom elektronickej komunikácie, ktorý označujeme ako prenos informácie. Veda, ktorá sa zaoberá princípmi výmeny informácií prostredníctvom elektronickej spracovanej informácie sa nazýva teória oznamovania. Informácia v teórii oznamovania je chápaná ako obraz reálneho sveta vyjadrený vo forme správy zloženej z prvkov abecedy zdroja správy. Množstvo informácie v správe sa hodnotí pomocou pravdepodobnosti prijatých prvkov abecedy zdroja pri prenose. Množstvo informácie v správe je tým väčšie, čím je menšia pravdepodobnosť výskytu prvkov správy. Správa ktorá obsahuje prvky s veľkou pravdepodobnosťou výskytu, nesie malé množstvo informácie.

Množstvo informácie I obsiahnuté v jednom prvku abecedy zdroja je dané vzťahom:

$$I(x_i) = \log_2 \frac{1}{p_i} = -\log_2 p_i = -\log_2 \frac{1}{x_i}$$

kde $1/x_i$ je pravdepodobnosť p_i výskytu prvku x_i .

Ak je pravdepodobnosť výskytu jednotlivých prvkov zdroja správy rôzna, počíta sa priemerné množstvo informácie ako stredná hodnota náhodnej veličiny. Stredná hodnota náhodnej veličiny je daná vzťahom:

$$E(x) = \sum_i x_i p_i$$

kde p_i je pravdepodobnosť výskytu i -teho prvku.

Stredná hodnota množstva informácie H , obsiahnutého v jednom prvku abecedy zdroja sa potom počíta podľa vzťahu:

$$H = -\sum_i p_i \log_2 p_i$$

Stredná hodnota množstva informácie H obsiahnutá v jednom prvku abecedy zdroja sa nazýva aj entropia zdroja správy a vyjadruje priemernú výdatnosť zdroja informácie.

Ak majú všetky prvky abecedy zdroja rovnakú pravdepodobnosť výskytu, počíta sa maximálne množstvo informácie H_{\max} , pripadajúce na jeden prvok abecedy zdroja informácie. Je dané vzťahom:

$$H_{\max} = \log_2 s$$

kde s je počet prvkov abecedy zdroja. Jednotka množstva informácie sa nazýva podľa amerického vedca C. E. Shannona, 1 Shannon, skratka [Sh].

Pre dva prvky zdroja správy, ktoré majú rovnakú pravdepodobnosť výskytu prvkov správy, sú maximálne množstvo informácie H_{\max} aj entropia H rovnaká hodnota, 1 Sh.

Poznámka: V minulosti sa jednotka množstva informácie označovala názvom bit.

Jednotka množstva informácie označená bit sa nazýva tiež technický bit a formálne je zhodná s definíciou dvojkovej jednotky (skratky dvojkového čísla binary digit – bit) z oblasti počítačovej techniky, kde znamená dvojestavové miesto v elektronickej pamäti, alebo v kódovej značke. Preto sa označenie množstva informácie zmenilo na Shannon [Sh]. Skupina 8 bitov sa nazýva byte [bajt], a používa sa pre účely ďalšieho spracovania informácie.

V ekonomických pojmoch sa používa pojem hodnota informácie. Týmto pojmom sa označuje hodnota informačného obsahu, z hľadiska jej ďalšieho praktického použitia. Pojem hodnota podľa ekonomických kritérií je špecifikovaná rôzne. Jedna zo špecifikácií je, že všeobecná hodnota produktu je daná jeho vzácnosťou. Potom je tento pojem v zhode so shanonovskou interpretáciou informácie. Hodnota informácie je tým väčšia, čím je menej známy jej informačný obsah pre ďalšie praktické použitie. Hodnota informácie je závislá na situácii, čase, mieste, predchádzajúcej skúsenosti apod. Napríklad správa, že televízne noviny sú vysielané pravidelne o 19.30 hodine, má menšiu hodnotu informácie pre tých ktorí sledujú tento program, ako pre tých, ktorí ho nesledujú. Pre ďalšie ekonomické zhodnotenie sú však dôležitejšie informácie z televíznych novín, ktoré môžu pomôcť napríklad pri realizácii obchodných aktivít. Takto chápaný pojem hodnoty informácie nemá pre teóriu oznamovania význam. Jej význam je dôležitý pri realizácii informačných služieb po komunikačných sieťach.

Hodnota množstva informácie resp. entropie nie je ekvivalentná s pojmom hodnota informácie. Hodnota množstva informácie, resp. entropie súvisí s počtom výskytu prvkov správy. Údaj o hodnote množstva informácie slúži k účelom prenosovej, meracej a riadiacej techniky, napríklad k dimenzovaniu prenosových kanálov. Pojem hodnota informácie je dôležitá pri ďalšom využití informačného obsahu.

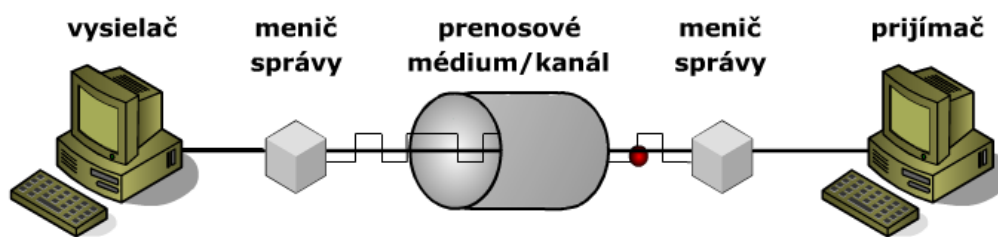
1.5.3 Prenosový reťazec

Ako už bolo uvedené, príkladom vyjadrenia určitej informácie je akákoľvek napísaná veta, fotografia, alebo videozáznam. Všeobecne sa informácia vyjadruje v štyroch základných typoch:

- hlas

- text
- obraz
- dáta.

Keď chceme takto vyjadrenú informáciu preniesť v elektronickej forme, musíme ju zmeniť na formu, ktorá takýto prenos umožňuje. Elektronicky spracovaná správa sa prenáša cez prenosové médium resp. prenosový kanál ako elektromagnetický signál. Schematické vyjadrenie prenosu od zdroja správy k prijímaču správy podľa obr. 1.6 sa označuje základný **prenosový reťazec**.



Obr. 1.6 Základný prenosový reťazec

Vytvorenie prenosového reťazca v elektronickej komunikácii znamená realizovať komunikačný okruh, ktorý umožňuje prenos správ medzi dvoma miestami bez ohľadu na druh použitých technických prostriedkov.

1.5.4 Elektromagnetické signály pre prenos informácie

Pri prenose informácie v komunikačných sieťach sa používajú dva základné tvary signálov:

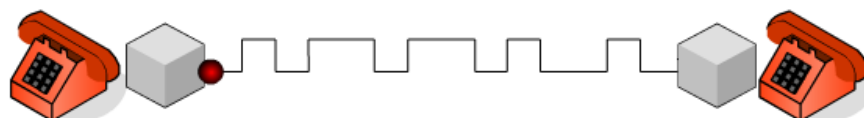
- analógový
- digitálny.

Analógový signál môže nadobúdať nekonečné množstvo spojitéch hodnôt v čase. Ilustračný priebeh signálu pri prenose komunikačným kanálom je možné vyjadriť podľa obrázku 1.7.



Obr. 1.7 Prenos analógového signálu

Digitálny signál je charakterizovaný ako veličina nespojitá v čase a nadobúda len určitý konečný počet hodnôt. Špecifickým prípadom digitálneho signálu je binárny, dvojstavový signál. Nadobúda iba dva stavy 0 a 1. Jeho ilustračný priebeh je znázornený na obr. 1. 8.



Obr. 1.8 Prenos digitálneho signálu

1.5.5 Analógový a digitálny spôsob prenosu

Z vedomostí získaných v úvode kapitoly je známe, že prvá služba elektronického prenosu správ bol telegraf. Prvý telegraf na elektrickom princípe bol Morseho telegraf, ktorý používal krátke a dlhé prúdové impulzy. Neskôr bol používaný telegraf s 5 prvkovou telegrafnou abecedou vytvorenou z 0 a 1. Bol to prenos digitálneho signálu a tento princíp je používaný i dnes v digitálnych systémoch. Používané sú len iné abecedy, dnes nazývané kódy.

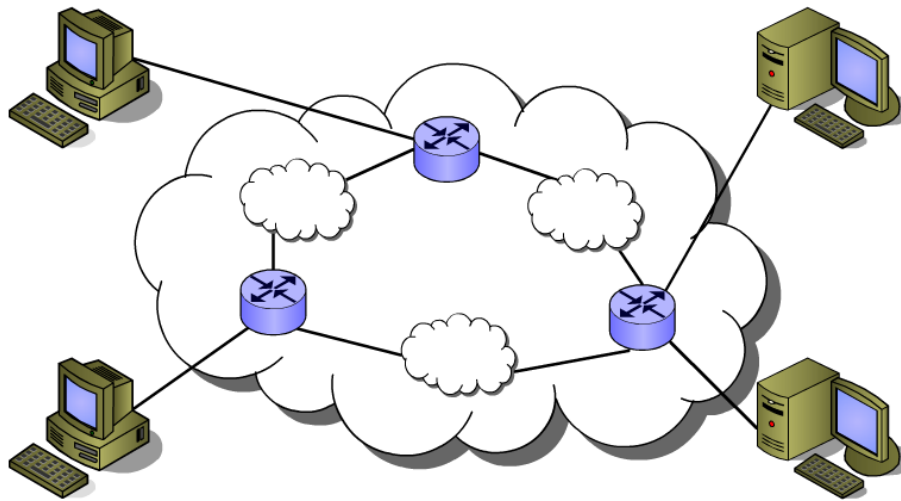
Ďalšia v postupe vývoja bola telefónna služba, ktorá sa od svojho vzniku budovala ako služba s analógovým prenosom signálu. Dôvodom bola tá skutočnosť, že nebol známy spôsob digitalizácie ľudského hlasu. Prenos hlasu v analógovej technike je podstatne zložitejší. Akustické záchvevy hlasu sa menia na analógové elektromagnetické kmity. Tieto kmity sa v analógovom spôsobe prenosu prenášali prenosovým kanálom kontinuálne vo frekvenčnom rozsahu 3,1 kHz. Dnes sa i prenos hlasu digitalizuje. Dôvodom je skutočnosť, že digitálne prenosy majú mnoho predností pred analógovými. Digitálny prenos je lepší pre prenos v tom zmysle, že prenášanú veličinu dokáže preniesť presnejšie, s menšími chybami, skreslením a šumom. Analógové prenosy sú vždy nejakým spôsobom skreslené, zaťažené šumom atď.. Postupne všetky komunikačné siete pracujú na digitálnom princípe. Technológia a techniky analógového prenosu sú síce dokonale vyriešené, ale sú technicky náročné a drahé, v porovnaní s digitálnym prenosom a digitálnym spracovaním informácie. Ďalší dôvod digitalizácie sietí je ten, že komunikačná technika využíva prvky mikroelektroniky, ktoré spracovávajú digitálny signál. Rovnako sú dnes pri prenose informácie používané na rôznych miestach komunikačných sietí zariadenia výpočtovej techniky a tá pracuje s digitálnym signálom.

Nemožno povedať, že by prenos digitálneho signálu bol absolútne ideálny, ale je jednoduchší a zaťažený menšou mierou nepresností ako signál analógový.

1.6 Vytváranie sietí

V praxi by bolo neefektívne vytvárať priame komunikačné kanály, podľa základného prenosového reťazca znázorneného na obr. 1.6, od každého zdroja správy ku každému prijímaču správy. Preto sa pre prenos informácií vytvárajú elektronické komunikačné siete, ktoré umožňujú vytvárať komunikačné kanály od ľubovoľného zdroja k ľubovoľnému prijímaču vždy vtedy, keď je požadovaný prenos informácie. Pojem **elektronická komunikačná sieť** tak označuje technický systém umožňujúci spracovanie, uloženie a prenos informácie v určitom rozľahlom priestore. Technický systém je vytváraný vzájomným

prepojovaním rôznych systémov v uzloch siete. Znázornenie komunikačnej siete v rozľahlom priestore je na obr. 1.9.



Obr. 1.9 Model elektronickej komunikačnej siete v územne rozľahlom priestore

Informácia v elektronickej komunikačnej sieti je prenášaná z jedného koncového zariadenia k druhému koncovému zariadeniu prostredníctvom komunikačného kanála. Ten je vytvorený cez medziláhlé systémy siete. V niektorých prípadoch je informácia v sieti na určitý čas uložená. Komunikačný kanál sa vytvára podľa požiadaviek koncového zariadenia zdroja. Pojem komunikačný kanál (channel), vyjadruje jednosmernú spojovaciu cestu. Obojsmerná cesta sa označuje ako komunikačný okruh, (circuit). Prenos informácie sa uskutočňuje po prenosových médiách, ktoré sú prepojené uzlami siete. Prenosový kanál je vytváraný podľa smerovania v uzloch siete.

1.6.1 Koncové zariadenia

Koncové zariadenie je posledným článkom komunikačného kanála. Tvorí rozhranie medzi koncovým používateľom a komunikačnou sieťou.

1.6.1.1 Funkcie koncových zariadení

Koncové zariadenia sú zdrojom a prijímačom správy. Ich úlohou je zabezpečiť nasledovné funkcie:

- premeniť informáciu vyjadrenú vo forme správy na elektromagnetický signál,
- upraviť signál do tvaru potrebného pre prenos k ďalšiemu prvku siete,
- premeniť prijatý elektromagnetický signál na požadovaný informačný typ,
- vytvoriť komunikačný kanál,
- dohliadať na vytvorené spojenie,
- dať pokyn na ukončenie spojenia.

1.6.1.2 Typy koncových zariadení

Existuje celý rad koncových zariadení buď pre konkrétnu službu alebo pre konkrétnu sieť. Medzi klasické koncové zariadenia elektronických komunikačných sietí patria:

- telefón,
- rádio prijímač,
- televízny prijímač,
- telefaxový prístroj,
- počítač,
-

Koncové zariadenia prechádzajú v súčasnosti rozsiahlym vývojom. Konvergencia sa v oblasti koncových zariadení vedie na univerzálny prijímač použiteľný pre akýkoľvek typ informačno-komunikačnej služby. U pevných komunikačných sietí dochádza k zblížovaniu televíznych prijímačov vybavených set-top boxmi a personálnych počítačov so zabudovanými zvukovými a video kartami. V oblasti mobilných sietí sú mobilné telefóny vybavované čoraz výkonnejšími procesormi s vlastným operačným systémom a výkonným zobrazovačom, na druhej strane PDA (*Personal Digital Assistant*) a počítače podporujú hlasové služby. Funkčné vlastnosti oboch trendov sú v podstate identické. Predpokladá sa používanie univerzálnych koncových zariadení pre rôzne typy informačno-komunikačných služieb.

1.6.2 Funkcie elektronických komunikačných sietí

Základnou úlohou elektronickej komunikačnej siete je vzájomná výmena informácií medzi dvomi koncovými používateľmi, realizovaná medzi vysielačom a prijímačom cez prenosový okruh resp. kanál. Komunikačný kanál sa vytvára v elektronických komunikačných sieťach spojením viacerých medziľahlých uzlov. K vytvoreniu komunikačného kanála medzi dvomi koncovými zariadeniami v komunikačnej sieti je potrebné zabezpečiť základné funkcie elektronickej komunikačnej siete, ktorými sú:

- prepojovanie (*switching*)
- smerovanie (*routing, forwarding*)
- adresovanie (*addressing*)
- signalizácia (*signaling*)
- prenos (*transmission*).

Prepojovanie a smerovanie sú veľmi úzko spojené a ich rozlíšenie je pomerne problematické pri prvom vysvetlení týchto pojmov. Nie sú to rovnaké funkcie a ich vysvetlenie je možné z viacerých pohľadov.

Prepojenie (*switching*) zabezpečuje, že informácia ktorá prichádza do medziľahlého uzla, odíde z neho k ďalšiemu uzlu tak, aby mal používateľ vytvorený komunikačný kanál. Princíp prepojovania príslušných uzlov je odlišný v rôznych používaných technológiách (tradičné telefónne siete, LAN, internet). Zariadenia, ktoré realizujú prepojenia sa nazývajú prepojovače – switches.

Smerovanie (*routing/forwarding*) je ďalšia funkcia, ktorá musí byť vykonávaná v uzle siete. Prostredníctvom smerovania sa vyberá prenosová cesta pre vytvorenie kanála, ktorou pôjde informačný tok z vysielача do prijímateľa informácie. Výber tejto cesty sa určuje podľa smerovacieho algoritmu. Rozdiel medzi routingom a forwardingom je v tom, že forwarding zabezpečuje prenos z prichádzajúceho smeru do odchádzajúceho smeru len v jednom uzle, kým routing zahrňuje všetky sieťové uzly, ktoré sú vo vzájomnej interakcii pri prenose zo zdroja do cieľa prenosu. Forwarding používa jednoduchší smerovací algoritmus ako routing. Zariadenia, ktoré realizujú smerovanie sa nazývajú routers. V niektorých technológiách vykonávajú prepojovalče aj funkciu smerovania, napríklad v internete je potom zariadenie pre smerovanie označované ako IP switch.

Adresovanie (*addressing*) slúži na jednoznačné určenie cieľa prenášanej informácie. Je to funkcia, ktorá obsahuje informácie pre uskutočnenie smerovania a prepojenia v uzle siete. Ďalší uzol kanála je vybraný na základe adresy prijímateľa. Adresa koncového zariadenia má presne definovanú štruktúru, na základe ktorej je vytvorený komunikačný kanál. K tomu, aby bol požadovaný cieľ identifikovaný, musí mať pridelenú určitú identifikáciu (meno, číslo, adresu). Adresovanie slúži aj na identifikáciu niektorých iných prvkov siete. Adresy majú priradené používateľské koncové zariadenie i uzly siete. Uzol v sieti je identifikovaný svojou adresou, identifikačným číslom, identifikátorom, a pod. Používateľské koncové zariadenia sú identifikované účastníckym číslom, IP adresou, a pod., v závislosti od typu siete. Rôzne typy komunikačných sietí majú rôzne spôsoby adresovania a pri spolupráci rôznych typov sietí je potrebné adresy konvertovať.

Signalizácia (*signalizing*) v komunikačných sieťach znamená výmenu riadiacich informácií. Prostredníctvom signalizácie a podľa údajov nastavených v smerovacích tabuľkách je uskutočnené prepojenie vstupu uzla s výstupom. Prepojovanie tak obsahuje dve funkcie smerovanie a signalizáciu. Signalizácia špecifikuje súbor riadiacich signálov a tieto signály sú prenášané za účelom zostavovania, udržiavania a zrušenia spojenia. Signalizácia bola základnou podmienkou prevádzky sietí od ich začiatku. Príkladom sú prvé telefónne ústredne, kde účastník krútením kľuky generoval striedavý prúd, aby spojovateľka vedela, že chce byť spojený s iným účastníkom. Iné riadiace informácie, napríklad telefónne číslo sa prenášali ústne. Signalizáciu dnes používajú telefónne siete a siete ATM – Asynchronous Transfer Mode.

Prenos (*transmission*) informácie po komunikačnej sieti je vlastný prenos signálu po komunikačnom kanáli medzi dvoma koncovými zariadeniami. Prenos signálu je podrobnejšie spracovaný v kapitole 3.

Okrem základných funkcií majú komunikačné siete mnoho ďalších funkcií. Napríklad:

- riadenie výmeny informácií, čo znamená organizáciu prenosu informácie medzi zdrojom a cieľom,
- detekcia a korekcia chýb, ktoré vznikajú počas prenosu,
- zabezpečenie informácie pred zneužitím,
-

1.6.3 Parametre elektronickej komunikačnej siete

Vyššie uvedené funkcie nie sú priamo vnímané používateľom komunikačnej siete pri používaní služieb elektronických komunikačných sietí. Viac sú vnímané parametre siete, ktoré určujú kvalitu poskytovanej služby. Základné parametre siete, podstatné pre používateľa sú:

- prenosová rýchlosť signálu,
- oneskorenie signálu,
- chybovosť.

Prenosová (dátová) rýchlosť (*Bit rate, data rate*) je všeobecne definovaná maximálnym množstvom informácie, ktoré môže preniesť signál za časovú jednotku.

Maximálne množstvo informácie bolo definované v podkapitole Informácia vzťahom

$$H_{\max} = \log_2 s$$

kde s je počet prvkov abecedy zdroja. Pri prenose informácie číslicovým signálom je maximálne množstvo prenášanej informácie vyjadrené počtom jeho stavov N .

Vyjadrenie prenosu signálu za jednotku času sa udáva prostredníctvom symbolovej rýchlosti.

Symbolová (modulačná) rýchlosť (*symbol rate, modulation speed, Baud rate*) vyjadruje počet zmien signálu za sekundu. Symbol môže predstavovať napríklad jeden impulz. Je definovaná ako prevrátená hodnota najkratšieho časového intervalu, ktorý je prenosový systém schopný preniesť bez ohľadu na to, koľko úrovní signálu je rozlíšených v tomto časovom intervale.

$$v_s = \frac{1}{T}$$

Meria sa v jednotkách nazvaných Baud (skratkou Bd), čo vyjadruje s^{-1} . Niekedy je preto označovaná aj ako Baud rate. Vyjadruje rýchlosť zmeny signálu. Ak má modulačná/symbolová rýchlosť hodnotu $1\text{kBd} = 1000\text{ Bd}$, znamená to, že za sekundu je prenesených 1000 symbolov. Trvanie jedného symbolu je $1/1000\text{ s}$, teda 1 milisekunda.

Na základe uvedených vzťahov možno vyjadriť vzťah pre určenie miery prenosovej rýchlosti

$$v_p = v_s \log_2 N$$

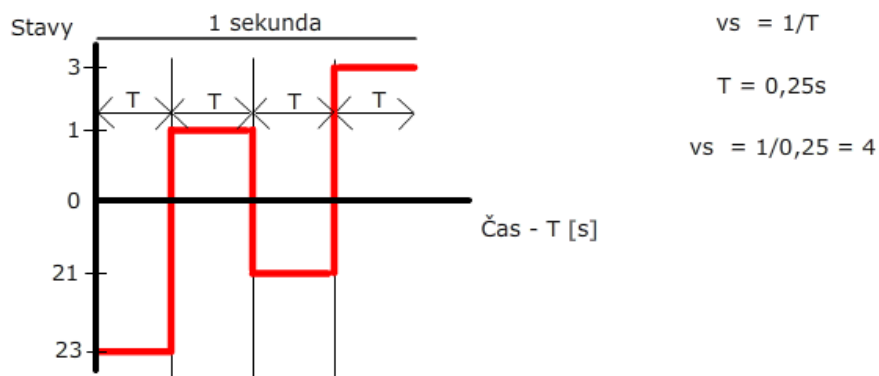
kde N je možný počet stavov číslicového signálu a v_s je symbolová (modulačná) rýchlosť tohto signálu. Miera prenosovej rýchlosti v_p sa vyjadruje v jednotkách $[\text{bit} \cdot \text{s}^{-1}]$ resp. bps (*bit per second*). Pre dvojstavový digitálny signál je číselne veľkosť oboch rýchlostí rovnaká. V tomto prípade sú jednotky $\text{bit} \cdot \text{s}^{-1}$ a Bd. rovnaké

$$v_p = v_s$$

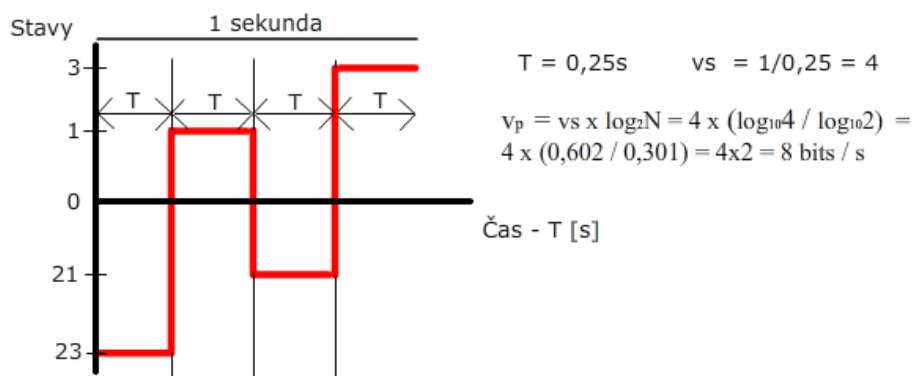
V prípade rovnosti prenosovej a modulačnej rýchlosti sa jedná o jednoduchú digitálnu komunikáciu číslicovým dvojestavovým signálom so symbolom binárna 0 alebo 1. Maximálne množstvo informácie je rovné 1 a modulačná/symbolová rýchlosť je rovná prenosovej rýchlosti vyjadrenej v bitoch za sekundu. V takomto prípade je možné zvyšovať prenosový rýchlosť len zmeňovaním časového intervalu binárnej 0 a 1.

Iný prípad nastáva vtedy, keď sú použité také techniky prenosu, kde symbol má viac, ako dva stavy. Vtedy je symbolová rýchlosť menšia, ako je prenosová rýchlosť, pretože je vynásobená maximálnym množstvom informácie, ktoré je prenášané v jednom symbole. Prenosová rýchlosť tak udáva počet prenesených bitov za sekundu. Ak použijeme prenosovú techniku kde $N=16$, znamená to, že jeden symbol reprezentuje 4 bity. Znamená to, že prenosová rýchlosť sa zvýši oproti modulačnej/symbolovej štvornásobne.

Vyjadrenie symbolovej a prenosovej rýchlosti je na obrázku 1.8.



Štvorstavová symbolová rýchlosť



Štvorstavová prenosová rýchlosť.

Obr. 1.10 Vyjadrenie symbolovej a prenosovej rýchlosti

Oneskorenie signálu (*signal delay*) predstavuje časové oneskorenie signálu pri prenose komunikačným kanálom. Oneskorenie ovplyvňuje hlavne aplikácie v reálnom čase ako je hlas a video. Jednosmerné oneskorenie predstavuje množstvo času od okamihu kedy je zo zdroja vyslaná správa, do okamihu kedy ju prijímač prijme. Obojsmerné oneskorenie predstavuje

súčet oboch jednosmerných oneskorení. Oneskorenie je spôsobené v rôznych častiach prenosového kanála. Hlavné zdroje oneskorenia sú:

- zdrojové kódovanie
- tvorba paketu
- kanálové kódovanie
- radenie do front
- šírenie signálu
-

Oneskorenie v komunikačnej sieti spôsobuje zníženie kvality komunikácie ako je okrem iného aj napríklad efekt ozvien. Pre služby v reálnom čase v sieťach s prenosom paketov predovšetkým v IP sieťach odporúčanie ITU-T G.114 definuje prípustné hranice oneskorení systému koniec – koniec. Sú

- *0 – 150 ms* – akceptovateľné oneskorenie pre väčšinu užívateľských aplikácií.
- *150 – 400 ms* - akceptovateľné oneskorenia pre medzinárodné spojenia.
- **400 ms – neakceptovateľné oneskorenia pre účely všeobecného sieťového plánovania.**

Chybovosť (*error rate*) vyjadruje početnosť chýb pri prenose. Označuje kvalitu prijímaného digitálneho signálu. Čím je chybovosť nižšia, tým je prijatý signál lepší. Všeobecne sa v komunikačných sieťach môže zisťovať chybovosť bitová (symbolová) alebo chybovosť bloková. Bitová chybovosť označovaná ako BER (*Bit Error Rate*) je definovaná pomerom chybne prijatých bitov ku celkovému počtu prijatých bitov za určitú dobu merania.

Bitová chybovosť sa počíta podľa vzťahu:

$$BER = b_E / (v_p * t) \quad [-; \text{bit}; \text{bit/s}; \text{s}],$$

b_E je počet chybne prijatých bitov

v_p je prenosová rýchlosť

t je celková doba merania.

Chybovosť sa obvykle sa udáva v percentách alebo v hodnote na desiatu. Príklad 0,000 003% alebo 3×10^{-6} predstavuje 3 chybné bity z 1000 000 bitov. Za ideálnych podmienok by mala byť hodnota nula, ale v reálnom prenosovom prostredí nemožno vylúčiť vonkajšie zdroje rušenia, akými môžu byť mobilné telefóny, atmosférická elektrina, vlastný šum v prenosovom médiu a pod..

1.7 Základné činnosti IKS

Komunikácia v elektronických komunikačných sieťach sa uskutočňuje v nasledovných fázach:

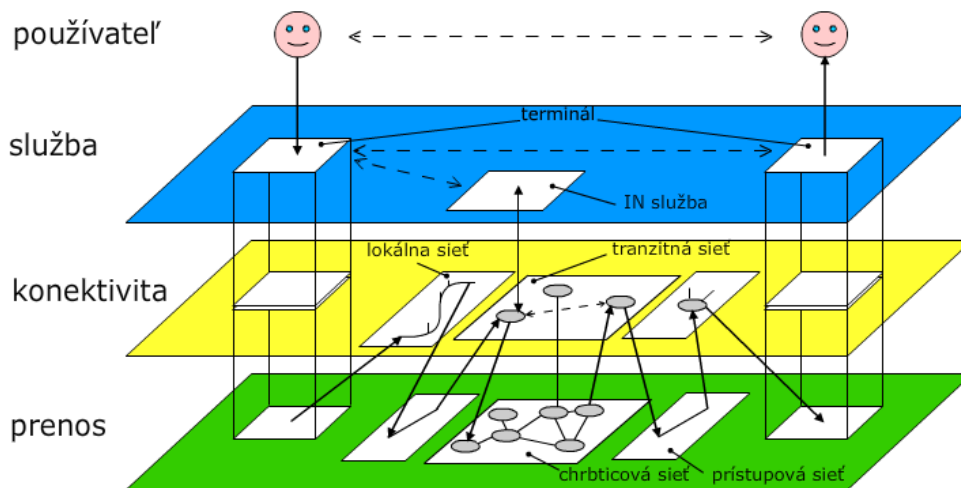
- začiatok prenosu,

- samotný prenos,
- ukončenie prenosu.

Komunikácia je zabezpečovaná cez funkcie elektronickej komunikačnej siete, ktorými sú prepojenie, smerovanie, adresovanie, signalizácia, prenos a ďalšie. Základné funkcie v elektronickej komunikačnej sieti sú realizované v troch rovinách, ktoré predstavujú hlavné činnosti komunikačných sietí:

1. služby,
2. konektivita,
3. prenos.

Znázornenie hlavných činností je na obrázku 1.11. Prenos je najnižšou rovinou a zabezpečuje fyzický prenos informácie. Rovina konektivity zabezpečuje funkcie prepojenia, smerovania a signalizácie. Úroveň služieb zabezpečuje aj ďalšie potrebné funkcie pre realizáciu príslušných služieb, prostredníctvom ktorých je informácia prenášaná.



Obr. 1.11 Úrovne činností elektronickej komunikačnej siete

1.8 Taxonómia sietí

V každom odbore, kde sa vyskytuje mnoho prvkov rôznych druhov s rôznymi vlastnosťami, vytvára sa ich zoskupovanie do určitých kategórií podľa klasifikovaných vlastností. Takéto triedenie sa označuje taxonómia. Podobné klasifikovanie sa robí i v elektronickej komunikačnej sieti. Dôvodom na vytváranie kategórií v elektronickej komunikačnej sieti je skutočnosť, že táto oblasť prechádza v posledných rokoch búrlivým vývojom a vznikajú neustále nové termíny a pojmy. Pre študujúcich je mnohokrát ťažké vyznať sa v spleti týchto pojmov a rozlíšiť kam patria a čo vyjadrujú. Preto je dôležité mať prehľad o tom do akej kategórie daná sieť patrí, aké sú typické príklady sietí jednotlivých kategórií, aké sú jej charakteristické vlastnosti oproti iným typom, resp. iným kategóriám. Rovnako je dôležité vedieť vlastnosti a parametre jednotlivých kategórií, ktoré vytvárajú

hodnotiace kritériá v jednotlivých kategóriách. Znalosť kategórií elektronických komunikačných sietí je dôležitá nielen pre odborníkov a pracovníkov v tejto oblasti, ale i pre používateľov. Podľa týchto vlastností sa zákazník rozhoduje pre určitý typ siete, ktorú bude používať. V publikovaných materiáloch z oblasti komunikačných sietí možno nájsť rôzne spôsoby kategorizovania, ktoré vznikali pre rôzne účely. Výrobcovia, predajcovia či prevádzkovatelia elektronických komunikačných sietí tvoria kategórie najčastejšie pre marketingové účely, teoretickí pracovníci pre vytvorenie princípov, ktoré by viedli k určitým systémovým pravidlám. Dnes neexistuje nijaké odporúčanie štandardizačných organizácií, podľa ktorého by sa mohli získať presné a vyčerpávajúce znalosti o kategorizácii elektronických komunikačných sietí. Nie je to ani celkom možné, pretože mnohokrát nie je možné stanoviť presné kritériá, podľa ktorých sa kategórie majú vytvárať. Samotná klasifikácia je skôr prostriedkom k lepšiemu pochopeniu toho, aké názvoslovie sa dnes používa, v čom sa komunikačné siete líšia a aké rozlišujúce kritériá vôbec môžu existovať. Uvádzané informácie sú súhrnom rôznych dostupných materiálov a znalostí.

1.8.1 Kritériá kategorizácie

Väčšina rozhodovacích kritérií pre klasifikáciu ľubovoľných systémov je taká, že v mnohých prípadoch dávajú jasnú odpoveď, ale v iných prípadoch nedokážu určiť jednoznačný záver a ponechávajú otvorený priestor subjektívnemu rozhodovaniu. Niekedy sa určitý systém nedá klasifikovať len podľa jedného jediného kritéria, je vhodnejšie určiť kombináciu kritérií. Rozhodovanie je potom multikritériálne, vychádzajúce zo súčasnej aplikácie niekoľkých kritérií. Je na používateľovi, aby si z jedného kritériálnych kategórií vytvoril podľa potreby potrebné hodnotenie určitého systému.

1.8.2 Kategorizácia elektronických komunikačných sietí

Členenie komunikačných sietí je možné vytvoriť podľa nasledujúcich kategórií:

- územnej rozľahlosti,
- šírky pásma/ prenosovej rýchlosti,
- zdieľania zdroja,
- topológie,
- vlastníctva,
- poskytovaných služieb,
- technológie,
- spôsobu prepojovania,
- smeru prenosu,
- použitej architektúry,
- hierarchického usporiadania,
-

1.8.2.1 Kategorizácia sietí podľa územnej rozľahlosti

Komunikačné siete sa najčastejšie rozdeľujú na lokálne a rozľahlé. Podľa územnej rozľahlosti sa zaužívali nasledovné základné označenia:

- PAN (Personal Area Network)
- LAN (Local Area Networks)
- MAN (Metropolitan Area Networks)
- WAN (Wide Area Networks)
- GAN (Global Area Network).

Svoje rozlišujúce kritérium si pritom nesú už vo svojom názve. Problematická je však exaktnosť tohto kritéria. Rozlišovacie kritérium, založené na veľkosti siete je zaťažené príliš veľkou mierou subjektívneho rozhodovania. Ak sa jedná o vzájomné prepojenie niekoľkých počítačov v rámci jednej miestnosti, je isté, že ide o sieť lokálnu. Ak pôjde naopak o sieť rozprestierajúcu sa cez niekoľko kontinentov, asi nebude pochyb o tom, že ide o sieť rozľahlú. Nemožno však určiť presné hranice. Vsunutie ďalších kategórií čiastočne tento problém rieši, nie však úplne.

Uvedené rozlíšenie je síce správne, ale dôvodom pre budovanie niektorého typu siete boli a sú často iné dôvody. Jedno z najdôležitejších je využívanie daného typu siete. V prípade typickej lokálnej siete ide najčastejšie o potrebu zdieľania technických a programových prostriedkov, úzko súvisiacich s prevádzkou a vlastníctvom siete. Naproti tomu rozľahlé siete historicky vznikali skôr z potreby komunikovať na diaľku. Ani tu však nie je hranica nijako ostrá a v rámci rozľahlej siete je už tiež využívané napríklad zdieľanie výpočtovej kapacity. Tiež v typických lokálnych sieťach sa stále častejšie začínajú používať rôzne komunikačné služby, v minulosti typické pre rozľahlé siete.

Trendom je postupné splývanie všetkých typov takto označených sietí, aspoň z pohľadu používateľa. Tento trend vedie k tomu, aby používateľ nepocíťoval žiadny významnejší rozdiel medzi tým, kedy v akom type siete pracuje, a všade mal v zásade rovnaké možnosti a mohol pracovať rovnakým spôsobom. Takže i väčšina kritérií, ktoré by mali pomôcť rozlíšiť kategórie sietí podľa územnej rozľahlosti má s postupom času stále menej a menej priestoru na poskytovanie jednoznačných záverov. Na základe tabuľky 1 uvádzanej v minulosti ako rozdiely lokálnych sietí (LAN) a rozľahlých sietí (WAN) sú v ďalších častiach spracované ďalšie kategorizácie elektronických komunikačných sietí.

Tab. 1 Charakteristické odlišnosti lokálnych sietí a rozľahlých sietí

Porovnávacie kritériá	LAN	WAN
kvôli čomu sa budujú	skôr pre potreby zdieľania	skôr pre potreby komunikácie
charakter uzla siete	prevažujú pracovné stanice	prevažujú servery
prenosová rýchlosť	vyššia	nižšia
dostupnosť uzla siete	podľa potrieb užívateľov	trvalá
topológia siete	systematická (pravidelná)	nesystematická (nepravidelná)
vlastníctvo infraštruktúry	vlastní používateľ	vlastní prevádzkovateľ

poskytované služby	privátne, neverejné	verejné, používateľské
technológia	Ethernet, Token Ring, FDDI, TCP/IP	ISDN, ATM, TCP/IP
hierarchické usporiadanie	prístupové siete	chrbticové

1.8.2.2 Kategorizácia sietí podľa zdieľania zdroja

Potreba zdieľania zdroja znamená sprístupnenie konkrétnych zdrojov informácie viacerým používateľom. Samotné zdieľanie môže byť realizované rôznymi spôsobmi, resp. vychádzať z rôznych koncepcií. Siete sa potom delia na siete typu:

- peer to peer,
- serverového typu / klient-server.

V sieťach serverového typu sú zdieľané zdroje sústredené na jedno miesto do spoločného centrálného servera, z ktorého sú zdroje zdieľané všetkými používateľmi. Pri sieťach typu peer to peer sú zdroje ponechané na pôvodnom mieste u ich majiteľov, alebo autorov a ich zdieľanie je umožnené z týchto miest. Peer to peer v preklade znamená „rovný s rovným“. Rozdiel medzi sieťami typu peer to peer a sieťami serverového typu je i v tom, že siete typu peer-to-peer bývajú optimalizované na jednoduchosť, spoľahlivosť a to i za cenu nižšieho celkového výkonu, rýchlosti, priepustnosti atď. Naopak siete serverového typu môžu mať relatívne vyššie nároky na inštaláciu a správu a môžu zároveň dosahovať vyššiu výkonnosť.

1.8.2.3 Kategorizácia sietí podľa prenosovej rýchlosti

Všeobecne možno povedať, že komunikačné siete sa dajú rozdeliť na:

- nízkorýchlostné,
- vysokorýchlostné.

Niekedy je tento rozdiel uvádzaný i rozdelením na:

- úzkopásmové,
- širokopásmové.

V minulosti bola prenosová rýchlosť hlavným rozdielom medzi LAN a WAN sieťami.

Súčasný trend je taký, že rýchlosť v lokálnych a rozľahlých sieťach sa zvyšuje a pôvodne priepastný rozdiel v rýchlostiach má tendenciu zmenšovať sa. Nie je žiadne jednoznačné kritérium pre určenie kategórie podľa prenosovej rýchlosti, aj keď sa tento pojem používa hlavne v marketingových súvislostiach. V minulosti sa za vysokorýchlostnú sieť považovala sieť s prenosovou rýchlosťou väčšou ako 2 Mbit/s.

1.8.2.4 Kategorizácia sietí podľa vlastníctva

Podľa vlastníctva sú siete rozdeľované na:

- privátne siete,
- verejné siete,
- virtuálne privátne siete (VPN - *Virtual Private Network*).

Pojem privátne siete je celkom jednoduchý. Je to taká sieť, ktorá slúži jednému konkrétnemu subjektu, napr. podniku, organizácii apod.. Funkcia vlastníka siete i funkcia používateľa tu splyvajú, čo znamená, že rozhodovanie i povinnosť starať sa o prevádzku siete je v kompetencii vlastníka i prevádzkovateľa súčasne. Príkladom privátnych sietí môžu byť siete LAN. Pri väčšine lokálnych sietí je ich prevádzkovateľ súčasne i majiteľom prenosových ciest, ktoré jeho sieť používa. Rovnako niektoré rozľahlé siete boli v minulosti privátne. Jednalo sa o sektor dopravy, energetiky a vojska. Časť z nich tento charakter stratila. Sieť zostáva privátnou i vtedy, keď vlastník a súčasne i používateľ siete nie je jej bezprostredným prevádzkovateľom. V mnohých prípadoch rutinnú prevádzku svojej siete zverí špecializovanému externému subjektu v rámci outsourcingu. Rozhodujúci je spôsob využitia a nie prevádzka siete. Príslušná sieť zostáva privátnou, keď je využívaná len jedným subjektom, ktorý si naďalej ponecháva všetky rozhodovacie a vlastnícke práva na využívanie.

Pre verejnú sieť je charakteristické to, že jej vlastník ju pre svoju vlastnú potrebu nevyužíva vôbec, alebo len minimálne a naopak väčšinu jej dostupnej prenosovej kapacity ponúka na komerčné využitie iným subjektom. Používatelia potom využívajú len služby verejnej siete. Typickými prevádzkovateľmi verejných sietí sú telekomunikačné organizácie.

Pojem virtuálna privátna sieť – VPN je pomerne nový. V podstate sa jedná o službu, spočívajúcu vo vytvorení virtuálnej privátnej siete v rámci verejných komunikačných sietí. Ide o taký typ, kde po logickej stránke ide o sieť, ktorá je plne k dispozícii jednému konkrétnemu subjektu, ale po stránke svojho technického riešenia ide o súčasť verejnej komunikačnej siete. Názov virtuálna zdôrazňuje, že sieť sa len chová ako privátna, ale v skutočnosti je vytvorená na verejnej sieti pomocou vhodných technických opatrení. Prevádzkovateľ verejnej siete preberá na seba celú starostlivosť o prevádzkyschopnosť virtuálnych privátnych sietí svojich používateľov. Výhody virtuálnej privátnej siete majú ako ekonomickú, tak i organizačnú a technickú povahu. Používanie virtuálnej privátnej siete môže byť napríklad pre používateľa lacnejšie, než vybudovanie a prevádzka skutočnej privátnej siete. Odlišná je i samotná skladba nákladov. V prípade privátnej siete sú relatívne veľké jednorazové zriaďovacie náklady a pri rutinnom prevádzkovaní vznikajú len skutočné prevádzkové náklady. Naproti tomu vo virtuálnych privátnych sieťach hradí zákazník len relatívne malé zriaďovacie náklady, zatiaľ čo priebežné poplatky za používanie siete môžu byť vyššie.

1.8.2.5 Kategorizácia sietí podľa komunikačných technológií

V komunikačných sieťach je používaných mnoho rôznych komunikačných technológií. Tie vznikajú z potreby efektívnejšieho využívania prostriedkov na prenos a spracovanie informácií v komunikačných sieťach. Výraznou odlišnosťou komunikačných sietí bývajú spôsoby realizácie funkcií siete, ich prenosových a spojovacích mechanizmov. Odlišujú sa podľa použitých technologických štandardov. Príklady niektorých štandardov sú v tabuľke 2.

Tab.2 Príklady štandardov rôznych technológií

Štandard	Označenie siete
IEEE	LAN (Ethernet)

ISDN	pevná telefónna sieť
ATM	metropolitná sieť
TCP/IP	internet
GSM/UMTS	mobilná telefónna sieť

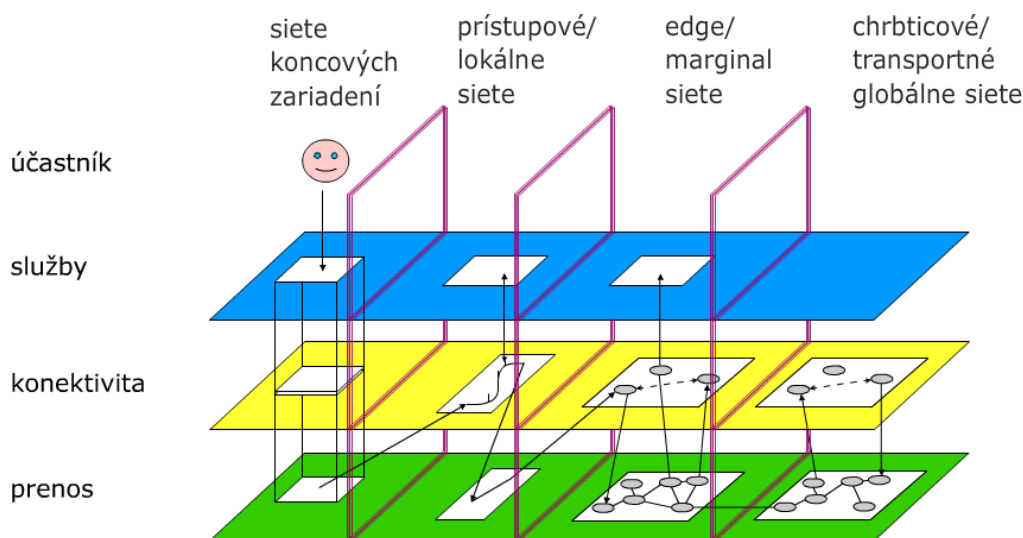
Komunikačné technológie, používané dnes v rôznych typoch sietí majú tendenciu k sebe konvergovať. Príkladom sú technológie ATM a TCP/IP. Obe sú vhodné i pre lokálne i pre rozľahlé siete.

1.8.2.6 Kategorizácia sietí podľa hierarchického usporiadania v sieti

Podľa časti komunikačného kanála sú rozlišované ďalšie kategórie sietí. Rozlišujú sa siete:

- sieť koncových zariadení (Personal Area Networks - PAN)
- prístupové (Access Networks , LAN),
- okrajové (Marginal Network, Edge Networks,),
- chrbticové/transportné /globálne (Backbone Networks, Transport Networks, Global Networks).

Ich znázornenie je na obrázku 1.12.



Obr. 1.12. Hierarchické usporiadanie sietí

1.9 Budúci vývoj technológií elektronických komunikačných sietí

Komunikačné siete už v začiatkoch vývoja dostávali rôzne názvy a mená. Tieto názvy väčšinou súviseli s účelom, na ktorý boli realizované, resp. podľa služieb, ktoré boli nimi poskytované. Prvá elektronická komunikačná sieť bola sieť na prenos textu - Telex, neskôr sieť na prenos hlasu, na prenos dát či obrazu. Každá vývojová etapa bola charakterizovaná určitou technológiou. Podľa použitej technológie a jej využitia vznikali v priebehu vývoja rôzne elektronické komunikačné siete. Napríklad:

- telegrafné,
- telefónne,
- dátové,
- televízne,
- rozhlasové,
- ISDN,
- ATM
- NGN
- inteligentné,
- apod.

Vývoj v elektronických komunikačných sieťach vedie k integrácii služieb a bol zahájený budovaním sietí ISDN (Integrated Services Digital Network), v slovenčine Digitálna sieť integrovaných služieb. Tieto siete ako prvé poskytovali viac než jednu službu. Rovnako iné siete poskytujú dnes viac než jednu službu. Napríklad telefónna sieť poskytuje službu prenosu dát a faxovú službu. Budúcnosť predpokladá vybudovanie jednej siete vzájomným prepojením existujúcich sietí. Konvergencia všetkých sietí sa nazýva sieť budúcej generácie a je označovaná ako NGN (Next Generation Network).

1.10 Záver

Vývoj spoločnosti v poslednom období najviac ovplyvňuje prudký rozvoj informačno-komunikačných technológií. Z pohľadu koncového používateľa je využívanie informačno-komunikačných technológií najviac vnímané prostredníctvom používania služieb. Služby pre koncového používateľa umožňujú meniť doterajšie postupy a činnosti v privátnom aj hospodárskom živote a tým prispievajú k zmene spoločnosti na spoločnosť informačnú. Poskytovanie služieb je podmienené vybudovaním informačno-komunikačnej infraštruktúry, prostredníctvom ktorej sú realizované požadované funkcie služieb.

Komunikačnú infraštruktúru tvoria komunikačné systémy nazývané častejšie elektronické komunikačné siete. Nosič informácie v elektronických komunikačných sieťach je elektromagnetický signál. Pre prenos signálu musia elektronické komunikačné siete zabezpečiť základné funkcie elektronickej komunikácie, ktorými sú prenos, adresovanie, prepojovanie, signalizácia. Spokojnosť používateľov elektronických komunikačných sietí sa určuje kvalitou poskytovaných služieb. Kvalita je súbor určitých merateľných vlastností, medzi ktoré patria aj základné parametre siete, ktorými sú prenosová rýchlosť, oneskorenie a chybovosť.

Dnes je prevádzkované veľké množstvo rôznych elektronických komunikačných sietí za rôznym účelom, rôznymi vlastnosťami a s použitím rôznych technológií. Prehľad jednotlivých kategórií, podľa rôznych kritérií tvorí taxonómiu elektronických komunikačných sietí. Vývoj smeruje ku konvergencii sietí, ktorá je často označovaná ako NGN. Platforma NGN je prostredie, ktoré ponúka nové možnosti a schopnosti v oblasti tvorby, implementácie

(nasadzovania) a poskytovania širokého spektra multimediálnych služieb a aplikácií. V rámci NGN sa kladie zvýšený dôraz na prispôsobenie služieb zákazníkom.

Kľúčové slová:

- | | |
|--|---|
| <i>1. Informačná spoločnosť</i> | <i>14. Digitálny signál</i> |
| <i>2. Informačno-komunikačné technológie</i> | <i>15. Elektronická komunikačná sieť</i> |
| <i>3. Výmena informácie</i> | <i>16. Prvky elektronickej komunikačnej siete</i> |
| <i>4. Elektronická komunikácia</i> | <i>17. Koncové zariadenia a ich funkcie</i> |
| <i>5. Elektronické komunikačné siete</i> | <i>18. Funkcie elektronickej komunikačnej siete</i> |
| <i>6. Informačná / informačno-komunikačná infraštruktúra</i> | <i>19. Parametre elektronickej komunikačnej siete</i> |
| <i>7. Informačno-komunikačné služby</i> | <i>20. Taxonómia elektronických komunikačných sietí</i> |
| <i>8. Štrukturálny model IK služieb</i> | <i>21. Technológie elektronických komunikačných sietí</i> |
| <i>9. Služby pridružené k sieti</i> | |
| <i>10. Služby poskytované po sieti</i> | |
| <i>11. Prenos informácie</i> | |
| <i>12. Prenosový reťazec</i> | |
| <i>13. Analógový signál</i> | |

Kontrolné otázky

1. Podľa čoho vznikol pojem informačná spoločnosť ?
2. Ktoré z vyjadrení charakterizuje informačnú spoločnosť?
3. Aké sú vplyvové faktory rozvoja informačno-komunikačných technológií?
4. Prečo by mali byť výsledkom implementácie IKT inovácie vo všetkých sférach spoločenského a hospodárskeho života?
5. Aké rôzne spôsoby výmeny informácií boli v historickom vývoji komunikácií?
6. Ako je dnes uskutočňovaná výmena elektronicke spracovaných informácií?
7. Aká je rozdiel medzi výmenou informácií stand alone a elektronicke komunikáciou?
8. Čo označuje pojem elektronicke komunikácia?
9. Ako sa označujú systémy elektronickej komunikácie?
10. Čo zahrňuje pojem informačná / informačno-komunikačná infraštruktúra?
11. Aké vyjadrenia platí pre pojem informačno-komunikačné služby?
12. Kto sú tvorcovia informačno-komunikačných služieb?
13. Ako sa bude meniť hodnota úloh tvorcov informačno-komunikačných služieb v budúcnosti?
14. Aké je základné členenie informačno-komunikačných služieb?
15. Ktoré zo služieb patria do kategórie služieb pridružených k sieti?

16. Ktoré zo služieb patria do kategórie služieb poskytovaných po sieti?
17. V akej forme sa informácia prenáša po elektronickej komunikačnej sieti?
18. Čo formálne vyjadruje správa?
19. Aký je rozdiel medzi množstvom informácie a hodnotou informácie?
20. Aké typy vyjadrenia informácie sú všeobecne používané?
21. Čo je nosičom informácie pri prenose cez elektronickeú komunikačnú sieť?
22. Aké základné tvary signálov sú používané pre prenos?
23. Ako je charakterizovaný analógový signál?
24. Ako je charakterizovaný digitálny signál?
25. Čo znamená pojem prenosový reťazec?
26. Aké sú základné prvky prenosového reťazca?
27. Prečo sa dnes používajú pre prenos viac digitálne ako analógové signály?
28. Prečo sa v minulosti používali pre prenos hlasu iba analógové signály?
29. Ako sa dá popísať elektronickeú komunikačnú sieť?
30. Ktoré sú základné prvky elektronickej komunikačnej siete?
31. Aký je rozdiel medzi komunikačným kanálom a komunikačným okruhom?
32. Aké funkcie majú koncové zariadenia v elektronickej komunikačnej sieti?
33. Ktoré základné funkcie musí spĺňať elektronickeá komunikačná sieť?
34. K čomu je určená funkcia prepojovania?
35. K čomu je určená funkcia smerovania?
36. Aký je rozdiel medzi prepojením a smerovaním?
37. K čomu je určená funkcia adresovanie?
38. Ktoré sú základné parametre elektronickej komunikačnej siete?
39. Ako je definovaný parameter prenosová rýchlosť?
40. Čo znamená pojem modulačná/symbolová rýchlosť?
41. Aký je vzťah medzi modulačnou a prenosovou rýchlosťou?
42. V čom sa udáva modulačná rýchlosť?
43. Čo znamená parameter oneskorenie signálu v elektronickej komunikačnej sieti?
44. Čo spôsobuje oneskorenie v elektronickej komunikačnej sieti?
45. Čo znamená parameter chybovosť pri elektronickej komunikácii,
46. Čo znamená skratka BER?
47. Prečo bola vytvorená taxonómia elektronickeých komunikačných sietí?
48. Čo znamenajú označenia PAN, LAN, MAN, WAN, GAN?
49. Aký je rozdiel medzi sieťami typu peer to peer a klient – server?
50. Aký je predpokladaný ďalší vývoj elektronickeých komunikačných sietí?
51. Čo znamená označenie ISDN?
52. Čo znamená označenie NGN?

1.11 Literatúra

- [1] Leo A. Nefiodow: Der sechste Kondratieff, Wege zur Produktivität und Vollbeschäftigung im Zeitalter der Information, Rhein-Sieg-Verlag, Sankt Augustin 1996, ISBN: 3-9805144-0-4
- [2] Reichwald, R.: Anwenderfreundliche Kommunikationssysteme, Heidelberg, Hüthig, 2000, ISBN 3-7785-3937-X
- [3] ITU-T Recommendation Y.110 Global Information Infrastructure principles and framework architecture, Geneva, (6/98)
- [4] Cairncross Frances: Konec vzdálenosti, Computer Press, Praha, 1999, ISBN 80-7226-155.X

2 Modely komunikačných systémov

Ciele učenia:

Po štúdiu tejto kapitoly by ste mali vedieť:

- Lineárny model elektronickej komunikácie
- Fyzikálny model elektronickej komunikačnej siete
- Topológie elektronickej komunikačných sietí
- Vysvetliť význam štandardizácie a poznať hlavné štandardizačné organizácie pre informačné a komunikačné technológie
- Dôvody a princíp vrstvovej štruktúry/hierarchie, komunikácie po jednotlivých vrstvách a súvislostiam medzi úrovňami
- Základný referenčný model OSI - Open System Interconnection
- Všeobecnú protokolovú štruktúru, pojmy protokol, funkcia, služba, funkčná entita vrstvy a význam protokolov a služieb medzi vrstvami
- Vysvetliť dôvody pre používanie vrstvových modelov v komunikačných sieťach
- Vedieť rozdiel medzi referenčným modelom OSI a sieťovou architektúrou.
- Porovnať modely jednotlivých sietí, spolupráca sietí s rôznymi modelmi (hlavne OSI a TCP/IP)
- Použitie modelov v komunikačných sieťach

2.1 ÚVOD

Navrhnuť a realizovať komunikačnú sieť je zložitá úloha, ktorá vyžaduje dodržiavanie rôznych kritérií a požiadaviek tak, aby bolo možné implementovať rôzne technológie v jednotlivých častiach siete, a aby komunikácia bola na požadovanej úrovni kvality.

K tomu, aby elektronickej komunikačné siete mohli flexibilne poskytovať súčasné a aj budúce služby, je potrebné vytvoriť úplnú sieťovú architektúru. Sieťová architektúra predstavuje štruktúru riadenia komunikácie v systémoch, čo je špecifikované súborom činností, umožňujúcich výmenu informácie medzi dvomi a viacerými subjektmi.

Skôr než je vytvorená sieťová architektúra, vytvára sa abstraktná predstava o komunikačnom systéme na základe modelov.

Model je všeobecne zjednodušené zobrazenie systému a jeho popis metódou analógie. Môže to byť určitá predstava, plán, reprezentácia alebo popis znázornenia hlavného objektu, alebo spolupracujúcich objektov v systéme. Pre elektronickej komunikačnú sieť ako systém možno vytvoriť viac modelov, prostredníctvom ktorých je možné získať predstavu o činnosti a návrhu komunikačných sietí.

2.2 Druhy modelov v elektronickej komunikácii

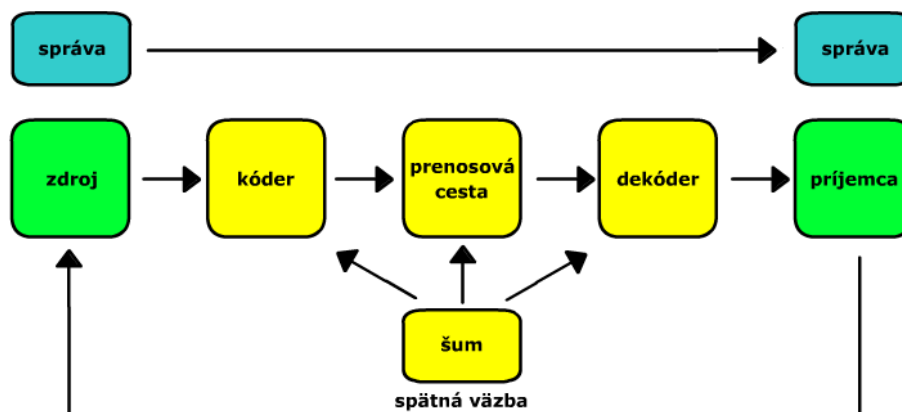
2.2.1 Shannon –Weaverov model (lineárny model, prenosový/komunikačný reťazec)

Základným a asi aj najstarším modelom elektronickej komunikácie je lineárny model nazývaný „Shannon-Weaverov model z roku 1947. Tento model je spojený s „kybernetickou teóriou komunikácie“ a je používaný ako základný model nielen pri elektronickej komunikácii prostredníctvom informačno-komunikačných systémov, ale aj v oblasti ľudskej komunikácie. Tento model, znázornený na obr.2.1, znázorňuje zjednodušenú schému komunikácie pozostávajúcu zo 6 základných komponentov:

1. **Informačný zdroj**, ktorý chce oznámiť správu. Môže ním byť človek, alebo technické zariadenie .
2. **Správa**, v ktorej je spracovaný určitý informačný obsah.
3. **Kóder**, ktorý mení správu do formy vhodnej pre prenos. Slúži k prispôbeniu správy technickým parametrom prenosového kanála.
4. **Kanál**, cez ktorý je správa prenesená.
5. **Dekodér**, ktorý podľa zakódovania dekóduje správu do tvaru zrozumiteľného pre prijímateľa.
6. **Prijímač** správy, ktorým môže byť rovnako človek ako aj technické zariadenie.

Súčasťou modelu môžu byť aj:

1. **Šum**, ktorý predstavuje skreslenie alebo poškodenie informácie pri prenose.
2. **Spätná väzba**, ktorou prijímač dáva zdroju informáciu o výsledku komunikácie.



Obr. 2.1 Shannon – Wieverov model

Lineárny model je všeobecným modelom komunikácie a znázorňuje postupnosť komunikačných aktivít. Tento model nerieši komunikáciu v čase ani v priestore a nerieši ani mnohé ďalšie problémy komunikácie. Slúži ako východiskový model pre základné pochopenie princípov komunikácie. Je rovnako základným modelom pre teóriu oznamovania.

2.2.2 Model fyzického usporiadania elektronickej komunikačnej siete

Pretože lineárny model znázorňuje komunikáciu iba medzi jedným zdrojom a jedným prijímačom, nedáva dostatočný obraz o možnostiach viacnásobnej komunikácie prostredníctvom elektronickej komunikačných sietí. Komunikačné siete umožňujú komunikáciu každého zdroja s každým prijímačom, ktoré sú pripojené v komunikačnej sieti. Modelové znázornenie fyzického usporiadania siete vychádza zo základných topológií sietí, ktoré vyjadrujú vzájomné usporiadanie zariadení v sieti.

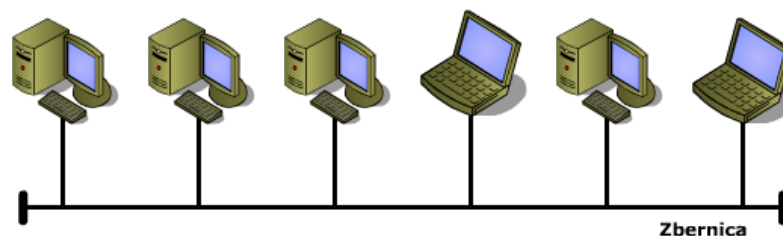
Topológia siete špecifikuje, akým spôsobom sú prepojené jednotlivé zariadenia alebo uzly komunikačnej siete. Rozlišujú sa dva druhy topológie:

- **fyzická topológia**, tvorená priestorovým rozložením prenosových médií a uzlov,
- **logická topológia**, tvorená vnútorným spôsobom prepojenia na danej fyzickej topológii.

V komunikačných sieťach sa používajú rôzne typy topológií, ktoré majú rôzne vlastnosti. Najčastejšie sú nasledujúce topológie:

2.2.2.1 Zbernica (Bus)

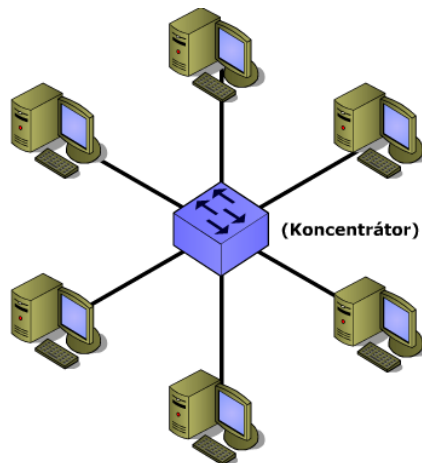
V topológii zbernica sú všetky koncové zariadenia pripojené na spoločné prenosové médium. Topológia zbernica je často používaná v lokálnych - sieťach LAN. Jednoduchosť a cena sú kladmi tejto topológie. Nedostatkom sú predovšetkým obmedzenosť počtu uzlov a vzdialeností medzi nimi, zložitá identifikácia príčin porúch a nízka bezpečnosť dát. Topológia zbernica je znázornená na obr. 2.2



Obr. 2.2 Topológia zbernica

2.2.2.2 Hviezda (Star)

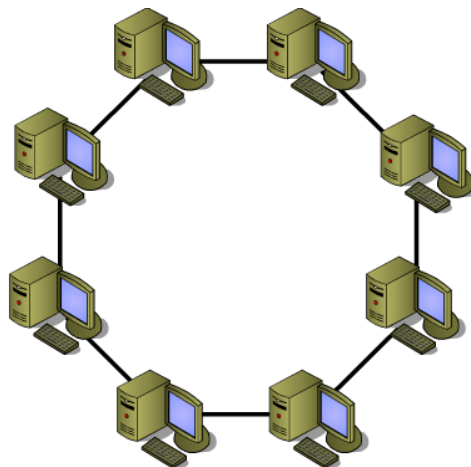
Topológia hviezda predstavuje najčastejší trend vytvárania lokálnych sietí. Prepojenia od koncových zariadení sú vedú do centrálného uzla, kde je prvok realizujúci prepojenie koncových uzlov. Výhodou sietí typu hviezda je ľahká detekcia chýb. Spoľahlivosť siete je závislá hlavne od spoľahlivosti centrálného uzla. Topológia hviezda je na obr. 2.3.



Obr. 2.3 Topológia hviezda

2.2.2.3 Kruh (Ring)

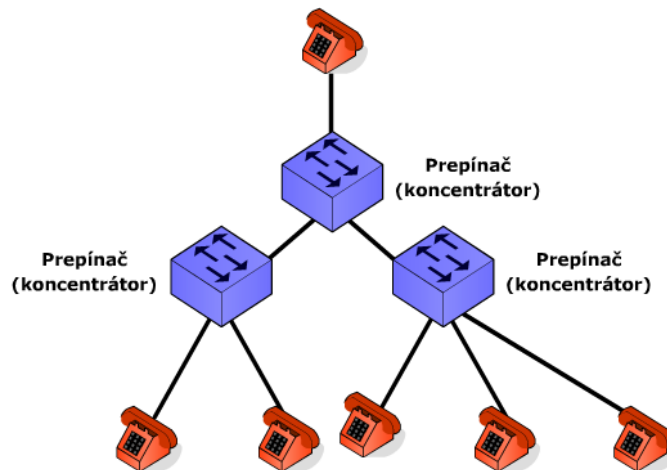
Princíp topológie kruh je v tom, že vysielacia časť jedného koncového zariadenia je zapojená do prijímacej časti nasledujúceho koncového zariadenia. Koncové zariadenia sú prepojené jedným prenosovým médium tak, že sú na konci opäť spojené. Logickú topológiu kruh používajú LAN siete typu Token Ring a FDDI, ale fyzicky je ich topológia tvorená hviezdou s centrálnym prvkom. Prenos je realizovaný len jedným smerom na základe distribuovaného pridelovania prenosového média. Spoľahlivosť je závislá od spoľahlivosti prípojných miest uzlov a prenosového média. Topológia kruh je znázornená na obr. 2.4.



Obr. 2.4 Topológia kruh

2.2.2.4 Strom (Tree)

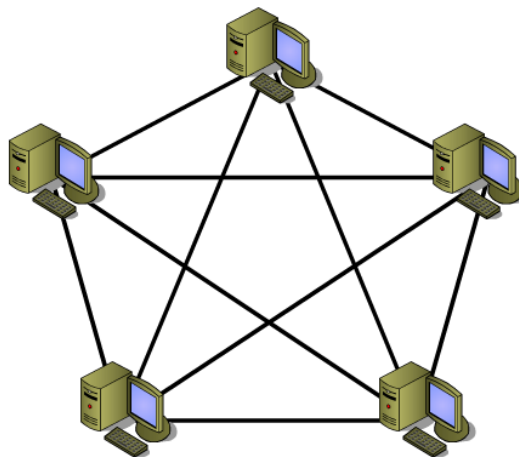
Topológia strom je vytváraná postupným pripojovaním jednotlivých koncových zariadení k vrcholovému uzlu stromu. Typickým príkladom topológie strom sú prístupové telefónne siete. Spoľahlivosť topológie strom je závislá od spoľahlivosti prenosových médií, vrcholového uzla, ale i rozvetvovacích uzlov. Dá sa zvýšiť zálohovaním kritických uzlov. Topológia strom je znázornená na obr.2.5.



Obr. 2.5 Topológia strom

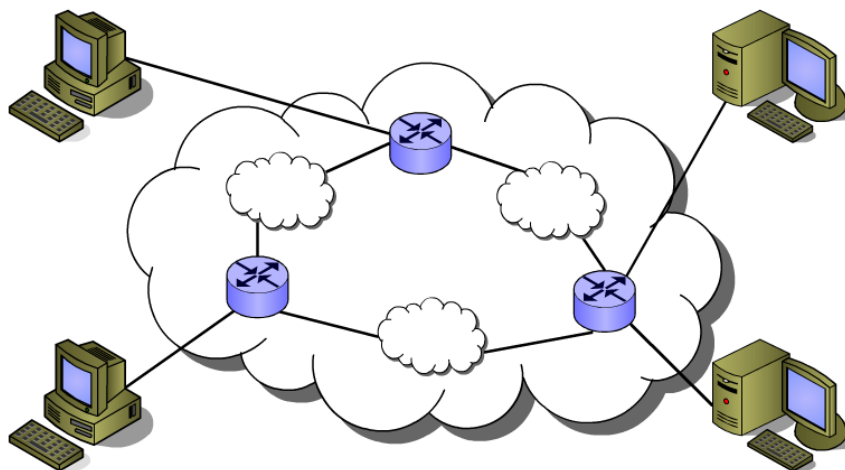
2.2.2.5 Polygón (mesh)

Topológia polygón (mesh) predstavuje spojenie každého zariadenia s každým. Používa sa najviac pri chrbticových sieťach. Neúplný polygón sa používa aj v iných typoch sietí. Polygón je najspoľahlivejšia topológia, umožňuje rôzne kombinácie vytvárania komunikačných kanálov medzi koncovými zariadeniami. Spoľahlivosť je závislá od spoľahlivosti prenosových médií a uzlov. Je to však zároveň najnákladnejší spôsob prepojenia zariadení. Topológia polygón je znázornená na obr.2.6.



Obr. 2.6 Topológia polygón

Model fyzického usporiadania konkrétnej siete môže obsahovať viac druhov topológií a znázorňuje všetky fyzické zariadenia elektronickej komunikačnej siete. Jeho znázornenie je na obr. 2.7. Najčastejšie je vytváraný na vyjadrenie spolupráce viacerých typov sietí, ktoré sa označuje ako interworking.



Obr. 2. 7 Všeobecný model fyzického usporiadania elektronických komunikačných sietí

Štruktúra siete v územne rozľahlom priestore je vhodná pre predstavu priestorového usporiadania základných prvkov siete. Procesy a funkcie siete sa takouto štruktúrou nedajú dostatočne vyjadriť.

2.3 VRSTVOVÉ MODELY SIETE

2.3.1 Dôvody pre vytvorenie vrstvomého modelu

Vytvorenie vrstvomých modelov sietí bolo podmienené množstvom úloh, ktoré boli spojené s návrhom elektronických komunikačných sietí. Rozširovanie, hlavne dátových sietí, vyžadovalo zložité technické a programové vybavenie pre všetky funkcie komunikačných sietí. Komunikácia a jej riadenie sa stávali čím ďalej tým viac zložitejším problémom. Preto sa pristúpilo k rozdeleniu komunikačného procesu na niekoľko parciálnych podprocesov, ktoré predstavovali všeobecnejšie problémy riešenia. Každý takýto podproces bol označený ako **vrstva** (*layer*). Vrstva je fiktívny pojem, ktorý v sebe zahŕňa vlastnosti technického alebo programového vybavenia konkrétneho komunikačného zariadenia vykonávajúceho určité funkcie. Rozčlenenie do vrstiev odpovedá hierarchii činností, ktoré sa pri riadení komunikácie v elektronických komunikačných sieťach vykonávajú. Požiadavky kladené na komunikačnú sieť sú tak dekomponované na menšie celky, ktoré sa riešia samostatne a nezávisle na sebe.

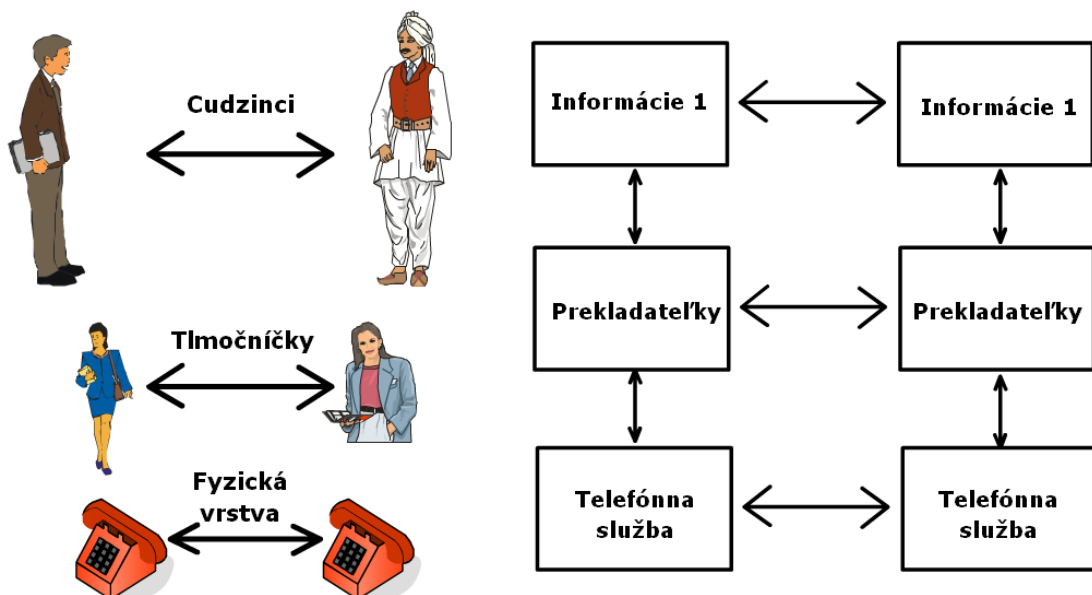
2.3.1.1 Príklad vrstvomého modelu ľudskej komunikácie

Princíp mechanizmu vrstvomého riadenia je možné vysvetliť aj na inom komunikačnom prostredí ako je elektronická komunikačná sieť. Komunikácia medzi dvoma zariadeniami a jej riadenie sa dá vysvetliť na príklade komunikácie dvoch cudzincov, obrázok 2.8. Každý z nich ovláda len svoj jazyk a preto musia vzájomnú komunikáciu riadiť tým, že si zaobstarajú prekladateľku do spoločného jazyka ak sú na vzdialených miestach aj komunikačnú službu, ktorou je v našom príklade telefónna služba. Vzájomne si obaja cudzinci vymieňajú

informácie, komunikujú medzi sebou. Z pohľadu skutočného prenosu informácie je táto komunikácia virtuálna nie reálna. V skutočnosti svoje informácie odovzdávajú svojim prekladateľkám a tie ďalej spolu komunikujú prostredníctvom telefónnej služby.

Ak sa na tento príklad pozrieme ako na vrstvomý model, na najvyššej vrstve sú dva subjekty, ktorými sú cudzinci, ktorý chcú spolu komunikovať. Na to, aby bola táto komunikácia úspešná, využívajú služby nižšej vrstvy, ktorými sú prekladateľky. Táto vrstva si musí najprv dohodnúť jazyk, v ktorom bude realizovaná komunikácia. Po dohodnutí spoločného dorozumievajúceho jazyka sa komunikácia posunie opäť o vrstvu nižšie, k telefónnej službe. Cudzinci využívajú služby prekladateľiek, čo je nižšia vrstva, prekladateľky využívajú telefónnu službu, čo je rovnako služba nižšej vrstvy. Pravidlá, ktoré dodržiavajú pri komunikácii na jednotlivých vrstvách sa všeobecne môžu označiť ako **protokoly**.

Pojem **komunikácia** možno vnímať z dvoch pohľadov. Komunikácia v zmysle výmeny obsahu vo vodorovnom smere, medzi cudzincami, medzi prekladateľkami, a skutočný prenos informácie komunikáciu vo zvislom smere. cudzinec – prekladateľka, prekladateľka– telefón.

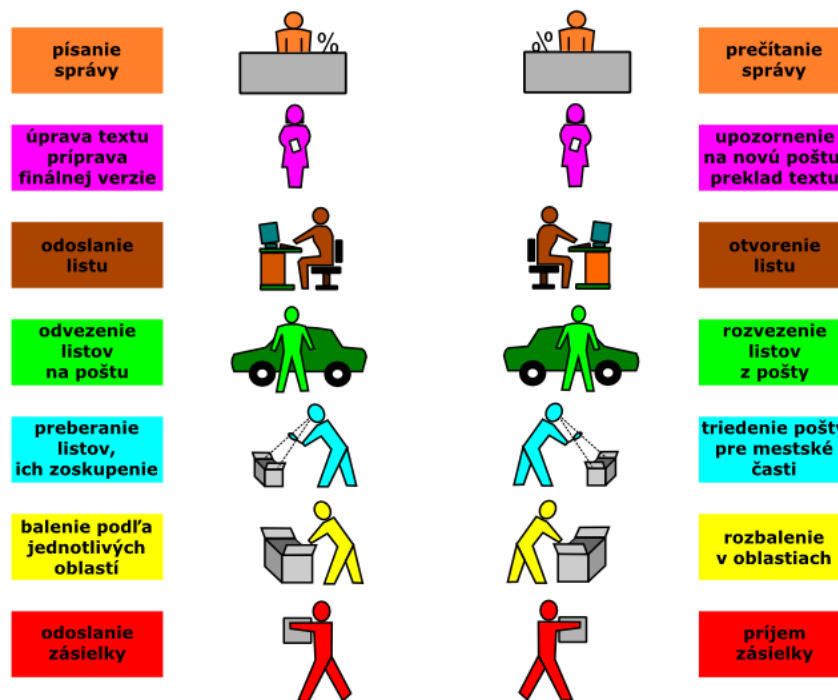


Obrázok 2.8. Trojvrstvová komunikácia medzi ľuďmi

2.3.1.2 Vrstvomý model v klasickej poštovej službe

Iným príkladom vrstvomého modelu je prenos informácie využitím poštovej služby. Na prenos informácie je v tomto prípade potrebných viac činností, ktoré majú veľa spoločného s elektronickým prenosom informácie. Prenos informácie začína vytvorením potrebného typu správy do ktorej je informácia uložená. Typ správy môže byť rôzny, písaný alebo tlačенý text, statický obraz prípadne audio alebo nahrávka na niektorom zo stand alone nosičov. Pokračuje úpravou správy a prípravou finálnej verzie správy pred odoslaním. Pre odoslanie je potrebné správu uložiť do obálky a napísať adresu. Obálku so správou je potrebné doručiť na poštu, kde je zatriedená do príslušného prepravného smeru. Všetky obálky so správami sú zabalené do prepravných kontajnerov a prepravované niektorým druhom dopravy do príslušného

vzdialeného poštového uzla. Tam je prepravný kontajner rozbalený, obálky so správami sú triedené pre jednotlivé územné celky a z pošty doručované k adresátovi. Adresát list otvorí, ak je potrebné tak ho upraví, prípadne odovzdá správu tomu, pre koho je informácia určená. Po prečítaní správy sa informácia dostane k požadovanému cieľu. Činnosti prenosu informácie poštovou službou sú podobné elektronickému prenosu informácie. Na obrázku 2.9 sú všetky potrebné činnosti uvedené vo vrstvách, ktoré odpovedajú vrstvovému modelu elektronickej komunikácie.



Obrázok 2.9 Vrstvový model komunikácie využitím poštovej služby

Vrstvový model elektronickej komunikačnej siete je založený na rovnakom princípe, ako vyššie uvedené vrstvové modely. Je však technicky zložitejší a má odporúčaný medzinárodný štandard.

2.4 Štandardizácia v komunikačných technológiách

Štandardy sú všeobecne určité dohodnuté normy, ktoré sú dodržiavané za určitým účelom. Štandardy v komunikačných technológiách sú pravidlá, ktoré umožňujú vzájomnú spoluprácu zariadení, vyrobených odlišnými výrobcami. Zameriavajú hlavne na rozhrania, ktoré špecifikujú vzájomné prepojenie rôznych zariadení. Rozlišujú sa dve skupiny štandardov. De facto štandardy, ktoré vznikli za nejakým účelom a svojim dominantným postavením sa stali štandardom. Druhú skupinu De jure štandardov tvoria štandardy vytvorené určitou štandardizačnou organizáciou. Príkladom môže byť štandard HTML (*Hypertext Markup Language*) pre tvorbu www stránok, ktorý bol vyvinutý ako De facto štandard a neskôr v roku 2000 bol prijatý ako ISO/IEC štandard 15445:2000, čím sa stal De jure štandard.

2.4.1 Štandardizačné organizácie

Štandardizačné organizácie pre oblasť komunikačných technológií sú vytvárané buď na základe medzivládnych dohovorov alebo ako dobrovoľné organizácie a ich pôsobnosť je buď celosvetová alebo je teritoriálne obmedzená. Medzi najznámejšie štandardizačné organizácie patria:

ITU (*International Telecommunication Union*), ktorá je celosvetovou medzivládnu organizáciou pre spoluprácu verejných a súkromných sektorov na rozvoji telekomunikácií. Vznikla v roku 1865 a jej úlohou bolo štandardizovať telekomunikácie, čo v tom čase predstavoval len telegraf. V rokoch 1956 – 1993 bola ITU rozdelená na CCITT (*Comité Consultatif International Télégraphique et Téléphonique*) a CCIR (*Comité Consultatif International Radiocomuniqué*), preto mnohé štandardy sú známe pod týmito označeniami. V súčasnosti je štruktúra ITU nasledovná:

- Konferencia vládnych z mocnencov – najvyššia autorita stanovuje smery normalizácie na nasledujúce 4 roky
- Rada ITU
- Svetové konferencie medzinárodných telekomunikácií
- Generálny sekretariát
- Normalizačné sektory:
 - Rádiokomunikačný sektor (ITU-R)
 - Telekomunikačný sektor (ITU-T)
 - Rozvojový sektor (ITU-D)

Jednotlivé normalizačné sektory majú 16 pracovných skupín podľa riešených oblastí. Výsledkom normalizačných aktivít sú série **odporúčaní** pre jednotlivé oblasti. Napríklad séria I je pre ISDN a B-ISDN. Štandardy sú dostupné v elektronickej forme z databázy ITU v Ženeve.

Slovensko má v súčasnosti v ITU dvoch členov. V kategórii M – veľký člen je s hlasovacím právom Ministerstvo dopravy a spojov, v kategórii m – malý člen so štatútom „Uznaný prevádzkovateľ“ je T-com.

ISO (*International Standards Organization*) je dobrovoľná medzinárodná organizácia pre tvorbu a šírenie technických štandardov a noriem pre priemysel a obchod. Vznikla v roku 1946. Nevyžaduje oficiálnych vládnych zástupcov a jej členmi sú aj národné štandardizačné organizácie z 89 členských štátov, medzi nimi ANSI – U.S., BSI – Veľká Británia, AFNOR – Francúzsko, DIN – Nemecko a iné. Štruktúra organizácie je nasledovná:

- technické výbory (TC – *Technical Committees*)
- pracovné podvýbory (SC – *Working Subcommittees*)
- pracovné skupiny (WG – *Working Groups*)

Najdôležitejšie výbory pre komunikačné technológie sú:

- TC 1 – pre telekomunikácie

- TC 97 – pre počítačové technológie, periférie a médiá.

V roku 1984 schválila organizácia model **OSI** (*Open Systems Interconnection*), ktorý sa stal medzinárodnou normou a slúži ako štandard pri tvorbe sietí.

ETSI (*European Telecommunication Standards Institute*) je európskou štandardizačnou inštitúciou, ktorá sa zaoberá tvorbou noriem pre výrobcov technických zariadení komunikačných technológií a ich používateľov. Združuje približne 500 členských organizácií z 32 európskych krajín, ktorými sú národné správy, verejní operátori sietí, používatelia, výrobcovia, privátni poskytovatelia služieb, výskumné inštitúcie a pod. Slovenská republika má troch členov, v kategórii štátna správa Ministerstvo dopravy pôšt a telekomunikácií, v kategórii operátori siete T-com a v kategórii výskumné inštitúcie Žilinská univerzita. Dokumenty publikované ETSI sú označované ako **reporty**, napríklad ETR 197 je ETSI Technical Report pre sieťové aspekty.

IETF (*Internet Engineering Task Force*) je otvorená organizácia formálne zastrešená internet Society – ISOC, ktorá vznikla v roku 1986. Vyvíja a podporuje internetové štandardy a úzko spolupracuje s konzorciom W3C – World Wide Web a s ISO. Zaoberá sa predovšetkým **štandardami TCP/IP** a internetovými protokolmi. Vydáva štandardy a nevyžaduje žiadne formálne členstvo. Všetci členovia sú dobrovoľníci a ich práca je financovaná zamestnávateľmi alebo sponzormi. Práca je organizovaná do pracovných skupín označovaných RFC (Request for Comments) a každá skupina pracuje na určitom konkrétnom riešení až do finálneho spracovania. Pracovné skupiny sú otvorené pre všetkých, ktorí sa chcú prác zúčastniť, diskutovať nad problémami alebo prednášať na stretnutiach. Na rozdiel od iných organizácií sa tu nehlasuje ale diskutuje. Oblasť riešenia sú kontrolované vedúcimi oblasťami, ktorí spolu s predsedníctvom IETF tvoria Internet Engineering Steering Group – IESG. Táto skupina je zodpovedná za celkovú činnosť IETF. Štandardizácia v oblasti internetu nie je oficiálne prijatá ako normalizačná činnosť a preto sú štandardy IETF označované ako De facto štandardy.

IEEE (*Institute of Electrical and Electronics Engineers*) je profesionálna organizácia elektronických inžinierov z asi 150 krajín, z celého sveta. Činnosť organizácie je rôznorodá. Vydáva odborné periodiká, knihy, organizuje konferencie a podporuje rozvoj odboru. IEEE je geograficky členené do desiatich oblastí a oblasti sa delia na sekcie. Pre potreby členov z Českej a Slovenskej republiky bola v roku 1992 založená Československá sekcia IEEE. Tá združuje viac organizácií. Pre oblasť komunikačných technológií je najdôležitejšia Československá národná organizácia spoločností pre obvody a systémy a komunikácie (*Circuits and Systems a Communications*). Známe sú štandardy LAN sietí, napríklad IEEE 802.3ab je označenie skupiny štandardov pre gigabitový Ethernet.

ANSI (*American National Standards Institute*) je americký normalizačný úrad, ktorý vytvára priemyselné štandardy v USA. Je členom organizácie ISO.

2.5 Vrstvový referenčný model elektronickej komunikačnej siete

Prvý štandard pre vrstvový model elektronickej komunikačnej siete bol vytvorený medzinárodnou štandardizačnou organizáciou ISO (*International Organisation for Standardisation*) a názov štandardu je *Reference Model of Open Systems Interconnection - Referenčný model prepojovania otvorených systémov, skratka OSI*. V praxi sa obvykle označuje skratkou RM OSI alebo ISO-OSI. Ako norma ISO má číslo 7498, ako odporúčanie organizácie CCITT (*Comité Consultatif International Télégraphique et Téléphonique*) má označenie X.200.

Dôvod pre vytvorenie štandardu spôsobil vývoj dátových a počítačových sietí rôznych koncepcií a od rozličných výrobcov, ktoré na začiatku vývoja uvedených sietí neboli kompatibilné. Jednotný štandard tak umožnil kompatibilitu komunikačných a počítačových systémov pochádzajúcich od rôznych výrobcov.

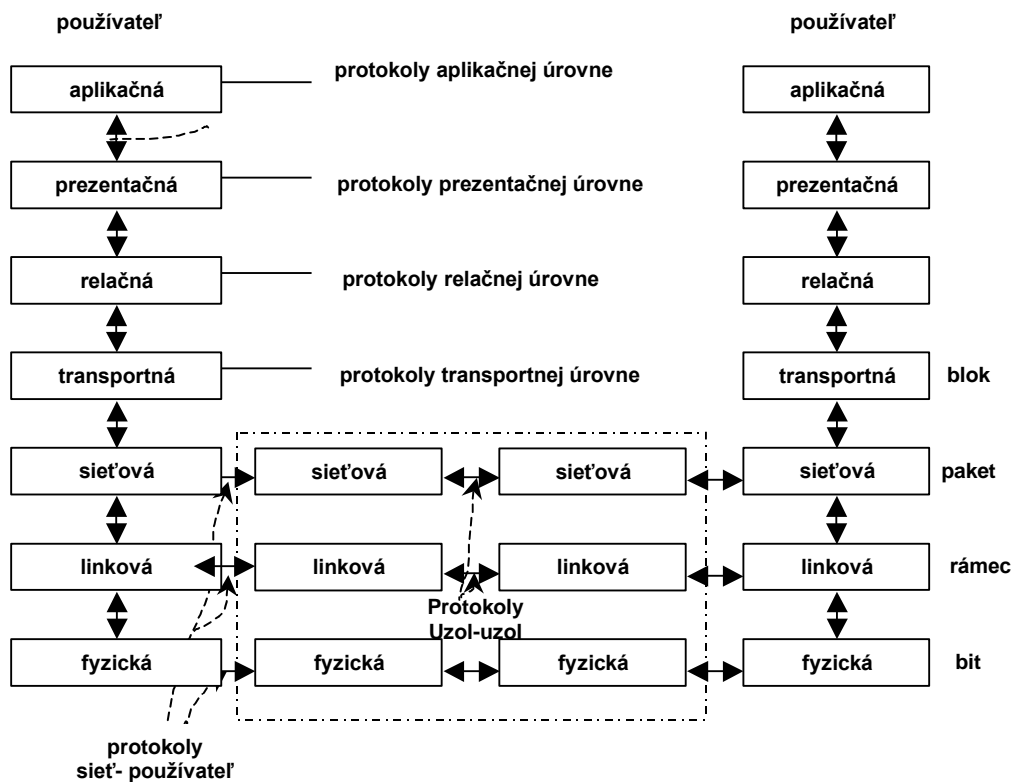
Pojem *Reference model (referenčný model)* znamená, že uvedený štandard nie je konkrétnym návrhom, ako riešiť vzájomné prepojovanie v konkrétnej komunikačnej sieti, ale je všeobecným modelom, podľa ktorého má byť vzájomné prepojovanie rôznych elektronickej komunikačných systémov riešené. Prívlastok **otvorený - open** zdôrazňuje, že systém, vyhovujúci štandardu je schopný vzájomného prepojenia so všetkými ostatnými systémami v sieti na celom svete, ktoré vyhovujú tomuto štandardu. Ide hlavne o základné programové vybavenie komunikačných sietí, ktoré bezprostredne ovláda technické prostriedky siete/sieťový hardvér a ich prostredníctvom prevádzku celej elektronickej komunikačnej siete.

Model OSI vytvára teoretickú predstavu o určitom počte vrstiev elektronickej komunikácie a o tom, čo je funkciou príslušnej vrstvy. Neurčuje konkrétne požiadavky, ako má ktorá vrstva svoje funkcie plniť. Funkcie konkrétnej technológie sú vyvíjané samostatne a sú špecifikované v „protokoloch“, ktoré sú neskôr implementované do modelu konkrétnej technológie. Ak je vrstvový model vytvorený pre konkrétnu technológiu, potom sa označuje ako **sieťová architektúra alebo protokolový sieťový model** príslušnej technológie.

OSI model vyjadruje princípy komunikácie. Je východiskovým modelom pre tvorbu sieťových architektúr. Je teoretickým základom pre realizáciu elektronickej komunikačných sietí.

2.5.1 Princíp komunikácie v OSI modeli

Referenčný model OSI rozdeľuje komunikáciu medzi dvoma komunikačnými zariadeniami A a B do siedmich **vrstiev (layers)**, ktoré sú znázornené na obrázku 2.8. Systém A a systém B sú koncové zariadenia elektronickej komunikácie, komunikačná sieť je znázornená dvoma uzlami medzi koncovými zariadeniami.



Obr. 2.8. Sedem vrstvový referenčný model OSI

Komunikáciu vo vrstvovom modeli je potrebné chápať z dvoch aspektov. Ako komunikáciu fyzickú a komunikáciu logickú. **Fyzická komunikácia** predstavuje prenos informácie zo zdrojového systému A do cieľového systému B. **Logická komunikácia** je virtuálna komunikácia medzi rovnoľahlými vrstvami. Logická a fyzická komunikácia sú vykonávané súčasne, ich rozlíšenie je potrebné pre pochopenie procesu komunikácie a úlohy komponentov komunikačného procesu.

Proces fyzickej komunikácie prostredníctvom OSI modelu možno popísať nasledovne. Na začiatku vznikne požiadavka v aplikačnej vrstve. Aplikačná vrstva požiada o vykonanie potrebných funkcií prezentačnú vrstvu. Prezentačná vrstva požiada o vykonanie ďalších funkcií relačnú vrstvu a takýto postup požiadaviek medzi susednými vrstvami končí na fyzickej vrstve, ktorá vytvára spojenie potrebných uzlov komunikačnej siete cez prenosové až do fyzickej vrstvy cieľového systému B. V systéme B je postup nasledovný. Fyzická vrstva poskytuje funkcie linkovej vrstve, linková vrstva poskytuje funkcie sieťovej vrstve a komunikácia končí na aplikačnej vrstve vytvorením komunikačného kanála alebo okruhu pre požadovanú službu elektronickej komunikačnej siete. Popísaný spôsob fyzickej komunikácie sa označuje ako **vertikálna komunikácia**, v obrázku 2.10 znázornená červenou farbou.

Logická komunikácia predstavuje zabezpečenie odpovedajúcich funkcie medzi rovnoľahlými vrstvami komunikujúcich zariadení. Partneri pri logickej komunikácii v sieti sú tie vrstvy, ktoré sa nachádzajú na rovnakej hierarchickej úrovni vrstiev komunikujúcich zariadení. Logická komunikácia je medzi všetkými rovnoľahlými vrstvami, s výnimkou

fyzickej vrstvy, ktorá je na obrázku 2.10 zároveň aj fyzickou komunikáciou. Komunikácia medzi rovnoľahlými vrstvami sa označuje ako **horizontálna komunikácia**.

Komunikačný proces v OSI modeli je vytváraný nasledovnými komponentmi:

1. **Protokol**, ktorý predstavuje súbor pravidiel, používaných pre vzájomnú komunikáciu rovnoľahlých vrstiev modelu, obr. 2.8. Prostredníctvom protokolu sú zabezpečované funkcie príslušných vrstiev. Pre jednu vrstvu môže byť špecifikovaných viac rôznych protokolov, označovaných aj ako sústava/rodina protokolov (*protocol suite*). Označenie protokolov je podľa názvu príslušnej vrstvy. V rámci aplikačných vrstiev obidvoch systémov je komunikácia aplikačným protokolom, v prezentačnej vrstve prezentačným protokolom, atď. Referenčný model ISO-OSI nešpecifikuje žiadne konkrétne protokoly, pomocou ktorých by funkcie jednotlivých vrstiev mali byť realizované. Referenčný model len vymedzuje jednotlivé vrstvy a špecifikuje funkcie, ktoré by tieto vrstvy mali riešiť. Protokoly pre jednotlivé vrstvy vznikajú ako samostatné štandardy. Výhoda vytvárania štandardov pre jednotlivé vrstvy je v tom, že pri zmene protokolu v jednej vrstve nie je potrebné meniť protokoly v iných vrstvách. Príklady niektorých protokolových štandardov na rôznych úrovniach OSI modelu sú v tabuľke 2.1.

Tabuľka 2.1 Príklady niektorých štandardov OSI modelu

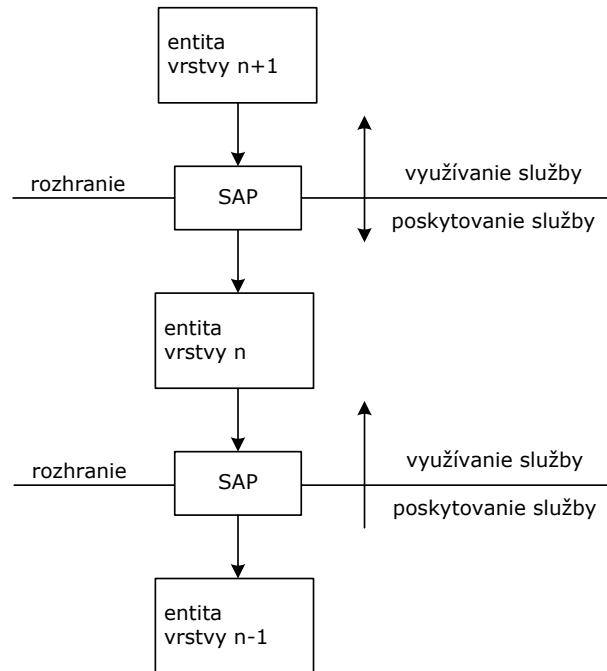
vrstva OSI/ štandardizačná organizácia	ITU	IETF	IEEE	IBM
7 Aplikačná	X.400	FTP, HTTP, SMTP, RTSP,		
6 Prezentačná	X.400, ASN.1,	TSL, SSL, SAP, PPTP		
5 Relačná	X.225	SSH		NetBios
4 Transportná		TCP, UDP, RTP, SCTP		
3 Sieťová	X.25, Frame Relay	IP, RIP, ARP, IPsec		
2 Linková	LAPB	PPP	802.xx	
1 Fyzická	X.21, PDH, SDH		802.xx	

2. **Služba**, označujúca množinu funkcií vykonávaných príslušnou vrstvou. Každá zo siedmich vrstiev OSI modelu vykonáva presne vymedzenú skupinu jednoznačne definovaných funkcií potrebných pre komunikáciu. **Vyššia vrstva využíva služby nižšej vrstvy a sama ponúka svoje služby bezprostredne vyššej vrstve.** Ale partnerom vzájomnej komunikácie dvoch systémov sú vrstvy rovnakej úrovne v rôznych uzloch siete. **Vrstvová služba alebo** služba príslušnej vrstvy je taká množina funkcií, ktoré príslušná vrstva poskytuje nadradenej vrstve. Pre vrstvovú službu sú používané aj pojmy poskytovateľ služby a používateľ služby. Poskytovateľ služby je nižšia vrstva a používateľ služby je vyššia vrstva.
3. **Rozhranie (*interfaces*)** je miesto, kde sa realizuje súčinnosť príslušných vrstiev pri zabezpečení služieb. Komunikácia medzi susednými vrstvami je

špecifikovaná vez prechodový bod označovaný *Service Acces Point - SAP*. Súčinnosť medzi rovnoľahlými vrstvami sa realizuje ako **peer to peer komunikácia**.

4. **Entita** je funkčná jednotka pre poskytovanie služby a jej aktivitou je vykonanie určitej funkcie. Entitou môže byť softvérový objekt, napríklad proces alebo na najnižších vrstvách hardvérový prvok.

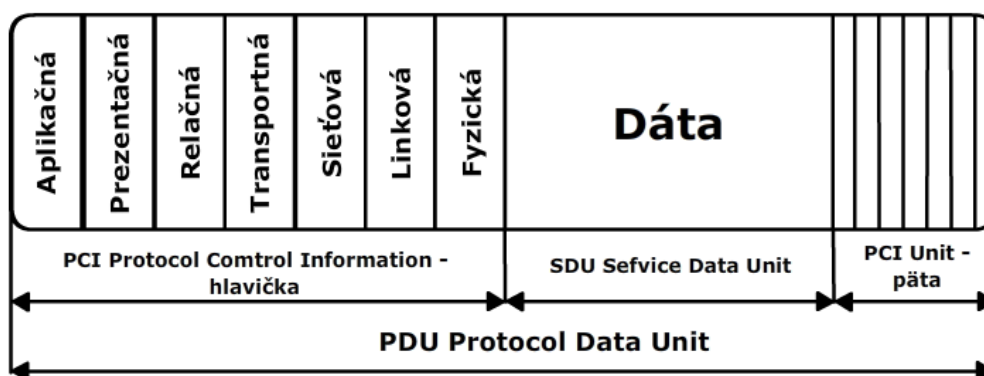
Znázornenie vertikálnej komunikácie prostredníctvom vrstvových služieb je na obrázku 2.11.



Obr. 2.11 Znázornenie vrstvovej komunikácie prostredníctvom vrstvových služieb

2.5.2 Prenos dát v OSI modeli

Výmena informácií medzi rovnoľahlými vrstvami je uskutočňovaná pomocou protokolu príslušnej vrstvy prostredníctvom blokov, označovaných **protokolárne dátové jednotky (PDU- Protocol Data Units)**. Obrázok 2.12 zobrazuje všeobecnú protokolovú dátovú jednotku - PDU OSI modelu. PDU obsahuje užitočné používateľské dáta označené *SDU – Service Data Unit* a hlavička (*header*) a päta (*trailers*) s kontrolnými informáciami (*PCI – Protocol Control Information*).

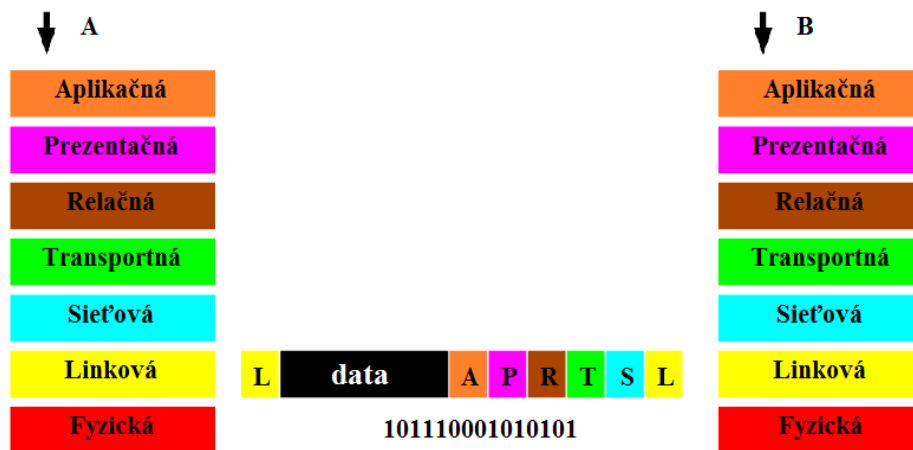


Obr. 2.12 Všeobecný OSI protokol

PDU sa vytvára poskytovaním vrstvových služieb v zdrojovom systéme tak, že sa pri prechode z vyššej vrstvy k nižšej pridávajú k používateľským dátam do hlavičky a päty PDU protokolové riadiace informácie jednotlivých vrstiev. Dochádza k postupnému **zapuzdrovaniu** (*encapsulate*) pôvodnej informácie. Zapuzdrovaním sa takto pridávajú k dátam pred prenosom po komunikačnom médiu potrebné informácie protokolov jednotlivých vrstiev. Pri zapuzdrovaní sa pri každom príchode na novú vrstvu blok prenášaných informácií zväčší o blok informačných dát príslušnej vrstvy. Keď sa blok dát dostane až k najnižšej vrstve, nasleduje prenos po prenosovom médiu k ďalšiemu uzlu siete a postupne k príjemcovi dát. U príjemcu sa riadiace informácie jednotlivých vrstiev postupne spracovávajú a prostredníctvom vrstvových služieb sa vykonávajú ich funkcie. Dochádza k „odpuzdrovaniu“ zapuzdrovaných dát a v aplikačnej vrstve objavia len prenášané používateľské dáta.

Keď riadiace informácie pridajú aplikačná, prezentačná, relačná a transportná vrstva, vytvoria PDU transportnej vrstvy, ktorá sa označuje **segment**. Je to PDU štvrtej vrstvy. Sieťová vrstva poskytuje službu transportnej vrstvy a transportná vrstva jej odovzdáva dáta. Sieťová vrstva zapuzdruje dáta z transportnej vrstvy a pripojením hlavičky ich prenáša rôznymi uzlami siete. Takto zostavená jednotka sa označuje **paket**. Je to PDU tretej vrstvy. Linková vrstva poskytuje službu sieťovej vrstvy. Zapuzdruje informáciu od sieťovej vrstvy do čo je PDU druhej vrstvy, ktorá sa označuje **rámec**. Linková vrstva poskytuje tak sieťovej vrstve službu zapuzdrením informácií sieťovej vrstvy do rámca. Fyzická vrstva poskytuje službu vrstve linkovej. Fyzická vrstva zakóduje linkový rámec do **postupnosti bitov** pre prenos po prenosovom médiu na prvej vrstve.

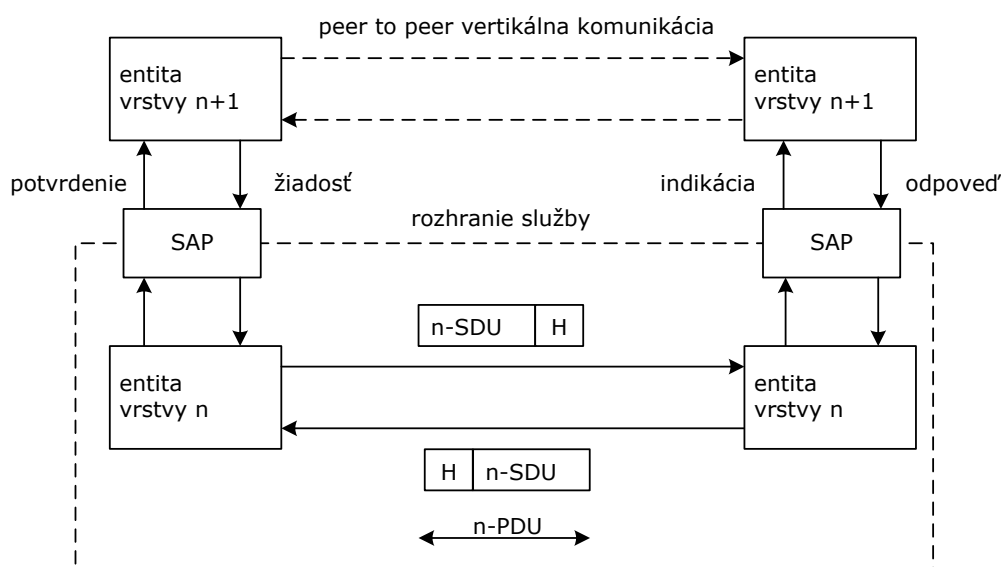
Znázornenie zapuzdrenia je na obr. 2.13.



Obr. 2.13 Zapuzdrenie dát

2.5.3 Vrstvové služby

Komunikácia medzi entitami rovnakých vrstiev dvoch komunikujúcich systémov je virtuálna, pretože medzi nimi nie je vytvorený žiadny priamy komunikačný kanál. Fyzicky sa realizuje prostredníctvom protokolovej dátovej jednotky PDU, ktorú entity n+1vej vrstvy prenesú ako blok informácií do nižšej n-tej vrstvy cez softvérový port označovaný ako **SAP - Service Access Point**. Každý SAP je označený unikátnym identifikátorom, spravidla číslom portu. Entita n-tej vrstvy použije svoje PCI na vytvorenia záhlavia, ktoré pripojí k SDU a tak vytvára PDU n-tej vrstvy. Na prijímacej strane n-tá vrstva použije záhlavie PCI na vykonanie protokolu a doručí SDU odpovedajúcej n+1 vrstve. Inak povedané, vrstva n+1 je používateľ služby poskytovanej vrstvou n. Poskytovanie služby vrstvou n znamená správne vykonanie požiadavky na prenos jej PDU. Znázornenie vrstvových služieb je na obrázku 2.14.



Obr. 2.14 Vrstvové služby a primitívy služieb

Poskytovanie a používanie vrstvovej služby je realizované pomocou primitív služieb (*service primitive*), ktorými sú:

- Žiadosť (Request)
- Indikácia (Indication)
- Odpoveď (Response)
- Potvrdenie (Confirmation)

Funkcie jednotlivých primitív služieb - *service primitive* sú nasledovné:

- Žiadosť (*Request*), ktorú generuje entita používateľa služby v zdrojovom systéme, aby vyvolal určitú službu a odovzdala poskytovateľovi služby parametre potrebné k úplnej špecifikácii požadovanej služby.
- Indikácia (*Indication*), ktorú generuje entita poskytovateľa služby, aby upozornila používateľa služby, že partnerský používateľ služby (na zdrojovom systéme) vyvolal akciu.
- Odpoveď (*Response*), ktorú generuje entita používateľa služby, aby potvrdil, že bola dokončená procedúra v predošlom kroku, ktorú používateľ vyvolal.
- Potvrdenie (*Confirmation*), ktorú generuje entita poskytovateľa služby a dáva tak správu pre entitu používateľa služby o výsledku procedúry, ktorú vyžadoval predšlou požiadavkou .

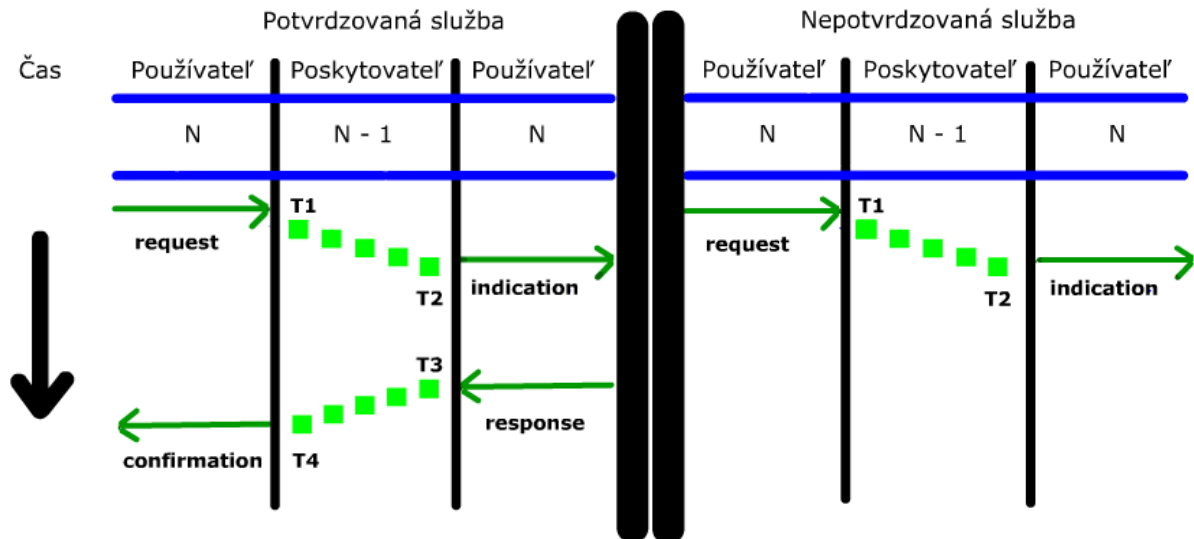
Služby poskytované príslušnou vrstvou môžu byť nespojovo alebo spojovo orientované.

Pri **spojovo orientovaných** službách je vytvárané virtuálne spojenie, ktoré má 3 fázy:

1. Vytvorenie spojenia medzi dvomi vrstvami cez SAP. Nastavenie obsahuje dohodnutie parametrov komunikácie.
2. Prenos SDU na základe protokolov.
3. Zrušenie spojenia a uvoľnenie alokovaného miesta pre spojenie.

Pri **nespojovo orientovaných** službách vyššie uvedený trojfázový proces nie je potrebný, pretože sa SDU posieľa priamo cez SAP bez vopred vytvoreného spojenia. V tomto prípade, však musia kontrolné informácie v SDU obsahovať všetky adresné informácie na jej prenos.

Služby poskytované vrstvami môžu byť **potvrdzované** alebo **nepotvrdzované**. Záleží to na tom, či odosielateľ musí byť informovaný o výsledku alebo nie. Príklad potvrdzovanej a nepotvrdzovanej služby je na obr. 2.15.



Obr. 2.15 Príklady potvrzovanej a nepotvrzovanej služby

2.5.4 Charakteristiky vrstiev OSI modelu

Aplikačná vrstva je z pohľadu hierarchického usporiadania RM OSI poslednou siedmou vrstvou. Je však prvou vrstvou z pohľadu použitia koncovým používateľom. Základnou funkciou aplikačnej vrstvy je poskytovať služby koncovému používateľovi tým, že umožňuje komunikáciu medzi aplikačnými procesmi prostredníctvom aplikačných protokolov. Poskytovanie služieb je realizované prostredníctvom používateľských aplikácií. Medzi najpoužívanejšie služby tejto vrstvy patria:

- Elektronická pošta
- World Wide Web
- File Transfer Protocol (FTP)
-

Aplikačná vrstva sprístupňuje informačno-komunikačným systémom a ich službám prostredie OSI.

Prezentačná vrstva je šiestou vrstvou RM OSI modelu. Poskytuje vrstvomé služby aplikačnej vrstve a požaduje vrstvomé služby od relačnej vrstvy. Jej základnou funkciou je poskytovanie služieb pre reprezentáciu/interpretáciu vymieňajúcich dát tak, aby odpovedali požiadavke aplikačnej vrstvy. Dáta zdrojového systému sú transformované do spoločného štandardného formátu v ktorom sú prenášané po komunikačnej sieti a v cieľovom systéme sú transformované do tvaru požadovaného aplikačnou vrstvou cieľového komunikačného systému. Prezentačná vrstva zabezpečuje zhodu v syntaxi a sémantike dát využívaním kódovanie, kompresie, šifrovania a iných techník.

Prezentačná vrstva zabezpečuje interpretáciu/reprezentáciu vymieňaných dát.

Relačná vrstva je piatou vrstvou RM OSI. Poskytuje služby prezentačnej vrstve a požaduje služby od transportnej vrstvy. Základnou funkciou relačnej vrstvy je vytvorenie,

udržiavanie a rušenie relácie medzi koncovými používateľmi. Relácia je chápaná ako vytvorenie logického spojenia komunikujúcich systémov pre dialóg. Pre vytvorenie relácie požaduje od transportnej vrstvy vytvorenie spojenia, prostredníctvom ktorého je vykonávaná komunikácia v rámci danej relácie. Po vytvorení relácie nastáva fáza prenosu dát, pri ktorej môže dôjsť ku chybám na niektorej nižšej vrstve. Pri rozpoznaní a korekcii chyby niektorou z nižších vrstiev, je možné po odstránení chýb opäť pokračovať v odosielaní dát, aj napriek tomu, že by sa muselo znovu nadviazať spojenie.

Relačná vrstva poskytuje informačným systémom nástroje pre riadenie a synchronizáciu ich dialógov.

Transportná vrstva je štvrtou vrstvou RM OSI. Poskytuje službu relačnej vrstve a požaduje službu od sieťovej vrstvy. Protokoly transportnej vrstvy vytvárajú zo správ prijatých z vyšších vrstiev bloky informácií označované ako **segmenty**, ktoré sú prenášané medzi komunikujúcimi systémami. Správy musia byť prijaté v rovnakom poradí, ako boli vyslané. Základnou funkciou transportnej vrstvy je vytvorenie, udržiavanie a ukončenie spojenia medzi komunikujúcimi systémami. Transportné spojenie je vytvorené end to end komunikáciou, ktorú mu sprostredkuje sieťová vrstva. Medzi rovnakým párom transportných adries môže byť vytvorených viac transportných spojení, každé pre inú službu aplikačnej vrstvy. Transportná vrstva tvorí rozhranie medzi koncovými zariadeniami a komunikačnou sieťou.

Transportná vrstva upravuje bloky dát pre prenos medzi koncovými zariadeniami a zabezpečuje požadovanú kvalitu prenosu.

Sieťová vrstva je treťou vrstvou RM OSI. Poskytuje službu transportnej vrstve a požaduje službu od linkovej vrstvy. Sieťová vrstva vytvára optimálny komunikačný okruh v sieti, podľa požiadaviek transportnej vrstvy. Prenos je realizovaný blokmi dát označovanými ako **pakety**. Pre vytvorenie komunikačného okruhu používa sieťové adresovanie. V uzloch siete sú pakety smerované prostredníctvom smerovacích protokolov, ktoré obsahujú procedúry pre výber najvhodnejšej cesty v sieti. Uzly musia navzájom spolupracovať, aby smerovanie bolo efektívne, preto je táto vrstva najkomplexnejšia v referenčnom modeli OSI. Okrem smerovania a adresovania je v sieťovej vrstve realizované riadenie toku dát, ktoré zabraňuje zahlteniu siete.

Sieťová vrstva smeruje tok prenášaných dát zoskupených do paketov a vytvára prenosový okruh medzi komunikujúcimi koncovými zariadeniami.

Linková vrstva, označovaná aj ako dátová alebo spojová, je druhou vrstvou RM OSI. Poskytuje službu sieťovej vrstve a požaduje službu od fyzickej vrstvy. Linková vrstva zabezpečuje prenos dát vo forme rámcov medzi dvoma uzlami, medzi ktorými je fyzické spojenie. Zabezpečenie prenosu je realizované synchronizáciou a reguláciou dátového toku a zabezpečením a opravou chýb pri prenose medzi danými uzlami. Pre sieťovú vrstvu vytvára komunikačný okruh a od fyzickej vrstvy vyžaduje prenos dát ako postupnosť bitov.

Linková vrstva mení tok bitov z fyzickej vrstvy na rámce a vytvára tak spoľahlivú cestu prenosu dátových blokov vo forme rámcov medzi dvomi bodmi elektronickej komunikačnej siete.

Fyzická vrstva, je prvou vrstvou RM OSI. Poskytuje službu linkovej vrstve tým, že prenáša jednotlivé bity prostredníctvom fyzického komunikačného kanála. Zabezpečuje elektrické, mechanické a optické rozhrania pre vytvorenie, udržanie a ukončenie fyzického prenosového okruhu medzi koncovými zariadeniami. Fyzická vrstva špecifikuje parametre prenosového média, napríklad úroveň prenosu, frekvenčné spektrum, ako aj mechanické vlastnosti, napríklad konektory pre pripojenie. Je reálnym fyzickým prepojením medzi uzlami komunikačnej siete.

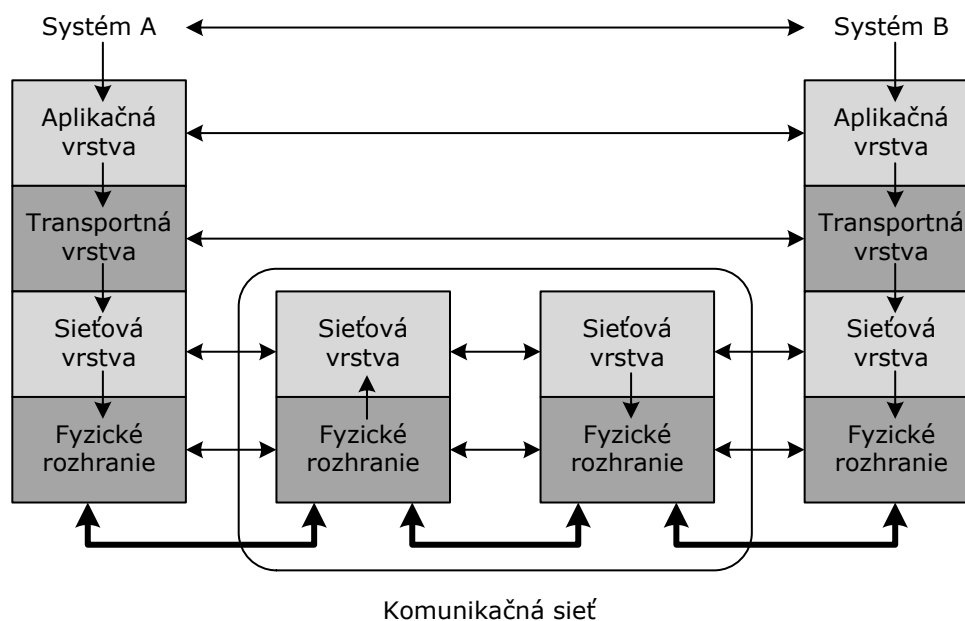
Fyzická vrstva prenáša tok bitov prenosovým médium, ktoré má špecifikované prenosové parametre.

2.6 Sieťové architektúry

Pravidlá vrstvových modelov nie sú uplatnené len pre referenčný model OSI. Sú používané aj v sieťových architektúrach. Sieťová architektúra príslušnej technológie je koncept pre návrh konkrétnej komunikačnej siete. Má špecifikovaný model vrstiev, služieb, funkcií a protokolov tejto technológie, čo je v podstate rozšírenie RM OSI o špecifikáciu protokolov príslušnej technológie. V sieťovej architektúre konkrétnej technológie nemusia byť špecifikované všetky vrstvy. V takomto prípade nie je vynechaná funkcia žiadnej vrstvy referenčného modelu OSI, ale niektoré vrstvy nemusia byť aktívne. Takéto vrstvy sa označujú ako nulové alebo transparentné. Okrem protokolov má sieťová architektúra špecifikovanú aj topológiu a prístupovú metódu. Často krát je v sieťovej architektúre elektronických komunikačných služieb aj podrobný popis produktov a služieb.

Sieťová architektúra TCP/IP je v súčasnosti najznámejšou sieťovou architektúrou. Tvoria ju súbor protokolov, ktoré umožňujú komunikáciu v rôznych typoch sietí. Architektúra TCP/IP bola vyvinutá pri riešení paketovej siete ARPANET, neskôr bola štandardizovaná organizáciou IETF – *Internet Engineering Task Force*.

Sieťová architektúra TCP/IP pozostáva zo štyroch vrstiev, ktoré sú znázornené na obr. 2.16.



Obr. 2.16 TCP/IP sieťová architektúra

Aplikačná vrstva poskytuje aplikačné programy, ktoré na rozdiel od OSI modelu komunikujú priamo s transportnou vrstvou. Protokoly využívané v aplikačnej vrstve sú napríklad TELNET, FTP, SMTP, DNS.

Transportná vrstva vytvára komunikáciu medzi koncovými zariadeniami. Táto vrstva využíva dva protokoly. TCP (*Transmission Control Protocol*), ktorý zabezpečuje spoľahlivú spojovo orientovanú službu. To znamená, že cieľový komunikačný systém potvrdzuje prijímané dáta. UDP (*User Datagram Protocol*) nezaistuje spoľahlivosť prenosu, prenesené dáta nie sú potvrdzované.

Sieťová vrstva označovaná aj internetová alebo IP, zabezpečuje, aby sa jednotlivé pakety dostali od zdroja k cieľu cez elektronickú komunikačnú sieť. K tomu využíva IP protokol.

Vrstva sieťového nie je bližšie špecifikovaná. Je závislá na použitej prenosovej technológii. Táto vrstva zabezpečuje všetko, čo je spojené s fyzickým prenosom dát.

Sieťová architektúra TCP/IP je architektúrou siete internet. Princípy komunikácie po vrstvách, vysvetľované pre RM OSI, platia aj v tejto architektúre.

2.6.1 Porovnanie RM OSI a architektúry TCP/IP

RM OSI aj TCP/IP architektúra majú mnoho spoločného. Obidva modely sú založené na používaní vrstvových protokolov. Približne rovnaká je aj funkčnosť vrstiev. Napriek týmto základným podobnostiam sú tu nasledovné odlišnosti.

1. Vytvorenie modelu

- a. RM OSI model bol navrhnutý skôr ako boli vytvorené konkrétne protokoly určitej technológie.
- b. TCP/IP architektúra využila princípy vrstvomého modelu, ale tieto boli špecifikované až potom, keď boli navrhnuté samotné protokoly.

2. Počet vrstiev

- a. RM OSI model má 7 vrstiev
- b. TCP/IP architektúra má 4 vrstvy. TCP/IP považuje vrchné tri vrstvy OSI modelu (aplikačná, prezentačná a relačná) za jedinú aplikačnú vrstvu a vrstva linková a fyzická tvoria vrstvu sieťového rozhrania. Porovnanie TCP/IP architektúry voči RM OSI je obrázku 2.17.



Obr. 2.17. Porovnanie TCP/IP architektúry voči RM OSI

3. Popis modelu

- a. RM OSI rozlišuje pomerne striktne medzi tromi základnými pojmami: služba, rozhranie, protokoly. Definícia služby hovorí o tom, čo vrstva robí. Vrstvomé rozhranie určuje procesom vyššej vrstvy ako do neho vstupovať. Protokoly špecifikujú, ako má vrstva využívať služby. Je to všeobecná špecifikácia princípu elektronickej komunikácie.
- b. TCP/IP sieťová architektúra nerozlišuje striktne služby, rozhrania a protokoly a tak nerozlišuje medzi špecifikáciou a implementáciou. Sieťová architektúra je predpis, ako vytvárať sieť s určitou technológiou. Iné technológie sa takto vytvárať nedajú. TCP/IP model nie je referenčný model, pretože je použiteľný iba pre konkrétnu technológiu a potom je správne označenie TCP/IP sieťová architektúra, alebo protokolový sieťový model TCP/IP.

4. Využitelnosť

- a. RM OSI model bol prvý krát použitý pri návrhoch dátových sietí podľa protokolu ITU-T X.25. Až zhruba do začiatku roku 1990, bola X.25 jedinou technológiou, ktorá bola používaná pre dátové prenosy. Za dobu

vývoja prenosu dát sa k zmenili mnohé z pôvodných predpokladov, z ktorých koncepcia X.25 vychádzala. Napríklad, zlepšila sa spoľahlivosť prenosových ciest sa a tak výrazne poklesla i potreba zložitých mechanizmov pre zaistenie spoľahlivosti na nižších vrstvách. Naopak výrazne vzrástol dopyt po rýchlosti a priepustnosti prenosových kanálov siete. Zmena nastala i v paradigme spoľahlivosť prenosu. Spoľahlivý prenos nie je jediný, ktorý je požadovaný. Mnohé aplikácie dávajú prednosť rýchlosti, zatiaľ čo spoľahlivosť si radšej zaistia samé, pretože tá ktorú by poskytovala prenosová časť siete pre ne nie je dostatočná.

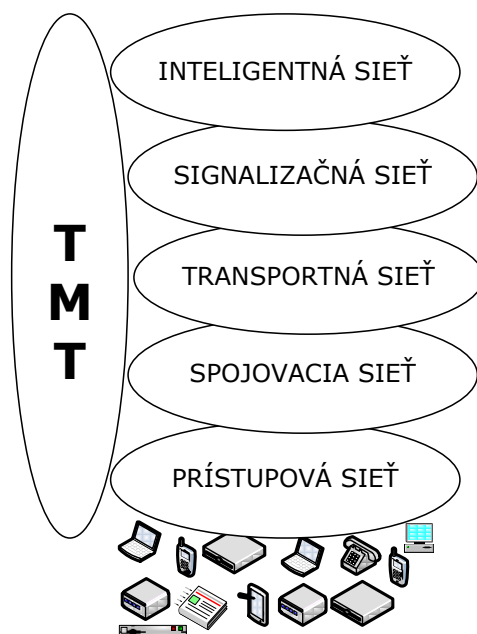
- b. TCP/IP sieťová architektúra sa stala veľmi perspektívnou technológiou práve kvôli tomu, že odstraňuje nedostatky technológie X.25.

2.6.2 Úrovňové modely sietí

Architektúry komunikačných sietí znázornené vrstvomými modelmi vyjadrujú konkrétnu technológiu, tak ako to bolo vysvetlené pre technológiu TCP/IP. Analogicky sú zostavené napríklad vrstvomé modely technológie ISDN (*Integrated Services Digital Network*) alebo ATM (*Asynchronous Transfer Mode*). V literatúre možno nájsť vyjadrenie pojmu architektúra sietí aj v iných súvislostiach. Napríklad pri riešení celkového konceptu návrhu a realizácie siete na konkrétnom území, alebo v súvislosti s integráciou sietí rôznych technológií. V takýchto prípadoch sa pre znázornenie architektúry používajú úrovňové modely v angličtine označované ako *level* alebo *plane*.

2.6.2.1 Úrovňový model telekomunikačnej siete

Príklad úrovňového modelu telekomunikačnej siete je na obrázku 2.18. Vyjadrené úrovne boli popísané v súvislosti s modernizáciou telekomunikačnej siete na Slovensku. Úrovne označujú integráciu v nových technológiách do existujúcej siete.



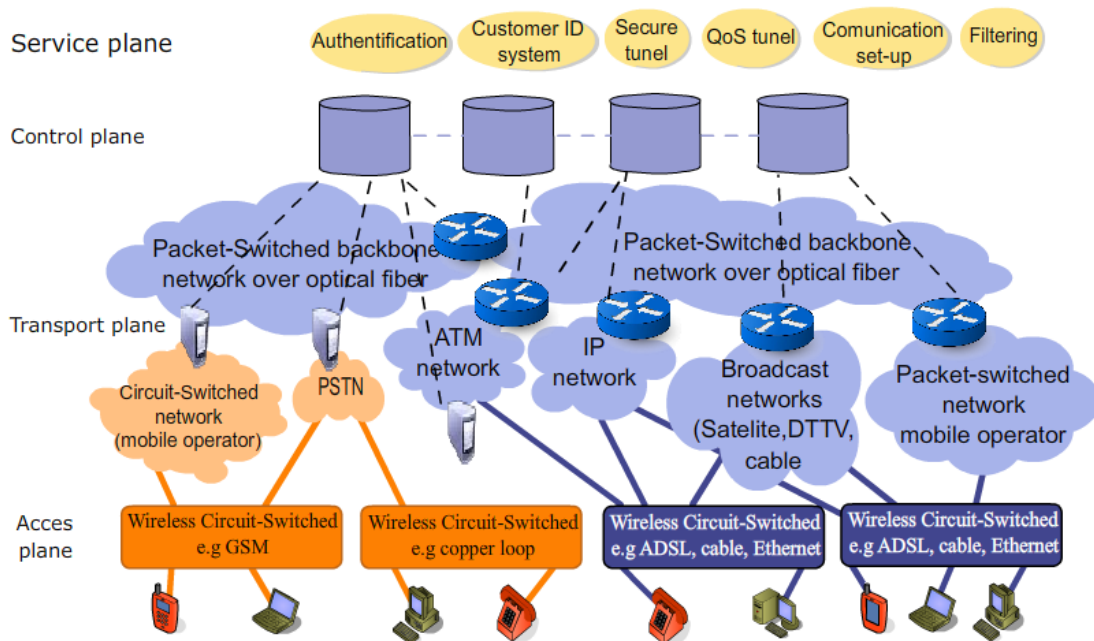
Obr. 2.18 Úrovňový model telekomunikačnej siete

2.6.2.2 Úrovňový model NGN (Next Generation Network)

Siete budúcej generácie označované ako NGN sú charakterizované ako jedna spoločná sieť pre prenos všetkých informačných typov. Takáto sieť poskytuje služby založené na všeobecnom koncepte RM OSI, ale cez rôzne sieťové architektúry, ktoré navzájom spolupracujú. Funkcie popísané v rámci RM OSI budú vo väčšine podsystémov poskytované. Ale funkcie v rámci siete NGN budú vrstvené odlišným spôsobom, preto sú označované ako plane - úroveň. Konkrétne funkcie modelu OSI, ktoré sú vhodné či nevhodné pre model NGN, sú popísané v dodatku odporúčania ITU-T Y.2011.

Základnou charakteristikou modelu NGN je oddelenie služieb a prenosu. Takéto oddelenie umožňuje poskytovať zvlášť komunikačné a prenosové služby alebo ich kombináciu. Oddelenie služieb je vo vrstvovom modeli vyjadrené dvomi vrstvami. Funkcie prenosových služieb sú realizované na **úrovni prenosu** a funkcie komunikačných služieb a aplikácií sú realizované na **úrovni služieb**. Na úrovni služieb môžu byť poskytované všetky typy služieb.

Ďalšie horizontálne roviny sú úroveň riadenia a úroveň prístupu. Úroveň prenosu predstavuje vrstvy 1 až 3 modelu OSI, pričom môže byť použitá akákoľvek technológia. Pre poskytovanie služieb je preferovaný IP protokol. Príklad úrovni siete NGN je znázornený na obr. 2.19.



Obr. 2.19. Príklad úrovni v NGN

2.7 Záver

Modely v komunikačných sieťach vyjadrujú abstraktné znázornenie konkrétneho komunikačného systému. Základným modelom pre vyjadrenie komunikácie je Shannon - Weaverov model, ktorý je nielen pri elektronickej komunikácii, ale aj pri ľudskej komunikácii. Tento model znázorňuje postupnosť komunikačných aktivít, ale nerieši mnohé problémy elektronickej komunikácie.

Druhým typom modelov sú modely fyzického usporiadania prvkov komunikačnej siete. Dávajú prehľad nielen o topológii siete, ale aj o spolupráci viacerých typov sietí, ktoré sa označujú interworking.

Tretím typom modelov sú vrstvomé modely, ktoré na rozdiel od predošlých, sú abstraktným vyjadrením komunikácie prostredníctvom protokolov. Protokolom je nazvaný súbor pravidiel, ktoré sa používajú pre vzájomnú komunikáciu. Všeobecným vrstvomým modelom je RM OSI **Referenčný model *Open System Interconnection***, štandardizovaný podľa ISO aj ITU. Princíp komunikácie po vrstvách je založený na poskytovaní služieb medzi jednotlivými vrstvami cez špecifikované rozhrania. Je štandardom a základným modelom pre vytváranie **protokolových modelov** rôznych technológií, ktoré sa označujú **ako sieťové architektúry**. Príkladom sieťovej architektúry je protokolový model TCP/IP.

Štvrtým typom modelov sú úrovňové modely. Vyjadruje sa nimi hlavne integrácia rôznych technológií a systémov.

Kľúčové slová:

1. *Sieťový model*
2. *Shannon-Weaverov model*
3. *Model fyzického usporiadania siete*
4. *Topológia sietí*
5. *Fyzická topológia*
6. *Logická topológia*
7. *Základný úrovňový model siete*
8. *Vrstvový model siete*
9. *Komunikácia vo vrstvovom modeli*
10. *Štandardizačné organizácie*
11. *RM OSI*
12. *Vrstva*
13. *Protokol*
14. *Rozhranie*
15. *Vrstvová služba / service primitive*
16. *Zapuzdrenie/encapsulate*
17. *PDU –Protocol Data Unit*
18. *SDU – Service Data Unit*
19. *Spojovo a nespojovo orientované služby*
20. *Potvrdzované a nepotvrdzované služby*
21. *Segment*
22. *Paket*
23. *Rámec*
24. *Sieťová architektúra/protokolový sieťový model*
25. *Sieťová architektúra TCP/IP*
26. *Sieťová architektúra NGN*

Kontrolné otázky

1. Čo predstavuje modelovanie v komunikačných technológiách?
2. Aké typy modelov sú používané v elektronickej komunikácii a jej systémoch?
3. Čo znázorňuje Shannon-Weaverov/lineárny model komunikácie?
4. Z akých komponentov sa skladá Shannon-Weaverov/lineárny model komunikácie?
5. Čo je možné rozumieť pod pojmom informačný zdroj?
6. Čo je možné rozumieť pod pojmom kóder?
7. Čo je možné rozumieť pod pojmom kanál?
8. Čo je možné rozumieť pod označením dekóder?
9. Čo je možné rozumieť pod označením prijímač správy?
10. Čo spôsobuje šum v prenosovom reťazci?
11. Aký je význam spätnej väzby v prenosovom reťazci?
12. Aký je vzťah medzi lineárnym modelom komunikácie a fyzickým modelom elektronickej komunikačnej siete?
13. Čo znamená pojem topológia siete?
14. Aké druhy topológie sú rozlišované?
15. V čom je rozdiel medzi fyzickou a logickou topológiou?
16. Ktoré topológie sú používané v elektronických komunikačných sieťach?
17. Ktoré topológie/topológie je najčastejšie používaná v LAN?
18. Čo vyjadruje všeobecný model fyzického usporiadanie elektronickej komunikačnej siete?
19. Aké úrovne sú rozlišované základnom úrovňovom modeli?
20. Aké druhy sietí sú rozlišované v základnom úrovňovom modeli?
21. Aký bol dôvod pre vytvorenie vrstvových modelov v elektronických komunikačných sieťach?
22. Čo predstavuje pojem vrstva vo vrstvových modeloch komunikácie?
23. Ako je vnímaný pojem komunikácia vo vrstvovom modeli?
24. Aký je dôvod pre štandardizáciu v komunikačných technológiách?
25. Ktoré z organizácií sú štandardizačné organizácie pre komunikačné technológie?
26. Čo znamená označenie RM OSI?
27. Čo znamená vyjadrenie Open System Interconnection?

28. Prečo bol vytvorený referenčný model pre vrstvovú komunikáciu v elektronických komunikačných sieťach?
29. Aký je rozdiel medzi sieťovým modelom OSI a sieťovou architektúrou?
30. Prečo bolo v OSI modeli navrhnutých 7 vrstiev?
31. Aký význam majú protokoly vo vrstvových modeloch?
32. Aká je úloha rozhrania medzi vrstvami?
33. Ako navzájom spolupracujú vrstvy vo vrstvovom modeli komunikačnej siete?
34. Čo je úlohou vrstvových služieb?
35. Ktorý z postupov je platný pre zapuzdrowanie?
36. Aký je rozdiel medzi blokom informácií na dvoch susedných vrstvách?
37. Ktoré z popísaných vyjadrení platia pre PDU – protokolárne dátové jednotky?
38. Z akých častí sa skladá všeobecný OSI protokol?
39. Ktoré vyjadrenie platí pre vzťah medzi PDU a SDU?
40. Ako je označovaná komunikácia medzi rovnoľahlými vrstvami?
41. Ktoré z uvedených príkazov požívajú service primitive?
42. Aká je úloha služby request?
43. Aká je úloha služby indication?
44. Aká je úloha služby response?
45. Aká je úloha služby confirmation?
46. Ktoré z vyjadrení platí pre spojovo orientovanú službu?
47. Ktoré z vyjadrení platí pre nespojovo orientovanú službu?
48. Aký je rozdiel medzi potvrdzovaou a nepotvrdzovanou službou?
49. Kde je vytvárané zoskupenie dát označované ako segment?
50. Prečo je vytvárané zoskupenie dát označované ako paket?
51. V ktorej vrstve OSI modelu je používané zoskupenie dát označované ako rámec a aká je jeho úloha?
52. Koľko špecifikovaných vrstiev má sieťová architektúra TCP/IP a prečo?
53. Ktoré vrstvy OSI modelu sú zhodné s TCP/IP architektúrou?
54. Ktoré vyjadrenia sú platné pre rozdiely RM OSI a TCP/IP architektúry?
55. V čom sa líšia sieťové architektúry iných technológií od OSI modelu?
56. Aký je vzťah OSI modelu a úrovňového modelu NGN?

3 Fyzická vrstva I – prenos signálu

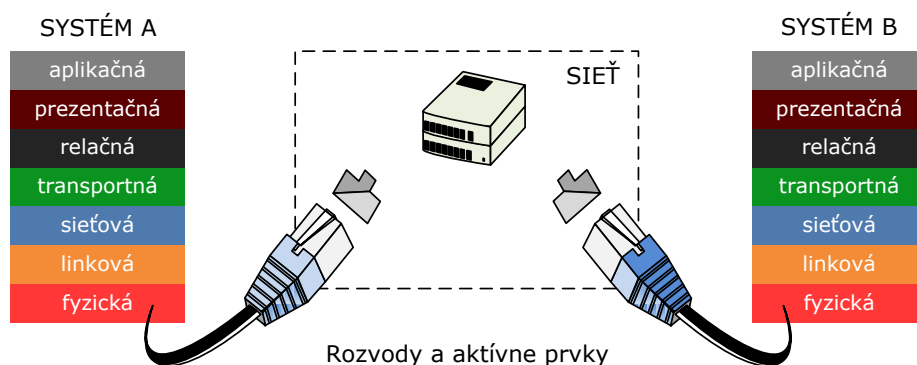
Ciele učenia

Po štúdiu tejto kapitoly by ste mali vedieť:

- Charakterizovať fyzickú vrstvu a jej funkcie
- Rôzne typy signálov používaných na prenos v elektronických komunikačných sieťach
- Vlastnosti signálov, harmonický signál, skladanie a rozklad signálu
- Spôsob určovania/výpočtu amplitúdy, frekvencie, spektra signálu, šírky pásma, jeho vzťah ku prenosovej a modulačnej rýchlosti, a ich význam pre prenos
- Služby fyzickej vrstvy poskytovaním špecifikovaných prenosových okruhových rôznych technológií

3.1 Funkcie fyzickej vrstvy

Komunikácia prostredníctvom elektronických komunikačných sietí začína pri fyzikálnych aspektoch prenosu signálu a končí napríklad pri webovej stránke počítača, alebo uskutočnení telefónneho hovoru. Preto aj model OSI začína fyzickou vrstvou (*physical layer*), označovanou číslom 1. Fyzická vrstva je základná sieťová vrstva, poskytujúca prostriedky pre prenos. Znárodnenie potrebných technických prostriedkov je na obr. 3.1.



Obr. 3.1. Znárodnenie základnej funkcie fyzickej vrstvy

Fyzická vrstva poskytuje elektrické a mechanické vlastnosti pre prenos informácie a plní funkčné a procedurálne požiadavky k nadviazaniu, udržaniu a zrušeniu spojenia medzi entitami linkovej úrovne. Všeobecne fyzická vrstva špecifikuje spôsob prenosu bitov od jedného komunikačného systému k inému systému cez prenosové médium. Preto základná funkcia fyzickej vrstvy je:

- špecifikácia vytvorenia fyzickej komunikácie, čo znamená:
 - aktiváciu,
 - udržovanie v aktívnom stave
 - deaktiváciu

fyzického spojenia medzi koncovými zariadeniami, respektíve entitami linkovej vrstvy.

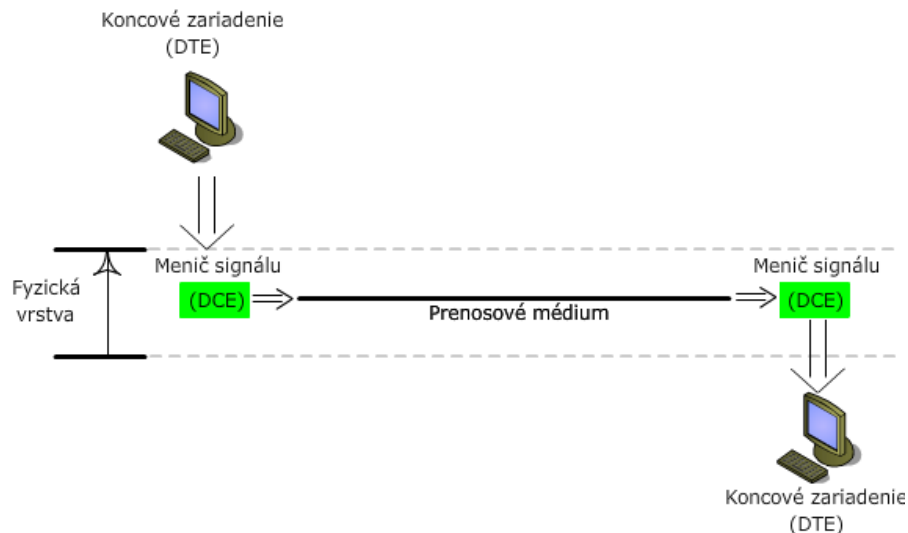
Ďalšie funkcie fyzickej vrstvy sú:

- zabezpečenie funkčných a procedurálnych požiadaviek na spojenie, čo predstavuje:
 - prevod digitálnej reprezentácie dát z používateľského zariadenia na zodpovedajúce signály, ktoré sú prenášané cez komunikačný kanál,
 - zorad'ovanie bitov podľa použitého multiplexu,
 - oznamovanie poruchových stavov linkovej vrstvy,
 - dodržiavanie výkonnostných veličín fyzickej vrstvy.
- Poskytnutie štandardizovaného rozhrania fyzickému prenosovému médiu v závislosti od príslušnej technológie.

Fyzická vrstva je technologicky závislá (príklady rôznych technológií: Ethernet, ISDN, ATM, GSM,...), je však protokolovo nezávislá. Protokoly fyzickej vrstvy špecifikujú možnosti pripojenia rôznych prenosových prostriedkov a zariadení, ktorými sú napríklad prenosové médiá, modemy a pod. V protokolových špecifikáciách musia byť určené:

- elektrické parametre signálu,
- význam signálu a časový priebeh,
- vzájomné nadviazanie riadiacich a stavových signálov,
- zapojenie konektorov prenosových médií,
- a mnoho iných parametrov technického a procedurálneho charakteru.

Poskytnutie štandardizovaného rozhrania prenosovému médiu je závislé od príslušnej technológie, ale všeobecne platí, že dáta z pripojeného koncového zariadenia DTE (*Data Terminal Equipment*) sú prenášané cez fyzickú vrstvu prostredníctvom ukončujúceho zariadenia DCE (*Data Circuit Equipment, Data Communication Equipment, Data carrier equipment*). V ukončujúcom zariadení DCE sa správa z koncového zariadenia prispôbi signálu konkrétneho prenosového média. Toto prispôbenie sa dosiahne zmenou jedného alebo viacerých parametrov signálu. Na prijímacej strane musí byť spätný menič, ktorý vykoná spätný prevod pre vstup do prijímacieho koncového zariadenia. Znáznornenie uskutočnenia zmeny správy na signál je na obr. 3.2.



Obr. 3.2 Pripojenie na fyzickú vrstvu

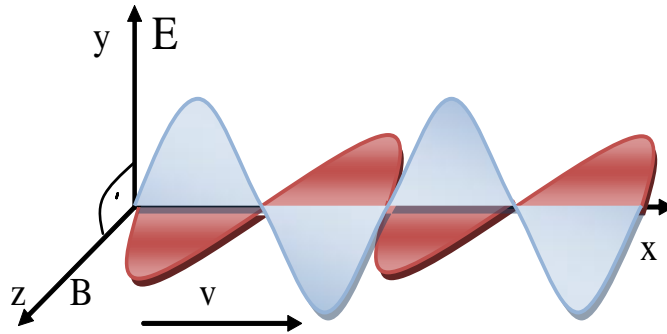
Fyzické spojenie je uskutočnené po prenosových médiách medzi dvoma alebo viacerými fyzickými vrstvami. Fyzická spojenie obsahuje okrem prenosových médií aj ďalšie prostriedky potrebné pre prenos a spolu tvoria komunikačný kanál alebo okruh pre prenos signálov. Signály sú nosiče prenášanej informácie. Preto spracovanie signálov je prvá časť, ktorá sa venuje fyzickej vrstve.

3.2 SIGNÁLY V KOMUNIKAČNÝCH SIEŤACH

3.2.1 Elektromagnetické signály

Signál v elektronických komunikačných sieťach je chápaný ako fyzický prostriedok (nosič) pre prenos správ, do ktorých je spracovaná prenášaná informácia. Všeobecne je signál dohodnutá kombinácia amplitúd, kmitočtov, intervalov svetla, zvuku, elektrického prúdu apod.. Signály, používané v elektronických komunikačných sieťach sú niektoré zo spektier elektromagnetického vlnenia.

Elektromagnetické vlny objavil James Clarc Maxwell v roku 1865 a v roku 1887 ich existenciu demonštroval Heinrich Hertz. Elektromagnetické vlnenie je vytvárané vzájomnými zmenami elektrickej a magnetickej zložky elektromagnetického poľa. Elektromagnetická vlna je tvorená dvomi zložkami – elektrickou a magnetickou, ktoré sú popísané vektorom elektrickej intenzity E a vektorom magnetickej indukcie B . Tieto dve polia sa sínusovo menia a výsledné sínusové pole zmien vytvára elektromagnetickú vlnu. Znázornenie elektromagnetickej vlny ako dvoch vektorov je na obrázku 3.3. Obidva vektory sú na seba kolmé a kolmé sú aj na smer šírenia.

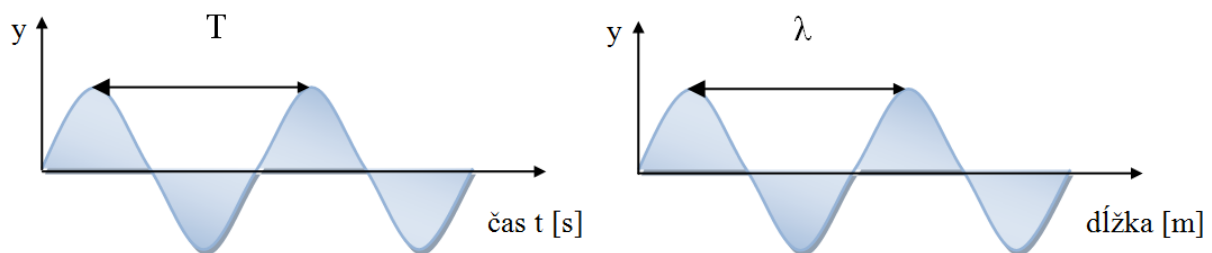


Obr. 3.3. Vektorové znázornenie elektromagnetickej vlny

Smer vektoru E určuje smer vektoru B a ich okamžité hodnoty sú zviazané rovnicou $E = B \cdot v$, kde v je vektor fázovej rýchlosti. Elektromagnetické vlny sa v dôsledku pohybu elektrónov šíria v priestore a majú špecifikované nasledovné parametre.

- Vzdialenosť medzi dvomi nasledujúcimi maximami alebo minimami sa označuje vlnová dĺžka označovaná ako λ (lambda). Udáva priestorovú vzdialenosť zhodných hodnôt elektromagnetickej vlny. Udáva sa v metroch, $1 \text{ m} = 10^3 \text{ mm}$ (milimetrov) = $10^6 \text{ }\mu\text{m}$ (mikrometrov) = 10^9 nm (nanometrov) = 10^{12} pm (pikometrov).
- Čas medzi dobou opakovania dvoch zhodných hodnôt elektromagnetickej vlny sa označuje doba periódy T . Udáva sa v sekundách (s) alebo v odvodených hodnotách $1 \text{ sec} = 10^3 \text{ ms}$ (milisekúnd) = $10^6 \text{ }\mu\text{s}$ (mikrosekúnd) = 10^9 ns (nanosekúnd).

Rozdiel medzi periódou a vlnovou dĺžkou je znázornený na obrázku 3.4. V prípade znázornenia periódy ide o časovú závislosť, v znázornení vlnovej dĺžky ide o dĺžkovú závislosť. V oboch prípadoch je priebeh sínusový.



Obr. 3.4 Rozdiel medzi periódou a vlnovou dĺžkou

Počet oscilácií vlny, ktoré znamená počet opakovania zhodných hodnôt elektromagnetickej vlny za sekundu, sa označuje frekvencia označovaná f . Udáva sa v hertzoch (Hz), alebo v násobkoch $1 \text{ Hz} = 10^3 \text{ kHz}$ (kilo) = 10^6 MHz (mega) = 10^9 GHz (giga) = 10^{12} THz (tera)

Medzi frekvenciou f a dobou periódy platí vzťah

$$f = 1/T.$$

Všetky elektromagnetické vlny sa šíria vo vákuu rýchlosťou svetla c . Jej hodnota je 299 792 458 m/s, čo je približne $3 \cdot 10^8$ m/s. Preto pre elektromagnetické vlnenie platí medzi rýchlosťou svetla, frekvenciou a vlnovou dĺžkou vzťah

$$c = \lambda \cdot f$$

Pretože c je konštanta, ak rastie frekvencia f , klesá vlnová dĺžka λ a naopak.

V medi alebo optickom vlákne, ktoré sa používajú v komunikačných technológiách, sa rýchlosť spomalí a stáva sa frekvenčne závislá. Rýchlosť svetla je doteraz limitujúca a žiadny signál sa nemôže šíriť rýchlejšie. Pretože rýchlosť svetla c je konštanta, ak vieme frekvenciu, vieme vypočítať vlnovú dĺžku a naopak. Napríklad vlnová dĺžka zdroja vysielajúceho na frekvencii 101,5 MHz predstavuje vlny s λ asi 3m.

3.2.2 Spektrum elektromagnetických signálov (vln)

Elektromagnetické vlny môžeme rozdeľovať podľa veľkosti vlnovej dĺžky respektíve frekvencie. Jednotlivé typy vln majú svoje označenie, ktoré spolu s približnými hodnotami vlnovej dĺžky a frekvencie sú uvedené v tabuľke 3.1.

Tabuľka 3.1.

elektromagnetické vlny	vlnová dĺžka vo vzduchu [m]	frekvencia [Hz]
rádiové vlny	30 km - 1 m	$10^4 - 10^{10}$
mikro vlny	1 m - 0,03 mm	$10^9 - 10^{12}$
infračervené vlny	0,3 mm - 790 nm	$10^{11} - 4 \cdot 10^{14}$
viditeľné vlny	790 nm - 390 nm	$4 \cdot 10^{14} - 8 \cdot 10^{14}$
ultrafialové vlny	400 nm - 10 nm	$8 \cdot 10^{14} - 10^{17}$
röntgenové vlny	10 nm - 1 pm	$10^{15} - 10^{20}$
gama vlny	< 300 pm	$> 10^{19}$

Rádiové elektromagnetické vlny majú vlnovú dĺžku od centimetrov až po kilometre. Používajú sa pre prenos informácie v elektronických komunikačných sieťach. Napríklad televízne vysielanie používa vlny s vlnovou dĺžkou λ 0,1 - 1 m čo predstavuje frekvenciu 3 GHz - 300 MHz. Mobilné telefóny štandardu UMTS mali pôvodne definované frekvenčné spektrum 1885-2025 MHz uplink a 2110-2200 MHz downlink, čo sú vlny približne okolo 0,1m. Pri prenose používajú špeciálnu technológiu označovanú modulácia.

Mikro vlny majú vlnovú dĺžku rádovo desiatky centimetrov až milimetrov. Bezdrôtové WiFi siete pracujúce na frekvencii 2,4 GHz používajú elektromagnetické vlny s λ asi 13 cm. V mikrovlnnej rúre používame vlny s λ asi 12 cm.

Infračervené vlny majú vlnovú dĺžku medzi 760 nm a 1 mm. Infračervené vlny sa používajú v elektronickej komunikácii pre prenos informácií na krátke vzdialenosti. Použitie je napríklad v mobilných telefónoch a diaľkových ovládačoch. Ďalšie účely využitia sú

napríklad v lekárstve ako fotónová terapia na liečbu kostí, hlbokých svalových tkanín a kĺbov, alebo na termografické vyšetrenia. Ďalšie využitie je v priemysle napríklad pri sledovaní kvality výrobkov. Pri vysokých teplotách sú vlny tak krátke, že ich dokážeme vnímať okom. Na tomto princípe sú založené infračervené ďalekohľady.

Viditeľné svetlo, ktoré vnímame ľudským okom je v oblasti vlnových dĺžok 390 nm až 770 nm. Najväčšie vlnové dĺžky má červené svetlo, nasleduje oranžové, žlté, zelené, modré. Ľudské oko najcitlivejšie reaguje na žltozelenú farbu s vlnovou dĺžkou 550 nm, čo odpovedá frekvencii 10^{15} Hz. To znamená kmitanie 1 000 000 000 000 000 (biliard) krát za sekundu.

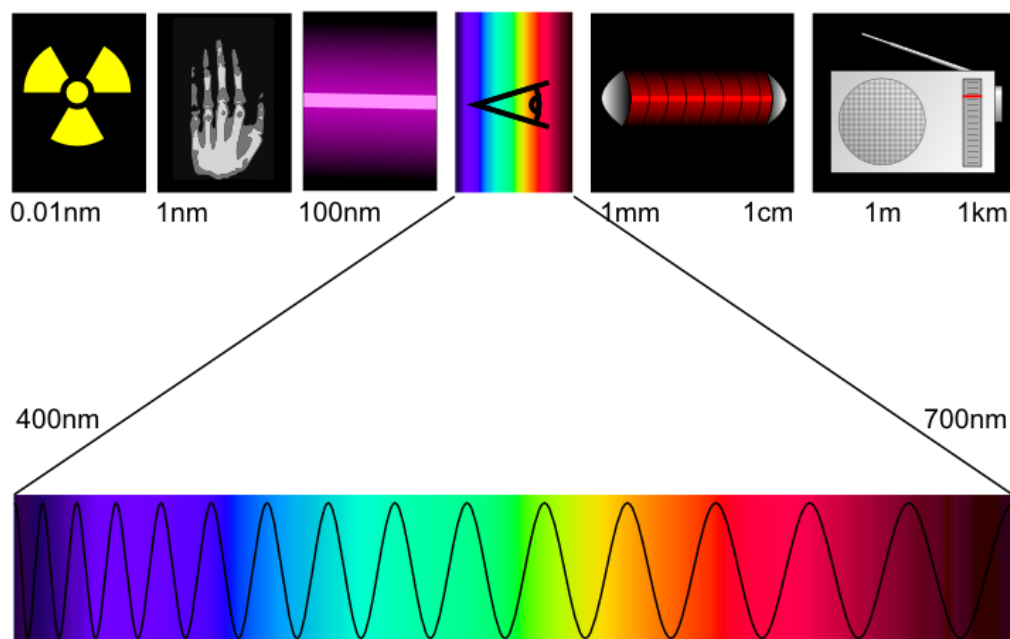
Ultrafialové vlny majú vlnovú dĺžku 400 – 10 nm. Využitie je veľmi široké. V komunikačných technológiách sú používané v optických prenosoch. Známe je využitie v laseroch. Na zem prichádzajú napríklad zo slnka a spôsobia zhnednutie kože.

Röntgenové vlny, označované aj ako X lúče majú vlnovú dĺžku od 10 nm do 100 pm. Známe sú najmä z využitia rádiológie ale používa sa aj v analytickej chémii. V röntgenovom spektre je možné pozorovať aj niektoré astronomické objekty, napríklad neutrónové hviezdy a čierne diery.

Gama vlny majú vlnovú dĺžku rádovo 10^{-14} . Vznikajú napríklad pri rozpade atómových jadier. Využitie v lekárstve je pre diagnostiku a v neurochirurgii (gama nôž, ktorý umožňuje presné zameranie pri ostraňovaní zhubných nádorov).

Nie všetky frekvencie sú vhodné na prenos informácie. Napríklad niektoré ultrafialové, röntgenové a gama žiarenie sú nepoužiteľné na spracovanie signálov pre prenos, neprejdú cez stavby a sú škodlivé.

Uvedené rozdelenie tvorí spektrum elektromagnetických vln. Známenie spektra, spolu s využitím pre prenosové médiá elektronických komunikačných sietí, je na obrázku 3.5.



Obr. 3.5 Spektrum elektromagnetických vln

Komunikačné technológie využívajú pre prenos informácie frekvenčné spektrum od rádiových po ultrafialové vlny. Rádiové vlny sú využívané pre prenosi po metalických vedeniach a bezdrôtové prenosi, ultrafialové vlny vlnových dĺžok okolo 1 mikrometer sú používané pre prenosi po optických kábloch. Podľa vlnových dĺžok, resp. frekvencie elektromagnetickej vlny sa určuje šírka pásma pre prenos v komunikačných technológiách. Šírka pásma je vo vzťahu s množstvom prenesenej informácie, preto je znalosť šírky pásma dôležitým parametrom prenosu. Šírka pásma pre rôzne využitia v komunikačných technológiách je v tabuľke 3.2.

Tab. 3.2. Rozdelenie rádiových vln podľa dĺžky a frekvencie a využitia

Názov frekvenčného pásma	Označenie podľa ITU	Vlnová dĺžka	Šírka pásma/rozsah frekvencií	Využitie
Extrémne nízka frekvencia	1 ELF – extremely low frequency	100 000 – 10 000 km	3 – 30 Hz	Komunikácia ponoriek
Super nízka frekvencia	2 SLF - super low frequency	10000 – 1000 km	30–300 Hz	Komunikácia ponoriek
Ultra nízka frekvencia	3 ULF ultra low frequency	1000 – 100 km	300–3000 Hz	Komunikácia v baniach
Veľmi nízka frekvencia	4 VLF – very low frequency	100 – 10km	3 – 30 kHz	Komunikácia ponoriek
Nízka frekvencia	5 LF - low frequency	10 – 1 km	30 -300 kHz	AM rádio (DV – dlhé vlny), navigácia
Stredná frekvencia	6 MF – medium frequency	1km – 100 m	300 kHz - 3 MHz	AM rádio (SV – stredné vlny)
Vysoká frekvencia	7 HF - high frequency	100 – 10 m	3 - 30 MHz	Krátkovlnné vysielanie, amatérske rádiá
Veľmi vysoká frekvencia	8VHF – very high frequency	10m – 1m	30 - 300 MHz	TV vysielanie, FM rádio (VKV – veľmi krátke vlny)
Ultra vysoká frekvencia	9 UHF – ultra high frequency	1m – 100 mm	300 MHz - 3 GHz	TV vysielanie, mobilné telefóny, WiFi, satelitné spojenia, pozemné bezdrôtové spojenia
Super vysoká frekvencia	10 SHF – super high frequency	100 – 10 mm	3 - 30 GHz	WiFi, mikrovlnné zariadenia, radary
Extrémne vysoká frekvencia	11 EHF - extremely high frequency	10 – 1 mm	30 - 300 GHz	Vysokorýchlostný mikrovlnný prenos dát, rádioastronómia

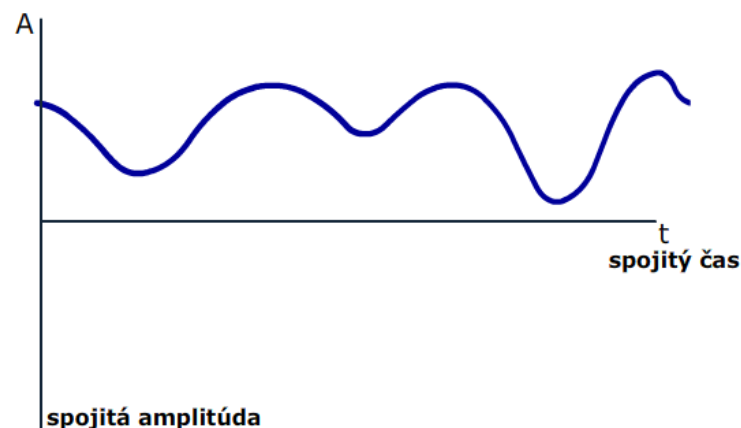
Nesmierne vysoká frekvencia	12 THF – tremendously high frequency	menšie ako 1 mm	300GHz - 3 THz	Infračervené spektrum
-----------------------------	--------------------------------------	-----------------	----------------	-----------------------

3.2.3 Grafické znázornenie signálov

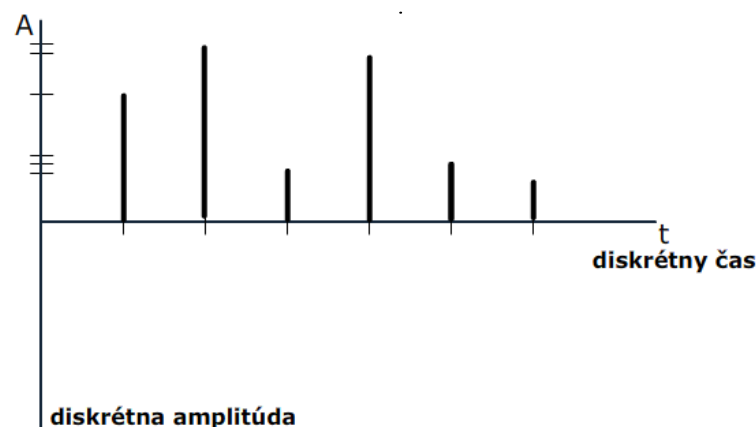
Signál je vyjadrovaný dvomi veličinami. Najčastejšie je to vyjadrenie **časového priebehu** amplitúdy signálu. **Amplitúda** je v teórii signálov chápaná ako fyzikálne vyjadrenie niektorej veličiny príslušného signálu. Signál mení svoje hodnoty času i amplitúdy buď v ľubovoľných hodnotách, alebo sú tieto hodnoty dané konečným súborom hodnôt. Podľa nadobudnutých hodnôt oboch vyjadrených veličín sú rozlišované nasledujúce typy signálov:

- **analogový** (spojitý v oboch vyjadrených veličinách),
- **diskrétny** (nespojité v jednej, alebo v oboch vyjadrených veličinách),
- **digitálny alebo číslicový**, ktorý je špeciálnym prípadom diskrétného signálu (nespojité v čase aj amplitúde).

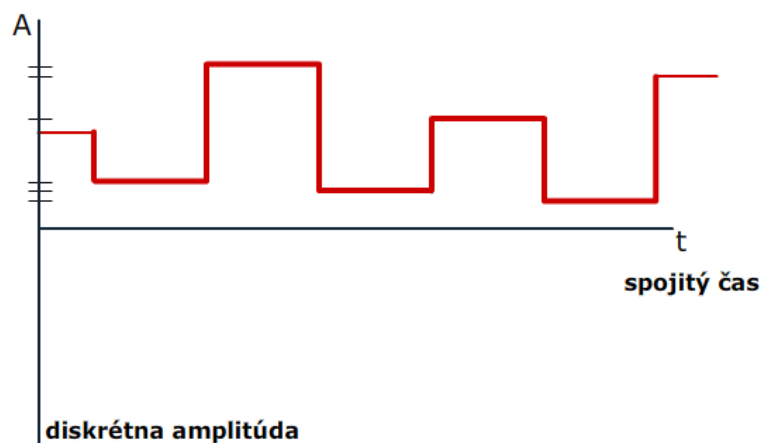
Príklady jednotlivých typov signálov pre časové priebehy amplitúd signálov sú na obr. 3.4.a až 3.4.d



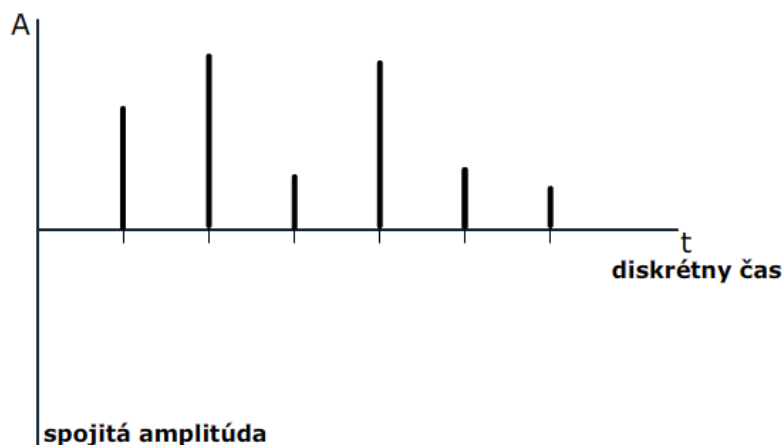
Obr. 3.4.a Signál spojitý v čase i v amplitúde



Obr. 3.4.b Signál diskrétny v čase i v amplitúde



Obr. 3.4.c Signál spojité v čase a diskretný v amplitúde



Obr. 3.4.d Signál diskretný v čase a spojité v amplitúde

Podľa priebehu delíme signály na:

- **periodické** (pravidelne sa opakujúce v určitých časových intervaloch), zvláštne označenie periodických signálov majú signály vyjadrené sínusovou a kosínusovou funkciou a označujú sa ako **harmonické signály**,
- **neperiodické** (neopakujú sa v pravidelných intervaloch).

3.2.3.1 Matematické vyjadrenie signálov

Vyjadrenie signálu spojitou alebo nespojitou matematickou funkciou, je nazývané matematický model signálu. Vyjadruje sa dvojakým spôsobom.

1. Ako **časová závislosť**, kde amplitúda signálu je závislá na čase, $A = F(t)$.
2. Ako **frekvenčná závislosť**, kde amplitúda signálu je závislá na frekvencii, $A = F(f)$, resp. fázová závislosť, kde fáza je závislá na frekvencii $P = F(f)$.

Matematickým modelom analógového signálu v časovej oblasti je matematická funkcia, alebo mnohočlen.

Časová závislosť pre periodické signály je vyjadrená Fourierovým radom:

$$g(t) = \frac{1}{2}c + \sum_{n=1}^{\infty} a_n \sin(2\pi nft) + \sum_{n=1}^{\infty} b_n \cos(2\pi nft)$$

Pre neperiodické signály je závislosť vyjadrená Fourierovou transformáciou.

Z Fourierovho radu aj z Fourierovej transformácie vyplýva, že signály sú zložené z jednoduchých sínusových alebo kosínusových signálov. Preto je potrebné pre pochopenie zložených signálov poznať model sínusového signálu.

Matematickým modelom najjednoduchšieho analógového signálu je sínusová funkcia:

$$g(t) = A \cdot \sin(2\pi f \cdot t + \varphi_0),$$

kde A je maximálna amplitúda signálu, f je frekvencia, t čas, φ_0 je počiatočná fáza signálu.

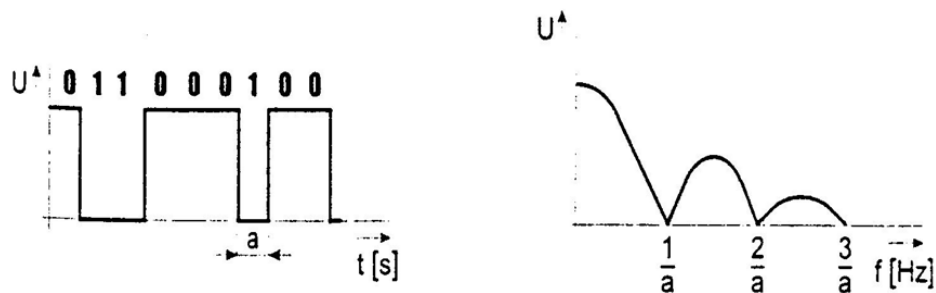
Takýto signál sa nazýva sínusový signál. Signál vyjadrený sínusovou, alebo kosínusovou funkciou sa nazýva **harmonický signál**.

Matematickým modelom diskrétného signálu v časovej oblasti je postupnosť funkčných hodnôt, ktoré predstavujú hodnotu fyzikálnej veličiny signálu v určitých časových intervaloch. Vyjadrenie diskrétného signálu je vyjadrené radom $x(n)$:

$$x(t_{-2}), x(t_{-1}), x(t_0), x(t_1), x(t_2), \dots,$$

kde $x(t_i)$ je hodnota signálového prvku v určitom časovom intervale.

Digitálny signál je napríklad postupnosť hodnôt 011000100, ktorých znázornenie v čase je na obrázku 3.5.



T- doba trvania signálového prvku

Obr. 3.5 Príklad vyjadrenie časovej postupnosti digitálneho signálu

Pre vzájomné vyjadrenie diskrétného signálu v časovej a frekvenčnej oblasti sa používa z-transformácia.

Všetky typy signálov sa vyjadrujú tromi veličinami:

- amplitúdou A
- frekvenciou f
- fázou φ .

Amplitúda elektrických signálov je vyjadrená elektrickým výkonom, napätím, alebo prúdom.

Frekvencia u harmonických signálov charakterizuje periodické opakovanie funkcie a je daná prevrátanou hodnotou periódy $f = 1/T$. Zložené signály majú viac frekvencií. Celkový výkon signálu je rozdelený medzi jednotlivé frekvencie.

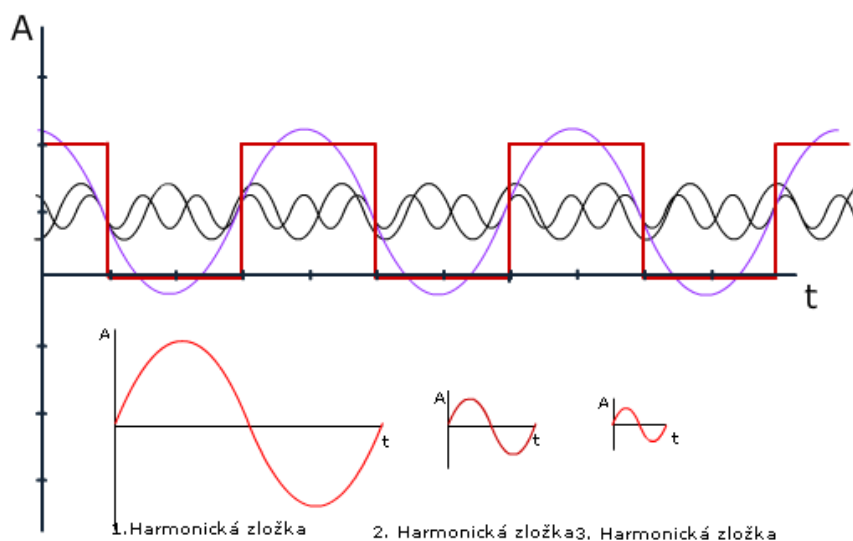
Fáza vyjadruje posunutie signálu v čase.

3.2.3.2 Rozklad signálov

Dá sa dokázať, že akýkoľvek zložitý signál je daný súčtom harmonických signálov s rôznou amplitúdou, frekvenciou a počiatočnou fázou. Toto tvrdenie platí aj opačne. Akýkoľvek zložitý signál je možné rozložiť na množstvo harmonických signálov. Postup rozkladu nazývame **harmonická analýza** a výsledný produkt **rozkladu** sa nazýva frekvenčné spektrum. Frekvenčné spektrum udáva rozsah frekvencií, ktoré musia byť prenesené komunikačným kanálom, aby bol signál prenesený správne. Ak nie sú prenesené všetky frekvencie spektra, na prijímacej strane nie je možné rekonštruovať presne rovnaký signál ako bol odoslaný, pretože rekonštrukcia signálu na prijímacej strane predstavuje skladanie signálu z jeho harmonických zložiek signálu. **Šírka frekvenčného spektra (*bandwidth*)** je dôležitý parameter na charakterizovanie signálu a prenosového kanálu. Frekvenčné spektrum signálu má dve časti:

- amplitúdové frekvenčné spektrum
- fázové frekvenčné spektrum.

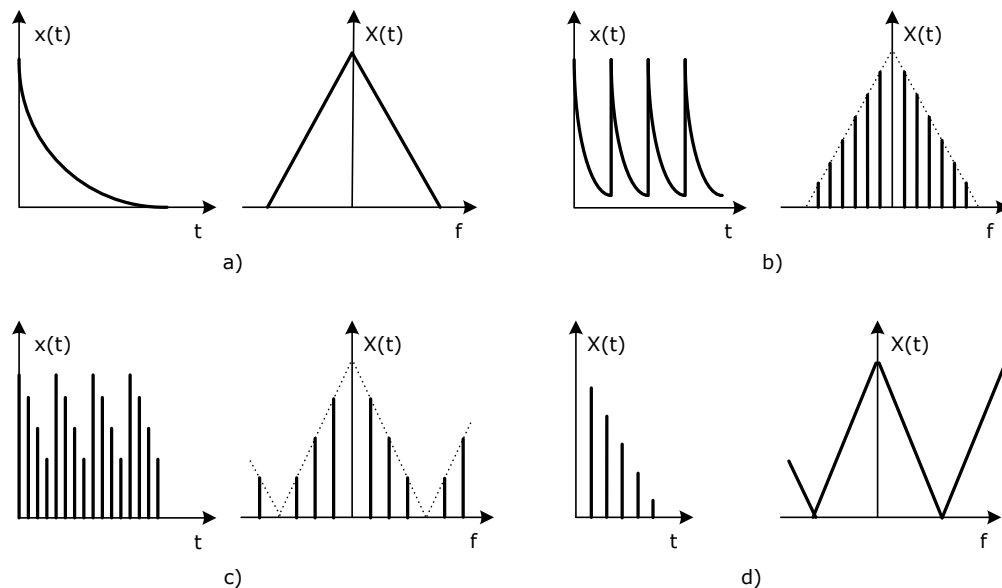
Ilustračný príklad vzťahu medzi časovým priebehom periodického obdĺžnikového signálu a jeho frekvenčnými spektrami je na obr. 3.6. Prevod signálu z časovej oblasti do frekvenčnej a naopak umožňuje Fourierova transformácia. Rozklad signálu na harmonické zložky sa označuje harmonická analýza signálu.



Obr. 3.6. Harmonická analýza signálu

Rôzne typy signálov majú rôzne frekvenčné spektrá. Dá sa vypočítať, že:

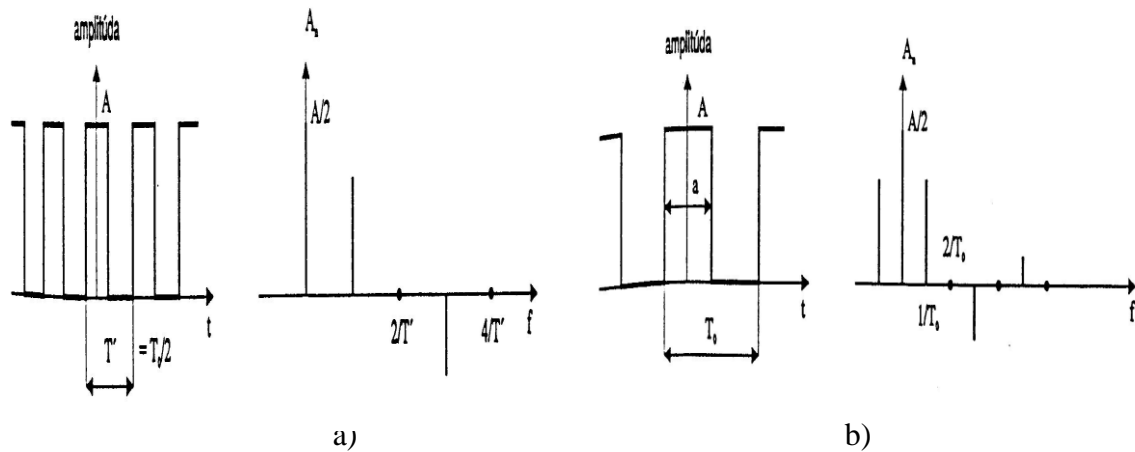
- Frekvenčné spektrum neperiodického analógového signálu je spojité a neperiodické, obrázok 3.7.a.
- Frekvenčné spektrum periodického analógového signálu je diskrétna a neperiodické, obrázok 3.7.b.
- Frekvenčné spektrum diskrétného neperiodického signálu je spojité a periodické, obrázok 3.7.c.
- Frekvenčné spektrum diskrétného a periodického signálu je diskrétna periodické, obrázok 3.7.d.



Obr. 3.7 Časové priebehy a frekvenčné spektrá rôznych typov signálov

Frekvenčné spektrum je rôzne u digitálnych a analógových signálov. Pri prenose informácií digitálnym signálom je spektrum periodické, čo znamená, že je teoreticky nekonečne veľké. Frekvenčné spektrum digitálneho signálu je rozdielne aj podľa doby trvania signálového prvku (bitu). Doba trvania signálového prvku udáva symbolovú rýchlosť, od ktorej je závislá prenosová rýchlosť. Čím je požadovaná vyššia prenosová rýchlosť, tým je požadovaný menší interval trvania signálového prvku respektíve vyššia symbolová rýchlosť.

Platí, že čím je kratšia doba trvania signálového prvku, tým je potrebný pre prenos kanál s väčšou šírkou pásma. Táto skutočnosť je znázornená na obrázku 3.8. Digitálny signál na obrázku a) má menšiu dobu trvania ako signál na obrázku b). Frekvenčné spektrum znázornené v obrázkoch vpravo znázorňuje počet harmonických zložiek. Tých je pre signál s menšou hodnotou bitu znázornených v obrázku a) menej. To znamená, že ak na strane prijímača chceme skladať signál, požadujeme potrebný počet harmonických zložiek, ktorých prenos vyžaduje širšie frekvenčné spektrum ako je to v prípade obrázku b), kde je signál s vyššou hodnotou bitu.



Obr. 3.8 Vzťah šírky trvania signálového prvku a frekvenčného spektra

3.2.3.3 Úroveň signálu (Signal Level)

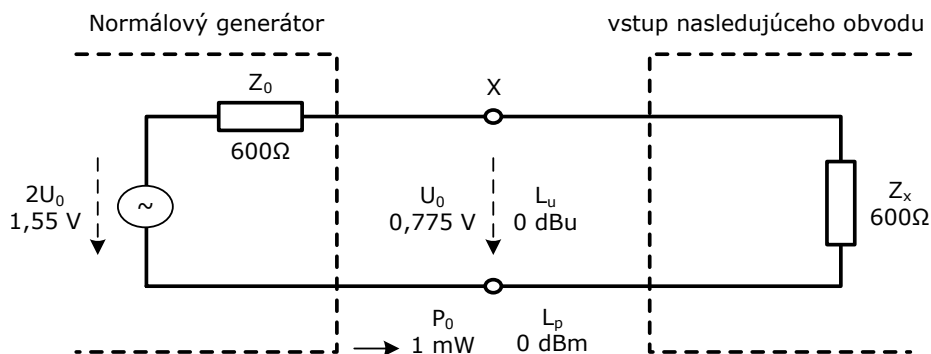
Úroveň signálu, niekedy tiež označovaná ako **hladina signálu**, vyjadruje pomernú hodnotu príslušnej fyzikálnej veličiny amplitúdy signálu. Fyzikálnou veličinou môže byť napätie, prúd, výkon. Pre pomerné vyjadrenie sú používané nižšie uvedené vzťahy absolútnej úrovne L_A , alebo relatívnej úrovne L_R .

$$L_A = 10 \log \left| \frac{P}{P_o} \right| \quad L_A = 20 \log \left| \frac{U}{U_o} \right| \quad [\text{dB}]$$

$$L_R = 10 \log \left| \frac{P}{P_x} \right| \quad L_R = 20 \log \left| \frac{U}{U_x} \right| \quad [\text{dB}]$$

Úroveň je vyjadrovaná ako logaritmus pomeru príslušnej veličiny amplitúdy vo vzťahu k referenčným hodnotám. Ak je referenčná hodnota daná normou, označujeme ju ako absolútna úroveň L_A , ak je referenčná hodnota daná iným vyjadrením, označuje sa ako relatívna úroveň L_R .

Referenčné hodnoty boli zvolené podľa referenčného obvodu na obrázku 3.9. Sú nasledovné: $U = 0,775 \text{ V}$, $P = 1 \text{ mW}$, $I = 1,29 \text{ mA}$. Jednotky úrovne sú decibely [dB].



Obr. 3.9. Referenčný obvod

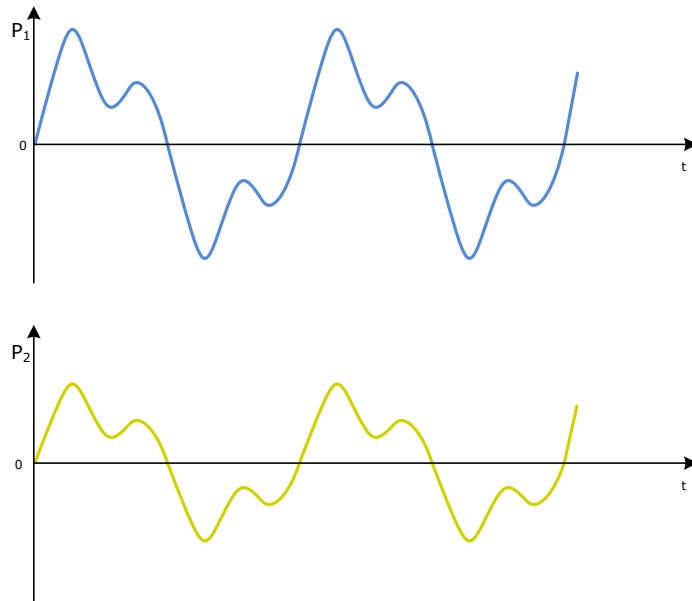
3.2.3.4 Tlmenie signálu (Signal Damping)

Pri prenose signálu po vedení vznikajú straty, ktoré spôsobujú zmenšenie amplitúdy signálu, čo je možné zistiť porovnaním úrovní na vstupe a výstupe prenosovej cesty/ kanálu.

Veľkosť tlmenia sa vyjadruje mierou tlmenia. Tá vyjadruje pomer medzi vstupným a výstupným výkonom prenosovej cesty. Tlmenie vstupného a výstupného signálu sa vyjadruje vzťahom

$$a = 10 \log \left| \frac{P_1}{P_2} \right| \text{ [dB]}$$

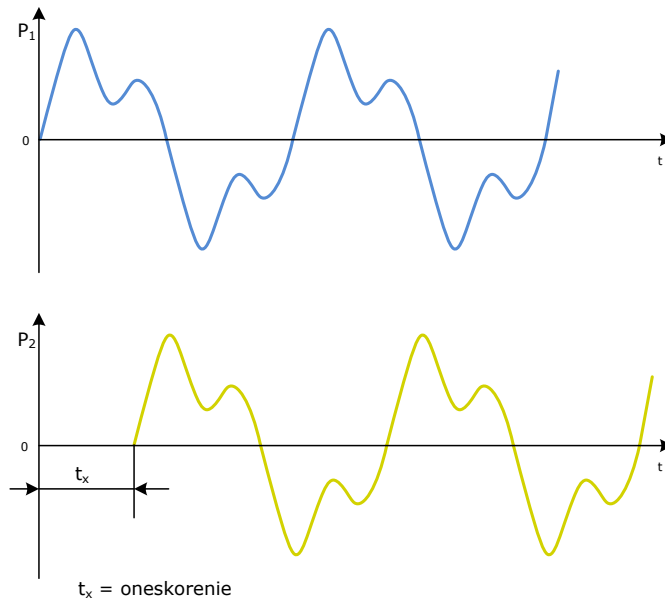
Znázornenie vstupného a výstupného signálu je na obr. 3. 8.



Obr. 3.8. Tlmenie signálu

3.2.3.5 Oneskorenie signálu /časový posuv signálu (Signal delay)

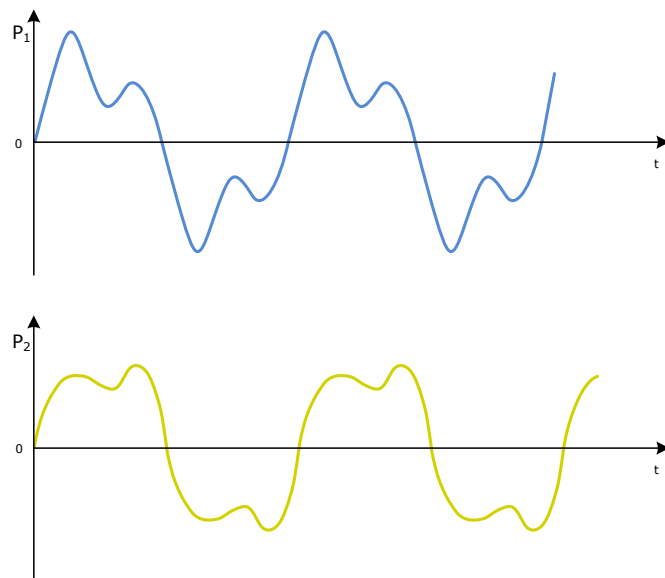
Rýchlosť, ktorou sa šíria signály v rôznych prenosových prostrediach je rôzna. Napríklad v kovových vodičoch je to približne 70% rýchlosti svetla. Hlavne pri veľkých vzdialenostiach sa oneskorenie signálu môže prejavovať ako súčet oneskorení všetkých čiastkových prenosových úsekov a má výrazný vplyv na celkové oneskorenie prenosu a na kvalitu prenosu informácie komunikačnou sieťou. Oneskorenie vstupného a výstupného signálu je na obr. 3.11.



Obr. 3.11 Oneskorenie signálu

3.2.3.6 Skreslenie signálu (Signal deformation)

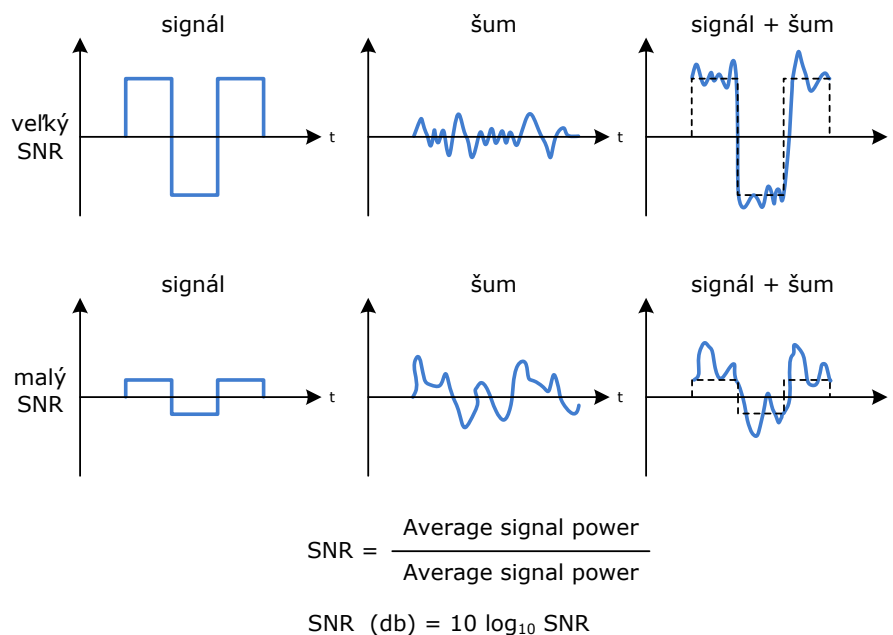
Zmena tvaru časového priebehu signálu počas prenosu sa označuje skreslenie signálu. Veľké skreslenie signálu môže viesť k chybnému vyhodnoteniu prijatej správy, ktorú signál nesie. Príklad skreslenia signálu je na obr. 3.12.



Obr. 3.12 Skreslenie signálu

3.2.3.7 Odstup signál – šum (Signal-to-Noise Ratio - SNR)

Ak je signál prenášaný bezšumovým kanálom, znamená to, že hodnota jeho úrovne a tvar signálu sa pri prenose nemenia, obr. 3.13.a) . Ak je signál prenášaný kanálom, v ktorom je prítomný šum, mení sa jeho tvar tým, že úroveň šumu sa pripočíta k úrovni signálu, ako je znázornené na obrázku 3.13. b) a c).



Obrázok 3.13. Odstup signál – šum

Odstup signálu od šumu sa označuje SNR (*Signal Noise Ratio*) a udáva pomer priemerného výkonu amplitúdy signálu ku priemernému výkonu šumu. Je bezrozmerné číslo.

$$\text{SNR} = \text{priemerný výkon signálu} / \text{priemerný výkon šumu}$$

Spravidla sa udáva v jednotkách decibel [dB], vtedy je vzťah pre výpočet nasledovný:

$$\text{SNR}(dB) = 10 \log |SNR|$$

Ak je úroveň signálu výrazne vyššia ako úroveň šumu, šum málo ovplyvní prenášaný signál. Ak je úroveň signálu nízka a zrovnateľná s úrovňou šumu, rozpoznanie užitočného signálu je zložité. Hodnota SNR je dôležitým parametrom pri určovaní správnosti prijatej informácie a aj pri výpočte kapacity kanála.

3.2.3.8 Prenosová rýchlosť signálu

Digitálne signály majú špecifikované dve prenosové veličiny:

- symbolová (modulačná) rýchlosť
- prenosová rýchlosť.

Symbolová (modulačná) rýchlosť (*symbol rate, modulation speed, Baud rate*), ktorá vyjadruje počet zmien signálu za sekundu, respektíve rýchlosť zmeny signálu. Symbol môže predstavovať napríklad jeden impulz. Symbolová rýchlosť je definovaná ako prevrátená hodnota najkratšieho časového intervalu, ktorý je prenosový systém schopný preniesť bez ohľadu na to, koľko úrovní signálu je rozlíšených v tomto časovom intervale.

$$v_s = \frac{1}{T}$$

Meria sa v jednotkách [Bd] Baud (čítaj bód), čo vyjadruje s^{-1} . Niekedy je preto označovaná aj ako Baud rate.

Ak má symbolová rýchlosť hodnotu $1\text{kBd} = 1000\text{ Bd}$, znamená to, že za sekundu je prenesených 1000 symbolov. Trvanie jedného symbolu je $1/1000\text{ s}$, teda 1 milisekunda.

Symbolová rýchlosť v_s môže vyjadriť číselne množstvo informácie prenesenej signálom len u signálu, ktorý sa mení medzi dvomi stavmi, to znamená, dvojstavového binárneho signálu.

Digitálne signály, ktoré sa používajú pre prenosové účely, majú viac stavov. Pre viacstavové digitálne signály s počtom stavov N sa používa pojem a miera prenosová rýchlosť v_p .

Prenosová rýchlosť (*speed rate*) je definovaná množstvom informácie, ktorý prenáša signál za časovú jednotku. Vyjadruje sa vzťahom

$$v_p = v_s \log_2 N$$

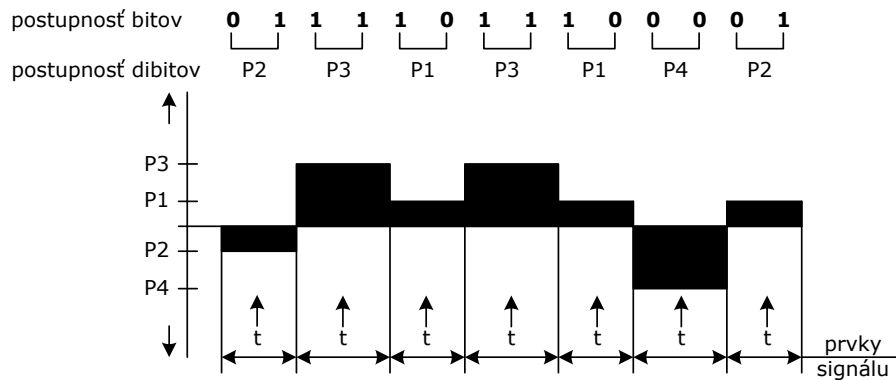
kde N je možný počet stavov amplitúdy digitálneho signálu a v_s je symbolová rýchlosť tohto signálu. Miera prenosovej rýchlosti v_p má rozmer s^{-1} ale vyjadruje sa v jednotkách $\text{bit}\cdot\text{s}^{-1}$ resp. *bps (bit per second)*. Pre dvojstavový digitálny signál je veľkosť oboch rýchlostí číselne rovnaká.

$$v_p = v_s$$

V tomto prípade sú jednotky $\text{bit}\cdot\text{s}^{-1}$ a Bd rovnaké.

V prípade rovnosti prenosovej a modulačnej rýchlosti sa jedná o jednoduchú digitálnu komunikáciu číslícovým dvojstavovým signálom so symbolom binárna 0 alebo 1, kde maximálne množstvo informácie je rovné 1. V takomto prípade je možné zvyšovať prenosovú rýchlosť len znižovaním časového intervalu binárnej 0 a 1, čo má svoje obmedzenia.

Ak sú pre prenos použité také techniky prenosu, kde symbol má viac, ako dva stavy, vtedy je symbolová rýchlosť menšia, ako je prenosová rýchlosť, pretože je vynásobená maximálnym množstvom informácie, ktoré je prenášané v jednom symbole. Prenosová rýchlosť tak udáva počet prenesených bitov za sekundu. Ak použijeme prenosovú techniku kde $N=16$, znamená to, že jeden symbol reprezentuje 4 bity. Znamená to, že prenosová rýchlosť sa zvýši oproti symbolovej štvornásobne. Vyjadrenie prenosovej a symbolovej rýchlosti je na obr. 3.14.



Obr. 3.14 Vyjadrenie modulačnej a prenosovej rýchlosti

3.2.3.9 Hodnotenie signálov

Signál je hodnotený z technickej stránky podľa troch vzájomne zviazaných veličín:

- Dynamický rozsah signálu D_s ; predstavuje v matematickom vyjadrení zmenu funkčnej hodnoty matematického modelu signálu. V praxi je táto veličina meraná a posudzovaná ako výkon. Pri prenose hlasu ju používateľ rozlišuje rozsahom hlasitosti hovoru. Pre praktické účely sa používa označenie odstup amplitúdy signálu od amplitúdy šumu a hodnota dynamického rozsahu signálu sa určuje ako odstup strednej hodnoty výkonu signálu P_s k strednej hodnote výkonu šumu P_ξ . Odstup signálu od šumu sa počíta ako dekadický logaritmus podielu uvedených hodnôt, ktorého vzťah je uvedený vyššie..
- Šírka pásma signálu F_s ; je daná rozsahom frekvenčného spektra signálu od minimálnej frekvencie f_{\min} po maximálnu frekvenciu f_{\max} .
- Doba trvania prvku signálu; je najmenšia časť signálu, ktorá sa musí dať rozoznať. Napríklad pri digitálnom signáli je to doba trvania 1 bitu v jednotkách času.

Súhrn všetkých veličín je nazývaný objem signálu V_s .

3.3 Protokolové dátové jednotky (PDU – *Protocol Data Unit*) fyzickej vrstvy

Dátové jednotky prenášané fyzickou vrstvou sú **bity**. Preto je bit možné označiť za PDU fyzickej vrstvy. Označenie bit reprezentuje v binárnej číselnej sústave hodnotu pri používaní dvoch symbolov, 0 a 1. Odtiaľ je aj názov jednotky *binary digits* a je základnou jednotkou digitálnej komunikácie aj ukladania informácie.

V oblasti digitálnej komunikácie znamená hodnota 1 bit vyjadrenie časového intervalu dĺžky trvania signálového prvku, ktorým je 0 alebo 1.

V informatike je bit jednotkou na meranie informačnej kapacity. 1 bit je najmenšou jednotkou kapacity pamäte. Bit môže nadobúdať jednu z dvoch logických hodnôt. V praxi to znamená napríklad zapnutý alebo vypnutý. Pre ukladanie informácie je používaná väčšia jednotka, bajt. Platí vzťah: **1 bajt = 8 bitov**.

Pri používaní jednotiek vyšších rádov je rozdiel medzi prefixami pri vyššie vysvetlenom rôznom využívaní jednotky bit. Napríklad *kilo* znamená v digitálnej komunikácii 1 000, čo je mocnina 10^3 a v ukladaní informácie 1 024, čo je najbližšia mocnina 2^8 . Tento významu predpôň sa zažil v oboch uvedených významoch a spôsoboval nepresnosti.

Aby sa tento zmätok odstránil, odporučila IEC - *International Electrotechnical Commission* pre mocniny čísla 2 blízke hodnotám SI (*Système International – Medzinárodná sústava jednotiek*) používať nové predpony. Tento medzinárodný štandard má číslo IEC 60027-2. Od roku 2004 je aj česká norma ČSN IEC 60027-2. Tabuľka 3.1 vyjadruje rozdiel v označení.

Tabuľka 3.1 Značenia prefixov v digitálnej komunikácii a meraní informačnej kapacity

Množstvo bitov			
SI prefixy		IEC prefixy	
názov (symbol)	hodnota	názov (symbol)	hodnota
kilobit (kbit)	10^3	kibibit (Kibit)	$2^{10} = 1\,024$
megabit (Mbit)	10^6	mebibit (Mibit)	$2^{20} = 1\,048\,576$
gigabit (Gbit)	10^9	gibibit (Gibit)	$2^{30} = 1\,073\,741\,824$
terabit (Tbit)	10^{12}	tebibit (Tibit)	$2^{40} = 1\,099\,511\,627\,776$
petabit (Pbit)	10^{15}	pebibit (Pibit)	$2^{50} = 1\,125\,899\,906\,842\,624$
exabit (Ebit)	10^{18}	exbibit (Eibit)	$2^{60} = 1\,152\,921\,504\,606\,846\,976$
zettabit (Zbit)	10^{21}	zebibit (Zibit)	$2^{70} = 1\,180\,591\,620\,717\,411\,303\,424$
yottabit (Ybit)	10^{24}	yobibit (Yibit)	$2^{80} = 1\,208\,925\,819\,614\,629\,174\,706\,176$

3.4 SLUŽBY FYZICJE VRSTVY

3.4.1 Prenos signálu

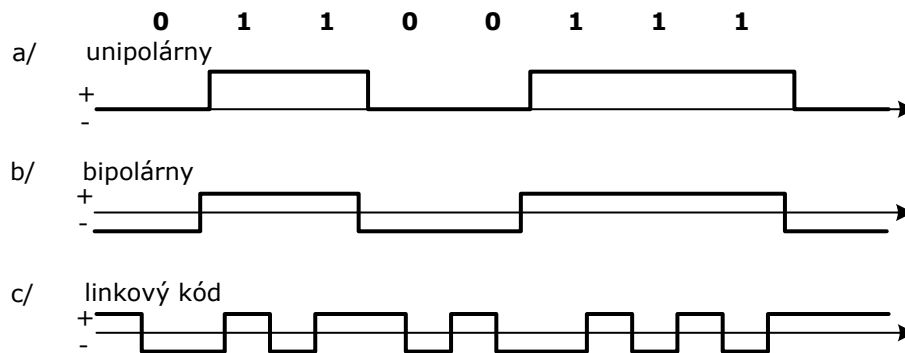
3.4.1.1 Spracovanie signálu pre prenos

Digitálny signál, ktorý predstavuje na výstupe z koncového zariadenia časovú postupnosť 0 a 1 nie je v takomto tvare prenášaný prenosovým kanálom. Pred prenosom je signál upravovaný rôznymi spôsobmi (metódami). Podľa spôsobu spracovania signálu rozlišujeme prenos:

- v základnom pásme (baseband transmissions)
- v preloženom pásme (broadband transmission).

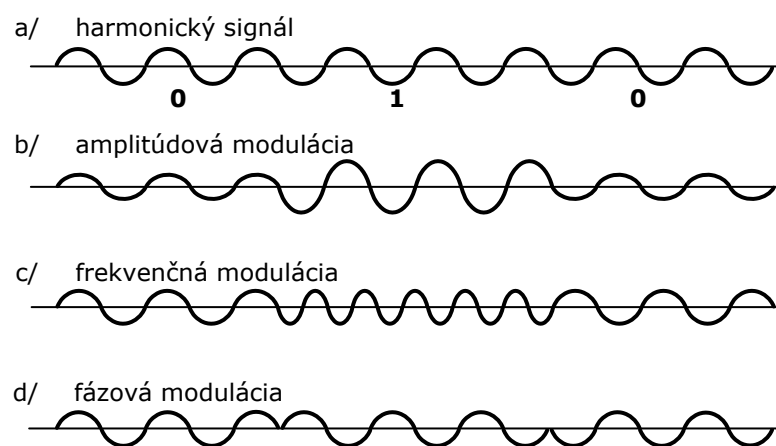
Pojem **základné pásmo** znamená, že frekvenčné spektrum signálu sa nemení. Prenášané dáta, po vyjadrení hodnotami 0 a 1 sú reprezentované pomocou úrovni napätí na prenosovom médiu, napríklad jednou nulovou a jednou nenulovou úrovňou, alebo jednou zápornou a jednou nezápornou úrovňou, obr. 3.15 a), b). Takýto tvar signálu je pre prenos nevýhodný, lebo má teoreticky nekonečne veľké frekvenčné spektrum, ktoré nie je možné prenosovým

médiom prenieť. Preto sa používajú zložitejšie spôsoby vyjadrenia logických hodnôt pomocou úrovni napätí. Takéto spracovanie signálu sa realizuje pomocou linkových kódov (*line codes*). Na obr.3.15c je príklad linkového kódu označovaného Manchester II. Viac o linkových kódach je popísané v kapitole 4.



Obr. 3.15 Kódovanie v základnom pásme

Prenos v **preloženom pásme** znamená, že signál je prenášaný v inom frekvenčnom spektre, ako je jeho pôvodné. Prenosovým médium sa prenáša taký signál, ktorý sa šíri s menšími stratami a v ňom je „uložený“ signál, ktorý nesie prenášanú informáciu. Takýto postup sa nazýva modulácia (*modulation*). Najjednoduchší princíp modulácie je vyjadrený na obr. 3.16. V časti a) je znázornený signál, do frekvenčného pásma ktorého sa „preloží“ digitálny signál. Tento signál sa nazýva tiež nosný signál, alebo nosná (*carrier*) a je ním harmonický signál. Podľa zmeny niektorého z parametrov harmonického signálu - amplitúdy, frekvencie, fáze- rozlišujeme rôzne typy modulácie, obr. 3.16. b) – d). Princípy modulácie sú spracované v kapitole 4.



Obr. 3.16 Preložené pásmo modulácia

3.4.1.2 Spôsoby prenosu signálu kanálom

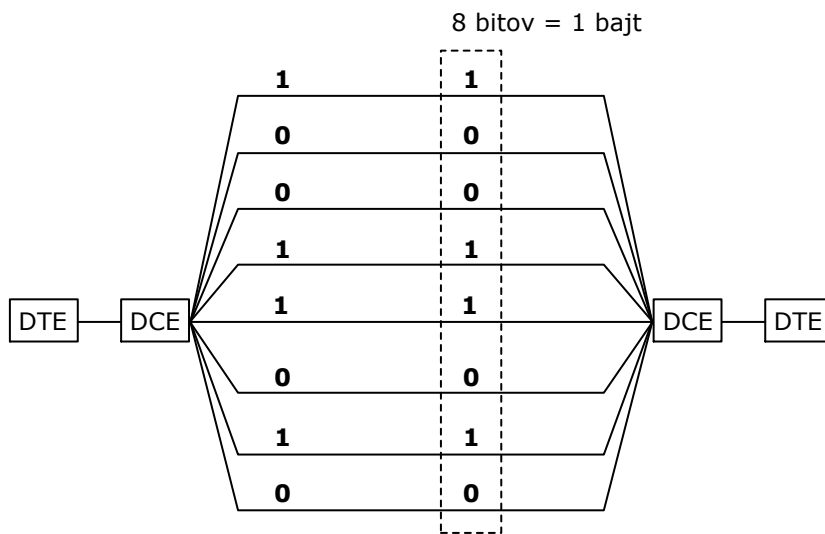
Digitálny signál je prenášaný prenosovým kanálom v blokoch dát dvomi spôsobmi:

- Paralelne (paralelný prenos), kde je pre každý prvok určitého bloku dát k dispozícii samostatný prenosový kanál.

- Sériovo (sériový prenos), pri ktorom sú jednotlivé prvky časovej postupnosti vysielané v jednom prenosovom kanáli.

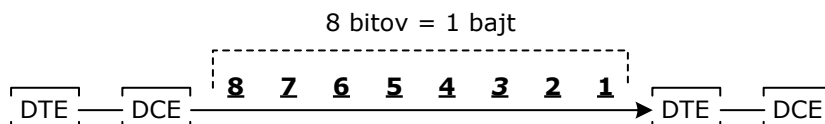
Každý spôsob prenosu má svoje špecifické charakteristiky, ktoré sú využité na konkrétny účel.

Paralelný prenos prenáša viac dát súčasne, ale vyžaduje viac kanálov, čo je cenovo náročné. Paralelný prenos používa naraz osem vodičov, alebo násobok osem, obr. 3.17 a. Používa sa na zberniciach počítačov a hlavne pri prenosoch na krátke vzdialenosti, napríklad pre paralelný port tlačiarne a v technike diaľkovej signalizácie. Prenos je rýchlejší ako sériový, odpadá potreba transformácie, treba však väčší počet kanálov. Vzhľadom na vysoké náklady je paralelný prenos pre diaľkové prenosy nevhodný.



Obr. 3.17.a Paralelný prenos dát

Sériový prenos je jeden z najrozšírenejších spôsobov prenosu. Jednotlivé prvky sú v časovej postupnosti vysielané po jednom prenosovom kanáli. Sériový prenos je technicky jednoduchšie realizovateľný a je najrozšírenejší spôsob prenosu, aj keď prenos trvá dlhšie v porovnaní s paralelným prenosom. Výhodou je, že stačí jeden prenosový kanál, obr. 3.17 b. Pretože v počítačoch sa pracuje prevažne s dátami v paralelnom tvare je potrebné pred vysielaním dáta transformovať z paralelného tvaru na sériový a v prijímači naopak.



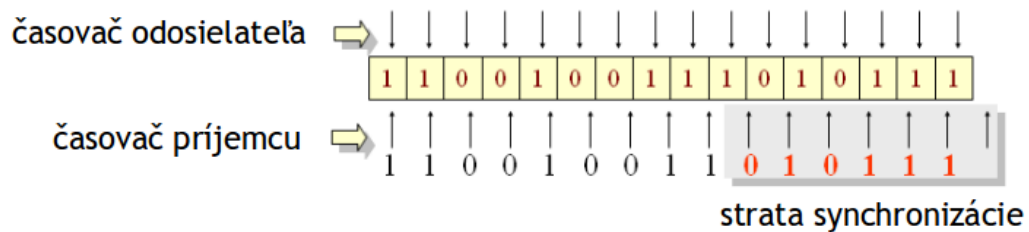
Obr. 3.17.b Sériový prenos dát

Rozdiely oboch spôsobov prenosu sú aj pri prijímaní dát. Kým paralelný prenos vyhodnocuje blok dát v jednom okamžiku, sériový prenos vyhodnocuje na prijímacej strane prvky časovej postupnosti signálu v časovom súlade s vysielacou stranou. Pri sériovom prenose musí byť zabezpečená časová synchronizácia vysielacej a prijímacej strany. Prijímač musí poznať začiatok a koniec kedy dochádza k zmene signálového stavu - začiatky a konce

blokov dát. Na základe týchto údajov prijímač stanoví rozhodujúci okamih pre vyhodnotenie signálového stavu jednotlivých prvkov.

3.4.2 Synchronizácia pri prenose

Priebeh digitálneho signálu má tvar obdĺžnika, ktorého skokové zmeny sa vysielajú v krátkych časových intervaloch. Aby prijímač vedel, ako často má zisťovať hodnotu signálu, ktorý bol vyslaný, musia byť vysielateľ a prijímač zosynchronizovaní. K synchronizácii je využívaná zmena digitálneho signálu. Pravidelné zisťovanie hodnoty digitálneho signálu sa realizuje s pomocou časovača. Na obrázku 3.18 a je znázornená situácia, kedy sa rozchádzajú časovače, lebo každý má inú frekvenciu - dĺžku jedného taktu časovača. To má za následok, že prijímač neprijme rovnakú informáciu, akú vysielal vysielateľ. Dochádza tým k strate synchronizácie. Zladenie časovačov je realizované prostredníctvom synchronizačnej informácie.

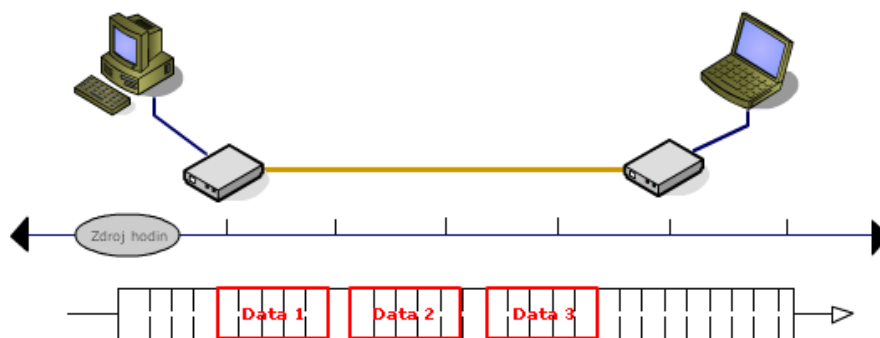


Obr. 3.18a Princíp synchronizácie

Podľa spôsobu synchronizácie rozlišujeme prenos:

- synchronný
- asynchronný.

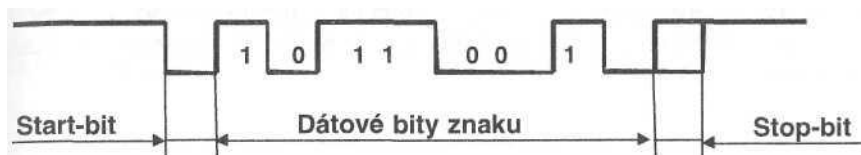
Synchronný prenos je založený na zosynchronizovaní prijímača a vysielateľa prostredníctvom synchronizačných znakov. Synchronizačné znaky zabezpečujú generátory taktovacích impulzov, ktoré majú zosynchronizované časové základne vysielacieho a prijímacieho generátora taktovacích impulzov. Dátové bloky majú rovnakú dĺžku. Celý blok dát je prenesený ako súvislý tok bitov nasledujúcich bezprostredne za sebou. V medzerách medzi blokmi dát sa automaticky vkladajú výplňové značky ako synchronizačné znaky. Začiatky a konce všetkých blokov musia súhlasiť charakteristickými okamžikmi časových základní. Synchronizačný signál je vysielaný aj keď nie sú prenášané žiadne dáta. Takáto synchronizácia je síce zložitá ale synchronný prenos veľmi efektívne využíva prenosový kanál a zabezpečuje prenos aj proti chybovosti. Synchronný prenos sa používa pre veľké objemy dát, napríklad na prenos videa a zvuku. Príklad synchronného prenosu je na obrázku 3.18 b.



Obr. 3.18.b Synchronný prenos

Asynchronný prenos umožňuje, aby bloky dát boli prenášané v ľubovoľných časových odstupoch. Objem prenášaných dát sa rozdelí na menšie časti - bloky, každá časť sa posiela nezávisle na ostatných. Časové intervaly medzi odosielaním jednotlivých častí sa môžu líšiť. Oddelenie bloku dát je prostredníctvom štart a stop bitov, obr. 3.15.c. Štart bit je úvodný bit, ktorého úroveň je logická 0. Za štart bitom nasledujú po sebe idúce bity dátového bloku. Za blok dát je vkladán jeden bit, ktorý slúži ako detektor chyby. Pri sériových prenosoch sa používa ešte paritný bit, ktorý slúži ako detektor chyby. Jeho význam bude zrejmý v kapitole 5. Stop bit ukončuje vysielanie, býva jeden alebo dvoj bitový. V skutočnosti ide o minimálnu časovú hodnotu, počas ktorej musí byť kanál po odoslaní v stave log 1 po odoslaní jedného bloku.

Asynchronný prenos vnáša do prenosu nadbytočnosť prenášaných znakov, preto je asynchronný prenos pomalší než synchronný.



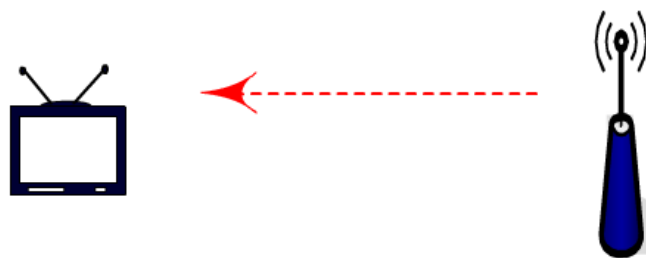
Obr. 3.15.c Asynchronný prenos

3.4.2.1 Typy spojenia

Podľa možného smeru prenosu dát rozlišujeme prenos:

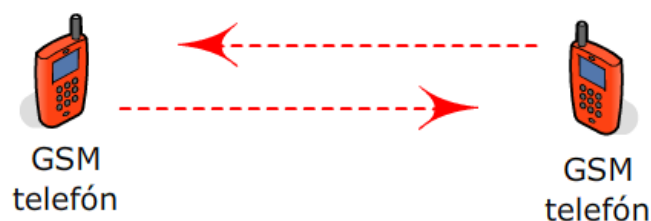
- Simplexný
- Duplexný
- Poloduplexný.

Simplexný prenos je charakteristický tým, že signály sú prenášané len jedným smerom. Jedno koncové zariadenie (KZ) je trvale vysielateľom a druhé prijímačom, obr. 3.16.a.



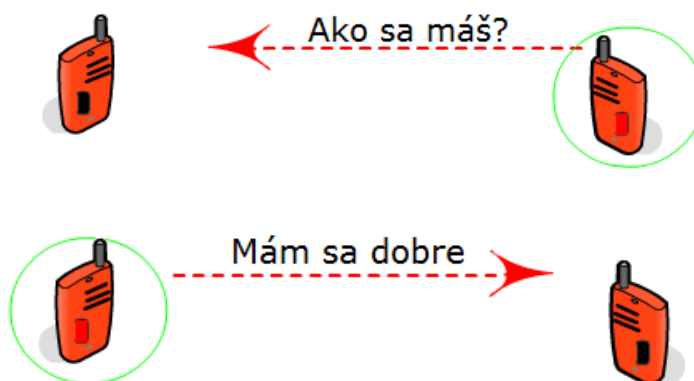
Obr. 3.16.a Simplexný prenos dát

Duplexný prenos umožňuje súčasný prenos signálov v oboch smeroch. Duplexný prenos môžeme chápať ako dva simplexné prenosi prebiehajúce súčasne v opačných smeroch. Obidve koncové zariadenia môžu byť súčasne vysielačom i prijímačom, obr. 3.16.b.



Obr. 3.16.b Duplexný prenos dát

Poloduplexný prenos umožňuje obojsmerný prenos dát, v danom okamihu však možno prenášať dáta len jedným smerom, pričom koncové zariadenia sa vo funkcii prijímača a vysielača striedajú podľa potrieb komunikácie, obr. 3.16.c.



Obr. 3.16.c Poloduplexný prenos

Okruhom vytvoreným dvomi protismernými kanálmi je možné uskutočňovať prenos:

- symetrický, kde je rýchlosť v oboch smeroch rovnaká
- asymetrický, kde sú prenosové rýchlosti rôzne v každom smere.

Podľa smeru prenosu sa rozlišuje:

- **downstream** – zostupný smer prenosu od komunikačnej siete ku koncovému zariadeniu (používateľovi),

- **upstream** – vzostupný smer prenosu od koncového zariadenia (používateľa) ku komunikačnej sieti.

3.5 Štandardizované rozhrania fyzickej vrstvy

Spôsoby prenosu signálu určujú spôsob reprezentácie hodnôt signálu, ale nedefinujú úroveň a typ signálu, rýchlosť prenosu, dĺžky vedení a ďalšie parametre výkonnostných veličín fyzickej vrstvy. Tieto parametre sú uvedené v štandardoch fyzickej vrstvy. Uvádzame stručný popis niektorých štandardov.

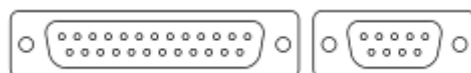
3.5.1 Rozhranie RS 232 (EIA-232-E)

Je štandardom ANSI/TIA/EIA-422-B a ITU-T *Recommendation* T-REC-V.11 Je určené na dvojbodovú sériovú komunikáciu dvoch koncových zariadení. Umožňuje prenos dát plným duplexom. Používa sa na ako komunikačné rozhranie osobných počítačov a iných zariadení. Podľa štandardu RS-232 sú definované vzájomne sériovo komunikujúce zariadenia počítač – DTE (*Data Terminal Equipment*) a pripojené zariadenie – DCE (*Data Communications Equipment*), ich napätia a prenosové rýchlosti. Štandard RS-232 definuje iba to, ako preniesť určitú sekvenciu bitov a nezaobera sa vyššími vrstvami komunikácie. Rozhranie definuje úroveň dátových a riadiacich signálov. Ich veličiny sú uvedené v tabuľke 3.2.

Tabuľka 3.2 Napätové úrovne údajových a riadiacich signálov rozhrania PS 232 (EIA-232-E)

Dátový signál	Riadiaci signál	Úroveň	Napätový rozsah	
			Vysielač	Prijímač
0	1	kladná	od +5 V do +15 V	od +3 V do +15 V
1	0	záporná	od -15 V do -3 V	od -15 V do -5 V

Úroveň signálov sú vzťahované voči nulovému potenciálu. Povolené prenosové rýchlosti: 600, 1200, 2400, 9600, 38400 bps. Maximálna dĺžka prepojovacieho vedenia je 50 m (závisí od prenosovej rýchlosti a typu použitého kábla). Má štandardizované zapojenie s 9, alebo 25 pinovým Cannon D sub konektorom, znázornenom na obr. 3.17. DTE zariadenia používajú 25-pinový konektor (zástrčku) a DCE zariadenia 25-pinový konektor (zásuvku). 25-pinové konektory boli postupne nahradené kompaktnjšími 9-pinovými, obr. 3.17. Konektory na strane DTE majú vždy kolíky (*male*).



Obr. 3.17 Konektory rozhrania RS 232

Postupne sa vyvíjali ďalšie RS rozhrania pre špeciálne potreby. Stručne sú uvedené charakteristiky niektorých z nich.

3.5.2 Rozhranie RS-423 (EIA-423-A)

Je určené na dvojbodové spojenie dvoch komunikujúcich zariadení. Umožňuje prenos dát plným duplexom. Vysielač signálu má nesymetrický výstup, ale vstupy prijímačov sú symetrické. Rýchlosť prenosu 3 kbps na vzdialenosť do 1000 m, alebo až 300 kbps na vzdialenosť 10 m.

3.5.3 Rozhranie RS 422 (EIA-422-A)

V využíva symetrické vedenie, na rozdiel od RS-232 a RS-423. Výhodou symetrických vedení je vyššia odolnosť voči poruchám, vyššie potlačenie súhlasných napätí a možnosť prenosu na väčšie vzdialenosti. Jeden vysielač však môže komunikovať až s desiatimi prijímačmi, potom je však možný len jednosmerný - simplexný prenos.

3.5.4 Mnohobodové elektrické rozhranie RS 485 (ISO/IEC 8482)

Rozhranie ISO/IEC 8482 vzniklo pôvodne ako rozšírenie rozhrania EIA-422-A, pričom prevzalo úroveň signálov a doplnila sa možnosť poloduplexného prenosu údajov na mnohobodovom údajovom spoji. Na prenos sa používa symetrické vedenie. Maximálna prenosová rýchlosť je 12 Mbps na vzdialenosť menšiu ako 100 m. Maximálna vzdialenosť medzi komunikujúcimi zariadeniami je 1200 m pri prenosovej rýchlosti 9600 bps). Na jedno vedenie je možné pripojiť maximálne 32 zariadení. Prenosové médium je krútená dvojlinka.

3.5.5 Priemyselné štandardy rozhraní

USB (Universal Serial Bus) – univerzálna sériová zbernica je novší spôsob pripojenia počítača pomocou univerzálneho sériového rozhrania. Používa sa nielen na pripojenie počítača, ale aj na pripojenie iných zariadení v oblasti počítačovej techniky. USB je veľmi rozšírené aj ako prenosné pamäťové zariadenie (USB kľúče, *Flash Drives*). Prenosové rýchlosti pre štandard USB 1.1 sú 1,5 Mbit/s a 12 Mbit/s, pre štandard USB 2.0 je 480 Mbit/s. Dĺžka kábla pripojenia je maximálne 5 metrov pri použití krútenej dvojlinky.

Existuje viac druhov USB konektorov. Základné rozdelenie je na typ A a B. Typ A sa používa smerom k počítaču (*upstream*), typ B na smerovanie k zariadeniam, ku ktorým sa pripája (*downstream*). Ich znázornenie je na obr. 3.18.



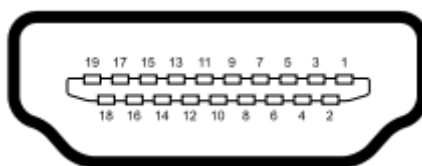
Obr. 3.18 USB konektory typ A a B

Na prepájanie zariadení USB sa používajú štvorvodičové káble. Význam jednotlivých pinov na konektore USB rozhrania je v tabuľke 3.3.

Tabuľka 3.3. Význam pinov USB rozhrania

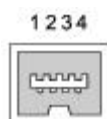
Pin na konektore	Význam
1	+5V
2	Dáta +
3	Dáta -
4	GND - zem

High-Definition Multimedia Interface (HDMI) je novšie rozhranie pre audio a video zariadenia s vysokým rozlíšením. Konštrukčne je podobný USB rozhraniu. V súčasnosti existujú tri typy HDMI konektorov A, B a C. Rozlišujú sa v počte pinov a v šírke prenášaného pásma. Znázornenie konektoru typu A je na obr. 3.19. HDMI rozhranie je schopné prenášať až 5 Gbit/s. Má dostatočnú rezervu aj do budúcnosti, priepustnosť je asi dvakrát vyššia, ako je potrebná v súčasnosti pre viackanálové video a audio. HDMI nedefinuje maximálnu dĺžku kábla. Jediným obmedzením je útlm signálu. Dĺžka závisí na konštrukcii a kvalite materiálov, ktoré boli použité.



Obr. 3.19 HDMI konektor

IEEE 1394 označovaný aj ako FireWire a iLink je štandard rozhrania vysokorýchlostnej sériovej zbernice pre osobné počítače s možnosťou asynchrónneho prenosu v reálnom čase. Názov FireWire si patentovala spoločnosť Apple a názov iLink spoločnosť Sony. Používa sa na pripojenie periférií ktoré vyžadujú vysoké prenosové rýchlosti. Najčastejšie sa používa na pripojovanie úložísk dát ako sú externé pevné disky, videokamery, na pripojenie priemyselných video systémov a profesionálnych audio systémov. Dosahovaná prenosová rýchlosť je do 400 Mbit/s. Znázornenie konektoru je na obr. 3.20.



Obrázok 3.20.

Kábel je tvorený dvomi párami diferenčných signálov TPA a TPB. Význam pinov je v tabuľke 3.4.

Tabuľka 3.4. Význam pinov rozhrania IEEE 1394

Pin na konektore	Význam
1	TPB -
2	TPB +
3	TPA -
4	TPA+

3.6 Záver

Fyzická vrstva je základná sieťová vrstva, poskytujúca prostriedky pre prenos. Fyzická vrstva poskytuje elektrické a mechanické vlastnosti pre prenos informácie a plní funkčné a procedurálne požiadavky k nadviazaniu, udržaniu a zrušeniu spojenia medzi entitami linkovej úrovne. V protokolových špecifikáciách musia byť určené:

- elektrické parametre signálu
- význam signálu a časový priebeh
- vzájomné nadviazanie riadiacich a stavových signálov
- zapojenie konektorov
- a mnoho iných parametrov technického a procedurálneho charakteru.

Fyzická spojenie obsahuje okrem prenosových médií aj ďalšie prostriedky potrebné pre prenos a spolu tvoria komunikačný kanál alebo okruh pre prenos signálov.

Signál v komunikačných sieťach je fyzickým prostriedkom (nosičom) pre prenos alebo spracovanie správ. Podľa nadobudnutých hodnôt oboch vyjadrených veličín sú rozlišované nasledujúce typy signálov:

- analógový (spojitý v oboch vyjadrených veličinách),
- diskretný (nespojité v jednej, alebo v oboch vyjadrených veličinách),
- digitálny alebo číslicový, ktorý je špeciálnym prípadom diskretného signálu (nespojité v čase aj amplitúde).

Ich grafické vyjadrenie a matematický model umožňujú pochopiť ich vlastnosti, ktoré sú ďalej využívané pri ich spracovaní pre prenos. Dôležitou súčasťou je rozklad signálu, označovaný ako harmonická analýza, ktorý dáva informáciu o jeho frekvenčnom spektre.

Pre hodnotenie signálov sú špecifikované veličiny, ktorých parametre sú potrebné pre hodnotenie kvality prenosu signálu. Sú to úroveň signálu, tlmenie signálu, oneskorenie signálu, skreslenie signálu a odstup signál – šum. Celkové hodnotenie niektorých veličín sa označuje ako objem signálu.

Protokolovou dátovou jednotkou PDU je bit. Jeho prenos je uskutočňovaný rôznymi technológiami a rôznymi spôsobmi. Použitie určitých spôsobov prenosu je pre každú technológiu špecifikované v normách a odporúčaníach.

Kľúčové slová:

1. Fyzická vrstva
2. Funkcie fyzickej vrstvy
3. Technológie pre fyzické spojenie
4. Protokoly fyzickej vrstvy
5. DTE (*Data Terminal Equipment*)
6. DCE (*Data Circuit-Terminal Equipment*)
7. Signál
8. Analógový signál
9. Diskrétny signál
10. Digitálny signál
11. Periodický signál
12. Harmonický signál
13. Neperiodický signál
14. Modely signálu
15. Veličiny/atribúty signálu
16. Amplitúda signálu
17. Frekvencia signálu
18. Fázový posuv signálu
19. Skladanie a rozklad signálu
20. Časová závislosť signálu
21. Frekvenčná závislosť signálu
22. Harmonická analýza signálu
23. Frekvenčného spektrum signálu
24. Amplitúdové frekvenčné spektrum
25. Fázové frekvenčné spektrum
26. Parametre hodnotenia signálu
27. Absolútna úroveň signálu
28. Relatívna úroveň signálu
29. Tlmenie signálu
30. Oneskorenie signálu
31. Skreslenie signálu
32. Odstup signál –šum
33. PDU fyzickej vrstvy
34. Bit, Bajt
35. Prenos v základnom pásme
36. Prenos v preloženom pásme
37. Sériový prenos
38. Paralelný prenos
39. Synchronný prenos
40. Asynchronný prenos
41. Simplexné spojenie
42. Duplexné spojenie
43. Polovičný duplex
44. Dvojbodové spojenie
45. Viacbodové spojenie
46. USB (*Universal Serial Bus*)
47. Komutovaná linka (*dial-up*)
48. DSL (*Digital Subscriber Line*)
49. ISDN pripojenie
50. Fyzická vrstva v LAN
51. GSM

Kontrolné otázky

1. Ktorá zo špecifikácií patrí fyzickej vrstve?
2. Čo poskytuje fyzická pre prenos informácie?
3. Je fyzická vrstva technologicky závislá?
4. Ktoré z uvedených špecifikácií musí obsahovať protokol fyzickej vrstvy?
5. Ako je charakterizovaná základná funkcia fyzickej vrstvy?
6. Akými hardvérovými prostriedkami je tvorená fyzická vrstva?
7. Čo je PDU fyzickej vrstvy?
8. Akými spôsobmi môže byť vytváraný prístup k prenosovému médiu vo fyzickej vrstve?
9. Čo je signál pre elektronickú komunikáciu?
10. Ako sa graficky znázorňuje signál?
11. Ktoré z uvedených formulácií je závislosť časového vyjadrenie signálu?
12. Ako je charakterizovaný analógový signál?
13. Ako je charakterizovaný diskretný signál?
14. Ako je charakterizovaný digitálny signál?

15. Aký je rozdiel medzi digitálnym a číslicovým signálom?
16. Aký je rozdiel medzi periodickým a harmonickým signálom?
17. Ktoré z uvedených formulácií platia pre harmonický signál?
18. Aké závislosti sú používané pre vyjadrenie signálu?
19. Čo znamenajú veličiny signálu vyjadreného v tvare $A(t) = A_{\max} \cdot \sin(2\pi f \cdot t + \varphi_0)$?
20. Čo vyjadruje amplitúda signálu?
21. Aký je vzťah medzi frekvenciou a periódou harmonického signálu?
22. Aký je vzťah medzi sínusovou funkciou a sínusovým signálom?
23. Čo vyjadruje harmonická analýza signálu?
24. Čo znamená pojem šírka frekvenčného spektra?
25. Aké je frekvenčné spektrum harmonického signálu?
26. Čo vyjadruje amplitúdové frekvenčné spektrum?
27. Čo vyjadruje fázové frekvenčné spektrum?
28. Prečo je dôležité poznať frekvenčné spektrá signálov?
29. Čo vyjadruje úroveň signálu?
30. Čo znamenajú veličiny vzťahu

$$L_A = 10 \log \left| \frac{P}{P_o} \right|$$

31. Čo znamenajú veličiny vzťahu

$$L_R = 10 \log \left| \frac{P}{P_x} \right|$$

32. Aký je rozdiel medzi relatívnou a absolútnou úrovňou?
33. V akých jednotkách sa vyjadruje úroveň?
34. Čo znamená tlmenie signálu?
35. Aký je vzťah medzi tlmením a úrovňou signálu?
36. Čo znamená oneskorenie signálu?
37. Od čoho závisí oneskorenie signálu pri prenose v prenosovom médiu?
38. Čo znamená skreslenie signálu?
39. Prečo je skreslenie signálu dôležitým parametrom kvality prenosu?
40. Čo spôsobí šum pri prenose signálu?
41. Kedy šum výrazne vplýva na kvalitu prenosu signálu?
42. Čo znamená skratka SNR?
43. V akých jednotkách sa udáva pomer signál-šum?
44. Čo udáva parameter dynamický rozsah signálu?
45. Čo znamená prenos v základnom pásme?
46. Čo znamená prenos v preloženom pásme?
47. Aký je rozdiel medzi paralelným a sériovým prenosom dát?
48. Ktoré tvrdenie je správne pre synchronný prenos?
49. Ktoré tvrdenie je správne pre asynchronný prenos?
50. Aký je rozdiel medzi simplexným a duplexným spojením?
51. Aký je rozdiel medzi polovičným duplexom a simplexom?
52. Ako sa pripájajú koncové zariadenia na fyzickú vrstvu?
53. Ako sú vytvorené pravidlá pre pripojenie rôznych zariadení na fyzickej vrstve?
54. Cez ktoré z uvedených technológií je možné vytvorenie fyzického spojenia?
55. Čo znamená označenie štruktúrovaná kabeláž?

4 Fyzická vrstva II. – prenosové kanály / médiá

Ciele učenia

Po štúdiu tejto kapitoly by ste mali vedieť:

- Čo je to prenosový kanál
- Aké sú parametre hodnotenia prenosového kanála
- Aké médiá sa používajú pre prenos informácie
- Aké sú vlastnosti prenosových médií
- Aké sú možnosti prispôsobenia signálu pre prenos po prenosových médiách
- Čo je to modulácia
- Aké typy modulácií sa používajú pri prenosoch v elektronických komunikačných sieťach
- Ako možno prenášať po komunikačných sieťach viac signálov súčasne
- Aké prenosové systémy sa používajú pre viacnásobný prenos signálu

4.1 Úvod

Ďalšie funkcie a služby fyzickej vrstvy sú spojené s prenosom elektromagnetického signálu cez fyzické prenosové médium. Funkcie a služby spojené s prenosom možno zoskupiť do nasledovných častí:

- poskytnutie prenosového média požadovaných parametrov,
- úprava signálu pre prenos:
 - modulácie,
 - linkové kódovanie,
- viacnásobné prenosy – multiplexovanie,
- poskytnutie štandardizovaného rozhrania fyzickému prenosovému mediu.

Prenosové médium je tá časť fyzickej vrstvy, ktorá fyzicky umožní prenos signálu z vysielača do prijímača. Každý druh prenosového média má špecifické prednosti a preto o konkrétnom použití rozhodujú vždy podrobné technicko-ekonomické rozbor. Prenosové médiá všeobecne poskytujú komunikačný kanál pre prenos príslušnej správy. Vlastnosti komunikačného kanála sú charakterizované parametrami, ktorých hodnoty sú potrebné na prenos signálu, nesúceho príslušnú správu. Neexistuje ideálne prenosové médium, preto je potrebné vyberať také prenosové médiá, ktoré najlepšie splňujú parametre, potrebné pre prenos signálu.

4.2 Parametre hodnotenia prenosových kanálov

Vlastnosti komunikačného kanála musia byť v zhode s prenášaným signálom, ktorého vlastnosti boli študované v kapitole 3. Preto sú parametre pre posudzovanie vlastností prenášaného signálu a prenosového kanála v princípe rovnaké. Z technického hľadiska

posudzujeme kvalitu prenosu príslušného kanála podľa podobných parametrov, akými je hodnotený signál. Sú to nasledovné veličiny:

- Dynamický rozsah kanálu D_k , ktorý je špecifikovaný ako odstup signálu od šumu v príslušnom kanáli. Tento pomer možno označiť tiež aj ako odolnosť proti rušivým vplyvom v kanáli. Označuje sa SNR – *Signal to Noise Ratio* a jeho definovanie je rovnaké ako u signálu. Počíta sa podľa vzťahu $SNR(dB) = 10 \log |SNR|$
Tento vzťah vyjadruje logaritmické narastanie hodnôt SNR v dB. Ak je pomer signál/šum 10, SNR je 10 dB, ak je pomer signál/šum 100, SNR je 20 dB atď.
- Šírka pásma kanála prenosového kanála F_k , (*Bandwidth*) je interval frekvencií, ktoré je prenosový kanál schopný preniesť. Jednotka šírky pásma je rovnaká ako jednotka frekvencie signálu, t.j. 1 Hz. V prípade telefónnych okruhov prenášajúcich frekvencie od 300 Hz do 3400 Hz, je šírka pásma 3100 Hz, t.j. 3,1 kHz. Ak šírka pásma prenosového kanála je menšia ako šírka frekvenčného pásma prenášaného signálu, nie sú prenesené všetky harmonické zložky signálu a prenesený signál je na prijímačej strane skreslený oproti signálu na vstupe do prenosového kanála. Šírka pásma prenosových médií môže byť výrazne vyššia, ako skutočne využívaná šírka pásma pre prenos určitého signálu.
- Doba trvania signálového prvku, od ktorej je závislá maximálna prenosová rýchlosť. Prenosová rýchlosť je dôležitým parametrom kvality aj pre prenosové médiá.

Súhrn všetkých posudzovaných veličín sa nazýva Pripustnosť prenosového kanálu P_k .

Pri prenose informácií je jedným z rozhodujúcich aspektov objem dát, ktorý je schopný prenosový kanál preniesť za určitý čas. Vo vzťahu k parametrom objemu signálu V_s musí platiť nasledovný vzťah: Pripustnosť prenosového kanálu P_k musí byť väčšia alebo rovná objemu príslušného prenášaného signálu V_s , vysvetlenom v predošlej kapitole.

V praxi je situácia o niečo zložitejšia. Musíme vziať do úvahy aj ďalšie obmedzujúce kritériá prenosu. Aj keď sme v kapitole 3 vysvetlili, že prenosová rýchlosť je daná vzťahom

$$v_p = v_s \cdot \log_2 N,$$

kde v_s je symbolová rýchlosť daná prevrátanou hodnotou doby trvania signálového prvku a N je počet stavov amplitúdy prenášaného digitálneho signálu, jej hodnota je závislá aj od šírky pásma prenosového kanála.

Túto skutočnosť zistil v roku 1924 Henry Nyquist a je známa ako Nyquistov vzorkovací teorém. Podľa tohto teorému platí: Ak máme požiadavku preniesť signál čo najvernejšie a ak je šírka pásma prenosového kanála F_k , tak je potrebné vzorkovať signál frekvenciou rovnou dvojnásobku šírky pásma prenosového kanála. V prípade telefónneho kanála je šírka pásma 4 kHz, preto nemá význam prenášať vzorky rýchlejšie ako 8000 krát za sekundu. Symbolová rýchlosť a šírka prenosového kanála je vyjadrená podľa Nyquistovho vzorkovacieho teorému vzťahom

$$v_s = 2 \cdot \text{šírka pásma} = 2 \cdot F_k.$$

Pri dodržaní takto stanovenej symbolovej rýchlosti je prenosová rýchlosť daná vzťahom

$$v_p = 2 \cdot \text{šírka pásma} \cdot \log_2 N = 2 \cdot F_k \log_2 N$$

Maximálne dosiahnuteľná prenosová rýchlosť je teoreticky číselne priamo úmerná šírke pásma a počtu stavov prenášaného signálu. V praxi sa často uvádza približný vzťah medzi šírkou pásma v Hz a prenosovou rýchlosťou v bit/s ako 1:1 alebo 1:2.

Je zaujímavé určiť podľa týchto vzťahov jednotku symbolovej a prenosovej rýchlosti. Z predošlého vzťahu ich môžeme vyjadriť v jednotkách Hz. Preto sa môžeme stretnúť aj s takýmto vyjadrením symbolovej a prenosovej rýchlosti. Nie je to zásadná chyba, ale ak sú dohodnuté jednotky pre symbolovú rýchlosť B_d a prenosovú rýchlosť bit/sek, nie je vyjadrenie v Hz správne.

V ideálnom prenosovom kanáli sú symbolová a prenosová rýchlosť limitované iba šírkou pásma kanála, v reálnych kanáloch sú použiteľné rýchlosti menšie. Závislosť medzi prenosovou rýchlosťou a šírkou pásma prenosového kanála závisí na konkrétnej realizácii. Dosiahnuteľná prenosová rýchlosť je daná súhrnom:

- fyzikálnych vlastností prenosového média,
- vlastnosťami ďalších technických prostriedkov, ktoré vytvárajú prenosový kanál, napríklad modemy, multiplexory a ďalšie.

Veľmi dôležitá otázka prenosu je, ako dosiahnuť čo najvyššiu prenosovú rýchlosť. Môžeme žiadať od prevádzkovateľa elektronickej komunikačnej siete väčšiu šírku frekvenčného pásma. Šírka pásma, daná použitým prenosovým kanálom, býva adekvátne spoplatnená. Čím väčšiu šírku pásma požadujeme, tým je vyššia cena. Vzniká tu otázka, či ponechať šírku prenosového pásma bez zmeny, aby sa nezvyšovali náklady, a zvyšovať počet stavov prenášaného signálu (hodnotu N). Ak by to bolo možné, znamenalo by to, že zdokonaľovaním technológie prenosu by sa dala ľubovoľne zvyšovať aj prenosová rýchlosť. Nie lineárne ale logaritmicky. Odpoveď na vyššie položenú otázku dal až zakladateľ modernej teórie informácie, Claude Shannon. Zistil, že ani najdokonalejšia technológia prenosu sa nikdy nedostane cez určitú hranicu, ktorá je daná:

- šírkou prenosového pásma,
- "kvalitou" prenosového kanála, vyjadrenou odstupom signálu od šumu.

Skutočná závislosť maximálnej prenosovej rýchlosti na šírke pásma a kvalite kanála vyjadreného odstupom signálu od šumu je vyjadrená nasledovným vzťahom

$$v_{pmax} = \text{šírka pásma} \cdot \log_2(1 + \text{signál/šum}) = F_k \cdot \log_2(1 + \text{SNR})$$

Tento vzťah nevyjadruje dokonalosť technológie alebo parameter, ktorý by sa dal meniť. Ide o principiálny limit, ktorý závisí od dokonalosti technológie, ktorá sa bude používať. Napríklad kanál, ktorého $F_k = 3000$ Hz a s odstupom signálu od šumu 30 dB nemôže prenieť viac ako 30 kbit/s, bez ohľadu na počet prenášaných úrovni signálu.

Kvalita prenosových médií sa posudzuje aj podľa toho, ako ovplyvňujú prenášaný signál.

Prenosový kanál a aj celková kvalita prenosu elektronickou komunikačnou sieťou sú hodnotené parametrami, ktoré sú podobné parametrom porovnania signálov. Sú to:

- Tlmenie, ktorým je znížený výkon signálu prechodom cez prenosové médium. Možno rozlišovať tlmenie napätia, prúdu a výkonu prenášaného signálu. Tlmenie výkonu signálu sa počíta podľa vzťahu

$$a = 10 \log \left| \frac{P_{\text{vstupu}}}{P_{\text{výstupu}}} \right|$$

P_{vstupu} je výkon na vstupe prenosového kanála, $P_{\text{výstupu}}$ je výkon na výstupe prenosového kanála. Udáva sa v [dB]. Tlmenie 3 dB znamená zníženie výstupného výkonu signálu na polovicu oproti vstupnému výkonu.

- Skupinové oneskorenie prenosového kanála je parameter, ktorý je spojený s fázovým posunom b harmonických zložiek signálu. Fázový posun harmonických zložiek prenášaného signálu v prenosovom kanáli je rôzny. To spôsobuje deformáciu tvaru časového priebehu signálu označovanú tiež ako skreslenie signálu. Z hľadiska prenosu signálu je dôležité, aby bolo konštantné skupinové oneskorenie dané vzťahom

$$\tau = \frac{\partial b}{\partial \omega}$$

- Presluchy sú interferencie vznikajúce pri súbežnom prenose po viacerých prenosových médiách alebo v kanáloch jedného prenosového média. Signály z iných kanálov sa namodulujú na prenášaný signál a spôsobujú tak rušenia v prenosových kanáloch.

$$T_s = \frac{db}{d\omega}$$

Hodnoty parametrov prenosového kanála sú dané nielen fyzikálnymi vlastnosťami prenosového média ale aj spracovaním signálu pri prenose.

4.3 Prenosové médiá

Prenosové médium je fyzické prostredie, ktorým je uskutočňovaný prenos signálu medzi dvoma prvkami siete. V elektronických komunikačných sieťach sa používajú nasledujúce typy prenosových médií:

- metalické vedenia (*metallic lines*):
 - symetrické: krútený pár (*twisted pair*),
 - nesymetrické: koaxiálny kábel (*coax cable*),
- optické vlákna (*optical fibre / fibre optic cables*),
- rádiové spoje (*radio links*):
 - pozemské (*terrestrial*),
 - satelitné (*satellite*).

Metalické vedenia a optické vlákna sú spolu označované ako pevné/drôtové prenosové médiá. Rádiové spoje sú označované ako bezdrôtové prenosové médiá.

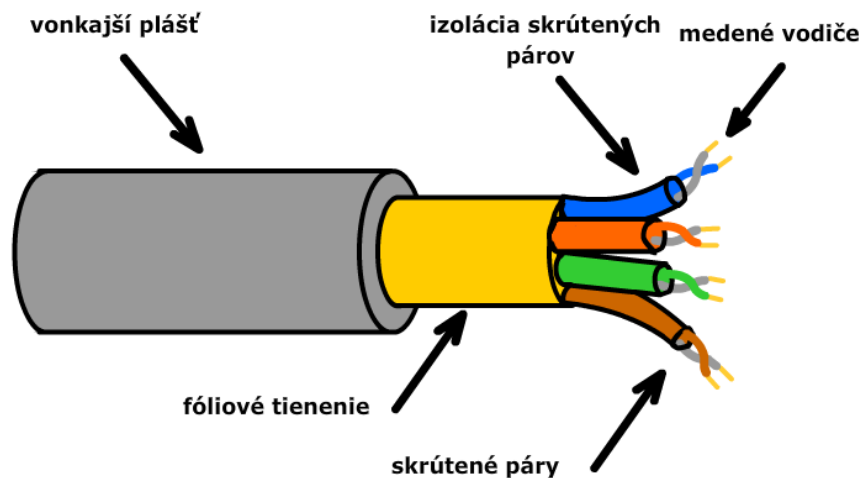
4.3.1 Metalické vedenia

Káblové metalické vedenia môžu byť:

- symetrické: krútená dvojlinka/pár (*twisted pair, TP*)
- nesymetrické: koaxiálny kábel (*coax cable*)

4.3.1.1 Krútená dvojlinka

Krútená dvojlinka je používaným prenosovým médiom v sieťach koncových zariadení a prístupových sieťach, kde slúži na pripojenie používateľov k elektronickej komunikačnej sieti. Je dominantným prenosovým médiom v lokálnych počítačových sieťach, hlavne v sieťach typu Ethernet. Rôzne typy sietí vyžadujú rôzne definované káble typu krútená dvojlinka: Ethernet 10Base-T, 100Base-TX, 100Base-T2, 100Base-T4, 1000Base-T (prvé číslo je rýchlosť v Mbit/s, písmeno T znamená Twisted - krútený, číslo počet párov ktoré sú využívané). Krútená dvojlinka je vyrobená z medi a polymérov. Jednotlivé vodiče sú uložené v pároch, páry sú skrútené navzájom okolo seba. Vodiče v páre sú rovnocenné (žiadne z vodičov nie je pripojený na zem, alebo zdroj napätia) preto sa takýto kábel označuje tiež ako symetrický. Znárodnenie konštrukcie krútenej dvojlinky je na obr. 4.1.



Obr. 4.1 Krútená dvojlinka

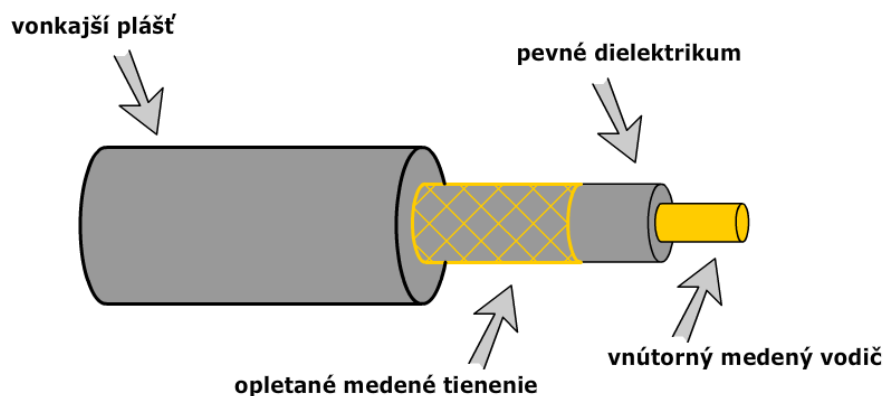
Krútená dvojlinka sa podľa použitého tienenia delí na tienenú a netienenú. Podľa typu tienenia sa rozlišujú:

- UTP – (*Unshielded Twisted Pair*) netienená, najčastejšie používaná, v súčasnosti najlacnejšie prenosové médium,
- STP – (*Shielded Twisted Pair*), tienená, každý pár vodičov je obalený v kovovej fólii,
- S/STP – (*Screened Shielded Twisted Pair*), jednotlivé páry sú tienené fóliou a zároveň všetky páry ešte tieniacou sieťkou,
- FTP – (*Foiled Twisted Pair*), tienená hliníkovou fóliou,

- S/FTP – (*Screened Foiled Twisted Pair*), tienená hliníkovou fóliou a kovovým opletaním.

4.3.1.2 Koaxiálny kábel

Koaxiálny kábel sa často používa v sieťach káblovej televízie CATV (*Cable Television*) a na pripájanie antén. Bol vyvinutý pre zlepšenie odolnosti vedenia voči šumu. Na rozdiel od krútenej dvojlinky má koaxiálny kábel dva rozdielne vodiče. Vnútorňý vodič je uložený v dielektriku tvorenom polyetylénom. Dielektrikum je obalené tienením vo forme kovovej sieťky, ktorá tvorí vonkajší vodič. Celý kábel je obalený vonkajšou izoláciou, ktorá chráni pred vonkajšími vplyvmi. Konštrukcia koaxiálneho kábla je znázornená na obr. 4.2

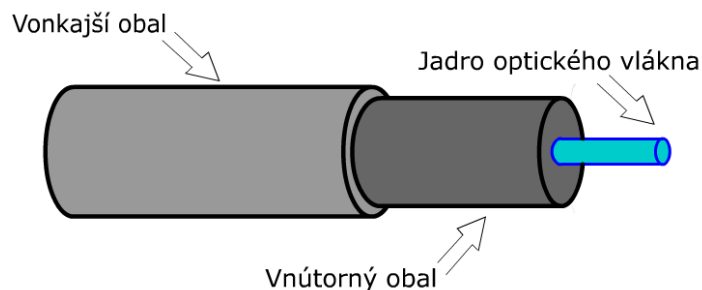


Obr. 4.2 Koaxiálny kábel

Koaxiálny kábel je v ostatnom období nahrádzaný hlavne optickými káblami.

4.3.2 Optický kábel/vlákno (Optical cable)

Optické káble sú používané pre celé spektrum komunikačných technológií. Používajú sa na prepojenie v budovách aj v diaľkových prenosoch. Optický kábel je tvorený skleneným alebo plastovým vláknom s priemerom 5 až 125 μm . Odtiaľ je aj častejšie používané označenie optické vlákno. Konštrukčne je optický kábel tvorený jadrom, obalom a plášťom, znázorneným na obr. 4.3.



Obr. 4.3 Optické vlákno

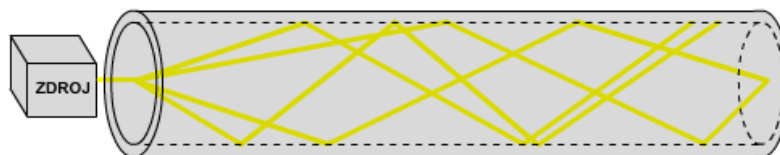
Optickým vláknom sa šíria elektromagnetické vlny vlnovej dĺžky svetla alebo infračerveného žiarenia. Elektromagnetická vlna je označovaná ako svetelný lúč. Šírenie svetelného lúča je v smere osi vlákna. Ak má vlákno veľmi malý priemer, porovnateľný

s dĺžkou svetla, lúč sa prenáša priamo od vysielača k prijímaču. Ak je priemer vlákna väčší, prenos je uskutočňovaný s využitím princípu totálneho odrazu na rozhraní dvoch prostredí s rozdielnym indexom lomu. Sériou takýchto odrazov sa elektromagnetická vlna šíri od vysielača k prijímaču a umožňuje šírenie svetelného lúča vo viacerých módoch/vidoch. Jednotlivé módy sa šíria rozličnou rýchlosťou a tým sú vytvárané akoby mnohonásobné prenosové kanály s rôznymi dobami prenosu signálu. To obmedzuje rýchlosť prenosu. Kompromisným riešením je vlákno s gradientovou zmenou indexu lomu. Požadovaný efekt sa dosiahne tým, že index odrazu v smere od jadra k jeho okraju sa gradientne mení.

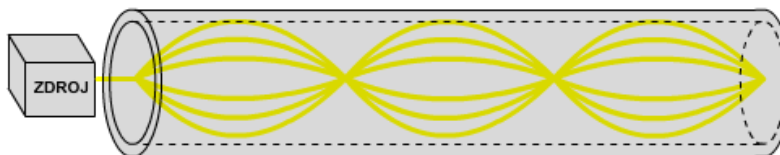
Podľa typu šírenia lúča vláknom sa rozlišujú tri základné typy optických vlákien:

- mnohovidové/multivoidové vlákna (*multi mode fiber*),
- mnohovidové vlákna s gradientným priebehom indexu (*gradient multi mode fiber*),
- jednovoidové/monovoidové vlákna (*single mode fiber*).

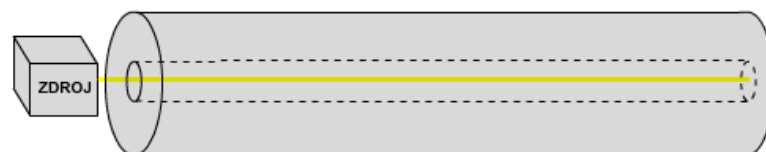
Príklady typov optických vlákien sú na obrázku 4.4.



a) mnohovidové / multivoidové vlákno



b) mnohovidové vlákno s gradientným priebehom indexu



c) jednovoidové / monovoidové vlákno

Obr. 4.4 Typy optických vlákien

Každý z typov optických vlákien sa využíva na iné účely:

- mnohovidové – krátke trasy (medzi miestnosťami, budovami) s menšími prenosovými rýchlosťami, majú nižšiu cenu,
- mnohovidové gradientné vlákna pre vzdialenosti 260 m až 2 km v závislosti od technológie,
- jednovoidové v diaľkových prenosoch, kde sú potrebné vysoké prenosové rýchlosti.

Charakteristiky optických vlákien:

- Veľká šírka pásma – optická frekvencia sa pohybuje v rozsahu 10^{13} až 10^{16} Hz, šírka pásma tak dosahuje rádovo THz.
- Malé rozmery a váha – optické vlákna pre komunikačné účely majú veľmi malý priemer, nepresahujúci priemer ľudského vlasu.
- Bezpečnosť prenosu – optické vlákna sú vyrábané zo skla, alebo plastických polymérov, čo sú izolačné materiály.
- Nízke straty pri prenose – optické vlákna majú nízke hodnoty tlmenia, čím sa znižuje cena i zložitosť prenosových zariadení a zvyšuje sa spoľahlivosť prenosu.

4.3.3 Rádiové spoje

Pri rádiových spojoch je prenosovým prostredím vzduch. Na realizáciu prenosu sa využívajú elektromagnetické vlny frekvencií 10^4 Hz – 10^{10} Hz. Vzduch, podobne ako kov pri metalických vedeniach, nie je ideálnym prenosovým médiom a spôsobuje tlmenie signálu. Tlmenie sa zvyšuje nepriaznivým počasím, zvýšenou vlhkosťou, prípadne dažďom. Vplyv počasia na veľkosť tlmenia je výraznejší pri prenose vyšších frekvencií nad 10 GHz. Ďalší obmedzujúci faktor je interferencia z iných rádiových spojov, ktorá vzniká s rastom počtu rádiových smerových spojov. Preto sú na národnej aj medzinárodnej úrovni dohodnuté rozdelenia frekvencií pre konkrétne prenosy. Dohody o rozdelení frekvenčného spektra rádiových vln vyústili k dohovoru medzi členskými štátmi OSN, ktorý má názov Medzinárodný dohovor o telekomunikáciách. Na základe neho Medzinárodná telekomunikačná únia vytvorila rádiokomunikačný poriadok, ktorý je prílohou Medzinárodného dohovoru o telekomunikáciách. Podľa pravidiel rádiokomunikačného poriadku organizácia CEPT (*European Conference on Postal and Telecommunications*) sleduje, koordinuje a reguluje využívanie frekvenčného spektra vyplývajúce z mandátov Európskej komisie. Slovenská republika má Národnú tabuľku frekvenčného spektra, ktorú schvaľuje vláda Slovenskej republiky raz za 3-4 roky. Aktuálna verzia NTFS 2011 je schválená uznesením vlády SR č. 573/2011. Správu frekvenčného spektra vykonáva Telekomunikačný úrad Slovenskej republiky.

Rádiové spoje možno kategorizovať podľa rôznych hľadísk. Podľa spôsobu vytvárania prenosovej cesty rozlišujeme

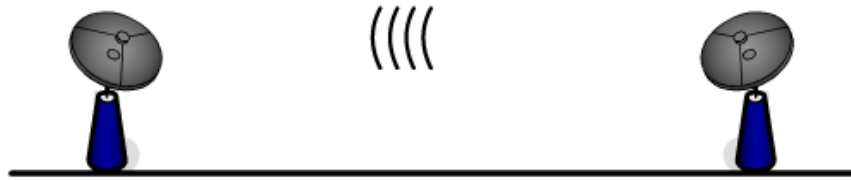
- smerové rádiové spoje,
- satelitné/družicové rádiové spoje,
- všesmerové rádiové spoje.

Charakteristiky rádiových spojov sú nasledovné:

4.3.3.1 Smerové rádiové spoje

- Smerové rádiové spoje patria do skupiny bezdrôtových prenosových médií.
- Vysielače a prijímače sú vybavené parabolickými anténami, ktoré slúžia na vysielanie a príjem úzko smerovaného mikrovlnného lúča. V princípe ide o dvojbodové spojenie, obr. 4.5.

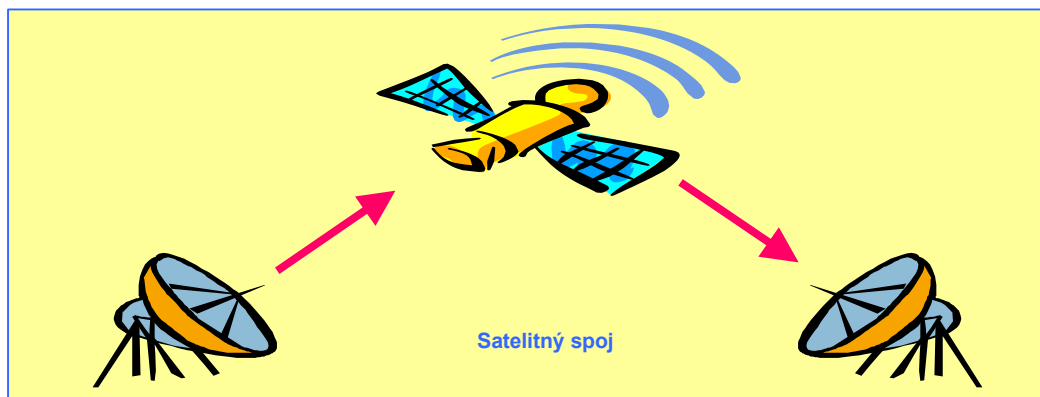
- Smerové rádiové spoje sa označujú aj ako spoje mikrovlnné.
- Sú vhodné i na prenos dát vysokými rýchlosťami, desiatky až stovky Mbit/s.
- V transportných sieťach sú používané na preklopenie ťažkých terénov.
- Ako prístupové siete na distribúciu dát v dosahu do 10 km.



Obr. 4.5 Smerový rádiový spoj

4.3.3.2 Satelitné rádiové spoje

- Satelitné rádiové spoje pracujú so satelitmi, umiestnenými mimo atmosféry.
- Satelit pracuje ako prepojovací uzol, ktorý spája pozemské vysielacie a prijímače a vytvára tak dvojbodové spojenia alebo spojenia typu 1:n, obr. 4.6.
- Satelit signál prijme, zosilní alebo obnoví a vysiela v inom frekvenčnom pásme (aby nedošlo k interferencii oboch signálov) smerom k zemi.
- Satelity kvôli vzájomnej interferencii signálov pôvodne nesmeli byť k sebe bližšie než 4° (merané na Zemi). Pokrok vo výrobe antén umožnil zmenšiť tento rozstup na 2° .
- Aby satelit mohol pracovať nepretržite, musí byť neustále „viditeľný“ z vysielateľa i prijímača.
- Optimálne frekvenčné pásmo pre satelitné spoje je 1-10 GHz.
- Používanie satelitných spojov je široké. Slúžia na prenos televíznych signálov, telefónnych hovorov i pre prenosy dát.



Obr. 4.6 Satelitný spoj

4.3.3.3 Všesmerové rádiové spoje

- Základný rozdiel oproti priamym spojom je v tom, že rádiové vysielanie je všesmerové, obrázok 4.7.
- Všesmerové rádiové spoje sa používajú hlavne pre:
 - rozhlasové a televízne vysielanie,

- mobilné telefónne systémy.



Obr. 4.7 Všesmerový rádiový spoj

4.4 Použitie prenosových médií

Pri vedeniach (krútený dvojpár, koaxiálny kábel, optické vlákno) má rozhodujúci vplyv na kvalitu prenosu samotná kvalita vedenia. Pri rádiových a satelitných spojoch je okrem prenosového prostredia (vzduchu) dôležitá kvalita vysielacieho zariadenia, hlavne antény.

- V zásade sa dá povedať, že v posledných rokoch postupne klesá význam metalických prenosových médií a narastá význam optických médií.
- Rovnako bezdrôtové spojenia nadobúdajú na význame nielen pre distribuované vysielacie služby (rozhlas, televízia), ale aj preto, že je nimi možné riešiť mobilitu koncového zákazníka komunikačnej siete.

Tab. 4.1 Niektoré približné reálne parametre prenosových médií

Prenosové médium	Maximálna rýchlosť prenosu	Šírka pásma prenosu	Použitie
Krútený dvojpár	4 Mbit/s	250 kHz – 1000 MHz	budovy, vnútorná inštalácia, prístupové siete
Koaxiálny kábel	400 – 800 Mbit/s	350 MHz	budovy, vnútorná inštalácia, prístupové siete
Optické vlákno	20 Gbit/s	20 GHz	budovy, vnútorná inštalácia, prístupové siete, transportné siete
Rádiové smerové spoje	12 – 274 Mbit/s	2-40 GHz	prístupové siete
Rádiové všesmerové spoje	0,1 – 2 Mbit/s	16 kHz – 30 MHz	transportné siete

4.5 Prispôbenie signálu prenosovému médiu

Signál, ktorý je nosičom správy, môže byť prenášaný po prenosovom médiu v analógovom alebo digitálnom tvare. Podľa typu prenášaného signálu označujeme prenos:

- v základnom pásme a
- v preloženom pásme.

Pojem základné pásmo znamená, že frekvenčný rozsah prenášaného signálu nie je zmenený oproti signálu, v ktorom je zakódovaná správa. Pojem preložené pásmo vyjadruje zmenu frekvenčného rozsahu prenášaného signálu oproti signálu, v ktorom je zakódovaná správa. Príklad rozdielu uvedených pojmov je na obrázku 4.8.



Obr. 4.8 Prenos v základnom a preloženom pásme

Binárny digitálny signál, ktorý je vytvorený na výstupe zdroja informácií má nasledovné vlastnosti:

- Frekvenčné pásmo začína na frekvenciách blízkyh nule.
- Obsahuje jednosmernú zložku, ktorú nie je možné prenášať niektorými prenosovými zariadeniami.
- Nedá sa jednoducho obnoviť vzorkovací/taktovací signál potrebný pre synchronizáciu.

Pre uvedené vlastnosti nie je vhodný pre prenos v elektronickej komunikačnej sieti. Preto boli pre prenos cez komunikačné systémy štandardizované linkové kódy, prostredníctvom ktorých sa vytvárajú linkové signály, ktoré tieto negatívne vlastnosti binárneho digitálneho signálu odstraňujú. Linkové signály upravujú signál nesúci správu do tvaru vhodného pre prenos po komunikačných sieťach

Prenos v preloženom kmitočtovom pásme sa realizuje použitím vhodnej modulácie.

4.5.1.1 Pojem kódovanie

Kódovanie je všeobecne priradovanie prvkov množiny signálov $S = (S_0, S_1, \dots, S_n)$ prvkom množiny správ $Z = (Z_0, Z_1, \dots, Z_n)$. Kód predstavuje algoritmus alebo pravidlo, ktoré priraduje každému konkrétnemu prvku správy z množiny (Z) jediný prvok z postupnosti signálových prvkov z množiny (S). Možno povedať, že kódovaním je priradované každému prvku správy jedno kódové slovo daného kódu.

Kódovanie sa robí z dvoch dôvodov:

1. Správa sa kódovaním upravuje do tvaru, ktorý je potrebný pre ďalšie spracovanie, prípadne uloženie do pamäti. Toto kódovanie sa nazýva kódovanie na výstupe zdroja informácií alebo zdrojové kódovanie. Takýto typ kódovania je použitý na prezentačnej vrstve OSI modelu a jeho princípy budú vysvetľované ako súčasť prezentačnej vrstvy.

2. Správa sa upravuje do tvaru vhodného pre prenos po komunikačných sieťach. Tento typ kódovania je označovaný ako kódovanie na vstupe kanála alebo kanálové kódovanie.

V oboch prípadoch sa kódovaním rieši rovnaký problém, prenos informácie zo zdroja na miesto určenia. Rozdiel je v účele kódovania:

- Pri kódovaní na výstupe zdroja informácií je účelom zakódovať správu čo najúspornejšie.
- Pri kódovaní na vstupe do komunikačného kanála je účelom dosiahnuť čo najbezpečnejší prenos. Tento typ kódovania je uplatnený na fyzickej úrovni OSI modelu. Signál je po prenosovom médiu prenášaný v základnom pásme. Postupy kódovania sú označované ako linkové kódy a výstupom kódovania sú linkové signály.

4.5.1.2 Kódovanie na vstupe kanála - Linkové kódy/ linkové signály

Linkový signál vzniká prekódovaním pôvodného binárneho digitálneho signálu použitím linkového kódu. Účelom takéhoto kódovania je dosiahnuť čo najlepší prenos signálu.

Používané typy linkových signálov môžeme klasifikovať podľa troch hľadísk:

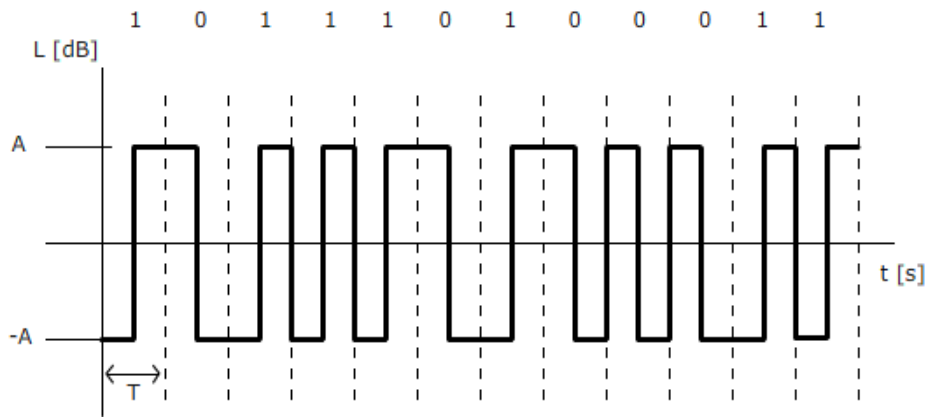
- Podľa použitej polohy signálových prvkov:
 - unipolárne linkové signály - signálové prvky len jednej polarity
 - polárne linkové signály - signálové prvky dvojakej polarity
 - bipolárne linkové signály – signálové prvky dvojakej polarity a aj nula
- Podľa toho, či sa signálový prvok vracia k nulovej úrovni alebo prechádza priamo k druhému charakteristickému stavu:
 - linkové signály s návratom k nule RZ (*Return to Zero*)
 - linkové signály bez návratu k nule NRZ (*Not Return to Zero*)
- Podľa počtu úrovní:
 - dvojúrovňové linkové signály
 - trojúrovňové linkové signály
 - bipolárne (pseudotrojkové), za jednu úroveň je považovaná 0,
 - trojkové majú tri rôzne úrovne
 - viacúrovňové linkové signály

4.5.1.3 Príklady rôznych druhov linkových kódov

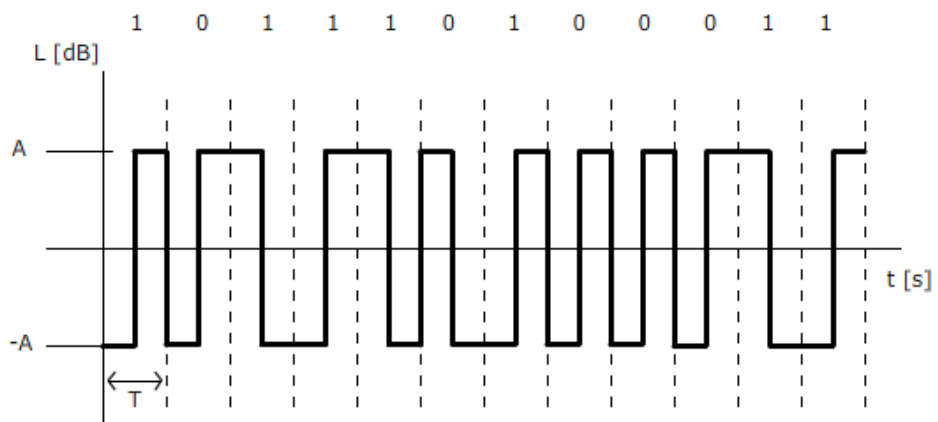
- Kód Manchester, obr. 4.8.
 - Je dvojúrovňový polárny kód bez návratu k nule.
 - Kódovanie symbolu 1:
 - $-A$ v prvej polovici dĺžky trvania signálového prvku T ,
 - $+A$ v druhej polovici dĺžky trvania signálového prvku T .
 - Kódovanie symbolu 0:
 - $+A$ v prvej polovici dĺžky trvania signálového prvku T ,
 - $-A$ v druhej polovici dĺžky trvania signálového prvku T .

- Používa sa v sieťach LAN na rozhraniach Ethernet 10BASE-T s rýchlosťou 10Mbit/s.
- Diferenčný variant kódu Manchester, obr. 4.11.
 - Je dvojúrovňový polárny kód bez návratu k nule.
 - Symbol 0 alebo 1 určuje charakter prechodu na začiatku signálového prvku. Ak nastáva na začiatku doby trvania signálového prvku zmena amplitúdy nasleduje symbol 0, ak sa amplitúda nemení nasleduje symbol 1.
 - Používa sa v sieťach typu Token Ring.
- Kód CMI (Coded Mark Inversion), obr. 4.12.
 - Je dvojúrovňový polárny kód s návratom k nule
 - Kódovanie symbolu 1 striedavo $-A$ alebo $+A$ počas celého intervalu signálového prvku.
 - Kódovanie symbolu 0:
 - $-A$ v prvej polovici dĺžky trvania signálového prvku T ,
 - $+A$ v druhej polovici dĺžky trvania signálového prvku T .
 - Používa sa pre rozhranie PHD č. rádu (E4) a v unipolárnom variante pre optické rozhrania.
- Kód AMI (Alternate Mark Inversion), obr. 4.13.
 - Je trojúrovňový bipolárny (pseudotrojkový) kód, s návratom k nule.
 - Symbolu 0 odpovedá nulová úroveň.
 - Symbolu 1 odpovedajú striedavo úrovne $\pm U$.
 - Striedaním polarity symbolov 1 je možné jednoducho monitorovať chybné prvky tým, že dôjde k narušeniu bipolarity.
- Kód HDB3 (High Density Bipolar), obr. 4.14
 - Je trojúrovňový bipolárny (pseudotrojkový) kód, s návratom k nule.
 - Je založený na AMI kóde.
 - Symbolu 1 odpovedajú striedavo úrovne $\pm U$.
 - Symbolu 0 odpovedá nulová úroveň. Prenášajú sa maximálne tri symboly 0 idúce za sebou. Postupnosť 4 a viac núl je nahradzovaná skupinou 000V alebo B00V.
 - Používa sa pre linkové systémy PCM30/32
 - Je štandardizovaný pre linková rozhrania E1, E2, E3 európskej plesiochronnej digitálnej hierarchie (PDH).
- Kód 2B1Q (Two Binary, One Quaternary), obr. 4.15
 - Je štvorúrovňový kód.
 - Dva bity (dibit) sú vyjadrené podľa danej tabuľky jednou zo štyroch napätových úrovní (quad).

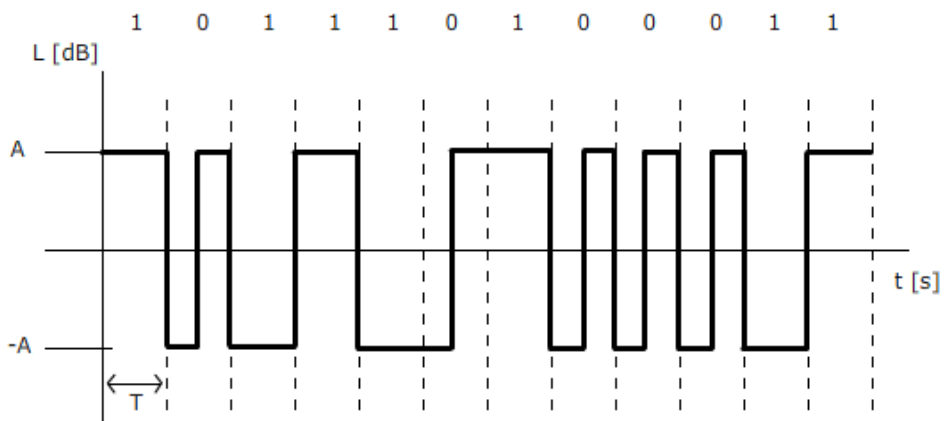
Binárna hodnota	Odpovedajúca úroveň napätí
0 0	-3 V
0 1	-1 V
1 0	+3 V
1 1	+1 V



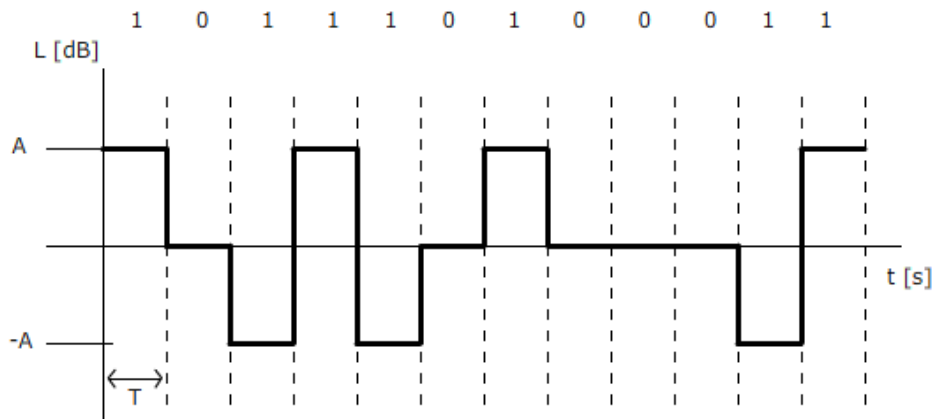
Obr. 4.10 Manchester



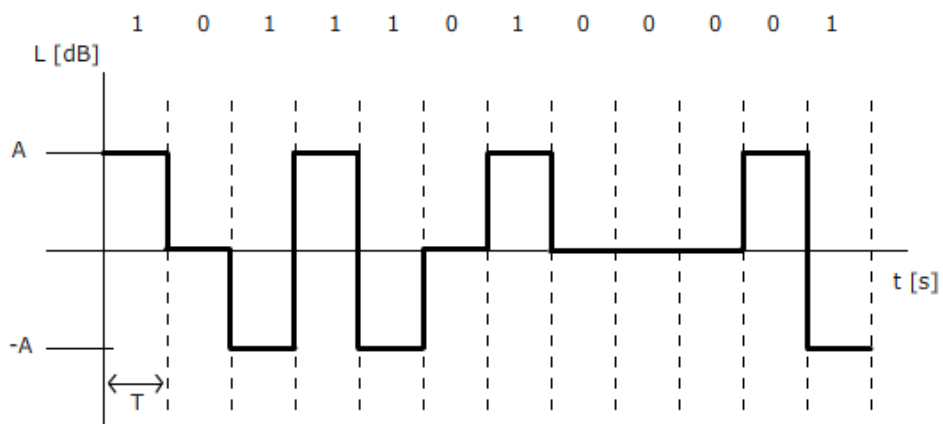
Obr. 4.11 Diferenčný Manchester



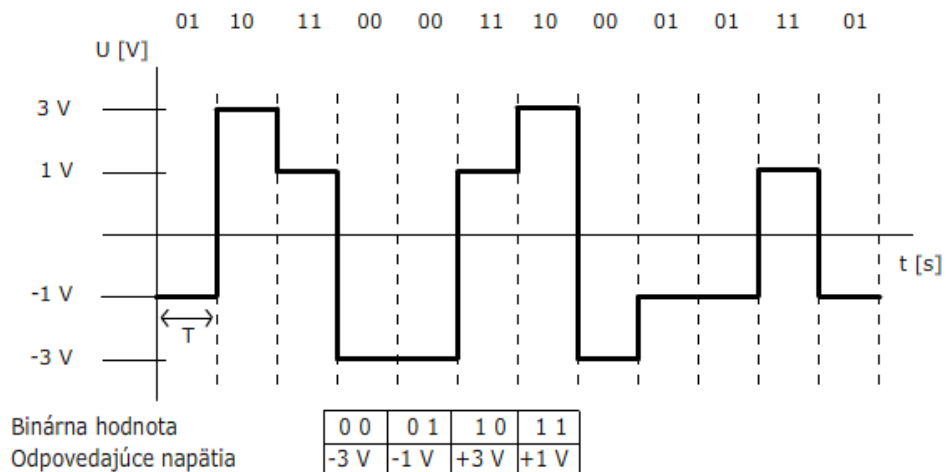
Obr. 4.12 CMI



Obr. 4.13 AMI



Obr. 4.14 HDB 3

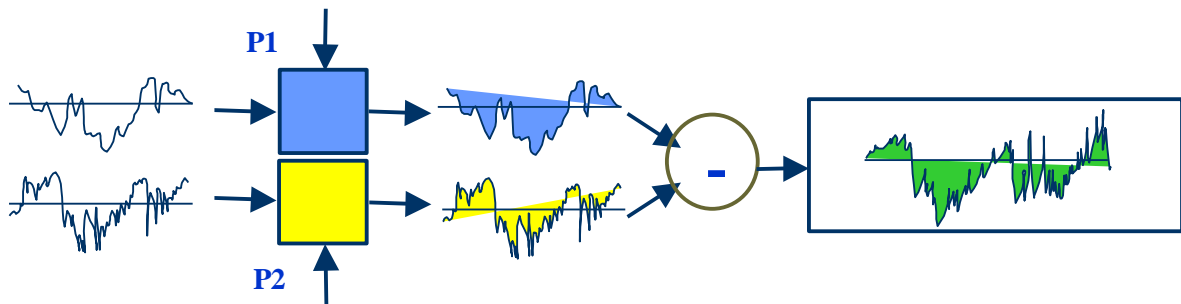


Obr. 4.15 B1Q

4.6 Modulácie

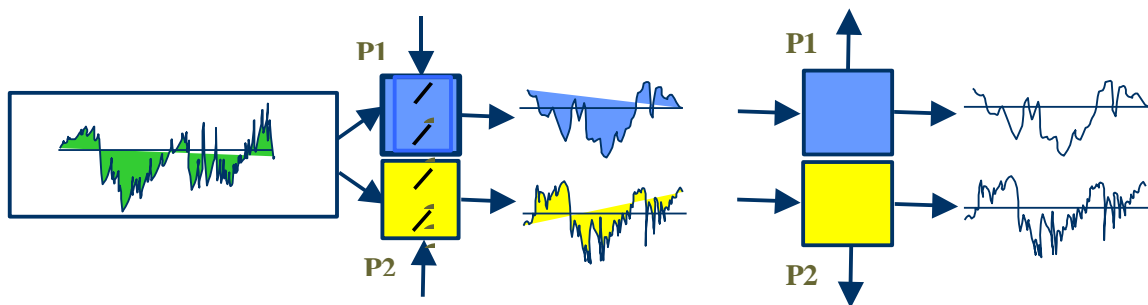
Moduláciou nazývame zmenu vyjadrenia signálu, vytváranú kvôli rôznym účelom prenosu signálu. Princípom modulácie je vytvorenie zmeny na vstupe prenosového kanála tým, že signálu priradíme určitý príznak. Pokiaľ by sme nepoznali parametre signálu, mohli

by sme si moduláciu priblížiť ako zafarbenie každého zo signálov a vytvorenie jednej farby, ktorá sa dosiahne ich zmiešaním. Dva rôzne signály sa tak prenášajú ako jeden signál. Znáznornenie princípu modulácie je na obrázku 4.16.



Obr. 4.16 Principiálne vyjadrenie modulácie

Na prijímacej strane je postup opačný. Oddelí sa priradený príznak a vytvoria sa dva pôvodné signály, nesúce informáciu. Postup získavania pôvodných signálov na prijímacej strane sa nazýva demodulácia. Principiálne znázornenie demodulácie je na obr. 4.17.



Obr.4.17 Principiálne vyjadrenie demodulácie

Prakticky je priradovanie príznaku realizované tak, že sa uskutočňuje zmena niektorého parametra signálu prostredníctvom iného signálu. Rozlišujeme preto dva druhy signálov:

- Modulačný signál - signál, ktorý vyvoláva zmenu.
- Nosný (modulovaný) signál - signál, na ktorom je vyvolaná zmena.

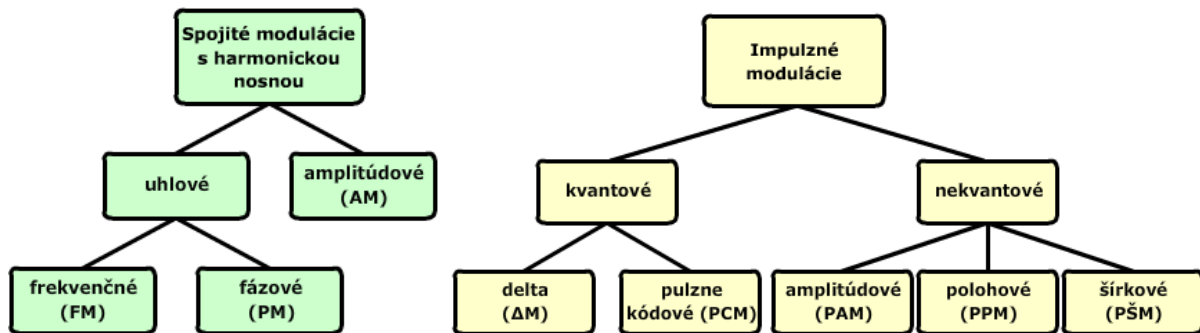
Podľa typu nosného a modulačného signálu sa rozlišujú rôzne typy modulácií.

4.6.1 Typy modulácií

Typy modulácií závisia od typu signálu, ktorý vyvoláva zmenu a od typu signálu, u ktorého je zmena vyvolávaná. Základné rozdelenie je na modulácie spojité a modulácie impulzné:

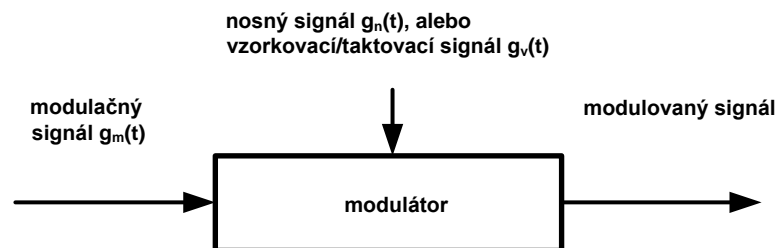
- Spojité (analogové) modulácie:
 - modulačný signál je analógový alebo digitálny,
 - nosný signál (nosná vlna), je harmonický signál.
- Impulzné modulácie:
 - modulačný signál je analógový alebo digitálny,
 - nosný signál (vzorkovací/taktovací signál) je digitálny.

V každom zo základných typov modulácie sa dajú vytvárať ďalšie typy modulácie podľa toho, ktorý parameter nosného signálu je ovplyvňovaný. Dostávame tak mnoho rôznych typov, ktorých názvy sú znázornené na obr. 4.18.



Obr. 4.18 Typy modulácií

Modulácia signálu sa robí v zariadení nazývanom modulátor. Všeobecné schematické znázornenie postupu modulácie je na obr. 4.19. Rozdiel je len v signáli, na ktorom je vyvolávaná zmena. V praktickom prevedení sú modulátory odlišné pre každý typ modulácie.



Obr. 4.19 Schematické znázornenie modulácie

4.6.2 Analógové modulácie

Podľa toho, aká veličina harmonického signálu je ovplyvňovaná, delíme ich na:

- amplitúdovú moduláciu AM,
- frekvenčnú moduláciu FM,
- fázovú moduláciu PM.

4.6.2.1 Amplitúdová modulácia AM

Pri amplitúdovej modulácii ovplyvňujeme v modulátore **modulačným signálom** $g_m(t)$ amplitúdu **nosného harmonického signálu** $g_n(t)$. Nosný - harmonický signál $g_n(t)$, je charakterizovaný amplitúdou A_n a frekvenciou Ω . Jeho časový priebeh je daný vzťahom

$$g_n(t) = A_n \cdot \sin(\Omega \cdot t)$$

Pre jednoduchosť vysvetlenia budeme uvažovať ako modulačný signál tiež harmonický signál $g_m(t)$, s amplitúdou A_m a frekvenciou ω

$$g_m(t) = A_m \cdot \sin(\omega \cdot t)$$

Amplitúdovo analógovo modulovať znamená priradiť nosnému signálu príznak do amplitúdy modulačného signálu. Zmena amplitúdy nosného signálu je tak závislá od modulačného signálu, v ktorom je vyjadrená prenášaná informácia.

Okamžitá amplitúda nosného signálu sa určí pričítaním prenášaného (modulačného) signálu k amplitúde nosnej vlny A_n :

$$A_n + g_m(t) = A_n + A_m \cdot \sin(\omega \cdot t)$$

$$m = \frac{A_m}{A_n}$$

Pre zjednodušenie určíme pomer amplitúd oboch signálov ako m a dostávame upravený vzťah amplitúdy nosného signálu:

$$A_n + g_m(t) = A_n (1 + m \cdot \sin(\omega \cdot t))$$

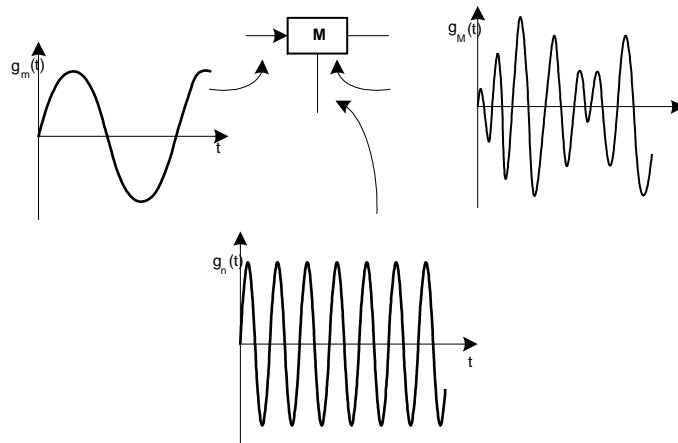
Nosný signál tak nadobúda nový tvar:

$$g_n(t) = A_n [1 + m \cdot \sin(\omega \cdot t)] \cdot \sin(\Omega \cdot t)$$

Úpravou rovnice a použitím vzorca pre súčin goniometrických funkcií ($\sin \alpha \cdot \sin \beta$) dostávame tvar modulovaného signálu:

$$g_M(t) = A_n [\sin \Omega \cdot t + m/2 \cdot \cos(\Omega - \omega)t - m/2 \cdot \cos(\Omega + \omega)t]$$

Proces amplitúdovej modulácie je ilustrovaný na obr. 4.20.

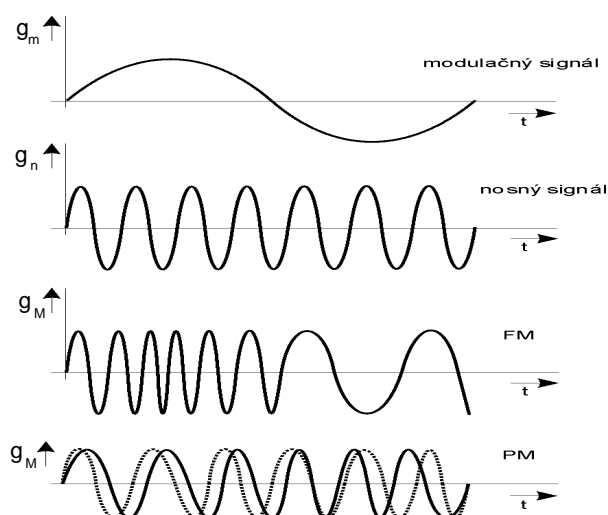


Obr. 4.20 Proces amplitúdovej modulácie

4.6.2.2 Frekvenčná a fázová modulácia, FM, PM

Pri frekvenčnej modulácii je okamžitá hodnota frekvencie nosného signálu f_N úmerná okamžitej hodnote amplitúdy modulačného signálu A_m .

Pri fázovej modulácii je ovplyvňovaná fáza φ_N okamžitou hodnotou modulačného signálu A_m . Matematické vyjadrenie fázovej a frekvenčnej modulácie je zložitejšie ako pri amplitúdovej modulácii. Pre porozumenie princípu posluži grafické znázornenie priebehu frekvenčnej a fázovej modulácie znázornené na obr. 4.21.



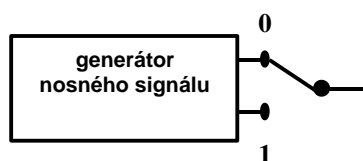
Obr. 4.21 Princíp frekvenčnej a fázovej modulácie

4.6.2.3 Analógové modulácie s digitálnym modulačným signálom

Analógová modulácia, kde modulačným signálom je digitálny signál sa tiež delí na tri základné typy, podľa toho, aká veličina nosného harmonického signálu je ovplyvňovaná. Rovnako ako v predošlých prípadoch sa označujú :

- amplitúdová modulácia,
- frekvenčná modulácia,
- fázová modulácia.

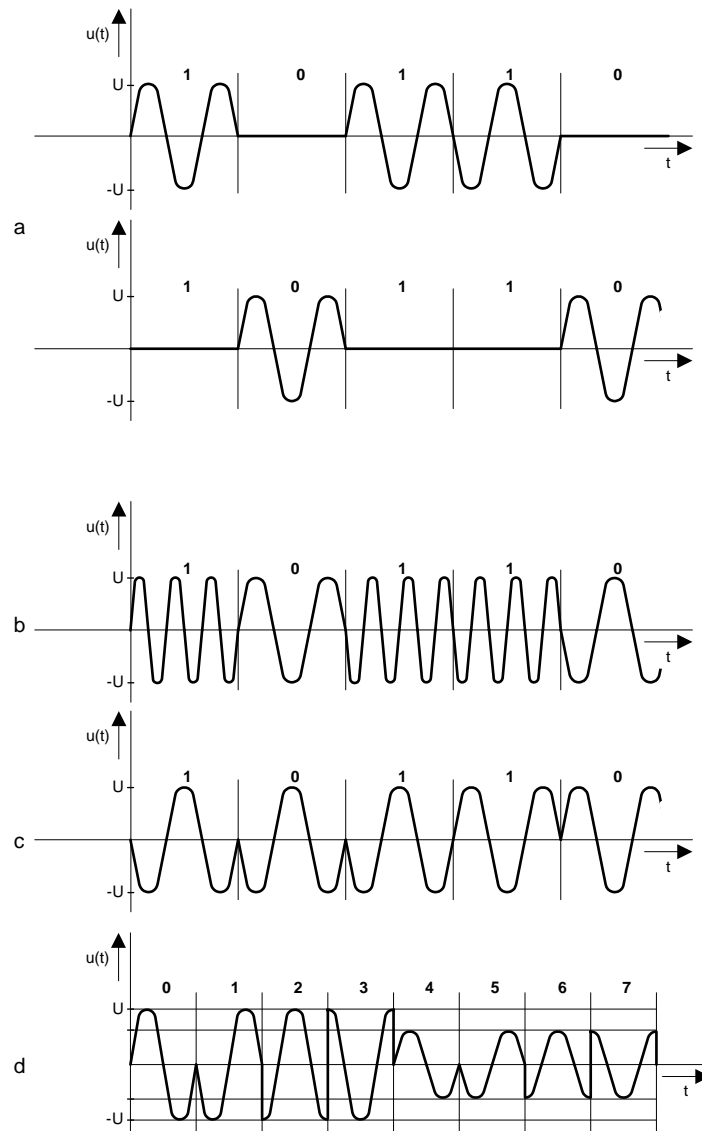
Princíp realizácie je však odlišný. Pri týchto typoch modulácie sa v podstate kľúčuje (prepína) nosný harmonický signál podľa hodnoty digitálneho signálu. Výsledný signál sa označuje ako číslicový signál v preloženom pásme. V niektorých prípadoch sa používa ako nosný signál jednosmerný prúd a vytvárajú sa tzv. číslicové signály v základnom pásme. Princíp kľúčovania (prepínania) je znázornený na obr. 4.22.



Obr. 4.22 Princíp kľúčovania

Príklady modulovaných signálov sú znázornené na obr. 4.23. Obr. 4.23.a znázorňuje amplitúdovo modulovaný signál, obr. 4.23.b frekvenčne modulovaný signál. Fázová modulácia sa označuje skratkou PSK (*Phase Shift Key*). Veľmi často sa používa princíp fázovej modulácie uvedený na obr. 4.23.c. Fáza každého nasledujúceho prvku sa určuje vo vzťahu k predchádzajúcemu prvku. Pre nasledujúci binárny stav sa fáza nemení, keď je tento stav opačný ako predchádzajúci, a mení sa vtedy, keď je stav rovnaký ako predchádzajúci. Taká modulácia sa nazýva fázová rozdielová (diferenčná) modulácia DPSK (*Different Phase Shift Key*). DPSK modulácia sa často kombinuje s amplitúdovou moduláciou do modulácie,

ktorá sa nazýva kvadratická amplitúdová modulácia QAM (*Quadrature Amplitude Modulation*). Je to viacstavová modulácia a jej znázornenie je na obr. 4.23.d.



Obr. 4.23. Princípy analógových modulácií s digitálnym modulačným signálom

Z princípov QAM vychádzajú ďalšie typy modulácií. Napríklad fázovo amplitúdová modulácia CAP (*Carrierless Amplitude/Phase Modulation*) s potlačenou nosnou, modulácia DMT (*Discrete Multitone Modulation*), kde sa pásmo delí do subkanálov, ktoré sú samostatne modulované QAM.

4.7 Impulzné modulácie

Impulzné modulácie namiesto nosného harmonického signálu používajú časovú postupnosť impulzov. Zo signálu sa odoberajú vzorky amplitúdy signálu v určitom čase. Tento postup sa nazýva vzorkovanie signálu. Vzdialenosť impulzov je daná vzťahom:

$$\Delta t \leq \frac{1}{2f_m}$$

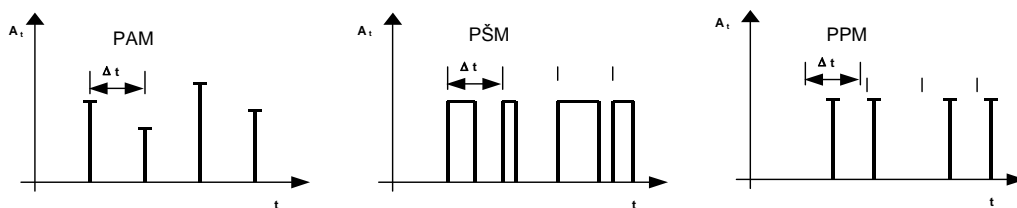
kde f_m je najvyššia frekvencia vzorkovaného signálu $g_v(t)$. Tento vzťah je známy ako Shannon-Kotelnikov teorém. Frekvencia $2f_m = f_v$ sa nazýva vzorkovacia frekvencia, alebo Nyquistova frekvencia. Hodnota vzorkovacej frekvencie je nutnou podmienkou pre vytvorenie pôvodného signálu na prijímacej strane po demodulácii.

4.7.1.1 Nekvantované impulzné modulácie

Nekvantované impulzné modulácie majú nosnú časovú postupnosť impulzov charakterizovanú buď veľkosťou amplitúdy impulzov, šírkou impulzov, alebo polohou impulzov na časovej osi oproti pevne určeným charakteristickým okamihom. V závislosti od toho, ktorý z týchto parametrov je ovplyvňovaný modulačným signálom, rozlišujeme:

- impulznú amplitúdovú moduláciu PAM
- impulznú šírkovú moduláciu PŠM
- impulznú polohovú moduláciu PPM.

Priebehy signálov týchto modulácií sú na obr. 4.24.



Obr.4.24. Impulzné nekvantované modulácie

Týmto spôsobom je možné analógový signál vyjadriť ako postupnosť vzoriek signálu a premeniť ho na nespojitý diskretný signál. Amplitúda každej vzorky môže nadobúdať nekonečné množstvo hodnôt. Rušivé napätie pri takto modulovaných signáloch spôsobujú skreslenie podobne ako pri analógových moduláciách. Preto sa v praxi nepoužívajú.

4.7.1.2 Kvantované impulzné modulácie

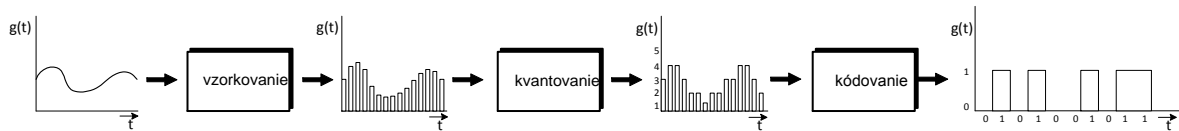
Pulzne kódová modulácia PCM

Postup modulácie sa dá popísať tromi krokmi:

- Signál sa ovzorkuje v intervaloch vzorkovacej frekvencie f_v , ktorá je dvojnásobkom maximálnej prenášanej frekvencie. Pre prenos hlasu je $f_v = 8$ kHz, pretože frekvenčný rozsah je od 0,3 do 3,4 kHz, čo je zaokrúhlené 4 kHz. Pri zázname na CD je to 44,1 kHz lebo zdravé ľudské ucho počuje maximálne cca do 20 kHz a tak vzorkovacia frekvencia 44,1 kHz bola zvolená s veľkou rezervou.
- Okamžitým hodnotám vzoriek signálu sa priradí diskretná hodnota úrovne podľa toho, do akej kvantovej úrovne vzorka spadá. Počet kvantovacích úrovní je vytvorený podľa požadovanej presnosti prijímaného signálu. Pre hlas je to $2^8 = 256$ kvantovacích úrovní, pre hudbu $2^{16} = 65536$ kvantovacích úrovní.

- Každý kvantovacej úrovni je priradený binárny kód. Každý vzorke je tak priradené binárne kódové slovo, dané týmto kódom.
- Jednotlivé kódové slová sú prenášané prenosovým kanálom k prijímaču správy. V ňom sa vzorky demodulujú na pôvodný signál.

Príklad postupu pri PCM je na obr. 4.25.



Obr. 4.25 Princíp PCM

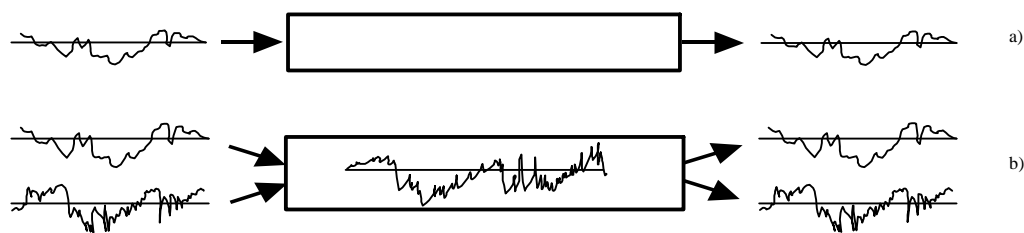
4.7.2 Použitie modulácií

Modulácie sú používané na rôzne účely:

1. Na lepšie využitie prenosového kanála, vytváranie multiplexu (analogová modulácie a PCM).
2. Keď je potreba posunúť signál do iného frekvenčného pásma, kde je možné napríklad znížiť straty pri prenose (FM, AM).
3. Možnosť súčasného vysielania rôznych kanálov, napríklad pri rozhlasových vysielaniach (AM, FM).
4. Zmena analogového signálu na digitálny (PCM).
5. Pre prenos dát (analogové modulácie s digitálnym modulačným signálom).

4.8 Viacnásobný prenos signálu

Prenosové médiá obvykle umožňujú prenos väčšieho množstva informácií než iba informáciu jedného kanála, ako je znázornené na obr. 4.26.a. Umožňuje to dostatočná šírka pásma, ktorá je napríklad v metalickom vedení 250 kHz, v koaxiálnom kanáli 350 - 500 MHz, u optického vlákna 20 GHz. Telefónny kanál potrebuje na prenos len 3,1 kHz, preto je možné združovať viac kanálov pochádzajúcich z rozličných zdrojov a určených rôznym príjemcom tak, aby bolo možné využívať celú kapacitu prenosového média. Prenosové médium tak prenáša súčasne viac komunikačných kanálov. V takýchto prípadoch hovoríme o viacnásobnom využívaní prenosového média, resp. o jeho používaní viacerými kanálmi, ako je znázornené na obr. 4.26.b. Viacnásobné využitie prenosového média dosiahneme princípom nazývaným multiplexovanie signálu, v angličtine *multiplexing*, ktorý umožňuje rozdeliť jeden prenosový kanál s veľkou šírkou pásma na niekoľko užších logických subkanálov/podkanálov, ktoré sa javia ako samostatné, od seba nezávislé prenosové kanály. Multiplexovanie má i ekonomické dôvody, hlavne v diaľkových prenosoch, kde je hlavne ich pokladanie finančne veľmi náročné. Rovnako najlepšie ekonomické zhodnotenie prenosových ciest sa dosiahne ich viacnásobným využívaním.



Obr. 4.26 Všeobecný princíp viacnásobného využitia prenosového média

V historickom vývoji viacnásobného využívania prenosových ciest sa postupne objavovali rôzne princípy a niektoré z nich sú dnes už málo využívané. V zásade môžeme multiplexovanie realizovať nasledujúcimi princípmi:

1. Priestorový multiplex – SDM (*Space Division Multiplex*), kde jednotlivé kanály sú oddelené fyzicky, čo znamená, že informácie jednotlivých kanálov sú prenášané na separátnych prenosových médiách, ktoré tvoria zväzok. Tento princíp bol v minulosti používaný napríklad pri nízkofrekvenčných prenosových systémoch na prenos telefónneho signálu.
2. Príznakový multiplex, kde sa signálom vtačí určitý príznak, ktorý mení niektorý z parametrov signálu. Príznakové multiplexy môžu byť rôzne, najznámejšie sú:
 - a. frekvenčný - FDM (*Frequency Division Multiplex*),
 - b. časový – TDM (*Time Division Multiplex*),
 - c. vlnový – WDM (*Wavelength Division Multiplex*),
 - d. kódový – CDM (*Code Division Multiplex*).

Prehľad systémov a typy príznakových multiplexov sú v tabuľke 4.2. Skratky systémov aj typy príznakov budú postupne vysvetľované v ďalších kapitolách.

Prehľad systémov a používaných typov príznakových multiplexov Tab. 4.2.

Typ príznaku	Systém	Príznak
Fyzikálny	FDM, WDM	frekvencia
	TDM	časová poloha
	GSM	FDM+TDM
Kombinovaný	SDH	číslo + TDM
	IPoWDM	adresa + frekvencia
Blokový	IP	adresa
	ATM	číslo VPI+VCI
	Konvolučný	CDMA

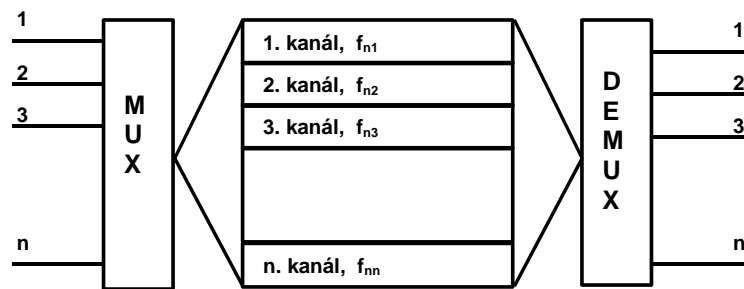
4.8.1 Frekvenčný multiplex, FDM (*Frequency Division Multiplex*)

FDM využíva skutočnosť, že je k dispozícii širšie frekvenčné pásmo prenosového média, než je frekvenčné spektrum prenášaného signálu. Základným princípom FDM je rozdelenie využiteľného frekvenčného pásma prenosového média na veľký počet kanálov, ktoré sa nazývajú subkanály. Tento postup umožňuje vytvárať kmitočtové delenie priepustného pásma

prenosového média. Prakticky sa tieto subkanály vytvárajú pomocou modulácie, kde sú signály jednotlivých informačných kanálov modulované na jednotlivé nosné frekvencie rozdeleného frekvenčného pásma. Ak modulujeme informačný signál na nosný signál harmonického tvaru, hovoríme o modulácii v kmitočtovej oblasti.

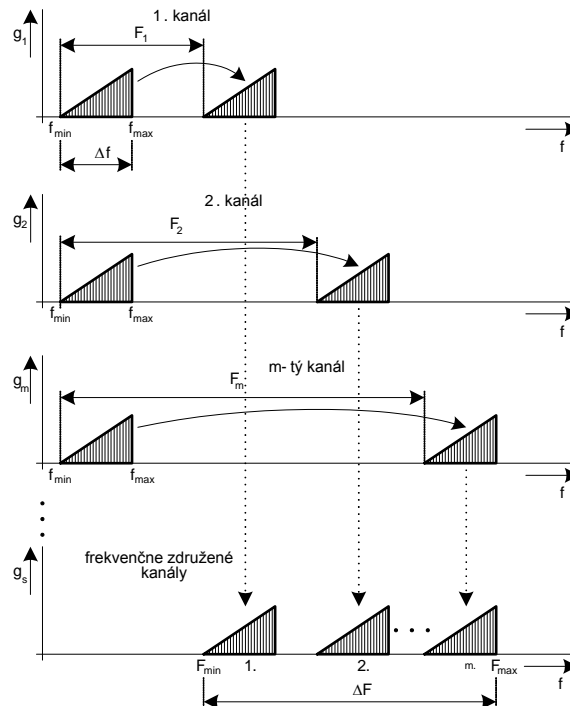
Každý kanál zaberá určitú šírku pásma v okolí jemu prislúchajúcej nosnej frekvencie. Aby bolo možné signály z jednotlivých subkanálov spoľahlivo oddeliť, vynechávajú sa medzi nimi tzv. ochranné pásma.

Technické zariadenie, ktoré zaisťuje takéto logické rozdelenie na niekoľko subkanálov, sa nazýva multiplexor - MUX. Zariadenie na prijímacej strane, ktoré opäť rozdeľuje združený signál do jednotlivých kanálov, sa nazýva demultiplexor - DEMUX. Princíp frekvenčného multiplexu je znázornený na obr. 4.27.



Obr. 4.27 Princíp frekvenčného multiplexu

Tu si možno predstaviť, že jednotlivé subkanály sú "navršené na sebe" v prenosovom pásme prenosového kanála, a každému z nich je pridelená taká časť celkovej šírky pásma, akú potrebuje, obr. 4.28.



Obr. 4.28 Pridelovanie frekvencií v FDM

Signál prenášaný v rámci určitého subkanálu, musí multiplexor najprv frekvenčne "posunúť" do časti pásma, prideleného danému subkanálu a na druhej strane spoja ho zase "vrátiť späť" do pôvodnej frekvenčnej polohy. Celý mechanizmus je pritom plne transparentný, to znamená, že používatelia jednotlivých kanálov majú dojem, že majú k dispozícii samostatné, od seba nezávislé prenosové kanály. Uvedený postup je analogický s obsadzovaním rádiového priestoru vysielača. Každý kanál má priradený svoj nosný kmitočet a využíva voľný priestor na šírenie elektromagnetickej vlny. Aj pri telefónnych prenosoch je postup rovnaký a pre systémy s frekvenčným delením sa používa termín nosné telefónne systémy. Rozdiel spočíva v tom, že v tomto prípade je signál prenášaný vedením, kde môžu byť použité rovnaké nosné frekvencie bez podstatného vzájomného rušenia. Nie je tu limit obmedzeného počtu nosných frekvencií ako pri rádiovom prenose a na všetky káble je možno nasadzovať štandardizované systémy so zhodným kmitočtovým rastrom.

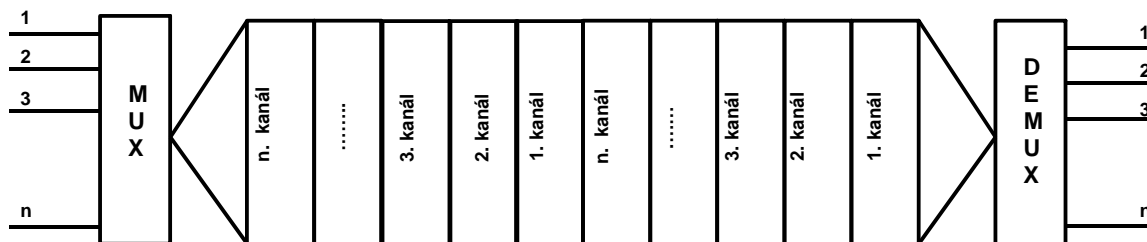
4.8.2 Časový multiplex, TDM (Time Division Multiplex)

Podobne ako pri systéme FDM, kde vychádzame z predpokladu šírky pásma prenosového média a prenášaného signálu, pri TDM vychádzame z predpokladu, že prenosová rýchlosť na danom prenosovom médiu je vyššia ako prenosová rýchlosť signálu, ktorý prenášame. Pretože medzi prenosovou rýchlosťou a šírkou pásma existuje závislosť, používa sa niekedy termín šírka pásma i vtedy, keď ide o prenosovú rýchlosť.

Delenie jedného prenosového kanála na viac subkanálov je vytvárané časovým delením. Časové delenie vytvára periodicky sa opakujúce okná na časovej osi. Tým sú po jednom prenosovom médiu prenášané súčasne vzorky n signálov a každý signál má vyhradené jedno okno na časovej osi. Postupnosť časových okien vyhradených jednému zdroju potom nazývame kanálom. Skupinu, obsahujúcu práve po jednom kanáli z každého okna, nazývame rámcom.

Časové okná aj ich poradie zostávajú pre dané spojenie pevné, bez ohľadu na to, či sa signál prenáša alebo nie. Toto umožňuje identifikovať poradové číslo kanála na prijímacej strane podľa jeho polohy na časovej osi.

Vlastný prenosový kanál je pravidelne pridelovaný s celou svojou šírkou pásma na krátke časové intervaly jednotlivým subkanálom. Najľahšie sa táto predstava ilustruje na príklade kanála, ktorý prenáša priamo číslicové dáta. Multiplexor najskôr "vyberie" napríklad po jednom bite od každého subkanálu, a zo všetkých týchto bitov zostaví viacbitový znak, ktorý prenesie kanálom. Na opačnej strane kanála potom demultiplexor rozdelí prijatý znak na jednotlivé bity a tie odovzdá príslušným subkanálom, obr. 4.29.

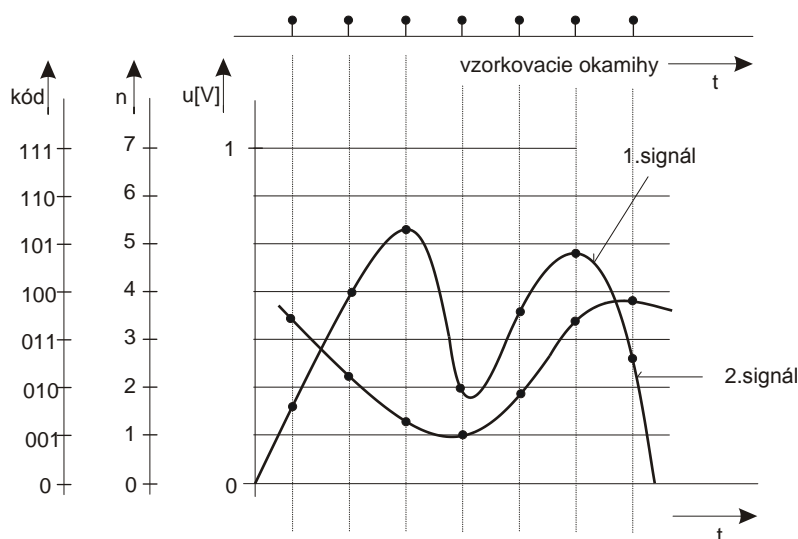


Obr. 4.29 Princíp časového multiplexu

Systém, ktorý vytvára časové okná, nazývame synchronným časovým multiplexom, alebo iba časovým multiplexom.

Pri časovom i frekvenčnom multiplexe samozrejme musí platiť, že súčet šírky pásma jednotlivých subkanálov musí byť menší než celková šírka pásma existujúceho prenosového kanála. Časový multiplex je všeobecne účinnejší v tom zmysle, že súčet šírky pásma subkanálov môže byť "bližšie" k teoretickej hornej hranici, teda celkovej šírke pásma existujúceho kanála.

Principiálne môžeme TDM vytvoriť na báze multiplexovania bitu alebo väčších celkov. Signály, ktoré sa multiplexujú môžu pochádzať z analógových alebo digitálnych zdrojov. Analógové signály pred multiplexovaním musíme premeniť na digitálne postupom pulznej kódovej modulácie - PCM, obr. 4. 30.



Obr. 4.30 Spracovanie signálov v PCM

4.8.3 Štatistický multiplex, STM (Statistical Time Division Multiplex)

Štatistický multiplex na rozdiel od TDM umožňuje dynamicky pridelovať kapacitu prenosového média len tým zdrojom, ktoré to práve potrebujú, to znamená sú aktívne. Štatistický multiplex nekladie obmedzenia na počet vstupných kanálov. Jediným obmedzením je to, aby súčet požadovaných časových okien v rámci neprekročil celkový počet okien, ktoré sú k dispozícii, ako je znázornené na obr. 4.31.



Obr. 4.31 Štatistický multiplex

Dynamické pridelovanie okien má výhodu v tom, že môžeme úplne využiť kapacitu prenosového média, pretože do rámca sa umiestňujú len tie okná, ktoré obsahujú dáta, to znamená prenášajú informácie z aktívneho zdroja. Nevýhodou je to, že nie je možné identifikovať jednotlivé kanály podľa ich polohy v rámci. Preto musí byť každá jednotka doplnená adresou, ktorá ju jednoznačne priraduje k príslušnému kanálu.

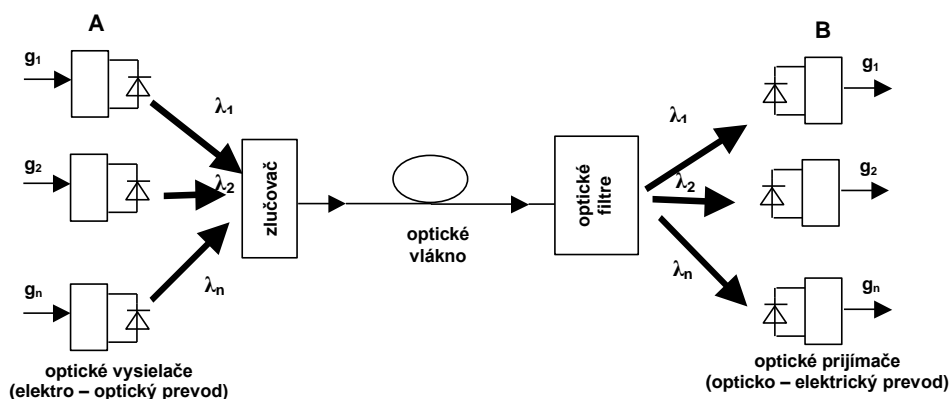
Prednosti štatistického multiplexu sa výrazne prejavajú predovšetkým vtedy, keď multiplexujeme signály zo zdrojov, ktoré vysielajú s rôznou prenosovou rýchlosťou. Takýmto zdrojom je napríklad videosignál vytvorený komprimovaním. V situácii, kedy kamera sníma statickú scénu, máme videosignál s malou prenosovou rýchlosťou. Keď dôjde k rýchlej zmene charakteru snímaného obrazu, zvýši sa prenosová rýchlosť skokom niekoľkonásobne.

Situácia, kedy prevládajú signály s premenlivou prenosovou rýchlosťou, je charakteristická pre širokopásmové siete, ktoré prenášajú hovorové, dátové i obrazové signály.

4.8.4 Vlnový multiplex, WDM (Wavelength Division Multiplex)

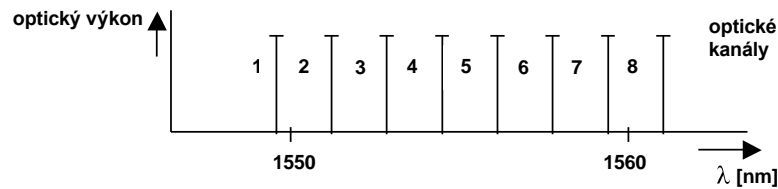
Vlnový multiplex, WDM je založený na prenose optického signálu rôznych vlnových dĺžok po jednom optickom vlákne. Každá vlnová dĺžka nesie namodulovaný jeden signál. Princíp vlnového multiplexu je znázornený na obr.4.32.

Signál z n optických vysieláčov v zariadení A (laserových diód) pracujúcich na vlnových dĺžkach λ_1 až λ_n je naviazaný do vlákna, prenesený k zariadeniu B, kde sa pomocou optických filtrov rozdelí opäť na n jednotlivých optických signálov, ktoré sa zmenia na elektrický signál. Týmto prenesieme n nezávislých elektrických signálov jediným vláknom. Pre opačný smer prenosu je potrebné druhé optické vlákno s rovnakými obvody. Dvojvláknový okruh zodpovedá 4-drôtovému metalickému vedeniu.



Obr. 4.32 Princíp vlnového multiplexu

Princíp WDM je analógiou FDM, kde sú signály jednotlivých kanálov modulované na jednotlivé nosné frekvencie a po vedení sa šíri elektromagnetická vlna s vlnovou dĺžkou rádovo desiatky metrov až jednotky km, ktoré zodpovedajú frekvencii 10 MHz až 100 kHz. Pri vlnovom multiplexe má nosná frekvencia dĺžku vlny okolo 1 μm . Znárodnenie jednotlivých kanálov v celkovom spektre optického signálu znázorňuje obr. 4.33.



Obr. 4.33 Rozloženie vlnových dĺžok u WDM

Na obrázku sú zobrazené vlnové dĺžky v okolí 1550 nm pre 8 elektrických kanálov. Iné systémy pracujú s prenosom na 16-tich vlnových dĺžkach a na 32 vlnových dĺžkach. V praxi sa optickým vláknom neprenášajú jednotlivé kanály, ale pracuje sa už s dopredu digitálne multiplexovanými signálmi vytvorenými pomocou TDM. Je to preto, aby sa maximálne využilo optické vlákno. Hovoríme o kombinácii TDM + WDM. Systémy WDM rozširujú možnosti multiplexovania tam, kde čisté TDM nestačí.

Odporúčanie ITU-T G.692 udáva ako množinu prípustných nosných frekvencií celočíselné násobky 100 GHz od 192,1 THz do 196,1 THz vrátane, čo je celkom 41 rôznych vlnových dĺžok od 1528,77 nm do 1560,61 nm, vzdialených od seba približne 0,8 nm. Takýto multiplex sa nazýva hustý vlnový multiplex DWDM. Dosahované prenosové rýchlosti idú rádovo od 140 Mbit/s až po 10 Gbit/s. Dnešné optické prenosové systémy zvládajú prekonať bez zosilnenia vzdialenosť viac než 100 km. Pre dlhšie trasy je potrebné signál priebežne zosilňovať, prípadne obnovovať jeho tvar.

4.9 Záver

Zabezpečenie prenosu signálu od zdroja ku cieľu po fyzickej vrstve je úloha prenosových médií. Každý relácii poskytnú komunikačný kanál, v ktorom je informácia prenášaná ako elektromagnetický signál. Prenosové médiá sú schopné poskytnúť súčasne viac kanálov. Jeden kanál obvykle prenáša jeden signál, ktorý nesie informáciu z jedného zdroja. Celková kapacita prenosu u prenosových médií sa tak rozdeľuje do menších častí.

Signál sa po kanáli neprenáša v tvare, do ktorého je správa zakódovaná ale pred prenosom sa upravuje. Úpravy signálu znamenajú jeho premenu na iný typ signálu (linkové kódy/signály) alebo premena postupom označovaným modulácia. Po týchto úpravách sa signály jednotlivých kanálov pomocou multiplexovania spoja do výslednej skupiny kanálov, ktorá sa potom prenáša po prenosových médiách. Multiplexovanie používa rôzne techniky v závislosti od použitej technológie. Systémy, ktoré realizujú viacnásobný prenos sa označujú prenosové systémy.

Kľúčové slová

- *Dynamický rozsah prenosového kanála*
- *Šírka pásma prenosového kanála*
- *Priepustnosť prenosového kanála*
- *Odstup signál šum*
- *Maximálna prenosová rýchlosť*
- *Nyquistovo kritérium*
- *Skutočná dosiahnuteľná prenosová rýchlosť*
- *Prenosové médiu*
- *Tlmenie prenosového média*
- *Fázový posuv v prenosovom médiu*
- *Presluchy v prenosovom médiu*
- *Kvalita prenosovej cesty*
- *Drôtový a bezdrôtový prenos*
- *Metalické prenosové médiá*
- *Krútená dvojlinka*
- *Koaxiálny kábel*
- *Optické prenosové médiá*
- *Smerové rádiové spoje*
- *Všesmerové rádiové spoje*

- *Satelitné rádiové spoje*
- *Prispôsobenie signálu prenosovému médiu*
- *Linkové kódy/signály*
- *Modulácie*
- *Modulačný signál*
- *Nosný signál*
- *Analógové modulácie*
- *Amplitúdová modulácia*
- *Frekvenčná a fázová modulácia*
- *Analógové modulácie s digitálnym modulačným signálom*
- *Impulzné modulácie*
- *Shannon-Kotelnikov teorém*
- *Pulzne kódová modulácia*
- *Vzorkovacia frekvencia*
- *Kvantovania úroveň*
- *Kódovanie*
- *Viacnásobný prenos signálu*
- *Frekvenčný multiplex*
- *Časový multiplex*
- *Štatistický multiplex*
- *Vlnový multiplex*
- *Prenosové systémy*

Kontrolné otázky

1. Čo označuje parameter dynamický rozsah kanálu D_k ?
2. Podľa akých veličín sa hodnotí priepustnosť prenosového kanála P_k ?
3. Aký je pomer signál/šum v prenosovom kanáli, ak parameter SNR je 3 dB?
4. Aký je vzťah medzi šírkou pásma prenášaného signálu a šírkou pásma prenosového kanála?
5. Ako je vyjadrená závislosť medzi modulačnou rýchlosťou a šírkou pásma?
6. Aký je vzťah medzi modulačnou rýchlosťou a šírkou pásma?
7. Ktoré z výrazov je označované ako Nyquistovo kritérium?
8. Aký je vzťah medzi šírkou frekvenčného spektra a prenosovou rýchlosťou?
9. Ktoré z vyjadrených vzťahov platí pre prenosovú rýchlosť a prečo?
10. O čoho teoreticky závisí maximálna dosiahnuteľná prenosová rýchlosť?
11. Aký je približný vzťah medzi šírkou pásma v Hz a prenosovou rýchlosťou v bit/s.
12. Na základe akých zmien je možné teoreticky zvyšovať prenosovú rýchlosť?
13. Prečo nie je efektívne zvyšovať prenosovú rýchlosť zväčšovaním šírky frekvenčného pásma?
14. Prečo nie je možné zvyšovať prenosovú rýchlosť zvyšovaním počtu stavov prenášaného signálu?
15. Od čoho je závislá maximálna prenosová rýchlosť?
16. Ktorý vzťah je platný pre výpočet maximálnej prenosovej rýchlosti?
17. Aké je frekvenčné pásmo kanála, ak SNR je 30 dB a prenosová rýchlosť je 56 kbit/s?
18. Aká je možná prenosová rýchlosť v kanáli, kde je pomer signál/šum 1000 a frekvenčný rozsah kanála je 6 kHz?
19. V akých veličinách sa udáva tlmenie prenosového kanála?
20. Aký je vzťah medzi tlmením a vstupnou a výstupnou úrovňou signálu?

21. Prečo je dôležitým parametrom prenosových médií fázový posuv?
22. Na aké typy môžeme rozčleniť prenosové médiá?
23. Ktoré typy prenosových médií patria k drôtovým prenosovým médiám?
24. Čo znamená označenie *Twisted Pair*?
25. Kde sa najčastejšie používajú krútené dvojlinky?
26. Ktoré prenosové médiá sa rozdeľujú na jednovidové a mnohovidové?
27. Prečo sú optické káble výhodné pre použitie v elektronických komunikačných sieťach?
28. Ktoré typy prenosových médií sú označované ako bezdrôtové?
29. Aký je rozdiel medzi všesmerovým a priamym rádiovým spojom?
30. Čo znamená kódovať signál na vstupe kanála?
31. Prečo sa kóduje signál na vstupe kanála?
32. Čo znamená označenie linkové kódy/linkové signály.
33. Aké typy linkových kódov sa používajú v digitálnych komunikačných systémoch?
34. Čo znamená pojem modulácia?
35. Podľa čoho sa rozdeľujú modulácie?
36. Aký typ nosného signálu používajú analógové modulácie?
37. Aký typ modulačného signálu používajú analógové modulácie?
38. Aký je výsledný signál po amplitúdovej modulácii, ak modulačný signál je analógový?
39. Ktorý parameter sa mení pri frekvenčnej modulácii?
40. Aké je iné označenie pre analógové modulácie, ktorých modulačný signál je digitálny?
41. Kde sa najčastejšie používajú analógové modulácie s digitálnym modulačným signálom?
42. Aký typ modulácie je DPSK (Different Phase Shift Key) modulácia?
43. Ktoré parametre sa menia pri DPSK (Different Phase Shift Key) modulácii?
44. Čo vyjadruje Shannon-Kotelnikov teorém?
45. Aký je základný postup pri pulzne-kódovej modulácii?
46. Ako sa nazýva postup, keď sa v PCM z analógového signálu vytvorí diskretný signál?
47. Ako sa nazýva postup, keď sa okamžitým vzorkám amplitúd priradí konkrétne dekadické číslo?
48. Ako sa nazýva postup pri PCM, keď sa okamžitým hodnotám vzoriek signálu priradí diskretná hodnota príslušnej úrovne?
49. Prečo sú vytvárané viacnásobné prenosy signálov?
50. Čo znamená pojem multiplex (*multiplexing*)?
51. Ako sa označujú systémy, ktoré využívajú princípy multiplexovania signálov?

5 Linková vrstva (Data link layer)

Ciele učenia

Čo by mal študent vedieť:

- funkcie linkovej vrstvy
- služby linkovej vrstvy
- prenos v linkovej vrstve, vytvorenie rámca, štruktúru rámca
- spoluprácu linkovej vrstvy so susednými vrstvami, poskytovanie služieb sieťovej úrovni
- základné spôsoby zabezpečenia proti chybám
- MAC adresáciu, spôsob kontroly adresy a veľkosti rámca
- prístup na spoločné komunikačné prostredie
- umiestnenie linkových protokolov v prostredí siete
- základné linkové protokoly, HDLC, Frame Relay

5.1 Úvod

Linková vrstva využíva služby fyzickej vrstvy, ktorá pre ňu poskytuje prenos bitov fyzickými prenosovými médiami. Na prvý pohľad by sa mohlo zdať, že prenos bitov nepotrebuje ďalšie spracovanie a bity môžu byť prenášané z jedného koncového zariadenia do druhého. Avšak komunikačné kanály môžu spôsobovať chyby prenosu, ktoré je potrebné eliminovať. Preto sú na linkovej vrstve vytvárané také opatrenia, ktoré umožňujú efektívnejší prenos. Možno povedať, že linková vrstva zaisťuje spoľahlivý prenos dát po fyzickom médiu. V tejto vrstve sú bity zoskupované do určitých celkov - dátových blokov a preto je táto vrstva niekedy označovaná ako dátová vrstva. V anglickej literatúre je označovaná ako *Data Link Layer*. Linková vrstva zostavuje jednotlivé bity do väčších celkov, ktoré sa označujú linkové rámce (*line frames*). Rámec je prenosovou jednotkou tejto vrstvy. Linkové rámce sú prenášané na linkovej vrstve medzi dvomi susednými bodmi prenosu, medzi ktorými je priame spojenie. Špecifikácie linkovej vrstvy sú dané príslušnými protokolmi linkovej vrstvy.

Linkovú vrstvu si môžeme predstaviť ako komunikáciu medzi dvomi susednými uzlami prenosového kanála. Hlavnou úlohou linkovej vrstvy je preto poskytovanie mechanizmu na komunikáciu medzi dvomi susednými uzlami. Jednotlivé systémy v sieti sa na tejto úrovni identifikujú adresami a komunikujú spôsobom „bod-bod“. Komunikujúce uzly si medzi sebou vymieňajú linkové rámce, ktorých jednotlivé časti informácie zaisťujú korektné rozpoznanie začiatku a konca každého jednotlivého rámca a informáciu príslušnej služby linkovej vrstvy.

5.2 Funkcie linkovej vrstvy

Základnou funkciou linkovej vrstvy je poskytovanie rozhrania a služieb sieťovej vrstve. Zabezpečenie základnej funkcie je uskutočňované prostredníctvom špecifických funkcií:

- Vytváranie, odosielanie a príjem rámcov – vytváranie rámcovej synchronizácie.
- Zabezpečenie proti chybám pri prenose, ku ktorým došlo vo fyzickej vrstve (*Error Control*).
- Fyzické adresovanie, prostredníctvom ktorého je každý rámec identifikovaný a kontroluje sa jeho príjem a určenie. K rámcom sa pridáva hardvérová adresa zdrojového a príjmového koncového zariadenia.
- Riadenie a regulácia toku dát prostredníctvom rámcov (*Flow Control*), ktoré obsahuje:
 - zahajovanie a záver prenosu rámcov,
 - riadenie poradia dodávaných rámcov,
 - potvrdzovanie prijatých rámcov,
 - ...

Pre splnenie týchto funkcií linková úroveň prijme paket zo sieťovej úrovne a „zabalí“ ho do rámca, ktorý prenesie. Každý rámec má hlavičku rámca (*frame header*), pole užitočnej informácie (*payload field*) a päť (*frame trailer*), obr. 5.1.



Obr. 5.1 Rámec v linkovej vrstve

V niektorých technológiách nie sú na linkovej úrovni poskytované všetky vyššie uvedené funkcie. Ide hlavne o kontrolu chýb a kontrolu toku dát, ktoré sú presunuté do vyšších vrstiev. Princípy, ktoré budú vysvetľované v tejto časti sú platné aj pre ich uplatnenie v iných úrovniach.

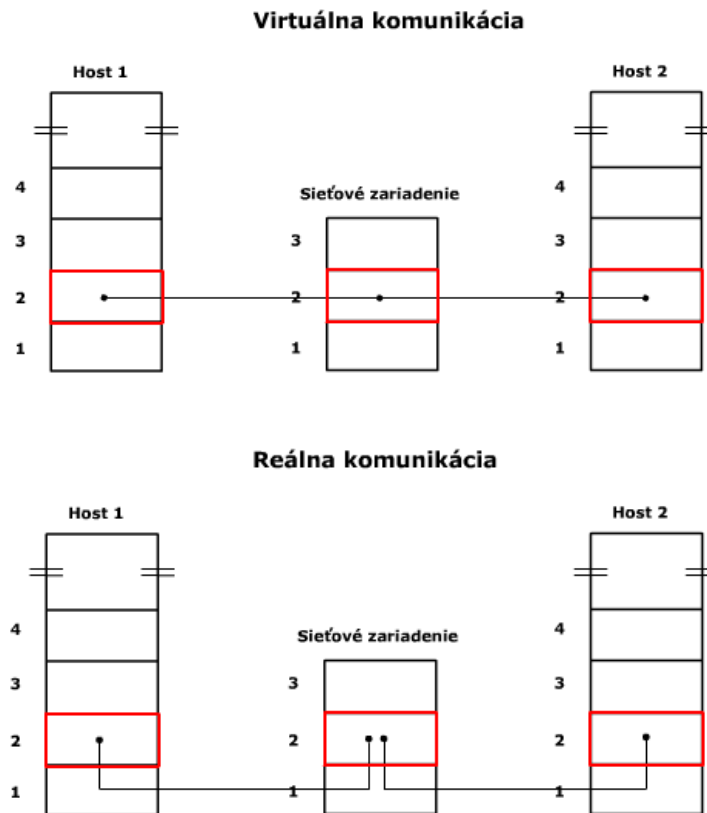
V lokálnych sieťach je linková vrstva rozdelená na:

- podvrstvu logických spojov (Logical Link Control - LLC),
- podvrstvu riadenia prístupu k médiu (Media Access Control – MAC).

5.3 Služby linkovej vrstvy

Linková vrstva poskytuje služby sieťovej vrstve. Úlohou tejto služby je, preniesť dáta zo sieťovej vrstvy zdroja do sieťovej vrstvy cieľa. Na to je potrebné využívať fyzickú vrstvu,

avšak vzájomná virtuálna komunikácia je uskutočňovaná medzi odpovedajúcimi linkovými vrstvami zdroja a cieľa, ako je znázornené na obr. 5.2



Obr. 5.2. Virtuálna a reálna komunikácia na linkovej úrovni

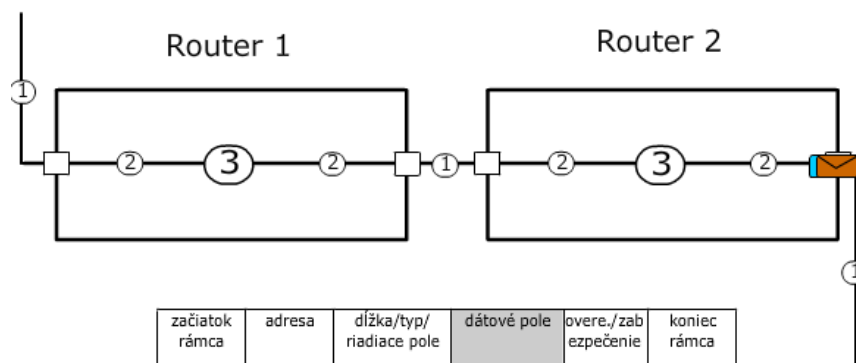
Služby, ktoré linková vrstva poskytuje sieťovej úrovni, môžu mať charakter spoľahlivých a aj nespoľahlivých služieb. Pre realizáciu spoľahlivých služieb musí mať linková vrstva k dispozícii mechanizmy pre zaistenie toho, že príjemca skutočne prijme všetky vyslané rámce, a to bez chýb, v prípade spojovanej služby ešte aj v správnom poradí.

Linková vrstva poskytuje sieťovej vrstve nasledujúce služby prenosu:

- **Nepotvrdená nespojovaná služba** (unacknowledged connectionless service)
 - posielajú sa samostatné rámce,
 - pred odoslaním nie je vytvorené spojenie,
 - pri poškodení alebo strate rámca nie sú urobené kroky na opätovné vyslanie,
 - vhodná pre spoľahlivé kanály, kde je nízka chybovosť,
 - vhodná aj pre prevádzku v reálnom čase, ako je hlas, kde oneskorené dáta sú horšie ako sú zlé dáta,
 - často používaná služba v LAN.
- **Potvrdená nespojovaná služba** (acknowledged connectionless service)
 - pred odoslaním nie je vytvorené spojenie,
 - každý samostatne vysielaný rámec je individuálne potvrdzovaný,

- ak nie je rámec prijatý v špecifikovanom intervale, je posielaný znovu,
- vhodná pre nespoľahlivé linky, ako sú bezdrôtové prenosy,
- pri spoľahlivých kanáloch, ako sú optické káble je takýto zložitý proces zbytočný.
- **Spojovaná služba** (connection-oriented service)
 - je najprepracovanejšia služba,
 - prenos je uskutočňovaný trojfázovo: vytvorí sa spojenie, posielajú sa rámce a po ukončení prenosu sa spojenie zruší,
 - každý rámec, posielaný počas spojenia je číslovaný a linková úroveň garantuje, že každý vyslaný rámec je prijatý,
 - v tomto prípade je garantované, že každý rámec je prijatý iba raz a všetky rámce sú prijaté v správnom poradí.

Príkladom poskytovania služieb linkovej úrovne vo WAN sieti je obr. 5.3. Uzly sieťovej vrstvy sú spojené prenosovým kanálom, ktorý tvorí fyzickú vrstvu. Na zabezpečenie prenosu medzi uzlami sú kontrolované linkové rámce.



Obr. 5.3 Vzťah linkovej a sieťovej vrstvy

Ak príde linkový rámec do prenosového bodu príslušného uzla, je prijatý hardvérom, ktorého softvér kontroluje prijatý rámec podľa protokolu linkovej úrovne. Ak je rámec prijatý správne, odstráni riadiace znaky rámca (*decapsulation*) a pakety, ktoré sú rámcom prenášané sú poskytnuté do sieťovej úrovne. Po nájdení príslušného smeru v spojovacích bodoch sú pakety opäť vložené do linkových rámcov a prenášané k ďalšiemu prenosovému bodu.

5.3.1 Tvorba rámcov

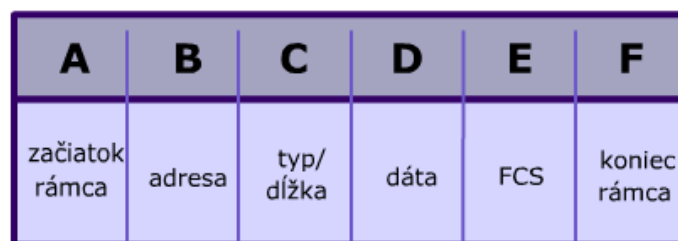
Dôvodom na vytváranie rámcov je tá skutočnosť, že služba fyzickej vrstvy, ktorou je prenos jednoduchého bitového toku, negarantuje bezchybný prenos. Je preto úlohou linkovej úrovne detekovať, aj ak je potrebné, aj opravovať chyby pri prenose medzi dvoma prenosovými bodmi. Táto služba je poskytovaná sieťovej úrovni tak, že linková úroveň rozdelí tok bitov do dátových rámcov a špeciálnymi bezpečnostnými kódmi určí kontrolný mechanizmus pre každý rámec. Keď rámec príde do cieľa, na základe kontrolných mechanizmov bezpečnostného kódu, je zisťovaná správnosť prenosu. Ak je zistená chyba,

linková vrstva robí opatrenia pre jej odstránenie, v závislosti na použítom spôsobe zabezpečenia proti chybám.

5.3.2 Všeobecný formát rámca

Všeobecný formát rámca, používaný na linkovej vrstve, znázornený na obr. 5.4, obsahuje šesť základných sekcií nazývaných polia, ktoré sú zložené z určitého počtu bajtov. Názvy týchto polí sú:

- začiatok rámca
- adresa
- riadiace pole
- dátové pole
- overenie/zabezpečenie
- koniec rámca



Obr. 5.4 Všeobecný formát rámca

Pole začiatok rámca

Slúži na oznámenie začiatku rámca. Viaceré technológie majú rôzne spôsoby pre tento proces, avšak nezávisle na technológii, všetky rámce majú úvodnú sekvenciu bytov.

Adresné polia

Všetky rámce obsahujú informácie o adrese. Je to fyzická šesť bitová adresa, kde prvé tri bity charakterizujú výrobcu sieťovej karty a ostatné unikátnu fyzickú adresu sieťovej karty.

Riadiace pole- pole dĺžka /typ

Je závislé od typu technológie. U niektorých technológií dĺžka vyjadruje presnú dĺžku rámca. Iné majú typ pol'a, ktoré špecifikuje žiadosť o vysielanie protokolu vrstvy 3. Niektoré technológie takéto polia nemajú.

Dátové polia

Dátové polia obsahujú prenášané dáta a riadiace informácie sieťovej vrstvy.

Kontrolné číslo

Frame Check Sequence (FCS) pole obsahuje kontrolné číslo vypočítané zdrojovým počítačom na základe dát v rámci. Keď cieľový počítač prijme rámec, prepočíta jeho FCS a porovná ho s FCS priloženom v rámci. Ak sa čísla nerovnajú, predpokladáme chybu a zdroj je požiadaný o opakovaný prenos.

Pole koniec rámca

Slúži na informáciu, že rámec končí. Koniec rámca určuje sekvencia bytov, ak nie je známa presná dĺžka rámca.

5.3.3 Typy rámcov

Podľa spôsobu vytvárania rámcov sú rozlišované dva typy:

- Znakovo orientované rámce (character oriented frames),
- Bitovo orientované rámce (bit oriented frames).

Znakovo orientované rámce sú vytvárané dvojicou špeciálnych znakov STX (*Start of TeXt*, začiatok textu) a ETX (*End of TeXt*, koniec textu), ktoré sú pre svoju funkciu označované ako riadiace znaky prenosu (*transmission control characters*). Znaky STX a ETX umožňujú správne rozpoznať začiatok a koniec rámca. Takto sa dosiahne synchronizácie na úrovni rámcov (*frame synchronization*) a prenos je znakovo orientovaný (*character oriented transmission*).

Tento spôsob tvorby rámcov sa používa pri asynchrónnom prenose na fyzickej vrstve, kde sú prenášané dáta oddeľované štart a stop impulzmi. Nevýhodou asynchrónneho prenosu je vkladanie štart a stop impulzov, čím sa znižuje prenosová rýchlosť. Pre vyššie rýchlosti sa preto používa synchronný prenos, pri ktorom sa používa synchronizácia na fyzickej vrstve na úrovni znakov (*character synchronization*), použitím špeciálneho znaku SYN. Aj v tomto prípade je možné použiť znakovo orientovanú rámcovú synchronizáciu, ale vkladanie riadiacich znakov spôsobuje zníženie efektívnej prenosovej rýchlosti. Preto sa viac používajú bitovo orientované rámce.

Bitovo orientované rámce sú založené na myšlienke indikovať začiatok a koniec rámca skupinou bitov. Pojem bitovo orientovaný znamená, že prenášané dáta sú vyhodnocované po bitoch a určitá skupina bitov indikuje začiatok a koniec rámca. Táto skupina bitov sa niekedy označuje ako krídlová značka (*flag*). Obvykle je tvorená postupnosťou „01111110“. Aby sa zabezpečilo tomu, že sa uvedená postupnosť vyskytne vo vnútri rámca, vkladá sa automaticky 0 za každých päť po sebe idúcich dátových bitov. V prijímači sa táto nula automaticky odstraňuje.

5.4 Základné spôsoby zabezpečenia proti chybám

Okrem rozpoznania preneseného rámca je potrebné zabezpečiť aj správnosť prenášaných dát. Preto sa prenos na úrovni linkovej vrstvy zabezpečuje proti chybám, ktoré môže spôsobiť fyzická vrstva. Existuje veľa spôsobov, ako signál, nesúci správu, zabezpečiť proti chybám.

Spôsoby zabezpečenia sa delia na dve skupiny:

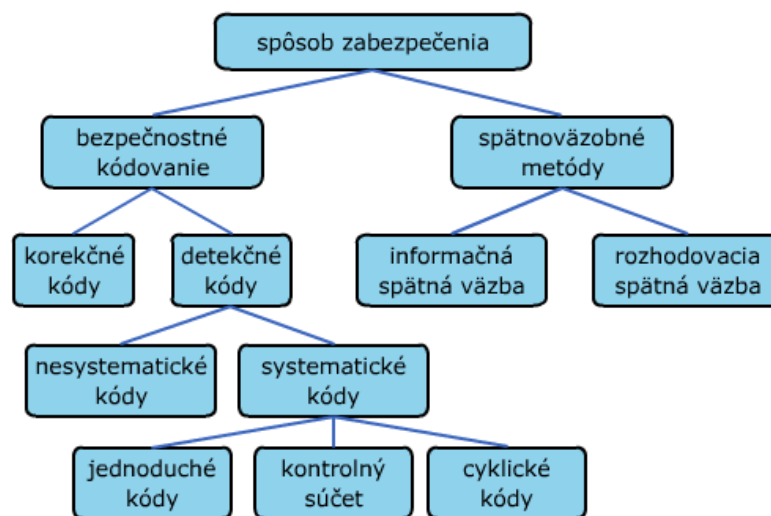
- bezpečnostné kódovanie,
- metódy so spätnou väzbou.

Princíp bezpečnostného kódovania je v tom, že sa k prvkom signálu nesúceho správu, pridajú ďalšie prvky signálu. Metódy so spätnou väzbou sú založené na interakcii medzi vysielačou a prijímacou stranou.

Bezpečnostné kódy delíme podľa spôsobu zabezpečenia na kódy:

- detekčné,
- korekčné.

Detekčné kódy chybu zistia, korekčné ju dokážu aj opraviť. Korekčné kódy sú menej využívané. Dôvodom je to, že korekcia chyby je často omnoho náročnejšia na čas aj technické prostriedky, ako opakovanie kódového slova po detekcii chyby. Rozdelenie spôsobov zabezpečenia je na obr. 5.5.



Obr. 5.5 Spôsoby zabezpečenia proti chybám pri prenose

5.4.1 Zabezpečenie paritou

Najjednoduchšie zabezpečenie vytvoríme, keď ku každému kódovému slovu pridáme jednoduchý symbol tak, aby počet jednotkových prvkov bol párný alebo nepárný. Takéto zabezpečenie sa nazýva zabezpečenie párnou alebo nepárnou paritou. Kódové slovo po zabezpečení paritou má tvar:

$$(S_k, S_{k-1}, \dots, S_1, r_1)$$

kde S_i sú binárne znaky zakódovanej správy, r_1 je **zabezpečovací symbol**.

Hodnotu zabezpečovacieho symbolu určí kóder na vstupe kanála podľa rovnice:

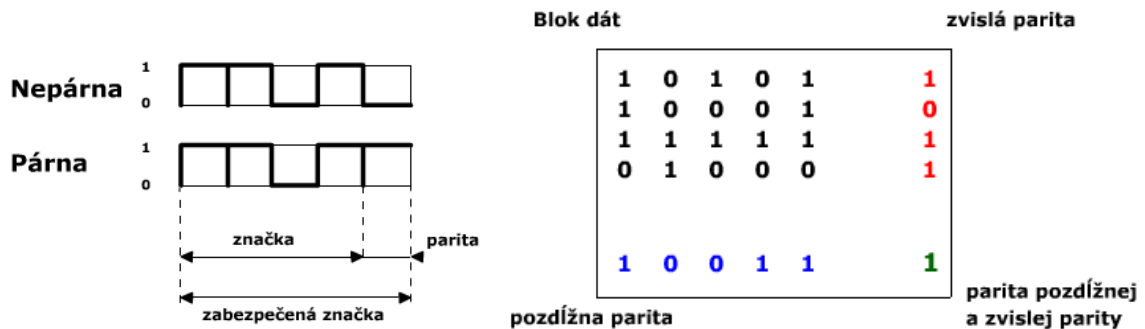
$$S_k + S_{k-1} + \dots + S_1 + r_1 = 0 \text{ pre párnou paritu}$$

$$S_k + S_{k-1} + \dots + S_1 + r_1 = 1 \text{ pre nepárnou paritu}$$

Princíp jednoduchej parity má svoje nedostatky v tom, že napríklad pri dvoch zmenách jednotiek kódového slova, je zabezpečovací symbol vyhodnotený ako správny a nie je zistená chyba. Tento nedostatok sa dá odstrániť použitím **krížovej parity**.

Pri krížovej parite sa zabezpečujú bloky dát obsahujúce niekoľko značiek. V bloku sa každá značka zabezpečí jedným paritným bitom (**zvislá parita**) a každý stĺpec bloku je znova zaistený jedným paritným bitom (**pozdĺžna parita**). Stĺpec zvislých parít a riadok pozdĺžnych parít sú zaistené ďalšou paritou, ktorá je paritou pre riadok i stĺpec. Krížovou paritou sa dajú zistiť aj niektoré zhluky chýb.

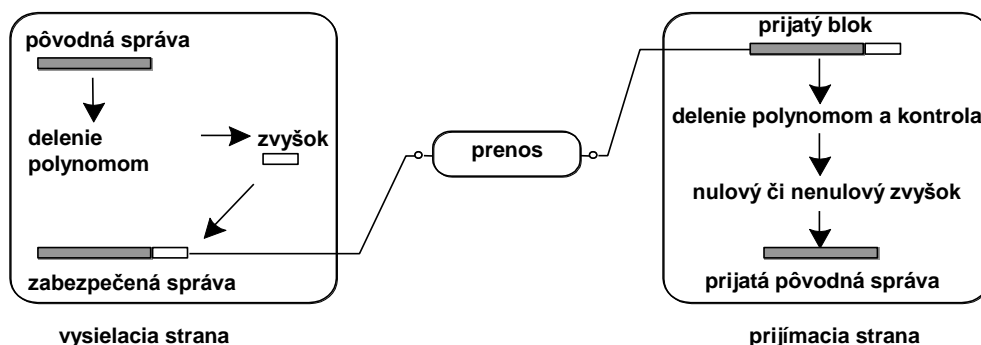
Príklady zabezpečenia paritou sú znázornené na obr. 5.6.



Obr. 5.6 Zabezpečenie jednoduchou a krížovou paritou

5.4.2 Cyklický kód

Často používaný spôsob zabezpečenia je cyklický kód, označovaný ako **CRC (Cyclic Redundancy Check)**. Princíp spočíva v delení dvoch mnohočlenov (polynómov). Jedným mnohočlenom je blok pôvodnej prenášanej správy, druhým je tzv. generický mnohočlen, ktorý je vytvorený špeciálnou kombináciou binárnych symbolov. Podľa dĺžky bloku správy a systému v ktorom je správa prenášaná, sa volí príslušný generický mnohočlen. Upravený blok prenášanej správy sa delí generickým mnohočlenom a zvyšok po delení tvorí kontrolné slovo, ktoré sa priradí k zabezpečovanému bloku. Na prijímacej strane sa tento blok delí opäť generickým mnohočlenom. Ak je zvyšok po delení nulový, bol blok správy prenesený s veľkou pravdepodobnosťou správne. Ak nie je zvyšok nulový, došlo k chybe pri prenose a je nutné blok správy opakovať. Zjednodušený princíp cyklického kódu je znázornený na obr. 5.7.



Obr. 5.7 Princíp cyklického kódu

Delenie mnohočlenov sa uskutočňuje na základe pravidiel Booleovej algebry, čo je veľká výhoda pretože binárne matematické operácie sa jednoducho realizujú pomocou obvodov číslicovej techniky.

Aby vysielateľ a prijímač cyklického kódu mohli spolupracovať, musia používať rovnaký generický mnohočlen. Preto je tvar mnohočlenov medzinárodne normalizovaný. Napríklad pre prenos dát je štandardizačnou organizáciou ITU (*International Telecommunication Union*) odporúčaný mnohočlen $x^{16} + x^{12} + x^5 + 1$, (10001000000100001). Tento mnohočlen umožňuje generovať cyklický kód, schopný zistiť všetky nepárne počty chýb, všetky zhluky chýb kratšie ako 16 bitov a veľké percento ostatných chýb. Prakticky to znamená, že na jeden nezistený chybný bit pripadá asi 10^{14} správne prenesených bitov.

5.5 Prístup na spoločné komunikačné prostredie

V komunikačných sieťach, bez ohľadu na používané prenosové médium, je vždy potrebné zabezpečiť efektívne využitie kapacity, poskytovanej prenosovým médium. To je vo väčšine prípadov riešené využívaním spoločného prenosového média mnohými koncovými zariadeniami. Preto vzniká potreba riadenia prístupu k prenosovému médium. Riadený prístup k prenosovému médium umožní:

- Rozdeliť celkovú kapacitu prenosového média na časti, ktoré sú pridelované jednotlivým prenosovým kanálom.
- Zabezpečiť rovnomerné pridelovanie kapacity prenosového média jednotlivým koncovým zariadeniam.
- Minimalizovať riziko kolízie súčasného pridelenia prenosového média viacerým kanálom, prípadne ho úplne vylúčiť.

Preto je dôležitou úlohou linkovej vrstvy **riadenie prístupu** jednotlivých komunikujúcich zariadení na prenosové médium. Komunikujúce zariadenia sú vzájomne prepojené spoločným médium, o ktoré sa medzi sebou musia pri vysielaní dát deliť. Pri „delení sa“ o médium musia byť pravidlá, ktorými sa budú zariadenia riadiť. Tieto pravidlá sa nazývajú **prístupová metóda**. Linková vrstva riadi, koľko komunikujúcich zariadení môže naraz v sieti vysielateľ svoje dáta a kedy môže ktorá zariadenie odoslať rámec do siete.

Prístupové metódy sa delia na:

- **Stochastické**, ktoré ako metódu využívajú náhodný proces. U týchto metód vždy hrozí menšie alebo väčšie riziko kolízií súčasného pridelenia prenosového média viacerým koncovým zariadeniam. Napriek tomu sú tieto metódy v praxi využívané.
- **Deterministické**, kedy sa prístupové práva pridelujú podľa určitých pravidiel, čím sa minimalizuje riziko. Deterministické prístupové metódy zabezpečujú na jednej strane každému zariadeniu pevnú časť kapacity prenosového média, čo však spôsobuje zvýšené oneskorenie pri prenose. Na druhej strane bezkonfliktné prostredie, pokiaľ uvažujeme prenos médium so zanedbateľnou bitovou chybovosťou, zaručuje prakticky ideálny priebeh riadenia siete.

Vlastné riadenie komunikácie môže byť:

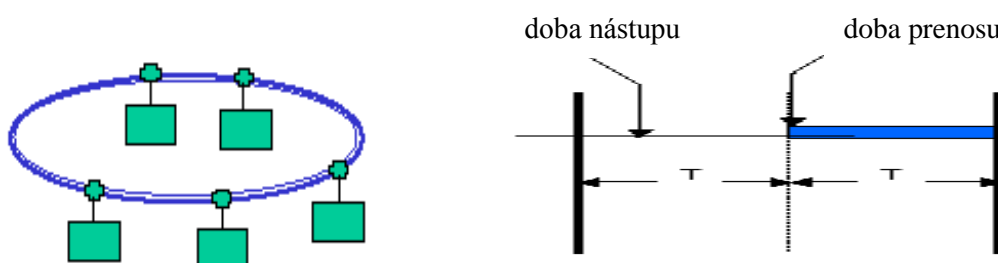
- Centralizované, kde jedno zariadenie je zvolené ako riadiace a prideluje ostatným podriadeným zariadeniam kapacitu kanála na základe ich požiadavky.
- Decentralizované, ktoré odstraňuje závislosť na jednom riadiacom zariadení. V závislosti od použitej metódy sa zariadenie pripája k spoločnému kanálu samé.

Stochastické prístupové metódy

5.5.1.1 Čistá Aloha (Pure Aloha)

Prístupové metódy Aloha vychádzajú z predpokladu, že najjednoduchším riadením je chaos. V komunikačnej sieti to znamená, že sa zariadeniam ponecháva voľnosť vysielat' správy v čase, kedy to potrebujú. Pri takomto postupe dochádza ku kolízii. Skutočnosť, že prišlo ku kolízii pozná vysielajúca strana tak, že monitoruje spoločný kanál. Keď zistí, že prišlo ku kolízii prestane vysielat'. Rovnako prijímacia strana zistí kolíziu a tiež prestane vysielat'. Vysielanie sa obnoví až po náhodne zvolenom čase. Použitím náhodne zvoleného času majú zariadenie šancu, že sa ich opakované vysielania nestretnú. Najväčšou nevýhodou metódy čistá Aloha je skutočnosť, že na vznik kolízie stačí, aby došlo k prekrytiu posledného bitu rámca vysielaného jedným zariadením a prvého bitu rámca zariadenia, ktoré začne vysielat'. Bez ohľadu na to, že bol zasiahnutý len jeden bit rámca, musí byť zrušený celý rámec a jeho vysielanie musí byť opakované. Môže vzniknúť otázka, aká je pravdepodobnosť, že sa rámec preniesie bez kolízie. Odpoveď je, že pravdepodobnosť výskytu kolízie je malá iba pri malom počte pripojených koncových zariadení. Preto sa Aloha používa len v sieťach s malým počtom pripojených zariadení.

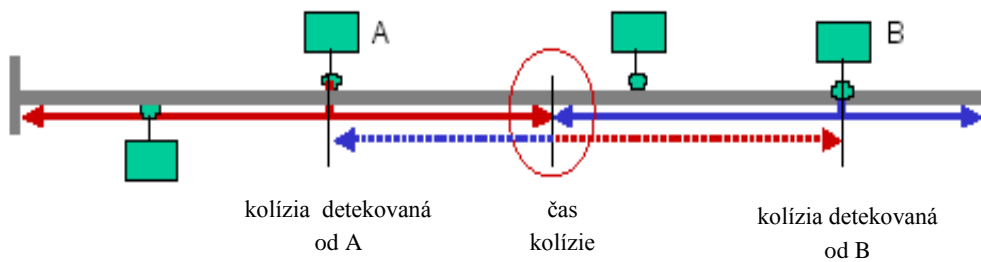
Riziko vzniku kolízie sa dá radikálne zmeniť, keď sa zariadeniam povolí vysielanie len v určitých časových okamžikoch. Prakticky to znamená prechod od spojitého času na čas diskretný. Na tejto myšlienke je postavený princíp synchronizovanej Alohy (*Synchronous Aloha, Slotted Aloha, S-Aloha*). Tým je zavedený deterministický prvok do stochastickej metódy. Pri S-Alohe zariadenie nemôže vysielat' kedykoľvek, ale iba v tzv. synchronizačných okamžikoch, vid'. obr. 5.8. Pokiaľ sa tento okamžik nevyužije, musí sa čakať na ďalší. Pravdepodobnosť úspešného prenosu sa tým zväčší, ale iba vtedy, keď sa nezvyšuje zaťaženie spoločného kanála. Aj malé zvýšenie zaťaženia má za následok značné zvýšenie výskytu kolízií. Protokoly Aloha nie sú vhodné pre siete, kde sa predpokladá väčšia prevádzka.



Obr.5.8 Prístupová metóda Aloha

5.5.1.2 Metoda CSMA (Carrier Sense Multiple Access)

CSMA je metóda mnohonásobného prístupu počúvaním nosnej, čo znamená, že každé zariadenie sleduje prevádzku na spoločnom kanáli a na základe detekcie zisťuje, či je kanál voľný. Zariadenie môže vysielat' len vtedy, keď je v kanáli ticho. V prípade kolízie sa prenos signálového bloku dokončí a až po určitom čakacom intervale sa obsadzovacia postupnosť vyšle znovu, pokiaľ je kanál voľný. Princíp metódy je znázornený na obr.5.9.



Obr. 5.9 Princíp metódy CSMA

5.5.1.3 Metóda CSMA/CD (CSMA/Collision Detection)

Ďalšie zlepšenie prístupu k spoločnému kanálu môže byť dosiahnuté vtedy, keď je použitý mechanizmus, ktorým každé zariadenie sleduje prevádzku v kanáli. Tento mechanizmus sa nazýva detekcia kolízie. Keď dôjde ku kolízii, obidve zariadenia ukončia vysielanie signálového bloku, vyšlú signál kolízie a odmlčia sa na náhodne dlhú dobu, čím s veľkou pravdepodobnosťou nedôjde medzi nimi k ďalšej kolízii. Kolízny signál sa nazýva „Jam“ a má dĺžku 32 bitov. Ak nedôjde ku kolízii, je odvysielaná celá správa. Vznik kolízie mimo začiatku vysielania je v tomto prípade vylúčený, pretože keď jedno zariadenie obsadí kanál, ostatné čakajú na vysielanie.

Mechanizmus „počúvania nosnej“ je považovaný za dostatočný prostriedok na zistenie skutočnosti, či je kanál voľný. Môže však nastať situácia, keď sa pri počúvaní nosnej kanál javí voľný, no v skutočnosti je obsadený. Zariadenie túto skutočnosť nedetekuje vplyvom nízkej rýchlosti šírenia elektrických signálov v prenosovom médiu. Metódy CSMA/CD nie sú vhodné pre riadenie prístupu k spoločnému kanálu v prevádzke v reálnom čase. Napriek tomu sa zo stochastických metód najviac používajú.

5.5.1.4 Token Passing

Prístupová metóda *Token Passing* je bezkolíznou metódou, založenou na princípe odovzdávania povoločovacieho vysielacieho práva. V režime kľudu sa medzi zariadeniami pohybuje malý rámec, nazývaný token. Zariadenie môže vysielat' až vtedy, keď vlastní token. Vlastníctvo tokenu zaisťuje právo vysielat' dáta. Ak zariadenie dostane token a nemá čo vysielat', odovzdá ho ďalej. Každé komunikujúce zariadenie môže token držat' určitú maximálnu dobu, v závislosti na implementovanej technológii. Tento spôsob prístupu je používaný v sieťach Token Ring a Token Bus.

5.5.2 Deterministické prístupové metódy

Deterministické metódy zabezpečujú bezkonfliktné pridelovanie prístupových práv k spoločnému prenosovému kanálu. Podľa spôsobu riadenia prístupu sa delia na metódy:

- s pevným priradením prenosového kanála,
- s priradením prenosového kanála na požiadanie,
- s rezerváciou prenosového kanála.

Prístupové metódy s pevným priradením prenosového kanála vychádzajú z princípov multiplexných metód používaných pri spojení typu bod-bod (*point to point*), a je ich možné rozdeliť na:

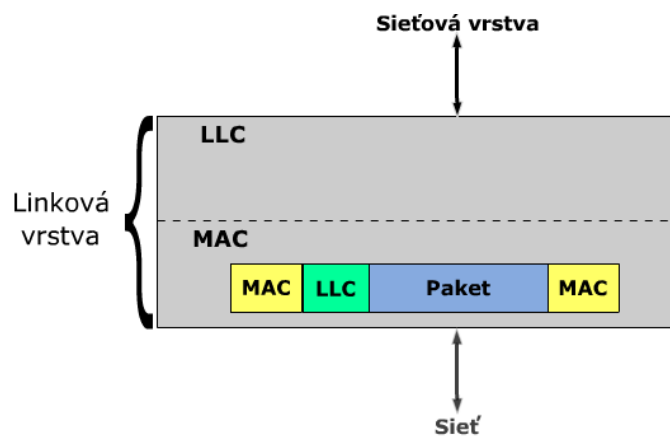
- **TDMA** (*Time Division Multiple Access*), kde sa dostupná prenosová kapacita delí v čase. Vychádza z časovo deleného - TDM princípu, ktorý je pre komunikáciu bod–multibod (*point to multipoint*) nutné doplniť o procedúry zabezpečujúce časovo delený prístup na prenosové médium (*A-access*), ktoré pri TDM nie sú potrebné. **FDMA** (*Frequency Division Multiple Access*), kde sa dostupná prenosová kapacita delí na frekvenčné pásma. Každému prenosovému kanálu je pevne pridelené určité frekvenčné pásmo, podobne ako pri frekvenčnom multiplexe - FDM. Používa sa hlavne v oblasti rádiových prístupových systémov a mnohokrát v kombinácii TDMA a WDMA.
- **WDMA** (*Wavelength Division Multiple Access*) je modifikáciou FDMA pre oblasť vlnových dĺžok spadajúcich do optickej oblasti. Na prenos signálu používa optické vlnové dĺžky. Riešenie bod-bod používa pre každý kanál samostatnú optickú vlnovú dĺžku, čím sa prístupová metóda redukuje na jednoduché WDM. Jednotlivé optické signály sú zlúčené do výsledného toku pasívnym optickým multiplexorom. Takto organizovaná optická prístupová sieť má pevné priradenie prenosových kanálov jednotlivým zariadeniam. Na vytvorenie prístupu niekoľkým zariadeniam, je potrebné vytvoriť väčší počet optických nosných. Pokiaľ je potrebné zabezpečiť flexibilitu v priradovaní kanála jednotlivým zariadeniam, musia byť WDM multiplexory preladiteľné. **CDMA** (*Code Division Multiple Access*) priraduje kanály na báze kódovania prenášaných signálov. Všetky zariadenia používajú rovnakú frekvenčnú a časovú oblasť. Oddelenie dát jednotlivých kanálov je realizované priradením špecifického kódového slova každému spojeniu. Každý bit prenášanej správy je násobený kódovacou sekvenciou s dĺžkou n bitov. To znamená, že operácie kódovania i prenosová rýchlosť výstupného toku dát musia prebiehať s n -násobne vyššou frekvenciou. Prenos kódovaných signálov vyžaduje podstatne väčšiu šírku pásma ako u iných prístupových metód. Jeho výhodou je však minimálne riziko príjmu signálu neoprávneným prijímačom. Preto sa prístupové metódy CSMA používajú v rádiových prístupových sieťach a aj pre vojenské účely.

5.7 Podvrstvy linkovej vrstvy

Linková vrstva lokálnych počítačových sietí je rozdelená podľa odporúčaní IEEE 802.2 na dve podvrstvy:

- podvrstvu logického spoja (*Logical Link Control* - LLC) ktorá je zodpovedná za koordináciu prístupu na sieť (detekcia chýb, riadenie toku dát).
- podvrstvu riadenia prístupu k spoločnému médiu (*Media Access Control* – MAC) čo je reálne rozhranie prístupu na fyzické médium,

Dôvodom takéhoto rozdelenia je možnosť spolupráce so sieťovou vrstvou pre rôzne použité technológie. Jeden logický spoj - LLC môže využívať niekoľko rôznych prístupov k spoločnému prenosovému médiu - MAC. Znáznovenie rozdelenia je na obrázku 5.8.



Obr. 5.10 Rozdelenie linkovej úrovne podľa IEEE 802.2

5.7.1 Riadenie logického spoja - LLC

LLC - Logical Link Control poskytuje služby sieťovým protokolom, ktoré sú nad ňou, a súčasne využíva služby rôznych technológií fyzickej vrstvy. LLC sa podieľa na procese zapuzdrenia (*encapsulation*). Spracováva dáta sieťového protokolu, spravidla IP paketu, a pridá svoje riadiace informácie, aby sa paket dostal do svojho cieľa. Takto zapuzdrený paket potom pokračuje do MAC podvrstvy a je podľa konkrétnej technológie ďalej spracovaný. Zároveň LLC zabezpečuje detekciu chýb a kontrolu toku dát linkovej vrstvy.

5.7.2 Riadenie prístupu k spoločnému médiu - MAC

MAC - Media Access Control je implementovaná nad fyzickou vrstvou a využíva služby tejto vrstvy na prenos bitov. Pre **riadenie prístupu používa prístupové metódy**, zaisťujúce korektný prístup na spoločné prenosové médium. Okrem toho **zabezpečuje fyzické adresovanie** prostredníctvom MAC adresy. MAC adresa je celosvetový jednoznačný identifikátor väčšiny sieťových zariadení, ktoré používa rôzne protokoly linkovej vrstvy OSI modelu. Označovaná je aj ako hardwarová adresa, layer adresa alebo fyzická adresa.

MAC adresa sa skladá zo 48 bitov, čo predstavuje 6 bajtov. Pridelovanie adries riadi organizácia IEEE (*Institute of Electrical and Electronics Engineers*). Tvar adresy je

xx:xx:xx:xx:xx:xx a je vyjadrovaná v hexadecimálnom tvare, napríklad 00:0C:2B:DE:3F:25. MAC adresa je súčasťou sieťovej karty.

5.8 Riadenie toku

Riadenie toku dát na linkovej vrstve je mechanizmus, ktorý zabezpečuje, aby vysielacie zariadenie nezahltalo prijímacie zariadenie, ktoré má iba obmedzenú veľkosť vstupných vyrovnávacích pamätí. Preto po určitej dobe dochádza k uvoľneniu vstupných vyrovnávacích pamätí a pripraví sa pamäťový priestor pre nové prijímanie dát. Riadenie toku dát sa realizuje prostredníctvom protokolov. Z množstva protokolov na riadenie toku dát v linkovej vrstve uvedieme dva:

- protokol stop-and-wait,
- protokol posuvného okna.

5.8.1 Protokol Stop-and-Wait

Protokol Stop and Wait je najjednoduchší protokol. Princíp protokolu je nasledovný. Entita zdrojového zariadenia vyšle rámec. Entita cieľového zariadenia ho prijme a odošle kladné potvrdenie o jeho prijatí. Vysielacie zariadenie čaká, kým nedostane potvrdenie. Až po prijatí tohto potvrdenia môže vysielacie zariadenie opäť vysielat'.

5.8.2 Protokol posuvného okna (*Sliding Window Protocols*)

V protokole posuvného okna obsahuje každé zariadenie „okno“, ktoré obsahuje postupnosť čísel v rozsahu 0 až maximum (obvykle 8 alebo 128). Tieto čísla určujú čísla vyslaných rámcov (okno vysielачa) a čísla prijímaných rámcov (okno prijímača).

Číslo vo vnútri "okna vysielачa" predstavuje číslo vysielaného a doposiaľ nepotvrdeného rámcu. Okno je rozdiel medzi množstvom vyslaných a potvrdených rámcov. Preto sa po príchode nového rámcu, zväčší okno nepotvrdených rámcov o jednotku. Ako náhle príde potvrdenie o prijatí rámcu okno sa o jednotku zmenší. Vysielач musí mať v pamäti uschované nepotvrdené rámce, aby ich v prípade nutnosti mohol zopakovať. Číslo vo vnútri "okna prijímača" odpovedá rámcu, ktorý má byť prijatý. Akýkoľvek iný neočakávaný rámec je zničený. Ak je prijatý rámec, ktorého číslo sa rovná dolnej hranici okna, potom je vygenerované potvrdenie a celé okno sa posunie o jedno číslo nahor.

5.9 Opravy prenosu rámcov

Chybné prenesené rámce sú opravované dvojakým spôsobom:

- Mechanizmami na opravu rámcov, ktoré sú založené na týchto princípoch:
 - detekcia bitových chýb zaist'ovaná pomocou CRC (*Cyclic Redundancy Code*),
 - kladné potvrdzovanie prijatia rámcu, čo znamená, že prijímač odosiela kladné potvrdenie pre bezchybne prijaté rámce,

- opakovanie vysielania rámcov po uplynutí času, tj. ak do definovanej doby nedostane vysielateľ potvrdenie o prijatí rámca prijímacou stanicou opakuje vysielanie,
- záporné potvrdzovanie doplnené o žiadosť o opakovanie vysielania rámcov, kedy prijímacia strana pri detekcii chyby odošle záporné potvrdenie.
- Použitím korekčných kódov, ktoré umožňujú zistiť a aj opraviť chybu vzniknutú pri prenose. Sú však málo používané.

5.10 Základné linkové protokoly

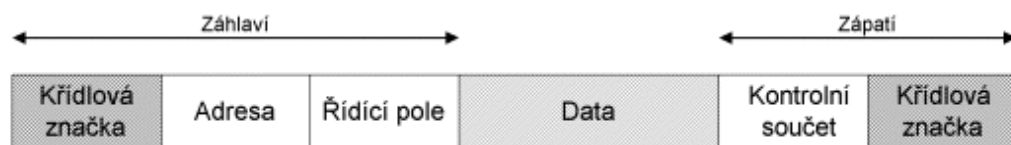
Protokoly linkovej vrstvy popisujú rámce, ktoré sú komunikačnou jednotkou linkovej vrstvy.

Typy rámcov a ich formáty sú špecifikované ako samostatné štandardy alebo v štandardoch rôznych typov technológií. Uvádzame niektoré príklady:

- HDLC (*High Level Data Link Control*)
- PPP (*Point to Point Protocol*)
- Frame Relay
- Ethernet a IEEE 802.3
- FDDI (*Fiber Distributed Data Interface*)
- Token Ring

5.10.1 Protokol HDLC – (*High Level Data Link Control*)

Protokol HDLC je ISO3309 linkový protokol pre synchronný prenos po sériových linkách. Podporuje detekciu chýb použitím CRC (*Cyclic Redundancy Code*) a riadenie toku dát princípom posuvného okna. HDLC môže pracovať vo viacerých režimoch. Vychádza z IBM SDLC protokolu. Bol vytvorený pre dátovú sieť X.25 ale môže byť použitý na rôznych technológiách. Základný typ rámca je na obr. 5. 11.



Obr. 5.11 Rámec protokolu HDLC

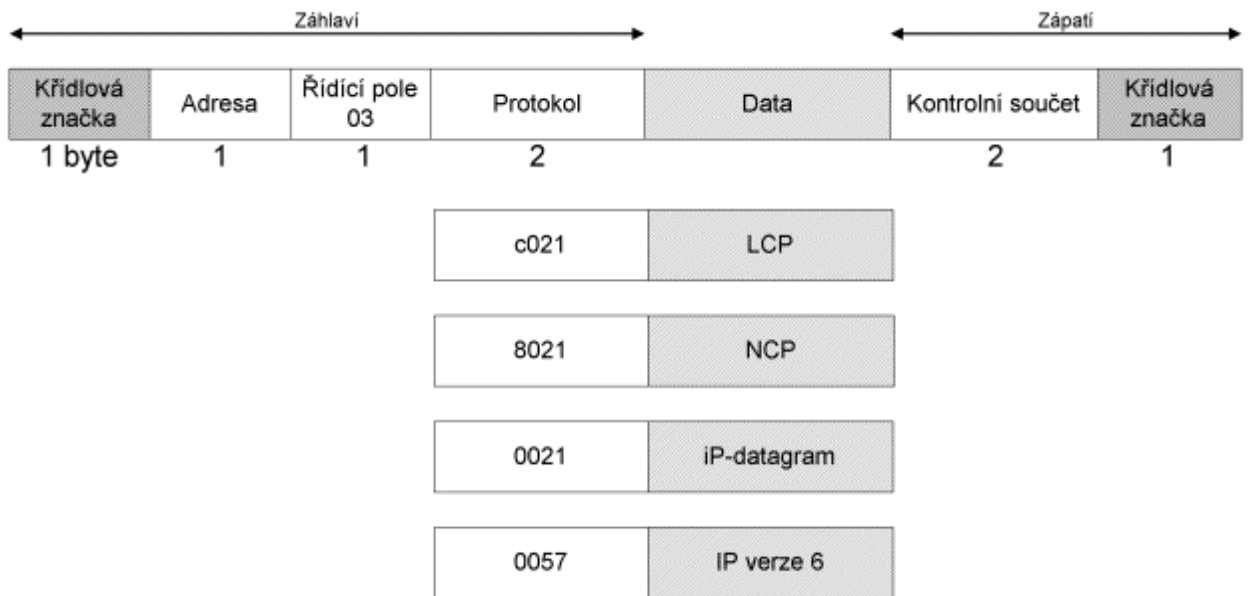
5.10.2 Protokol PPP (*Point to Point Protocol*)

Protokol PPP je proprietárne riešenie štandard RFC- 1661. Používa rámce tvaru protokolu HDLC. Protokol je určený pre riadenie dátových spojení medzi uzlami. Skladá sa z dvoch protokolov:

- LCP (*Link Control Protocol*) – riadenia spojenia medzi uzlovými zariadeniami.
- NCP (*Network Control Protocols*) – riadenie sieťových protokolov. Je to skupina protokolov, kde každý sieťový protokol, ktorý bude využívať linkový protokol PPP,

má definovanú v rámci PPP vlastnú normu pre protokol NCP. Súčasťou tejto normy je aj číslo protokolu, ktoré je v poli protokol PPP rámca. Pre NCP začína číslom 8, pre dátové rámce číslom 0. Napríklad označenie 0057 sú dátové rámce prenášané protokolom IPV6, NCP protokol pre IPV6 má označenie 8057.

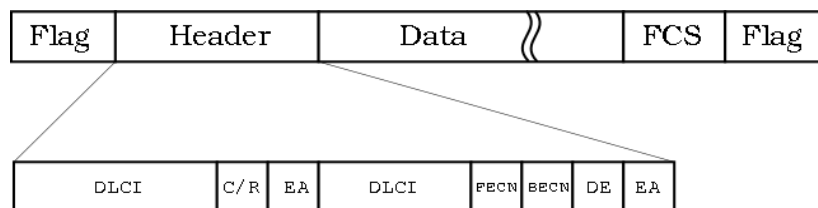
Na obr. 5.12 sú znázornené tvary rámcov protokolu PPP.



Obr. 5.12 Rámce protokolu PPP

5.10.3 Protokol Frame Relay

Frame Relay je technológia, ktorá slúži na prenos dát cez rozľahlé (WAN) siete. Prenášané dáta sú rozdelené na rámce a každý rámec obsahuje informáciu o tom, kam má byť doručený. Prepojovanie v uzloch je na úrovni linkovej vrstvy. Pretože sa Frame Relay sieť obvykle prevádzkuje na dátových spojoch s vysokou spoľahlivosťou, nepoužíva žiadnu metódu opravy chýb. Každý rámec je zabezpečený CRC kódom a pokiaľ tento odhalí poškodenie rámca pri prenose, je chybný rámec zahodený.

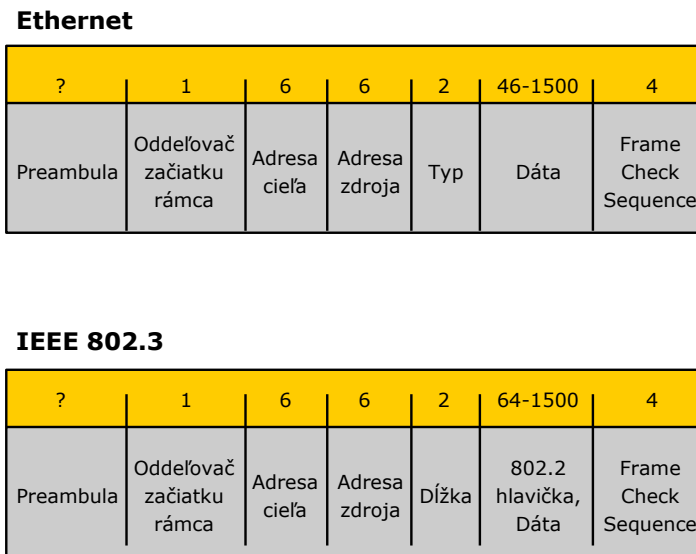


Obr.5.13 Formát rámca Frame Relay

5.10.4 Protokol Ethernet

Ethernet je najpoužívanejšia LAN technológia. Protokol Ethernet pôvodne vyvinuli firmy DEC, Intel a Xerox, neskôr bol Ethernet normalizovaný organizáciou IEEE ako norma 802.3. Rozdiely medzi Ethernetom a IEEE 802.3 sú malé. Ethernet poskytuje služby v súlade s OSI

modelom. IEEE 802.3 špecifikuje fyzickú vrstvu, prístup linkovej vrstvy, ale nedefinuje LLC protokol. Znázornenie rámcov je na obr. 5.14.



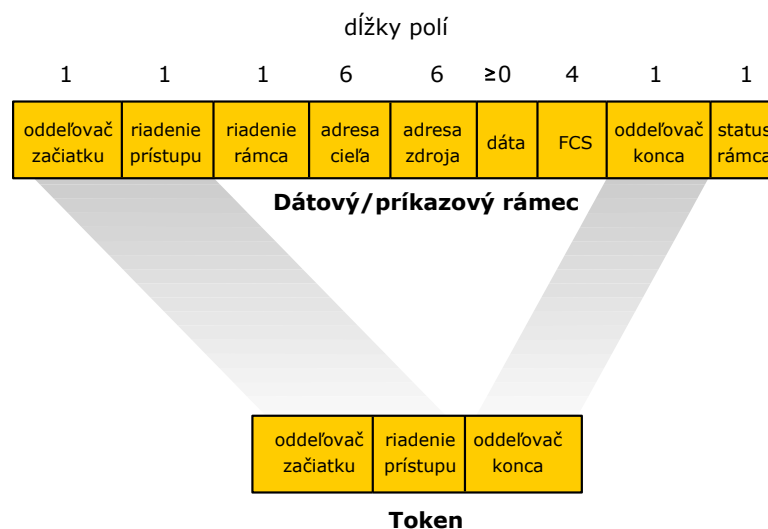
Obr. 5.14 Formát rámca Ethernet

5.10.5 Protokol Token Ring

LAN technológiu Token Ring vyvinula firma IBM v sedemdesiatych rokoch. V súčasnosti sú dva, takmer identické štandardy:

- IMB Token Ring
- IEEE 802.5

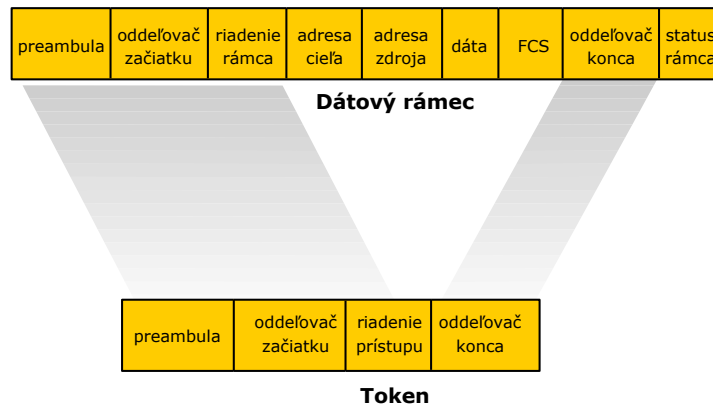
Formát rámca je znázornený na obr. 5.15.



Obr. 5.15 Formát rámca Token Ring

5.10.6 Protokol FDDI (Fiber Distributed Data Interface)

FDDI je normalizovaná normou ISO 9314. Zariadenia sú prepojené dvojitém kruhom čo zabezpečuje jej spoľahlivosť. Ako prenosové médium často používa optické vlákno. Prístupovou metódou je *Token Passing*. Používa dva typy prenosu - synchronný a asynchrónny. Príklad rámca v FDDI je na obrázku 5.16.



Obr. 5.16 Formát rámca v FDDI

5.11 Technické zariadenia linkovej vrstvy

Medzi komponenty komunikačných sietí, ktoré pracujú na linkovej vrstve, patrí:

- sieťová karta
- bridge (most)
- switch (prepínač, viacportový bridge)

Všetky tieto zariadenia sú aktívnymi prvkami siete.

5.11.1 Sieťová karta

Sieťová karta označovaná aj ako **NIC** (*Network Interface Card*) je komponent počítača, ktorý umožňuje komunikáciu počítača cez elektronickú komunikačnú sieť. Sieťová karta tvorí rozhranie medzi počítačom ako koncovým zariadením a komunikačnou sieťou. Sieťová karta obsahuje špecializované elektronické obvody, ktoré umožňujú komunikáciu na úrovni fyzickej a linkovej vrstvy OSI modelu. V pamäti sieťovej karty je uložený firmware, ktorý zabezpečuje riadenie logického spoja a riadenie prístupu na spoločné médium na úrovni linkovej vrstvy.

Najviac používané sú ethernetové sieťové karty. Výrobca kariet prideluje karte MAC adresu. V 48 bitovom identifikátore prvá časť identifikuje výrobcu, druhá časť zaisťuje jedinečnosť adresy v sieti. Ak sa vyskytnú v sieti dve rovnaké sieťové karty, je možné adresu nastaviť inak pomocou špeciálneho programu.

Iné technológie, napríklad ATM majú iný formát adresy.

Sieťové karty sa líšia v niektorých parametroch, napríklad, použité zariadenie (server, koncový počítač) typ siete (Ethernet, Token Ring, ATM,...), typ prenosového média (krútená dvojlinka, optický kábel, bezdrôtové pripojenie,...), prenosová rýchlosť.



Obr. 5.17 sieťová karta

5.11.2 Most (*Bridge*)

Most je zariadenie linkovej vrstvy, ktoré sa používa na prepojenie dvoch častí siete. Mostom sa oddeľuje prevádzka dvoch rôznych segmentov siete a tým sa znižuje zaťaženie siete. Mostom sú prenášané len tie rámce linkovej vrstvy, ktoré patria prepojenej sieti. Rámce, ktorých odosielateľ i príjemca sú v tej istej časti siete, most neprenesie. Most patrí na linkovú vrstvu preto, lebo sa riadi MAC adresami. Dnes sa však most používa už len výnimočne.

5.11.3 Rozbočovač (*HUB*)

HUB umožňuje vetvenie siete a v principiálne je to opakovač. Všetky prijaté dáta z jedného zariadenia posielajú ostatným zariadeniam, bez ohľadu na to, či sú im adresované. To má za následok preťaženie tých zariadení, ktorým dáta nie sú určené. Zariadenie sa nachádzajú v starších typoch sietí, postupne sú nahradzované prepínačmi (switch).



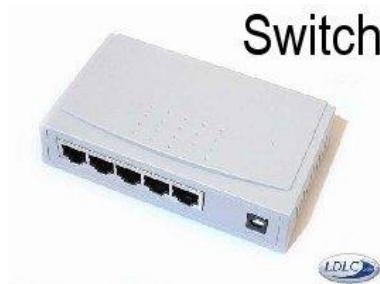
Obr. 5.18 Hub

5.11.4 Prepínač (*Switch*)

Prepínač je v podstate viacportový most na linkovej úrovni OSI modelu. Umožňuje prepojenie viacerých sietí. Adresovanie v prepínači je automaticky podľa adresy rámca. Každý rámec, ktorý odošlú pripojené zariadenia, prepínač prevezme a vyšle ho do toho portu,

v ktorom sa nachádza adresát rámca. V súčasnosti sú prepínače hlavným stavebným prvkom lokálnych počítačových sietí. Novšie prepínače sú vybavené bufferom a poskytujú aj iné funkcie, napríklad manažment siete, podporu virtuálnych sietí a pod..

Pojem switch sa používa aj v iných typoch sietí. Napríklad technológia ATM ho používa v úlohe smerovača na sieťovej vrstve.



Obr. 5.9 Switch

5.12 Záver

Linková vrstva poskytuje službu sieťovej vrstve tým, že pakety zo sieťovej vrstvy prenáša „zabalené“ v blokoch, ktoré nazývame **rámce**. Rámec je základnou komunikačnou jednotkou zariadení na linkovej vrstve. Prenos rámcov je realizovaný medzi dvomi komunikačnými bodmi siete a jeho základnou úlohou je bezpečný prenos bitov, ktorý linkovej vrstve poskytuje fyzická vrstva. Tvorba rámcov má špecifikované pravidlá tvorby, každá technológia však používa svoje vlastné štandardizované rámce.

Prenos rámcov v linkovej vrstve zabezpečuje prenos vo fyzickej vrstve, ktorá poskytuje túto službu linkovej vrstve. Zabezpečenie prenosu je realizované pomocou bezpečnostných kódov a riadením toku dát rámcov.

Kľúčové slová

1. Linková vrstva
2. Funkcie linkovej vrstvy
3. Služby linkovej vrstvy
4. Nepotvrdená nespojovaná služba (unacknowledged connectionless service)
5. Potvrdená nespojovaná služba (acknowledged connectionless service)
6. Spojovaná služba (connection-oriented service)
7. Linkové rámce
8. Tvorba linkových rámcov
9. Návestie rámca
10. Vkladanie bajtov (byte stuffing)
11. Vkladanie bitov (bit stuffing kladanie bitov (bit stuffing))
12. Zabezpečenie proti chybám
13. Bezpečnostné kódy
14. Metódy spätnej väzby
15. Zabezpečenie paritou
16. CRC (*Cyclic Redundancy Check*)
17. Podvrstvy linkovej vrstvy
18. Vrstva riadenia logického spojenia – LLC
19. Vrstva riadenia prístupu na médiá – MAC
20. Riadenie prístupu k spoločnému komunikačnému médiu
21. Prístupová metóda
22. Stochastické prístupové metódy
23. Deterministické prístupové metódy

- | | |
|---|---|
| <p>24. CSMA (<i>Carrier Sense Multiple Access</i>)</p> <p>25. TDMA (<i>Time Division Multiple Access</i>)</p> <p>26. FDMA (<i>Frequency Division Multiple Access</i>)</p> <p>27. WDMA (<i>Wavelength Division Multiple Access</i>)</p> <p>28. CDMA (<i>Code Division Multiple Access</i>)</p> <p>29. MAC adresovanie (MAC address)</p> <p>30. Riadenie toku</p> | <p>31. Opravy prenosu rámcov</p> <p>32. Linkové protokoly</p> <p>33. Pole začiatok rámca</p> <p>34. Adresné pole</p> <p>35. Polia dĺžka/typ</p> <p>36. Dátové polia</p> <p>37. Kontrolné číslo</p> <p>38. Pole koniec rámca</p> <p>39. Štandardy pre vytváranie rámcov</p> <p>40. Formát rámcov v Ethernete</p> <p>41. HDLC protokol</p> <p>42. Rámce Frame Relay</p> |
|---|---|

Kontrolné otázky

1. Ktoej úrovni poskytuje služby linková vrstva a ako?
2. Ktorá úroveň poskytuje služby linkovej úrovni a ako?
3. Čo je základnou funkciou linkovej vrstvy?
4. Ktoré z vymenovaných špecifických funkcií patria linkovej vrstve?
5. Medzi akými bodmi v sieti sú používané mechanizmy linkovej vrstvy?
6. Aký charakter môžu mať služby poskytované na linkovej vrstve?
7. Ktoré z charakteristík patria nepotvrdzovanej nespojovanej službe (*unacknowledged connectionless service*) ?
8. Ktoré z charakteristík patria potvrdenej nespojovanej službe (*acknowledged connectionless service*)
9. Ktoré z charakteristík patria spojovanej službe (*connection-oriented service*)
10. Čo znamená označenie linkový rámec (line frame)?
11. Ktoré sú základné časti/polia rámca?
12. Aká komunikačná jednotka sa balí do rámca?
13. Čo znamená encapsulácia na linkovej vrstve?
14. Ako sa uskutočňuje decapsulácia v linkovej vrstve?
15. Čo znamená vkladanie bajtov/znakov (byte stuffing) do rámca?
16. Prečo sa uskutočňuje vkladanie bajtov do rámca?
17. Čo znamená vkladanie bitov (*bit stuffing*) do rámca?
18. Ktoré základné spôsoby zabezpečenia proti chybám sa používajú v komunikačných technológiách?
19. Aký je rozdiel medzi detekčnými a korekčnými kódmi?
20. Ktoré dva druhy kódov sa najčastejšie používajú na linkovej vrstve?
21. Ktoré z vyjadrení platí pre zabezpečenie paritou?
22. V čom je hlavný nedostatok pri zabezpečení paritou?
23. Čo znamená označenie CRC?
24. V čom spočíva princíp CRC?
25. K čomu sú určené prístupové metódy?
26. Aké je základné delenie prístupových metód?
27. Ktoré prístupové metódy patria k stochastickým metódam?
28. Ktoré prístupové metódy patria k deterministickým metódam?
29. V čom je rozdiel medzi stochastickými a deterministickými prístupovými metódami?

30. Ako je špecifikovaná linková úroveň v LAN?
31. Prečo je v linková úroveň v LAN rozdelená na dve podvrstvy?
32. čo je hlavnou úlohou podvrstvy LLC – Logical Link Control?
33. Čo je hlavnou úlohou podvrstvy MAC – Media Access Control?
34. Akým spôsobom je riadený prístup komunikujúcich zariadení na spoločné prenosové médium?
35. Čo znamená označenie MAC adresa?
36. Ktoré z označení sú iné označenia MAC adresy?
37. Kto prideliuje MAC adresy?
38. V akom tvare sa vyjadrujú MAC adresy?
39. Z akého dôvodu sa na linkovej vrstve uskutočňuje riadenie toku dát?
40. Ktoré z vymenovaných spôsobov/mechanizmov sú používané pri opravách prenášaných rámcov?
41. Ktoré z vymenovaných polí sú základné polia linkového rámca?
42. Aký je význam poľa začiatok rámca?
43. Čo je vyjadrené v poli adresa?
44. Aký je význam poľa kontrolné číslo - *Frame Check Sequence (FCS)*?
45. Aký je význam poľa koniec rámca?
46. Kto, resp. čo určuje typ rámca pre konkrétnu technológiu?
47. Prečo existuje viac typov rámcov?

6 Sieťová vrstva (*Network layer*)

Ciele učenia

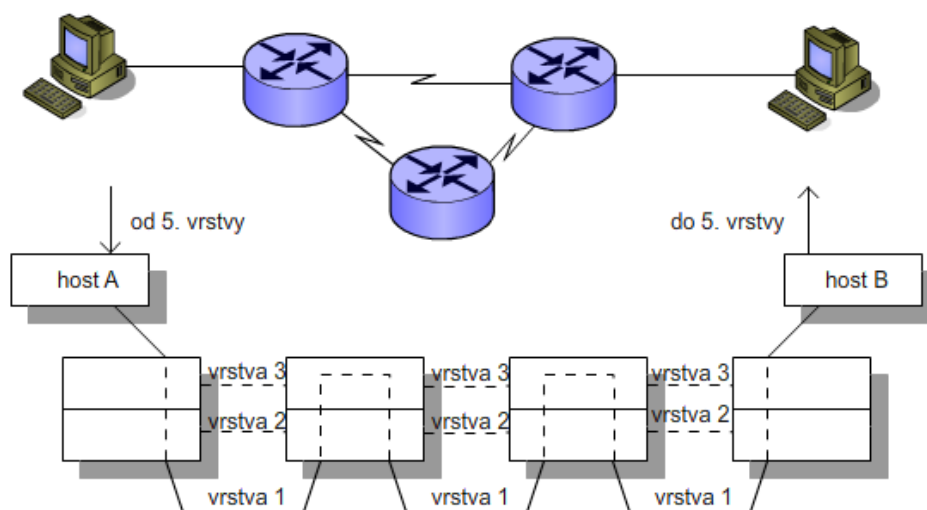
Čo by mal študent vedieť:

- spoluprácu sieťovej vrstvy so susednými vrstvami, prenos medzi transportnými entitami, fragmentácia správ a tvorba paketov
- základné funkcie sieťovej vrstvy: prepojovanie (*switching*), smerovanie (*routing, forwarding*), adresácia (*addressing*), spojovanie (*connecting*), signalizácia (*signalling*)
- spôsoby prepojovania v sieti, spôsoby adresovania, smerovacie tabuľky
- služby sieťovej vrstvy: spojovo a nespojovo orientované siete a služby
- riadenie toku dát, zabezpečenie pred zahltením siete
- protokoly sieťovej vrstvy
- zariadenia sieťovej vrstvy

6.1 Úvod

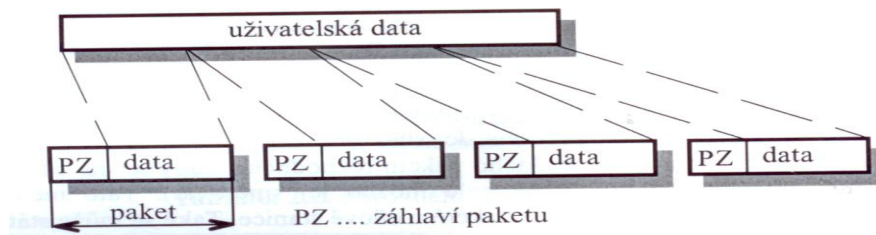
Pri vzniku potreby komunikácie medzi dvoma zariadeniami, ktoré nemajú priame spojenie, je potrebné nájsť spojenie prostredníctvom iných uzlov. Takýchto spojení môže byť viac a je úlohou **sieťovej vrstvy** vybrať jednu prenosovú cestu, ktorá zaistí správne prenesenie dát.

Úloha sieťovej vrstvy vo vzťahu susedných vrstiev je nasledovná. Sieťová vrstva dostane od transportnej vrstvy dáta, ktoré obsahujú informáciu o tom, kto je konečným príjemcom dát. Sieťová vrstva potom identifikuje koniec komunikačného systému pre transportnú vrstvu pomocou sieťovej adresy. Sieťová vrstva musí rozhodnúť, ktorým smerom budú dáta odosielané. Rozhodnutie o smerovaní odovzdá príslušnej linkovej vrstve spolu s informáciou o zvolenom smere. Umiestnenie sieťovej vrstvy je na obr. 6.1.



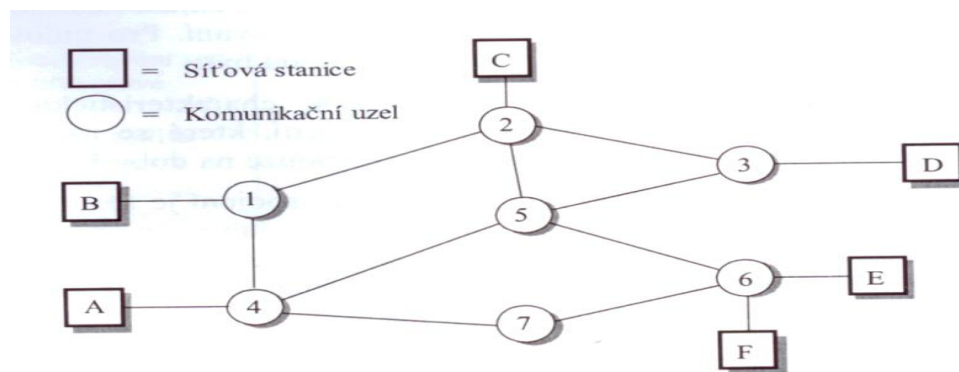
Obr. 6.1 Umiestnenie sieťovej vrstvy

Komunikačná jednotka na sieťovej vrstve je tvorená blokom dát, označovaným **paket**. Pakety sú vytvárané z používateľských dát postupom uvedeným na obr. 6.2



Obr. 6.2 Vytváranie paketov na sieťovej vrstve

Každý paket obsahuje svoju **hlavičku**, v ktorej sú **riadiace informácie**, a časť používateľských dát. Konkrétne znázornenie paketu a jeho riadiacich informácií je závislé od konkrétnej protokolovej špecifikácie jednotlivých technológií. Na základe riadiacich informácií je paket smerovaný v uzloch siete, napríklad podľa obrázku 6.3 v topológii neúplného polynómu.



Obrázok 6.3 Uzly ako základné časti sieťovej vrstvy

Sieťová vrstva takto poskytuje špecifické funkcie a služby transportnej vrstve, ktorá poskytuje transparentný prenos dát medzi dvomi koncovými zariadeniami. **Funkcie sieťovej vrstvy sú zabezpečované v medziľahlých uzloch a spojenie môže byť uskutočňované cez viaceré typy sietí**, cez ktoré je vytváraný komunikačný kanál medzi zdrojom a príjemcom správy.

Sieťová vrstva zodpovedá za prepojovanie v sieťach nezávisle od ich typu. Cieľom je umožniť každému koncovému zariadeniu komunikovať s iným koncovým zariadením, bez ohľadu na to, v akom type siete sú pripojené. Komunikačný kanál môže byť vytvorený cez rôzne komunikačné uzly, ktoré patria jednej alebo niekoľkým sieťam. Výsledkom je potom sústava navzájom prepojených sietí, cez ktoré je uskutočňovaná komunikácia. Sieťová vrstva prenáša pakety cez medziľahlé uzly tak dlho, pokiaľ ich nedoručí príjemcovi. V medziľahlých uzloch vykonáva sieťová vrstva **hľadanie vhodnej prenosovej cesty** a vytvára potrebný **komunikačný kanál**.

Pretože prenosový kanál, ktorý vytvára sieťová vrstva môže byť tvorený rôznymi technológiami, je potrebné riešiť **problém veľkosti prenášaných paketov**. Každá

technológia prenášajúca pakety, má istú maximálnu veľkosť prepravovaného paketu označovanú MTU (*Maximum Transmission Unit*). Napríklad v technológii Ethernet je táto hodnota 1500 bajtov. Medzi niektorými uzlami siete môže byť MTU nastavené na nižšiu, alebo naopak na vyššiu hodnotu. Preto pri smerovaní paketu do prenosového kanála s nižším MTU, je uskutočnená fragmentácia (*fragmentation*) paketu. V hlavičke všetkých fragmentov okrem posledného je nastavený príznak *More fragments*. Opačný postup k fragmentácii je označovaný defragmentácia (*reassemble*). Týmto postupom sa fragmenty spájajú do pôvodného paketu.

Sieťová vrstva je poslednou vrstvou OSI modelu, ktorá súvisí iba s komunikačnou sieťou. Sieťová a transportná vrstva tvoria **rozhranie** medzi používateľom a sieťou. Služby prvých troch úrovní OSI modelu sa súhrnne označujú ako **nosné služby alebo služby prenosu, anglicky *bearer services***. Sú poskytované prevádzkovateľmi/operátormi elektronických komunikačných sietí.

6.2 Funkcie sieťovej vrstvy

Základnou funkciou sieťovej vrstvy je spolupráca so susednými vrstvami, čo znamená, že poskytuje službu transportnej vrstve, ktorá požaduje preniesť správu od jedného zdrojového zariadenia k cieľovému zariadeniu. V tomto prípade sa informácia, ktorá začína v jednom uzle (zdrojovom), prenesie do druhého uzla (cieľového). Takéto riešenie je však možné len pri sieťach s malým počtom uzlov. V prípade rozľahlých sietí je potrebné pri spojení uzlov, ktoré nemajú priame spojenie, prechádzať cez jeden alebo viac medzilahlých uzlov. V takomto prípade musia medzilahlé uzly zabezpečiť **prepojovanie (*switching*)**, čo znamená zabezpečiť, že informácia ktorá do uzla prichádza, odíde z neho k ďalšiemu uzlu. Takýto spôsob umožňuje to, že všetky sieťové prostriedky (uzly a komunikačné okruhy) môžu využívať viacerí používatelia.

Pretože väčšina sietí má komplikovanú architektúru a väčšinou existuje viac možností ako sa dostať z jedného uzla do druhého, musí sieť vykonávať okrem prepojovania ďalšiu funkciu, **smerovanie (*routing*)**. Na to, aby bol požadovaný cieľ identifikovaný, musí mať pridelenú určitú identifikáciu (meno, číslo, adresu), čo znamená ďalšiu funkciu **adresovanie (*addressing*)**. V niektorých typoch sietí je prepojovanie do požadovaného smeru je vykonané prostredníctvom signalizácie a následného spojovania vstupu uzla s výstupom podľa údajov nastavených v smerovacích tabuľkách. Prepojovanie tak obsahuje dve funkcie spojovanie (*connecting*) a signalizácie (*signalising*).

Vytvorenie prenosovej cesty pre koncové zariadenia poskytuje sieťová vrstva na základe špecifických služieb, ktorými sú:

- Prepojenie (Switching)
- Smerovanie (Routing)
- Adresovanie (Addressing)
- Signalizácia (Signalising)

- Spojovanie (Connecting)
- Riadenie toku (Flow Control)

6.2.1 PREPOJOVANIE (SWITCHING)

Pojem prepojovanie (*switching*), označuje zostavovanie okruhov potrebných na prenos informácie zo zdroja do cieľa cez komunikačnú sieť. V skutočnosti ide o zostavovanie dielčích častí, ktoré dočasne poskytnú okruh pre prenos informácie.

Komunikačné okruhy sa vytvárajú buď **pevné**, kedy medzi komunikujúce zariadenie nie je vložené žiadne prepojovacie zariadenie, alebo **komutované** (s prepojovaním). Pevné okruhy sú buď trvalé alebo sa prenajímajú na vopred dohodnutú dobu. Komutované okruhy sa vytvárajú v komutačných sieťach na žiadosť vysielacieho komunikujúceho zariadenia vždy len na dobu nevyhnutnú pre komunikáciu. V paketových sieťach sa nevytvárajú **fyzické okruhy**, ale len **virtuálne okruhy**. Ich rozdiel bude vysvetlený neskôr.

V komunikačných sieťach sa špecifikujú tri spôsoby prepojovania:

1. prepojovanie okruhov/kanálov, (*circuit switching*),
2. prepojovanie paketov, (*packet switching*),
3. prepojovanie správ (*message switching*).

6.2.1.1 Prepojovanie okruhov

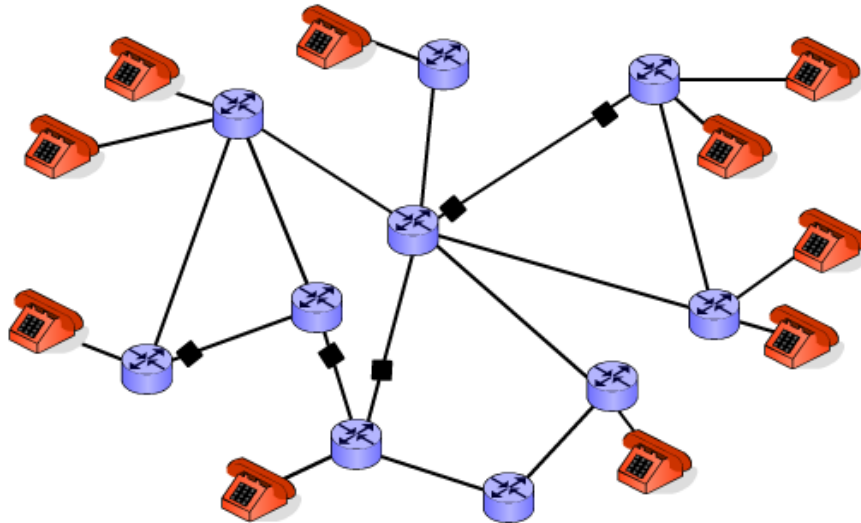
Prvú formu prepojovania predstavovali v minulosti telefónne spojovateľky. Účastník jednoducho zdvihol mikrotelefón a požiadal spojovateľku o sprostredkovanie spojenia k inému účastníkovi. Spojovateľka prepojovacou šnúrou prepojila účastnícku linku volajúceho s volaným. I keď dnes spojenie v komunikačných sieťach vykonávajú automatické telefónne ústredne alebo počítače, možno prepojovanie okruhov prirovnať k tomuto mechanizmu.

Prepojovanie okruhov sa delí na **priestorové** a **časové**. Priestorové prepojovanie bolo v klasických ústredniach s mechanickými, elektromechanickými alebo elektronickými prvkami. Časové prepojovanie vychádza z podstaty časového delenia tým, že sa zo spoločného časového rámca vydeľujú časové úseky do rôznych smerov (TDM, *Time Division Multiplex*).

Prepojovanie okruhov je založené na tom, že pred tým, než môže začať samotný prenos informácie medzi koncovými zariadeniami, musí byť zostavený medzi nimi okruh, po ktorom sa bude informácia prenášať. Dochádza k prepojoванию prenosových úsekov tak, aby medzi dvoma prístupovými bodmi k sieti vznikol jediný prenosový okruh, znázornenie obr. 6.4.

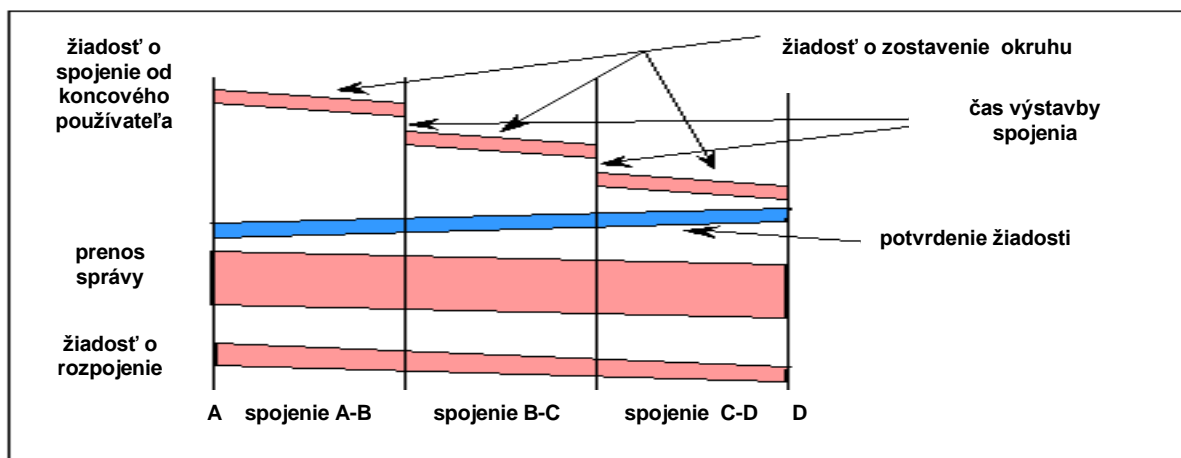
Okruh musí byť najprv zostavený na žiadosť toho, kto spojenie cez komunikačnú sieť iniciuje a potom existuje až do tej doby, než je opätovne rozpojený. Obidve koncové zariadenia spojenia majú po celú dobu komunikačný okruh výlučne iba pre seba. Prenos informácií po vytvorení okruhu môže byť uskutočňovaný akýmkoľvek spôsobom, telefónnou službou, službou prenosu dát,... Pritom pre každé spojenie je vyhradený kanál s pevnou šírkou pásma respektíve prenosovou rýchlosťou, aké sa v danom type siete s danou

technológiou používajú. Kanál je vždy pevne priradený danej dvojici používateľov a v tomto čase ho nemôže používať nikto iný.



Obr. 6.4 Prepojovanie okruhov

Každá komunikácia v sieti s prepojuvaním okruhov začína fázou zostavenia (vytvorenia) spojenia medzi zdrojovým a cieľovým zariadením a končí jeho zrušením (rozpojením). Tieto fázy sú ilustrované na obr. 6.5.



Obr. 6.5 Fáza komunikácie pri prepojuvaní okruhu

Výhody prepojovania okruhov

- pevná šírka pásma, konštantná rýchlosť prenosu nezávislá od zaťaženia siete,
- malé a takmer konštantné oneskorenie, po vytvorení spojenia sa správa prenáša takmer bez oneskorenia,
- garancia kvality služby,
- jednoduché spoplatňovanie za službu pre operátora,
- pre každé spojenie je vyhradený samostatný kanál (okruh), komunikujúci sa nedelí o kanál s inými používateľmi.

Nevýhody prepojovania okruhov

- používateľ platí za okruh i keď neprenáša dáta,
- iní používatelia nemôžu využiť okruh i keď sa po ňom nič neprenáša,
- keď sú obsadené všetky komunikačné okruhy, siete odmietajú žiadosti o nové spojenie,
- zostavovanie a rušenie spojenia vyžaduje prídavnú réžiu.

Použitie sietí s prepojením okruhov

Siete s prepojením okruhov sa používajú pri klasickej telefónnej službe. Sú výhodné pre služby vyžadujúce prenos v reálnom čase. Len zriedka sa používa pre prenos dát.

6.2.1.2 Prepojovanie paketov

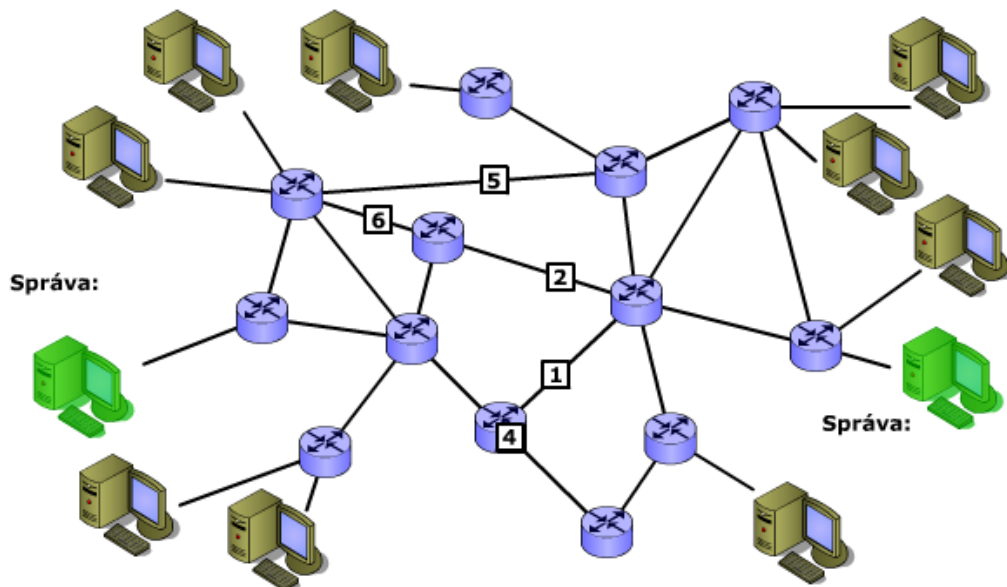
Princíp prepojovania paketov je založený na tom, že prenášaná správa sa rozdelí do bloku dát určitej dĺžky, ktoré sa nazývajú pakety (*packets*). Každý paket sa doplní o niektoré ďalšie údaje (adresa odosielateľa a adresa príjemcu, poradové číslo paketu a iné). Adresa zdroja a cieľa plus poradové číslo paketu tvoria hlavičku paketu (*header*). Pakety sa prenášajú komunikačnou sieťou podľa princípov smerovania sieťovej vrstvy. Nevzniká tu žiadny skutočný fyzický okruh medzi odosielateľom a príjemcom paketu. Jednotlivé vnútorné uzly komunikačnej siete si odovzdávajú pakety medzi sebou, pokiaľ ich nedoručia až do prístupového bodu, na ktorý je pripojený adresát paketu. Každý paket obsahuje všetky informácie, potrebné pre jeho smerovanie zo zdroja do cieľa a je v dátovom toku nezávislou jednotkou. V uzloch siete sú smerovacie tabuľky, podľa ktorých je určovaný smer paketu. Uzly siete s prepojením paketov vykonávajú funkciu vzájomne prepojených paketových prepojovačov (*switchov*). Paketový prepojovač, ktorý prijme paket, ho následne analyzuje a zistí ktorému ďalšiemu uzlu na prenosovej ceste paket patrí a tam ho smeruje. Všeobecne môžu pakety pri prenose prechádzať rôznymi smermi a tiež prísť v inom poradí než boli odoslané. Keď príde paket do cieľa, je jeho informácia o poradovom čísle paketu použitá na to, aby sa pakety zoradili znovu do pôvodného poradia. Prepojovanie paketov umožňuje aj prenos od jedného zdroja súčasne do viacerých cieľov (*multicasting*), čo pri prepojení okruhu nie je možné. Pri prepojení paketov môže vzniknúť oneskorenie, ktoré je spôsobené tým, že sa o rovnaký okruh môžu uchádzať pakety z rôznych zdrojov. Tento prípad sa rieši ukladaním paketu vo vyrovnávacej pamäti (*bufferi*) uzla. Pokiaľ kapacita vyrovnávacej pamäti nestačí, sú pakety zo siete vyradované.

6.3 Služby sieťovej vrstvy

Prepojovanie paketov môže byť realizované dvoma odlišnými spôsobmi, ktoré špecifikujú dve rôzne služby sieťovej vrstvy, **datagramovú službu a službu virtuálnych okruhov/kanálov**.

6.3.1 Datagramová služba (datagram service)

Datagramová služba znamená, že každý vnútorný uzol komunikačnej siete, ktorý prijme paket, sa vždy znovu rozhoduje o tom, kadiaľ ho má poslať ďalej. Ide o analógiu bežnej listovej pošty, v ktorej dátový paket odpovedá obálke listu, opatrenej adresou príjemcu a vnútorný uzol komunikačnej siete je triedička poštového úradu, ktorá triedi obálky podľa PSČ – poštového smerového čísla. Pritom sa môže stať, že pošta nedoručí všetky listy, prípadne doručovanie môže trvať rôzne dlhú dobu. Analógiu s listovou poštou symbolizuje i názov tohto spôsobu prepojovania paketov, ktorý sa označuje datagramová služba a dátové pakety sú označované **datagramy** (*datagrams*). Každý datagram má cieľovú adresu a komunikačná sieť pri prenose datagramu dokáže priebežne reagovať na svoje okamžité zaťaženie tak, že v prípade potreby volí rôzne alternatívne cesty prenosu. V dôsledku toho komunikačná sieť nezaručuje správne poradie doručovania jednotlivých datagramov. Môže sa stať, že použitím alternatívnych trás v komunikačnej sieti sa niektoré datagramy "predbiehajú" a nie sú doručené v poradí, v akom boli vysielané, obr. 6.6. Problém nastáva vtedy, ak má komunikačná sieť súčasne viac požiadaviek na prenos paketov. V niektorých prípadoch môžu byť pakety odmietnuté alebo vyradené zo siete. Datagramová služba tak negarantuje doručenie datagramu a takýto spôsob je nazývaný **nespoľahlivá** (*best effort*) služba.

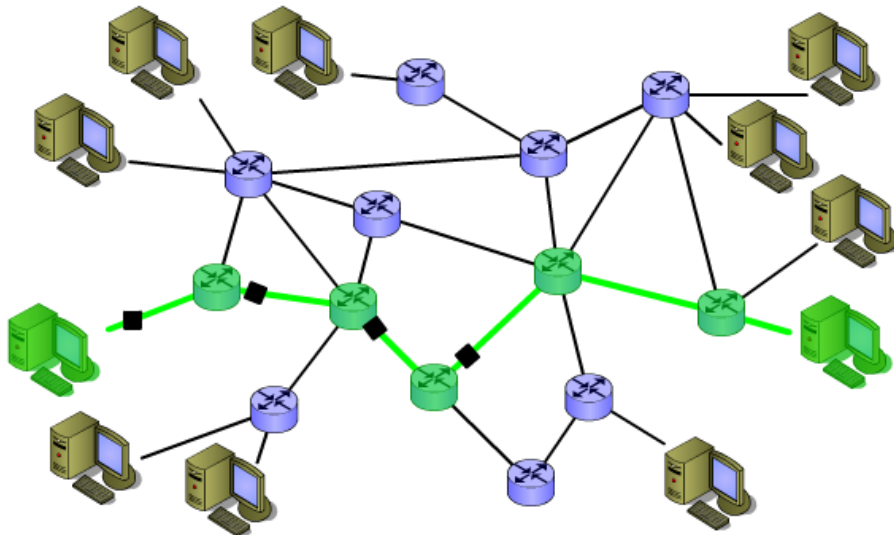


Obr. 6.6 Komunikačná sieť s datagramovou službou

6.4 Služba virtuálnych kanálov (virtual circuits service)

Služba virtuálnych kanálov je realizovaná tak, že najskôr sa od odosielateľa vyšle zvláštny paket, ktorý "vytýči" momentálne najvhodnejšiu cestu medzi obidvomi koncovými zariadeniami a informáciu o nej zanesie do každého vnútorného uzla, ktorý na tejto ceste leží. Vzniká tak analógia komunikačného okruhu ako pri prepojení okruhov, ale virtuálny okruh existuje len ako konvencia o tom, kadiaľ sa majú pakety prenášať. Preto je prívlastok "virtuálny". Ešte pred vlastným prenosom dát sa tak zvolí jedna pevná cesta od odosielateľa k

príjemcovi a po celú dobu prenosu sa potom používa práve a iba táto cesta, ako je znázornené na obr. 6.7. Túto cestu vytyčuje paket žiadosti o spojenie. Ten pri prechode sieťou zaistí všetkým paketom dátové správy o pridelení určitých čísiel pre jednotlivé úseky prenosovej cesty. Tieto čísla predstavujú číslo logického kanála. Pakety, ktoré sa prenášajú virtuálnym spojom, nie sú opatrené adresou svojho príjemcu, ale označením virtuálneho spoja, ktorý ich vedie k príjemcovi. Každý vnútorný uzol komunikačnej siete ktorý takýto paket prijme, podľa svojich smerovacích tabuliek zistí, kadiaľ príslušný virtuálny spoj pokračuje ďalej, a tým smerom prijatý paket opäť odovzdá. Tým, že sú všetky pakety prenášané po rovnakom virtuálnom okruhu, je zaručené, že do cieľa dorazia vždy v správnom poradí. Virtuálne okruhy sa zriaďujú až v okamihu potreby prenosu a po jeho dokončení sa zase zrušia. Virtuálne okruhy dynamicky vznikajúce podľa okamžitej potreby sa nazývajú komutované (*Switched Virtual Circuit - SVC*). Na **komutovaných virtuálnych okruhoch** sa tak komunikácia skladá z vytvorenia virtuálneho okruhu, z jeho vlastného využitia na komunikáciu a zrušenia virtuálneho okruhu vyslaním paketu záveru.



Obr. 6.4 Komunikačná sieť so službou virtuálnych okruhov

6.4.1 Porovnanie datagramovej služby a služby virtuálnych kanálov

Nevýhodou datagramovej služby je réžia, spojená s rozhodovaním o ďalšom smere prenosu a veľký počet služobných informácií v každom pakete. To je pri službe virtuálnych okruhov minimalizované.

Výhodou datagramovej služby je pružná reakcia na zmeny prevádzkového zaťaženia v sieti a topológie siete i relatívne krátky čas doručenia paketu.

6.4.1.1 Výhody prepojovania paketov

- sieťové prostriedky a kapacita prenosového média sú využívané efektívnejšie; jeden okruh môžu používať pakety z rôznych zdrojov,
- komunikujúce systémy môžu vysielat' a prijímať rôznymi prenosovými rýchlosťami,

- nie sú odmietané žiadosti o spojenie, pri nedostatočnej kapacite komunikačných kanálov sú pakety oneskorované,
- účastník platí iba za objem prenesených dát.

6.4.1.2 Nevýhody prepojovania paketov

- príliš veľa paketov môže spôsobiť zahltenie siete,
- nie je garantovaný čas doručenia paketu,
- oneskorenie paketu pri prenose sieťou je variabilné, pakety môžu prísť v rôznych časoch,
- pre služby v reálnom čase môžu nastať komplikácie spôsobené oneskorením a stratou paketov.

Použitie prepojovania paketov

Na paketovom spôsobe prepojovania sú dnes založené siete protokolu TCP/IP, X.25, Frame Relay, ATM. Prepojovanie paketov sa dnes používa tak v lokálnych sieťach (*LAN, Local Area Network*), ako aj v rozľahlých sieťach (*WAN, Wide Area Network*).

Paketové siete sa stali základom internetu. Paketová komunikácia je v poslednom období aj mobilných sieťach. Prepojovanie paketov je v technológiách GPRS a 3G.

6.5 Smerovanie

Smerovanie (routing) je základnou funkciou sieťovej vrstvy. Rozhoduje o smere odosielania jednotlivých paketov v uzloch siete. Smerovanie je spôsob, akou prenosovou cestou sa paket dostane z určitého miesta siete na iné miesto.

Funkciu smerovania možno prirovnať k triedeniu listov na pošte. Pri smerovaní v komunikačných sieťach sa netriedia listy, ale pakety alebo datagramy.

Spôsob smerovania závisí od použitého smerovacieho protokolu. Smerovanie používa dva princípy:

- **Zdrojové smerovanie** (*source routing*), v ktorom celá informácia o tom ako sa paket dostane k cieľu je daná zdrojom. Úlohou uzla siete je analyzovať informáciu z paketu a určiť ďalší smer.
- **Hop-by-hop routing**, kde zdroj nemá informáciu ako sa paket dostane k cieľu, ale iba o tom, ako sa dostane k ďalšiemu uzlu. Prenos paketov medzi susednými uzlami znamená **posun** – *next-hop* paketu k nasledujúcemu uzlu.

Rozlišuje sa tak medzi pojmami *routing* - smerovanie a *forwarding* - poslanie ďalej. *Routing* znamená celkový proces získania a distribúcie informácie o smerovaní paketu komunikačnou sieťou, *forwarding* použije získanú informáciu o smerovaní na to, aby sa paket dostal z jedného uzla do druhého. *Routing* je tak výsledok opakovaného *forwardingu*.

Zariadenie, ktoré tento proces vykonáva sa označuje **smerovač (router)**. Smerovač „vyberie“ z linkového rámce paket, určí jeho smer a dá ho do iného linkového rámce. Na

každom rozhraní smerovača môže byť iný linkový protokol, ale aj keď sú linkové protokoly rovnaké dochádza k „vybratiu“ paketu, jeho smerovaniu a uloženiu do ďalšieho linkového rámca.

Pre potreby smerovania musí mať sieťová vrstva základné informácie o topológii celej siete, ako aj ďalšie parametre statického a aj dynamického charakteru, podľa ktorých sa uskutočňuje smerovanie. Existuje množstvo konkrétnych **spôsobov smerovania**, ktoré predstavujú rôzne **algoritmy smerovania** (*routing algorithms*). Od jednoduchých statických metód, ktoré nie sú schopné reagovať na dynamické zmeny v sieti, až po adaptívne metódy, ktoré dokážu prispôbiť aktuálnemu stavu siete, jej zaťaženiu, prípadným výpadkom niektorých uzlov či spojení a podobne.

Algoritmy smerovania by mali byť čo najjednoduchšie, najľahšie implementovateľné a ich réžia by mala byť minimálna. Súčasne s tým by algoritmy smerovania mali byť schopné vyrovnávať sa s nepredvídanými výpadkami, poruchami či inými neštandardnými situáciami. Mali by optimalizovať využitie celej siete a jej prenosovej kapacity.

Algoritmy smerovania môžeme deliť na dve skupiny:

- **adaptívne algoritmy** (*adaptive algorithms*) – dokážu sa prispôbiť okamžitému stavu siete,
- **neadaptívne algoritmy** (*nonadaptive algorithms*) – používajú informácie statického charakteru (*static routing*).

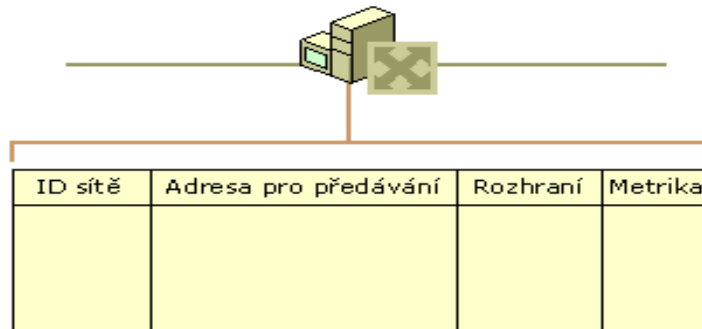
Adaptívne algoritmy smerovania môžeme rozdeliť do niekoľkých skupín:

- Centralizované smerovanie, pri ktorom sú informácie o smerovaní zo všetkých uzlov ukladané v *Routing Control Center*.
- Izolované smerovanie, v ktorom je rozhodovanie o smerovaní určované v každom uzle samostatne.
- Spätné učenie, pri ktorom sa zaznamenávajú informácie z uzlov od ktorých boli prijaté pakety a na základe záznamov sa pakety smerujú.
- Záplavové smerovanie, pakety sa vysielajú na všetky smery s výnimkou smeru z ktorého paket prišiel.
- Distribuované smerovanie, v ktorom sa informácie o zmenách odovzdávajú postupne medzi susednými uzlami, až sa rozšíria po celej sieti.

Výber príslušného smerovacieho algoritmu závisí od použitej technológie. Výsledným efektom aplikácie algoritmov smerovania má byť to, aby sieťová vrstva v každom z uzlov siete smerovala prijatý paket čo najefektívnejšie.

Konkrétne pokyny pre smerovanie paketov, ktoré vznikajú na základe aplikácie algoritmov smerovania, sa v jednotlivých uzloch uchovávajú vo forme **smerovacích tabuliek** (*routing tables*). Smerovacia tabuľka je sústava položiek, ktoré sa označujú ako trasy a obsahujú informácie o tom, kde sú umiestnené jednotlivé identifikátory siete dostupné v prepojených sieťach. Rozhodnutie o trase, po ktorej budú pekety smerované, závisí od znalosti sieťových adries a od použitých smerovacích algoritmov. Smerovacie tabuľky sa

nachádzajú v smerovačoch a slúžia na vyhľadávanie optimálnej trasy. Základné položky smerovacej tabuľky sú znázornené na obr. 6. 5.



Obr. 6.5 Položky smerovacej tabuľky

- **ID siete** je identifikátor prenosovej cesty alebo adresa v štruktúre prepojených sietí.
- **Cieľová adresa** na ktorú má byť paket prenesený.
- **Rozhranie** označuje sieťové rozhranie pre odovzdanie paketu.
- **Metrika** vyjadruje mieru uprednostnenia danej trasy, pre smerovanie je použitá najnižšia metrika – najvhodnejšia trasa.

Rovnako ako smerovacie protokoly aj smerovacie tabuľky sú dvoch typov: statické a dynamické.

Statické smerovacie tabuľky sú dopredu definované, respektíve naprogramované, a počas prenosu sa nemenia. Toto má síce za následok vyššiu rýchlosť smerovania, ale menšiu flexibilitu v prípade dynamických rekonfigurácií siete.

Dynamické smerovacie tabuľky sa flexibilne prispôbujú zmenám v sieti, čo však spôsobuje pomalšie spracovanie dát pre prenos.

Podľa vzniku záznamu v smerovacej tabuľke rozlišujeme smerovanie na:

- **Statické**, kde sú smerovacie tabuľky vytvorené správcom siete a nie sú počas prenosu menené. Používajú sa v koncových zariadeniach alebo v smerovačoch malých počítačových sietí LAN.
- **Dynamické (adaptívne)**, pri ktorom sa obsah smerovacích tabuliek mení podľa typu smerovacieho protokolu. Sú používané v transportných sieťach.

6.6 Adresovanie

Adresovanie slúži na identifikáciu prvkov komunikačnej siete. **Adresa (Address)** je identifikátor priradený sieti, koncovému alebo inému zariadeniu pre jednoznačné určenie odosielania a prijímania správ. Adresa môže byť dátová štruktúra alebo iná logická konvencia. Adresy sú priradené koncovým používateľským zariadeniam a aj uzlom siete. V rozľahlých sieťach existuje hierarchické adresovanie uzlov. Uzol v sieti je identifikovaný svojou adresou, identifikačným číslom, identifikátorom, a pod. Používateľské koncové

zariadenia sú identifikované účastníckym číslom, IP adresou, a pod., v závislosti od technológie siete.

Typickým príkladom hierarchického adresovania, je telefónna sieť. Telefónne číslo používa kód krajiny (*hop*), nasledujúce dve čísla mesto (*next hop*) a zostávajúce číslice cieľovú telefónnu stanicu (*last hop*).

Sieťová vrstva môže pracovať aj nad viacerými sieťami, ktoré majú **rôzne adresovanie**. K tomuto účelu je potrebná spolupráca pri preklade adres medzi dvomi formátmi rôznych technológií. Technika umožňujúca rôznym protokolom preklad adres sa označuje **mapovanie adresy (*address mapping*)**. Používaná je napríklad pri smerovaní IP protokolov v sieťach s technológiou ATM (*Asynchronous Transfer Mode*), kde sa IP adresa mapuje do ATM adresy, aby IP pakety mohli byť prenesené ATM sieťou. Inou technikou používanou pri riešení rozdielov medzi rôznymi schémami adres je **rozlíšenie adresy (*address resolution*)**. Táto technika špecifikuje metódy pre mapovanie sieťovej adresy sieťovej vrstvy do adresy linkovej vrstvy.

6.6.1 Adresovanie v rôznych typoch sietí

Adresovanie v LAN sieťach je realizované MAC adresami na podvrstve MAC linkovej vrstvy. MAC adresa označuje jedinečnosť zariadenia vo vlastnej sieti, ale aj každé pripojenie zariadenia do vyšších hierarchických štruktúr, k mostom, smerovačom. MAC adresa v LAN je funkciou linkovej vrstvy a je popísaná v kapitole 5.

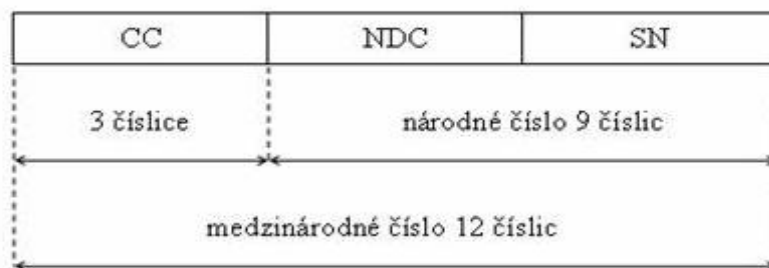
6.6.2 Adresovanie v telefónnych sieťach

V rozľahlých sieťach je adresovanie rozdielne podľa technológie, ktorú daná sieť používa. **Rozdielnosť adresovania** je rôzna aj podľa toho, či ide o **siete s prepojovaním okruhov** alebo **s prepojovaním paketov**. Ďalšia **rozdielnosť adresovania** je, či ide o **spojovanú**, alebo **nespojovanú** službu v určitej sieti. Adresovanie v sieťach so spojovanou službou je podstatne jednoduchšie, pretože kanál je vytvorený pevne, alebo je prednastavený na začiatku relácie vytyčovacím paketom. Naopak služba bez spojenia musí zaistiť úplnú adresáciu každého paketu.

6.6.2.1 Adresovanie vo verejnej telefónnej sieti

Verejná telefónna sieť používa rôzne technológie, ktoré spoločne poskytujú telefónnu službu a preto majú spoločný číslovací plán (*Network Routing Numer – NRN*), ktorý je vypracovaný na základe odporúčaní ITU a ETSI. Číslovací plán pre Slovenskú republiku vypracováva Telekomunikačný úrad Slovenskej republiky. Aktuálne opatrenie Telekomunikačného úradu Slovenskej republiky z 1. februára 2007 č. O - 14/2007 o číslovacom pláne je na linke <http://www.teleoff.gov.sk/index.php?ID=202>.

Vo **verejnej pevnej telefónnej sieti** sú účastníci identifikovaní účastníckymi číslami. Formát čísla je daný odporúčaním ITU-T, E.164. Štruktúra medzinárodného čísla vo verejnej telefónnej sieti v Slovenskej republike je na obr. 6.7.

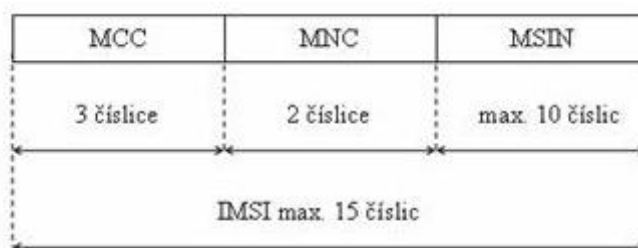


CC - medzinárodné smerové číslo
 NDC - národný cieľový kód
 SN - účastnícke číslo

Obr. 6.7 Štruktúra medzinárodného čísla vo verejnej telefónnej sieti

Dĺžka účastníckeho čísla nesmie byť väčšia ako 12 číslic, bez medzinárodného prefixu 00. Uzly sú identifikované smerovým číslom. Medzinárodné smerové číslo Slovenskej republiky je 421. Pri volaniach z národnej do medzinárodnej siete sa volí rozlišovacie číslo „00“.

Identifikáciu mobilného účastníka vo **verejnej mobilnej telefónnej sieti** sa používa identifikačný kód mobilného účastníka, ktorého štruktúra je definovaná v odporúčaní ITU-T E.212 a v slovenskej technickej norme STN ETS 300 523. Štruktúra medzinárodného identifikačného kódu mobilného účastníka je na obr. 6.8.



MCC - medzinárodné smerové číslo mobilnej siete
 MNC - kód mobilnej siete
 MSIN - identifikačné číslo mobilného účastníka
 IMSI - medzinárodný identifikačný kód mobilného účastníka

Obr. 6.8 Štruktúra medzinárodného identifikačného kódu mobilného účastníka

Medzinárodný identifikačný kód sa skladá z trojmiestneho medzinárodného smerového čísla mobilnej siete, dvojmiestneho kódu mobilnej siete a identifikačného čísla mobilného účastníka. Medzinárodný identifikačný kód mobilného účastníka má najviac 15 číslic.

6.6.2.2 Adresovanie v sieti internet

Adresa v internete je určená pre adresovanie medzi sieťami (internet je zložený z viac sietí) a pre doručenie správy koncovému používateľovi. Sieť internet používa na sieťovej vrstve IP (Internet Protocol). Dnes je najčastejšie používaná štvrtá verzia internet protokolu IPv4, postupne sa prechádza na novšiu verziu IPv6. IP protokol využíva princíp datagramovej služby prepojovania paketov a definuje mechanizmus pre adresovanie konkrétnych zariadení

siete. Pojem zariadenie siete v kontexte siete internet, je označované aj inými názvami: počítač, host, stanica, sieťové rozhranie, uzol, systém.

V sieti internet je každé zariadenie siete identifikované unikátnou sieťovou IP adresou (Internet Protocol Address). Adresy sú pridelované celosvetovo organizáciou IANA (Internet Assigned Numbers Authority), ktorá deleguje pridelovanie blokov IP regionálnym registrátorom. V Európe je to RIPE Network Coordination Centre.

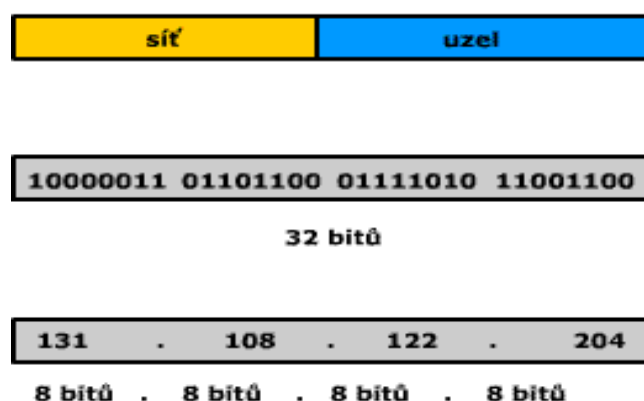
6.6.2.3 Adresy v IPv4

Adresy protokolu IPv4 sú 4 bajtové (32 bitové) čísla, rozdelené na 4 časti. Jednotlivé bajty sú oddelené bodkami. Vyjadrenie adresy býva spravidla v binárnej (dvojkovej), dekadickej (desiatkovej) alebo hexadecimálnej (šestnástkovej) sústave/notácii. Ak je adresa vyjadrená číslom dekadickej sústavy, môže každý bajt nadobúdať hodnoty od 0 do 255. Maximálny teoreticky rozsah adries je od 0.0.0.0 do 255.255.255.255. Adresa vyjadrená v binárnej sústave nadobúda hodnoty jednotlivých bajtov od 00000000 po 11111111. Čísiel adries môže byť $2^{32} = 4\,294\,967\,296$. Určité adresy sú rezervované pre vnútorné potreby a nie sú pridelované.

Príklad zápisu adresy v rôznych notáciách:

255.0.0.0 (dekadická) = 11111111.00000000.00000000.00000000 (binárna) = ff.00.00.0 (hexadecimálna).

IP adresy sa interpretujú ako dvojzložkové. **Identifikátor siete (IDnet)**, označovaný ako sieťová adresa alebo **prefix adresa**, určuje sieťový segment v štruktúre prepojených sietí protokolov TCP/IP. Všetky zariadenia pripojené k jednej spoločnej sieti majú v IP adrese rovnaké číslo siete. **Identifikátor zariadenia (IDhost)**, označovaný aj ako adresa hostiteľa alebo **sufix adresa**, určuje koncové zariadenie/ server/ smerovač alebo iné sieťové zariadenie v rámci jednej siete. Identifikátor zariadenia slúži k jednoznačnému odlíšeniu zariadení v jednej sieti. Znázornenie adresy je na obr. 6.9. Dĺžky prefixu a suffixu nie sú pevne stanovené.



Obr. 6.9 Časti IP adresy

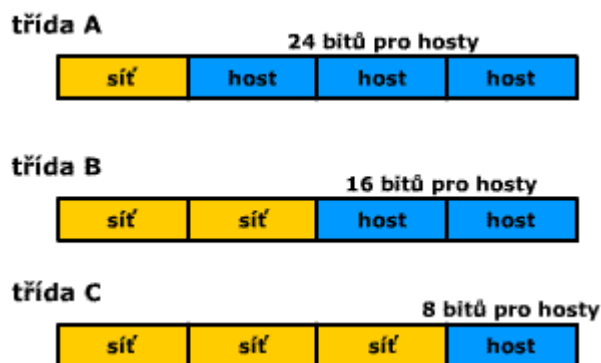
Takto vytvorená adresa odpovedá topológii IP sietí, ktorá je tvorené z parciálnych sietí. Každé zariadenie, ktoré chce odoslať IP datagram inému zariadeniu, vie z IP adresy príjemcu

rozpoznať či je zapojené v rovnakej parciálnej sieti. Ak áno, pošle mu odosielateľ svoj datagram priamo. Ak sa príjemca nachádza v inej sieti, pošle odosielateľ svoj datagram najbližšiemu smerovaču. Smerovač rozhodne, ktorým smerom datagram pošle ďalej.

Adresu siete prideluje poskytovateľ pripojenia. O jej pridelenie je potrebné požiadať. O štruktúre lokálnej časti adresy, rozdelení na podsiete a časti určené podsieti a pripojeným zariadeniam rozhoduje administrátor alebo správca príslušnej siete.

6.6.2.4 Triedy IP adries

Triedy adries sú vytvárané podľa dĺžok *suffixu* a *prefixu*. Boli zavedené preto, že do internetu sú pripojované rôzne veľké siete. Podľa toho majú pridelovanú rôznu časť adresy pre sieť a pre zariadenie. Triedy sú označené A, B a C. Ich znázornenie je na obr. 6.8.



Obr. 6.10 Triedy IP adries

V triede A je adresou siete prvý bajt IP adresy a pre adresu zariadenia sú vyhradené zvyšné 3 bajty. Vo vzťahu k obrázku 6.10 môžeme adresu znázorniť v tvare s.z.z.z. Trieda A umožňuje adresovať $2^7 = 128$ sietí. Prvý bajt adresy nemôže byť nulový a sieť 127 má špeciálne určenie ako *localhost* a nesmie byť na internete verejne používaná. Preto zo 128 možných sietí zostáva reálne 126 sietí. Prvý bajt je tak v intervale 1 – 126. V každej sieti je $2^{8+8+8}=16\,777\,214$ zariadení. Trieda A je určená pre veľké siete.

V triede B sú adresou siete prvé dva bajty a pre adresu zariadenie v rámci siete sú vyhradené 2 bajty. Znázornenie podľa obrázku 6.10 je v tvare s.s.z.z. Trieda B umožňuje adresovať $2^{14} = 16\,384$ sietí. Prvý bajt je v intervale 128 – 191. V každej sieti je $2^{8+8} = 65\,534$ zariadení. Adresy triedy B sú určené pre stredne veľké siete s desiatkami tisícov zariadení.

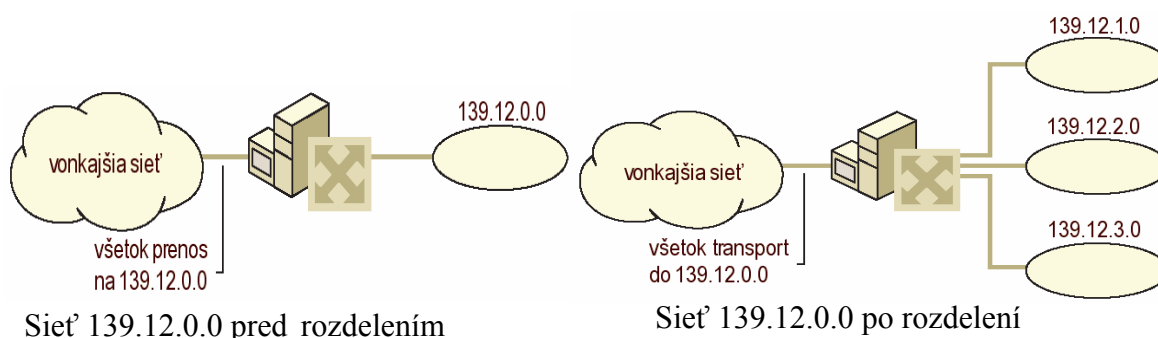
V triede C sú adresou siete prvé tri bajty, posledný bajt je určený pre adresu zariadenia. Znázornenie podľa obrázku 6.10 je v tvare s.s.s.z. Prvý bajt je v intervale 192 – 233. Umožňuje adresovať $2^{21} = 2\,097\,152$ sietí. Trieda C je určená pre najmenšie siete, s 256 zariadeniami, pretože pre adresu zariadenia v rámci siete je vyhradených len 8 bitov ($2^8 = 254$).

Okrem toho sú špecifikované ešte trieda D a E, kde nie je definované, čo je sieť a čo zariadenie. Trieda D sa používa pre skupinové adresovanie (*multicast*), trieda E je pre experimentálne účely. Prehľad tried a ich vlastností je v tabuľke 6.1.

Prehľad IP tried a ich vlastností je v tabuľke 6.1.

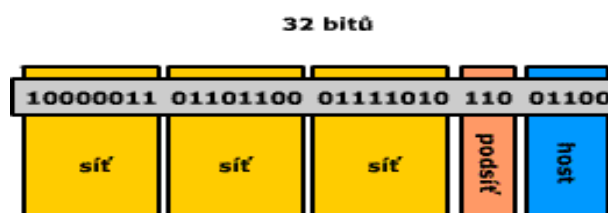
trieda	rozsah prvého bajtu	prvý bajt binárne	počet sietí	počet uzlov v sieti
A	1 - 126	0xxxxxxx	126	16 777 214
B	128 - 191	10xxxxxx	16 384	65 534
C	192 - 223	110xxxxx	2 097 152	254
D	224 - 247	1110xxxx	multicast	
E	248 - 255	1111xxxx	rezerva	

Uvedený koncept adresovania definuje len adresu siete a zariadenia. Neskôr sa takéto členenie ukázalo ako nedostatočné a lokálna časť adresy sa rozdelila na **podsieť (subnet)** a zariadenie, ktorým je spravidla počítač. Dôvodom pre vytváranie podsietí je tá skutočnosť, že žiadna z tried neumožňuje jemné delenie adresných priestorov sietí s niekoľkými desiatkami počítačov. Vytvorenie podsiete je na obrázku 6.11.



Obr. 6.11 Vytvorenie podsiete

Celá sieť vystupuje voči vonkajšej sieti ako jeden celok. Na adresu podsiete sa použijú bity zo suffix časti adresy. Znázornenie vytvorenia adresy podsiete je na obrázku 6.12



Obr. 6.12 Vytvorenie adresy subsiete

Hranicu medzi adresou podsiete a počítača určuje **maska podsiete (subnet mask)**. Maska má podľa odporúčania RFC 950 32 bitovú hodnotu zapisovanú rovnako ako IP adresa. Masky jednotlivých tried adries sú uvedené v tabuľke 6.2.

Tabuľka 6.2 Zápis masiek pre triedy adries

trieda	binárne	dekadicky	sieťová predpona
A	11111111 00000000 00000000 00000000	255.0.0.0	/8
B	11111111 11111111 00000000 00000000	255.255.0.0	/16
C	11111111 11111111 11111111 00000000	255.255.255.0	/24
D	11111111 11111111 11111111 11111111	255.255.255.255	
E	-----	-----	

Maska podsiete v binárnom tvare obsahuje jednotky tam, kde sa v adrese nachádza sieť a podsieť, nuly tam, kde je zariadenie. U masiek podsietí sa používa aj skrátенý spôsob označenia počtu bitov, ktoré partia siete použitím sieťovej predpony. Napríklad adresu siete triedy B s maskou podsiete 255.255.0.0 je možné vyjadriť zápisom 138.96.0.0/16.

Príklad: Určite adresu siete, na ktorej je počítač s adresou 170.85.255.248, binárne 1010108.01010101.11111111.1111100.

Riešenie:

1. Adresa je triedy B – zistíme podľa prvého čísla
2. Používaná maska pre triedu B je 11111111.11111111.00000000.00000000
3. Vynásobíme IP adresu bit po bite sieťovou maskou a získame adresu siete

1010108.01010101.11111111.1111100

11111111.11111111.00000000.00000000

adresa siete = 1010108.01010101.00000000.00000000 – dekadicky 170.85.0.0

Maska podsiete, spoločne s IP adresou je súčasťou konfigurácie zariadenia. Platné podsiete a masky podsietí špecifikované odporúčaním RFC 1878, ktoré sa používajú v technológii TCP/IP sú dostupné na <http://www.internic.net>.

Prideľovanie adries v internete je hierarchické a celý priestor adries nie je možné využívať. Táto skutočnosť spôsobila nedostatok IP adries protokolu v4. Tento nedostatok sa rieši rôznymi spôsobmi:

1. Dynamickým prideľovaním adries, keď používateľ zariadenia dostane dočasnú IP adresu len počas jedného pripojenia k sieti. Pri ďalšom pripojení môže dostať inú adresu.
2. Prekladom adries (*Network Address Translation*), kde prístup zariadení z lokálnej siete na internet je pod jednou adresou.

Iné.

Rozvojom internetu vznikala možnosť vyčerpania IP adries. Preto bol vyvinutý protokol IPv6.

6.6.2.5 Adresovanie IPv6

Protokol IPv6 sa označuje aj ako „IP novej generácie“ (*IPnG, IP Next Generation*). V protokole využíva mechanizmus CIDR (*Classless InterDomain Routing*), ktorý odstraňuje delenie na triedy a nahrádza ich ľubovoľne veľkými logickými celkami, ktoré zodpovedajú celým sieťam. Mechanizmom CIDR je možné IP adresy pridelovať po skupinách, ktoré majú veľkosť ľubovoľnej mocniny 2.

Najväčšou zmenou oproti IPv4 je dĺžka adresy. Adresa v IPv6 je tvorená 128 bitmi. Zápis je v ôsmich skupinách po štyroch čísliciach v hexadecimálnej sústave, navzájom oddelených dvojbodkou, čo odpovedá 32 hexadecimálnym čísliciach. Príklad zápisu adresy v IPv6 je:

2001:0db8:85a3:08d3:1319:8a2e:0370:7334.

Adresa IPv6 sa skladá z dvoch logických častí, 64-bitového prefixu siete a 64-bitovej adresy sufixu zariadenia v sieti, ktorá sa často generuje automaticky z MAC adresy zariadenia. Adresu IPv4 je možné previesť na IPv6 adresu. Napríklad desiatkovo zapísaná IPv4 adresa 135.75.43.52 je hexadecimálne 0x874B2B34. Potom je možné konvertovať ju do adresy IPv6 v tvare 0000:0000:0000:0000:0000:0000:874B:2B34 alebo ::874B:2B34.

Počet adres IPv6 môže byť $2^{128} \approx 3.4 \times 10^{38}$. Číslo IPv6 adresy je tiež možné určiť ako 16^{32} , keďže každé z 32 hexadecimálnych číslic môže nadobúdať 16 bitov. Mnohokrát sa diskutuje o tom, že 128-bitové adresy sú zbytočne veľké a internet ich nikdy toľko nebude potrebovať. Dôvodom použitia 128-bitových adres nie je iba zabezpečenie, aby sa nikdy neminuli, ale zabezpečenie zlepšenia smerovania tým, že bude adresný priestor čo najmenej fragmentovaný. To je ďalší rozdiel od súčasného stavu s IPv4, kedy mnohokrát býva viac intervalov adres priradených jednej organizácii.

Iným typom adresovania v internete sú alias adresy /symbolické adresy vytvárané protokolom DNS (*Domain Name Server*). Dôvodom je tá skutočnosť, že pre používateľov je komplikované zapamätať si číselné adresy. Je to hlavne v službách, napríklad e-mail adresa, www adresa. Tvoria ju alfanumerické znaky oddelené bodkou. Preklad IP adresy na *alias* adresu zabezpečuje aplikačný softvér. Ich vytváranie bude vysvetľované v kapitole 9 Aplikačná vrstva.

6.7 Spojovanie

Samotné spojovanie v uzle je realizované v spojovacích systémoch (*switching systems*). Podľa typu prepojovania sa delia aj spojovacie systémy na dva typy:

- systémy pre prepojovanie okruhov,
- systémy pre prepojovanie paketov.

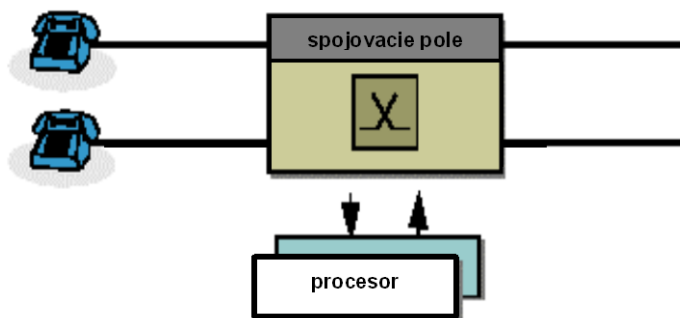
Spojovacie systémy obsahujú dve základné časti:

- spojovacie pole,
- riadenie.

6.7.1 Systémy pre prepojovanie okruhov

Na začiatku vývoja komunikačných sietí boli spojovacie systémy realizované ako manuálne telefónne ústredne. Operátor prijal žiadosť o spojenie a manuálne, pomocou kolíky prepojil volajúceho s volaným. Keď sa spojenie ukončilo, operátor rozpojil kolíky a okruh rozpojil. Princiipiálne išlo už vtedy o prepojovanie okruhov. Operátor realizoval riadiacu funkciu signalizácie, keď na základe požiadavky účastníka realizoval prepojenie a rozpojenie.

Ďalšou generáciou spojovacích systémov boli elektromechanické systémy. Prvá generácia týchto systémov bola založená na spojovacích prvkoch nazývaných krokové voliče (*step by step*), ktoré boli riadené priamo (*synchronne*) voľbou z telefónneho prístroja. Druhá generácia využívala ako spojovací prvok krížový spínač (*crossbar*). Obsahovali jednoduchú pamäť, kde bola uložená a analyzovaná voľba. Až po analýze bol vytvorený komunikačný okruh. Ďalším dôležitým medzníkom boli systémy programovo riadené (*System Program Control - SPC*). Prvé boli analógové, neskôr s nástupom impulznej kódovej modulácie v prenosovej časti siete, digitálne. Dochádza k programovému riadeniu všetkých funkcií počítačom, resp. procesorom, ako je znázornené na obr. 6.13. Tieto systémy sa označujú ako digitálne spojovacie systémy. Sú to integrované systémy, ktoré pracujú na rovnakom princípe digitálneho prenosu na sieťovej a linkovej vrstve.

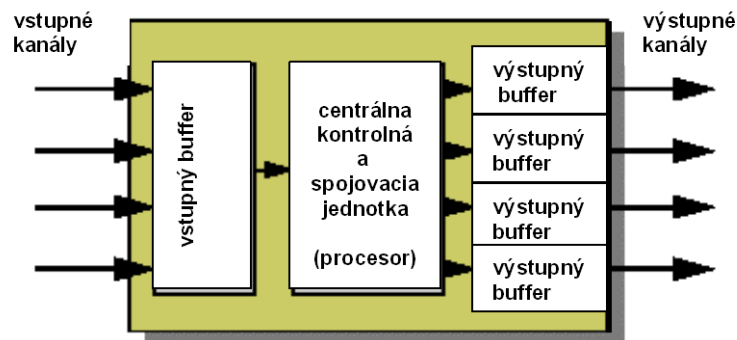


Obr. 6.13 Základná schéma spojovacieho systému

Posledný vývoj smeruje k optickým spínačom. Zatiaľ sú úzkym miestom siete. Kým optické prenosové systémy pracujú s prenosovými rýchlosťami až desiatky Gbit/s, spojovacie systémy dosahujú omnoho menšie prenosové rýchlosti. Je to však iba otázka času ďalšieho vývoja. V budúcnosti sa uvažuje nad plne optickými spojovacími systémami s elektronickým riadením.

6.7.2 Systémy pre paketový prenos

Pri paketovom prenose sa na spojovanie používajú paketové spínače, ktoré plnia úlohu spojovacieho systému. Procesor plní úlohu riadiacej i prepojovacej jednotky. Prístup do siete je neobmedzený a pokiaľ nie je voľná kapacita na spojovanie, ukladá pakety dočasne vo vstupnej vyrovnávacej pamäti (*bufferi*). Pakety prepojuje podľa adresy v hlavičke a ukladá ich do výstupných vyrovnávacích pamätí. Adresa je analyzovaná prostredníctvom smerovacích tabuliek. Bloková schéma systému je na obr. 6.14.



Obr. 6.14 Spojovací systém pre paketový prenos

Podľa charakteru vytvárania spojenia môžu byť siete spojovo (*with connection*) a nespojovo (*connectionless*) orientované. Správnejšie by bolo, nazývať ich ako siete s realizáciou nadväzovania spojenia a bez nadväzovania spojenia.

6.7.3 Spojovo orientované siete

Pri spojovo orientovaných sieťach je pred zahájením prenosu potrebné nadviazať spojenie, to znamená, že uzly sa musia dohodnúť s aktívnymi prvkami koncových zariadení, ktoré následne vytvoria kanál, prostredníctvom ktorého je prenášaná informácia. Spojovo orientovaná komunikácia sa realizuje dvoma spôsobmi:

1. Fyzickým spojením pri spôsobe prepojovania okruhov, keď je medzi koncovými zariadeniami vybudovaná trvalá komunikačná cesta.
2. Virtuálnym spojením pri prepojení paketov, keď je medzi koncovými systémami vybudovaná virtuálna cesta.

Spojovo orientovaná služba umožňuje nadviazanie spojenia, ktorým sú potvrdzované prijaté dáta a v prípade straty dát je možné požadované zopakovanie vysielania. Siete využívajúce virtuálne okruhy poskytujú spojované sieťové služby a označujú sa (*Connection Oriented Network Services - CONS*)

6.7.4 Nespojovo orientované siete

Pri nespojových sieťach sa spojenie nenadväzuje. Komunikácia nevyžaduje vybudovanie a zrušenie spojenia od zdroja k prijímaču. Príkladom je realizovanie datagramovej služby pri prepojení paketov. Paket musí mať dostatočné množstvo informácií na to, aby sa dostal do cieľového koncového zariadenia. Príslušný uzol vždy rozhoduje, či je adresátom alebo nie je. Siete, v ktorých sú pakety prenášané bez zostavenia virtuálnych okruhov poskytujú nespojované služby a označujú sa (*Connection-Less Network Services - CLNS*).

6.8 Signalizácia

Signalizácia v komunikačných sieťach znamená výmenu riadiacich informácií. Je špecifikovaná súborom riadiacich signálov, ktoré sú prenášané za účelom zostavovania, udržiavania a zrušenia spojenia. Signalizácia bola základnou podmienkou prevádzky

elektronických komunikačných sietí od ich začiatku. Príkladom sú prvé telefónne ústredne, kde účastník krútením kľuky generoval striedavý prúd, aby spojovateľka vedela, že chce byť spojený s iným účastníkom. Iné riadiace informácie, napríklad telefónne číslo sa prenášali ústne. Neskôršie sa telefónna sieť automatizovala a uvedené procedúry sa nahradili signalizáciou. Podľa stavu, v ktorom sa koncové zariadenie účastníka nachádza, spojovací systém vie či účastník chce nadviazať spojenie alebo nie. Číslo sa prenáša pomocou voľby z klávesnice. Signalizácia je najlepšie vnímaná v telefónnej službe vyzváňacím a obsadzovacím tónom. Signalizácia je rôzna pre rôzne typy služieb. Napríklad telefónna služba na kreditnú kartu vyžaduje v porovnaní s klasickou telefónnou službou zložitejšiu signalizáciu, ktorá umožní overiť v určitej databáze platnosť kreditnej karty. Služby mobilných sietí majú, v porovnaní s pevnými sieťami, ďalší problém, ktorý musí byť riešený signalizáciou. Musí vedieť, kde sa dané zariadenie, alebo mobilný účastník s mobilným telefónom, práve nachádza.

S vytváraním nových sietí a služieb sa menia aj požiadavky na signalizáciu. Špecifikujú sa signalizačné systémy, ktoré sú tvorené súborom funkcií, komponentov a protokolov. Signalizačné systémy sú rôzne pre rôzne typy sietí a technológií. Ale hlavná úloha je pre všetky typy služieb rovnaká, preniesť riadiace informácie pre zostavenie spojenia, dohľad nad spojením a zabezpečiť jeho rozpojenie. Prostredníctvom signalizácie sú prenášané:

- riadiace signály, obsahujúce informácie potrebné pre zostavovanie a rušenie spojenia,
- dohľadové signály, obsahujúce informácie súvisiace s dohľadom nad zostaveným spojením,
- informácie o tarifovaní, alarmy, údržbové informácie a pod.

Vo väzba na štruktúru telefónnej siete sa signalizácia člení podľa miest, kde sa riadiace signály prenášajú na:

- signalizáciu účastnícku (*subscriber signalling*), medzi používateľom a prvým uzlom v sieti,
- vnútornú signalizáciu v spojovacom systéme (*exchange signalling*), niekedy označovanú tiež ako systémovú,
- signalizáciu sieťovú (*interexchange signalling*), medzi uzlami v sieti.

Účastnícka signalizácia – je výmena riadiacich informácií medzi účastníckym koncovým zariadením a spojovacím systémom. Účastnícku signalizáciu tvorí súbor riadiacich signálov pre:

- Volajúceho účastníka
 - žiadosť o spojenie,
 - voľba adresy,
 - ukončenie spojenia.
- Volaného účastníka
 - vyzváňanie – účastník je žiadaný o spojenie,
 - prihlásenie,

- ukončenie spojenia.

Vnútná signalizácia v ústredni nie je špecifikovaná, závisí od výrobcu spojovacieho systému.

Sieťová signalizácia býva viazaná na určitý signalizačný systém. Typy signalizačných systémov sú uvádzané pri jednotlivých typoch sietí. Najpoužívanejším štandardom je signalizačný systém č. 7.

Siete s prepojaním paketov nepoužívajú signalizáciu, riadiace informácie sú prenášané v hlavičke paketu.

6.9 Riadenie toku dát

Okrem smerovania, ktorým rozumieme len rozhodovanie o ďalšom smere, musí sieťová vrstva zaisťovať aj realizáciu smeovania. To znamená, že v medziľahlých uzloch musí zaisťovať odovzdávanie jednotlivých paketov na prenosovej ceste ku koncovému zariadeniu. S touto funkciou súvisí aj ďalšia úloha sieťovej vrstvy, predchádzať preťaženiu/zahlteniu časti siete, riadiť tok dát a dbať o čo možno najrovnomernejšie využitie všetkých prenosových prostriedkov a kapacít. Pri vzájomnom prepojení dvoch a viac sietí pribudne sieťovej vrstve ešte jedna dôležitá úloha, zaisťovať nevyhnutné odovzdávanie paketov medzi jednotlivými sieťami.

V snahe vyhnúť sa zahlteniu vo vnútri siete alebo k zahlteniu prijímacej jednotky transportnej vrstvy je nevyhnutné riadenie prenosu paketov. Riadenia môže byť realizované viacerými spôsobmi:

- riadenie toku (*flow control*) reguláciou medzi dvoma uzlami.
- predchádzanie zahltenia siete (*cognetion avoidance*) metódami zabraňujúcimi stavu, keď väčšina uzlov v sieti je zahltená,
- predchádzanie uviaznutia v sieti (*deadlock*),
- riadenie prístupu toku dát (*access control*),
-

Riadenie toku medzi dvoma uzlami sa používa pre obmedzenie rýchlosti generovania dátových jednotiek vo vysieláči. Používajú sa tri metódy riadenia:

- Úprava rýchlosti generovania dátových jednotiek zmenou časovania, ktoré riadi ich generovanie.
- Odmietnutie paketu označované ako vyhodenie (*discard*) paketu, čo znamená, že prijímač paket neuloží do pamäti a paket je stratený.
- Povolenie k vysielaniu, keď je vysielanie povolené na základe príkazu prijímača.

Predchádzanie zahltenia siete, ktoré používa nasledujúce metódy:

- Riadenie prístupu dynamickou zmenou zaťaženia siete podľa stavu prevádzky v sieti.
- Zníženie existujúcej záťaže vyhadzovaním paketov.

Predchádzanie uviaznutia v sieti, ktoré môže byť riešené napríklad:

- Štruktúrovanou vyrovnávacou pamäťou, ktorá uchováva pakety podľa ich hierarchie.
- Definovaním doby životnosti paketu TTL (*Time to Live*), ktorý určuje dobu, po ktorej môže byť paket zničený. Tým sa zabráni obiehaniu paketov.

6.10 Protokoly sieťovej vrstvy

Smerovacích protokolov vyvinutých v histórii vzájomného prepojovania sietí je celý rad a práce na nich stále pokračujú. Väčšina súčasných smerovacích protokolov vychádza z normalizovaných protokolov ISO/OSI alebo normalizovaných protokolov RFC.

Najznámejším protokolom sieťovej vrstvy je **IP protokol (*Internet Protocol*)**. Jeho verzie IPv4 a IPv6 boli už uvedené v časti adresovanie. Poskytuje nespoľahlivú datagramovú službu (*best effort*). Datagram môže prísť, poškodený, ľubovoľnom poradí alebo môže byť v sieti zahodený. Spoľahlivosť doručenia sa zabezpečuje inými prostriedkami. IP protokolu je označovaný aj ako rodina protokolov a jeho súčasťou sú aj nasledovné protokoly:

- ARP - *Address Resolution Protocol*, ktorý premieňa 32 bitovou IP adresu na 48 bitovou MAC adresu.
- RARP - *Reverse Address Resolution Protocol*, ktorý naopak premieňa MAC adresu na IP adresu. Tento protokol používajú bezdiskové zariadenia, ktoré nepoznajú svoju IP adresu.
- ICMP - *Internet Control Message Protocol*. používaný k signalizácii chýb a rôznych neštandardných situácií.
- IGMP - *Internet Group Management Protocol* na podporu skupinového vysielania (*multicasting*).

Pre vzájomnú komunikáciu medzi sieťami bol navrhnutý protokol EGP. Rozoznávame dva typy smerovacích protokolov:

- Exterior Gateway Protocol (EGP) – zabezpečuje smerovanie medzi autonómnymi systémami
- Interior Gateway Protocol (IGP) – zabezpečuje smerovanie v rámci autonómneho systému

V lokálnych sieťach LAN sa používajú ešte ďalšie smerovacie protokoly, niektoré ako proprietárne riešenia:

- RIP - Routing Information Protocol
- IGRP - Interior Gateway Routing Protocol
- OSPF - Open Shortest Path First
- BGV - Border Gateway Protocol

6.11 Zariadenia sieťovej vrstvy

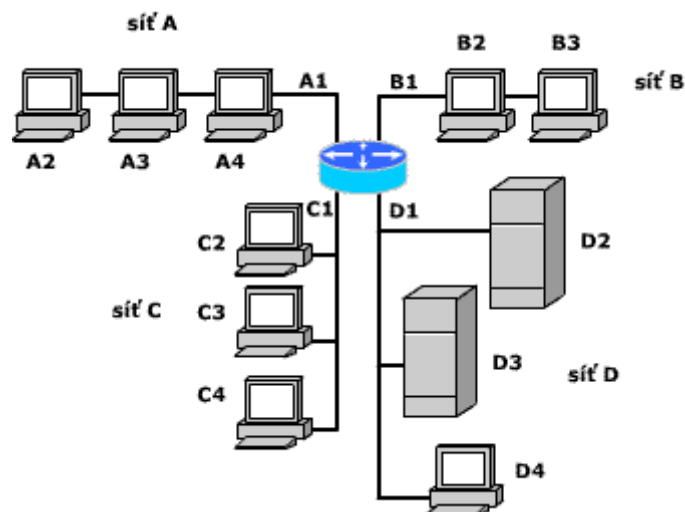
6.11.1 Smerovače

Smerovač je zariadenie sieťovej vrstvy komunikačnej siete, prostredníctvom ktorého sa v uzloch komunikačnej siete smerujú dáta. Smerovače kontrolujú hlavičky sieťových paketov, a na základe týchto informácií potom prijímajú konkrétne rozhodnutia o tom, kam smerovať paket v uzle siete. Odoslaný paket je odovzdaný svojmu prednastavenému smerovaču na doručenie. Smerovač z paketu zistí adresu príjemcu, prehľadá svoju databázu podsietí, určí do ktorej z nich paket patrí a cez ktorý najbližší ďalší smerovač má paket ísť. Keď túto informáciu získa, odošle paket takto určenému smerovaču. Tento proces sa opakuje, až pokiaľ sa paket nedostane do cieľovej siete.

Smerovače si vzájomne informácie vymieňajú, takže po istom čase každý smerovač v sieti má prehľad o všetkých podsieťach a o tom, cez ktoré smerovače sú tieto podsiete dostupné.

Smerovače sú aktívne manažovateľné komponenty počítačových sietí, vytvárané potrieb konkrétnych sieťových protokolov, napríklad IP. Smerovač je možné vybudovať na PC, stačí, aby malo aspoň dve sieťové karty a vhodný operačný systém (napríklad Linux). Existujú však aj jednoučelové zariadenia – smerovače špecializované len na úlohu smerovania.

Zapojenie smerovača v sieti je na obrázku



Obr. 6.15 Zapojenie smerovača v sieti

6.11.2 Ústredne

Ústredne sa používajú v telefónnych sieťach, ktoré pracujú na princípe prepojovania okruhov.

6.12 Záver

Sieťová vrstva poskytuje službu transportnej vrstve. Poskytovanie služby je rozdielne podľa toho, či je na sieťovej vrstve používané prepojenie okruhov alebo prepojenie paketov. Pri prepojení okruhov vytvorí sieťová vrstva podľa adresy prijímajúceho zariadenia fyzický prenosový okruh medzi dvomi komunikujúcimi zariadeniami. Tento spôsob prepojenia je používaný v telefónnych sieťach.

Pri prepojení paketov sieťová vrstva „zabalí“ segmenty z transportnej vrstvy do blokov, ktoré sa označujú pakety. Pakety sú smerované v uzloch siete dvomi spôsobmi: službou virtuálnych kanálov alebo datagramovou službou. Službou virtuálnych kanálov je prvým paketom označená prenosová cesta, ktorou budú prenášané všetky pakety. Datagramovou službou sú pakety, označované ako datagramy, prenášané rôznymi prenosovými cestami.

Pre vytvorenie prenosovej cesty je potrebné v uzloch siete spracovať adresu prijímajúceho zariadenia a riadiť tok dát. Zariadenia sieťovej vrstvy sú smerovače (*routers*) alebo telefónne ústredne (*exchanges*).

Kľúčové slová

1. *Sieťová vrstva*
2. *Paket*
3. *Fragmentácia*
4. *Rozhranie používateľ – sieť*
5. *Nosné služby/služby prenosu (bearer services)*
6. *Prepojenie (switching)*
7. *Smerovanie (routing)*
8. *Adresovanie (addressing)*
9. *Spojovanie (connecting)*
10. *Signalizácia (signalising)*
11. *Pevné okruhy*
12. *Komutované okruhy*
13. *Fyzické okruhy*
14. *Virtuálne okruhy*
15. *Prepojenie okruhov*
16. *Prepojenie paketov*
17. *Služba virtuálnych okruhov*
18. *Datagramová služba*
19. *Forwarding*
20. *Zdrojové smerovanie*
21. *Hop-by-hop routing*
22. *Algoritmické smerovania*
23. *Adaptívne algoritmy smerovania*
24. *Neadaptívne algoritmy smerovania*

25. *Smerovacie tabuľky (routing tables)*
26. *Statické smerovacie tabuľky*
27. *Dynamické smerovacie tabuľky*
28. *ID siete*
29. *Metrika smerovania*
30. *Cieľová adresa*
31. *Adresa siete*
32. *Mapovanie adresy (address mapping)*
33. *Rozlíšenie adresy (address resolution)*
34. *Maska adresy (address mask)*
35. *Adresa v LAN*
36. *Adresovanie v rozľahlých sieťach*
37. *Adresovanie vo verejnej telefónnej sieti*
38. *Číslovací plán (Network Routing Numer – NRN)*
39. *Adresovanie v internete*
40. *Prefix adresy v internete*
41. *Suffix adresy v internete*
42. *Alias adresy*
43. *Trieda adresy*
44. *Broadcast adresa*
45. *Adresovanie podsietí*
46. *Maska podsiete*
47. *Riadenie toku dát*

- 48. *Zahltenie siete*
- 49. *Odmietnutie paketu*
- 50. *Doba životnosti paketu*
- 51. *IP protokol*
- 52. *ARP - Address Resolution Protocol*
- 53. *RARP - Reverse Address Resolution*
- 54. *Zariadenia sieťovej vrstvy*

Kontrolné otázky

1. Pre ktorú vrstvu poskytuje sieťová vrstva svoje služby?
2. Služby ktorej siete využíva sieťová vrstva?
3. Aké komunikačné jednotky sú používané na sieťovej vrstve?
4. Z akých základných častí sa skladá paket?
5. Aká je veľkosť paketu?
6. V akých základných častiach siete je špecifikovaná sieťová vrstva?
7. Ako je vytváraný komunikačný kanál cez sieťovú vrstvu?
8. Prečo je problém s veľkosťou paketu?
9. Čím sa rieši problém, ak má paket väčšiu veľkosť ako MTU (*Maximum Transmission Unit*)?
10. Aký problém rieši fragmentácia?
11. Kde je v OSI modeli rozhranie medzi sieťou a koncovým používateľom?
12. Ako sa označujú služby poskytované podľa 1. až 3. úrovne OSI modelu?
13. Čo znamená pojem služby prenosu (*bearer services*)?
14. Ktoré z vymenovaných funkcií patria k sieťovej úrovni?
15. Aký je rozdiel medzi pevným a komutovaným okruhom?
16. Aký je rozdiel medzi fyzickým a virtuálnym okruhom?
17. Aké sú spôsoby prepojovania?
18. Ktoré fázy sú nevyhnutné pri prepojení okruhov?
19. Ktoré sú výhody prepojovania okruhov?
20. Ktoré sú nevýhody prepojovania okruhov?
21. Aké služby sú poskytované pri prepojení paketov?
22. V čom je rozdiel poskytovania datagramovej služby a služby virtuálnych okruhov?
23. Aké sú výhody prepojovania paketov?
24. Aké sú nevýhody prepojovania paketov?
25. Ktoré z vymenovaných sietí používajú prepojenie okruhov?
26. Ktoré z vymenovaných sietí používajú prepojenie paketov?
27. Aké prepojenie je používané v internete?
28. Čo vyjadruje označenie forwarding pri smerovaní na sieťovej vrstve?
29. Aký je rozdiel medzi *source routing* a *hop-by-hop routing*?
30. K čomu slúžia smerovacie algoritmy?
31. Aké druhy smerovacích algoritmov sú používané v komunikačných sieťach?
32. K čomu slúžia smerovacie tabuľky?
33. Ktoré z uvedených identifikátorov sú uvedené v smerovacích tabuľkách?
34. Aký je rozdiel medzi statickými a dynamickými smerovacími tabuľkami?
35. K čomu slúži adresa v komunikačnej sieti?
36. Ktoré prvky siete majú priradené adresy?

37. Čo znamená mapovanie adresy (*address mapping*)?
38. Kde sa používa technika rozlíšenia adresy (*address resolution*)?
39. K akému účelu sa používa maska adresy (*address mask*)?
40. K čomu slúži číslovací plán (*Network Routing Numer – NRN*)?
41. Aké sú rozdiely v číslovaní rozľahlých sietí?
42. Ako je vyjadrená adresa v sieti internet protokolu IPv4?
43. Koľko bitov má internetová adresa IPv4?
44. Čo vyjadruje prefix a sufix v internetovej adrese?
45. Ako sú vyjadrené alias adresy?
46. Aké triedy adries sú v IP technológii?
47. V čom je rozdiel v triedach adries IPv4?
48. Ako je vyjadrená adresa v IPv6?
49. K čomu sa využíva broadcast adresa?
50. Prečo sa adresujú podsiete v internete?
51. Ako sa vyjadruje maska podsiete?
52. Aký je rozdiel medzi spojovo a nespojovo orientovanou sieťou?
53. K čomu je v komunikačných sieťach využívaná signalizácia?
54. Za akým účelom je vytvárané riadenie toku dát v sieťovej vrstve?
55. Ktoré z vymenovaných mechanizmov sú používané pre riadenie toku v sieťovej vrstve?

7 Transportná vrstva (Transport Layer)

Ciele

Čo by mal študent vedieť:

- Úlohy a funkcie transportnej vrstvy
- Charakteristické vlastnosti protokolu TCP
- Charakteristické vlastnosti protokolu UDP

7.1 Úvod

Aplikačná, prezentačná a relačná vrstva, ktorými sme sa zaoberali v predchádzajúcich kapitolách, sú zamerané na využívanie alebo poskytovanie konkrétnej služby, ktorú má sieťová aplikácia sprostredkovať. Aplikačná vrstva poskytuje priamo nástroje na tvorbu a využívanie sieťových služieb, prenesene do nej patria všetky aplikácie, ktoré podporujú komunikáciu medzi rôznymi uzlami prepojenými komunikačnou sieťou. Prezentačná vrstva zodpovedá za to, že dáta odosielané jednotlivými aplikáciami v aplikačnej vrstve budú u príjemcu správne vyhodnotené a interpretované, stará sa teda o spoločný zrozumiteľný formát dát a jeho konverziu. Relačná vrstva sa stará o to, aby sa dáta vytvorené aplikáciou v aplikačnej vrstve a identifikované či konvertované do akceptovateľného formátu prezentačnou vrstvou usporiadali do dialógov a vo vhodnom slede preniesli k príjemcovej aplikácii (procesu). Všetky tieto tri horné vrstvy RM OSI sa vlastne zaoberajú aplikačnými dátami, ich významom, formátovaním, adresovaním vhodnému procesu, prípadne riadením dialógov, v ktorých sa tieto dáta prenášajú. Žiadna z týchto vrstiev sa však nezaobera technickými detailmi prenosu dát medzi koncovými komunikujúcimi uzlami – riešia len obsah a formu, prípadne časovú následnosť prenášaných aplikačných dát.

Dáta i vo forme dialógov, ako ich pripraví relačná vrstva, nie sú bezprostredne vhodné pre prenos komunikačnou sieťou. Predovšetkým, blok dát vytvorený aplikačnou vrstvou a spracovaný na prezentačnej a relačnej vrstve nemá nijaké obmedzenia na svoju veľkosť. Komunikačné siete s prepínaním paketov však vyžadujú, aby prenášané dáta boli rozdelené na malé, veľkosťou obmedzené úseky, ktoré sa sieťou prenášajú nezávisle a späťne sa rekonštruujú u príjemcu. O túto tzv. **segmentáciu** dát u odosielateľa a ich opätovnú rekonštrukciu u príjemcu sa musí postarať nová vrstva nachádzajúca sa pod relačnou vrstvou, ktorú budeme nazývať **transportná vrstva**. Transportná vrstva bude teda preberať bloky dát z relačnej vrstvy, pripraví ich pre prenos paketovou sieťou tým, že dáta rozdelí na vhodné veľké segmenty, a u príjemcu z prijatých segmentov opätovne zloží pôvodný blok dát, ktorý odovzdá príjemcovej relačnej vrstve. Transportná vrstva nebude však riešiť samotný proces prechodu (doručovania) segmentov cez sieť a zariadenia – to bude starosťou nižších vrstiev RM OSI.

Segmentácia blokov dát prichádzajúcich z relačnej vrstvy je teda jednou z hlavných funkcií transportnej vrstvy. Jednotlivé úseky, tzv. segmenty, sa komunikačnou sieťou

s prepínaním paketov prenášajú nezávisle na sebe. Pri tomto prenose jednotlivých segmentov môže dôjsť k ich preusporiadaniu a prijatiu v inom poradí, než v akom boli odoslané. Navyiac, z rôznych dôvodov sa niektoré segmenty počas doručovania môžu stratiť. Transportná vrstva je okrem segmentácie dát zodpovedná aj za to, aby bola schopná prijaté segmenty usporiadať do pôvodného poradia a pokiaľ niektoré segmenty chýbajú, má zabezpečiť ich opakované prenesenie. Od transportnej vrstvy okrem segmentácie a spätnej rekonštrukcie dát preto navyše očakávame, že zariadi, aby cieľový uzol získal prenesené dáta v presne takom tvare, v akom boli odoslané – všetky a v pôvodnom poradí. Túto vlastnosť nazývame **spoľahlivosť**.

Segmenty, ktoré transportná vrstva z dát vytvorí, môže nechať doručiť príjemcovi hneď, bez predchádzajúcej dohody s ním, alebo je pred prenosom segmentov potrebné najprv s príjemcom vytvoriť dohodu o vzájomnej komunikácii. Táto dohoda o vzájomnej komunikácii sa nazýva **spojenie**. Pojem spojenie znamená, že dve komunikujúce strany sa vzájomne dohodli na výmene segmentov a po vytvorení spojenia si kedykoľvek môžu odosielať segmenty s istotou, že druhá strana je na ich príjem pripravená a očakáva ich. Ak už nie je potrebné žiadne ďalšie segmenty prenášať, spojenie sa zruší. Transportná vrstva pomocou spojenia presne ohraničuje, kedy komunikačný vzťah začal (otvorením spojenia), či trvá a kedy skončil (zrušením spojenia). Pojem spojenie pritom neznamená, že v sieti sú pre prenos segmentov vyhradené nejaké prenosové prostriedky, prípadne že všetky segmenty pôjdu k príjemcovi tou istou cestou – toto je častý omyl. Spojenie v zmysle transportnej vrstvy je vzájomná dohoda komunikujúcich uzlov o pripravenosti pre výmenu dát vo forme segmentov. Transportné protokoly, ktoré pred prenosom segmentov vyžadujú vytvorenie spojenia, sa nazývajú **spojovo orientované** alebo jednoducho **spojované** transportné protokoly. Naopak, transportné protokoly, ktoré umožňujú prenášať segmenty okamžite, bez predchádzajúceho vytvárania spojenia s príjemcom, sa nazývajú **nespojovo orientované** alebo jednoducho **nespojované** protokoly. Všeobecne túto vlastnosť transportných protokolov nazývame **spojovanosť**.

Pri tvorbe segmentov neraz nastáva situácia, že buď komunikačná sieť alebo príjemca nie sú schopní prenášať segmenty tak rýchlo, ako ich odosielateľ vytvára a odosiela. Ak odosielateľ nespomalí odosielanie segmentov, potom preťaženie kapacity siete alebo príjemcu nevyhnutne spôsobí, že sa niektoré segmenty stratia alebo nebudú môcť byť spracované. Transportná vrstva preto bude mať ešte jednu zodpovednosť, a to tzv. **riadenie toku dát**. Pod pojmom riadenie toku dát sa rozumie schopnosť transportnej vrstvy odosielať jednotlivé segmenty väčšej alebo menšej dĺžky a s rôznymi intervalmi medzi odoslaním dvoch za sebou idúcich segmentov. Tým transportná vrstva dokáže (v istých skokoch) regulovať prenosovú rýchlosť a prispôbiť sa aktuálnemu stavu komunikačnej siete alebo príjemcu.

Celkovo transportná vrstva zodpovedá za prenos dát vo forme segmentov medzi koncovými komunikujúcimi uzlami, pričom od transportnej vrstvy môžeme požadovať, že dáta musia byť prenesené všetky, v pôvodnom poradí, s prispôbením sa aktuálnemu stavu siete (spomalenie či zrýchlenie prenosu) a prípadne v spojovanom či nespojovanom režime. Pretože sa jedná mnohokrát o spoľahlivé doručovanie dát medzi koncovými komunikujúcimi

uzlami, zvykneme o tejto komunikácii tiež hovoriť ako o **end-to-end** alebo **koniec-koniec** komunikácii.

Je potrebné ešte raz zdôrazniť, že transportná vrstva nerieši samotný proces presunu vytvoreného segmentu zo zdrojového uzla na cieľový. Transportná vrstva na tento účel používa služby sieťovej vrstvy. Transportná vrstva vytvára segmenty a necháva ich odoslať, prijaté segmenty usporadúva do pôvodného poradia a rieši prenos chýbajúcich segmentov, riadi tok dát, prípadne vytvára a uzatvára spojenia medzi zdrojovým a cieľovým uzlom, avšak prenos segmentu cez sieť je starosťou nižších vrstiev. Z tohto pohľadu má transportná vrstva postavenie istej prispôsobovacej, adaptačnej vrstvy – zaoberá sa aplikačnými dátami (horné 3 vrstvy RM OSI), ktoré prispôsobuje pre prenos paketovou sieťou (spodné 3 vrstvy RM OSI), pritom však pracuje stále na koncových uzloch.

Funkcie transportnej vrstvy teda sú

- Segmentácia dát a ich opätovné zostavenie
- Spôľahlivý prenos dát resp. prenos dát bez spoľahlivosti
- Spojovo resp. nespojovo orientovaný prenos dát
- Riadenie toku dát

7.2 Transportné protokoly v protokolovom modeli TCP/IP

Účelom transportnej vrstvy v rodine protokolov TCP/IP je poskytovať transparentný prenos dát medzi koncovými komunikujúcimi aplikačnými procesmi. Rozlišujú sa dva druhy služieb na transportnej úrovni:

- Spojovo orientované, ktoré vyžadujú vytvorenie, riadenie a zrušenie logického spojenia medzi komunikujúcimi procesmi pred prenosom dát.
- Nespojovo orientované, ktoré umožňujú prenos dát bez predchádzajúceho vytvárania logického spojenia.

So spojovo orientovanými službami sa často spája predstava, že poskytujú automaticky aj spoľahlivý prenos dát s riadením toku. Pri nespojovo orientovaných službách sa zasa predpokladá, že nezabezpečujú spoľahlivosť ani riadenie toku dát. Pri typických transportných protokoloch táto korešpondencia skutočne i platí, no nie je nevyhnutná – existujú i spojovo orientované protokoly, ktoré neriešia spoľahlivosť, a naopak, existujú nespojovo orientované protokoly schopné riešiť spoľahlivosť i riadenie toku. Charakter spojovanosti protokolu nemá preto priamy dopad na to, či poskytuje aj spoľahlivosť alebo riadenie toku.

V protokolovom modeli TCP/IP existuje niekoľko rôznych transportných protokolov. Dva hlavné transportné protokoly sú:

- Protokol UDP (User Datagram Protocol) – nespojovo orientovaný protokol bez poskytovania spoľahlivosti a riadenia toku

- Protokol TCP (Transmission Control Protocol) – spojovo orientovaný protokol s poskytovaním spoľahlivosti a riadenia toku dát

Aplikácie si môžu samé vybrať, ktorý transportný protokol chcú používať. Tradičné počítačové aplikácie, prenos súborov, elektronická pošta preferujú spoľahlivosť a dávajú prednosť TCP. Naproti tomu multimedialne aplikácie dávajú prednosť UDP, pretože sa nezdržuje zaisťovaním spoľahlivosti, a tak dokáže prenášať dáta rovnomernejšie a s menším oneskorením.

7.3 Transportný protokol Transmission Control Protocol

Protokol TCP (Transmission Control Protocol) je jedným z dvoch najbežnejších transportných protokolov, ktoré protokolový model TCP/IP na úrovni transportnej vrstvy ponúka. Protokol TCP patrí medzi spoľahlivé spojovo orientované transportné protokoly. Pred prenosom dát v TCP je potrebné medzi komunikujúcimi uzlami vytvoriť TCP spojenie a po skončení prenosu je potrebné ho opäť uzatvoriť. TCP prenáša dáta spoľahlivo, t.j. dáta po ich prijatí usporiada do pôvodného poradia a v prípade, že došlo počas prenosu sieťou k strate segmentu, TCP zabezpečí jeho opätovné prenesenie. TCP má navyše schopnosť spomaliť alebo zrýchliť prenos dát podľa aktuálneho stavu komunikačnej siete. Tieto vlastnosti robia TCP veľmi obľúbeným, no i zodpovedajúco komplexným protokolom.

Protokol TCP od svojej nadradenej vrstvy očakáva, že mu na strane odosielateľa bude postupne odovzdávať jednotlivé bajty, a na strane príjemcu si ich zase bude postupne odoberať. Tým vzniká ilúzia prúdu (angl. stream) jednotlivých bajtov, ktorý nie je nijako štruktúrovaný – všetky prenášané bajty sú považované za rovnocenné. V skutočnosti samozrejme nie sú jednotlivé bity prenášané každý zvlášť. Protokol TCP na strane odosielateľa postupne akumuluje jednotlivé bajty do vyrovnávacej pamäte a po jej naplnení odošle celý jeho obsah naraz vo forme segmentu. Analogicky na strane príjemcu sa dátový obsah segmentu ukladá do vyrovnávacej pamäte a jednotlivé bajty sú entitám vyššej vrstvy poskytované z tejto vyrovnávacej pamäte. Celý mechanizmus združovania jednotlivých bajtov do blokov – segmentácia – je v réžii protokolu TCP, ktorý sa prenosom väčších celkov snaží znížiť pomer objemu riadiacich informácií voči objemu užitočných dát. Pre vyššiu vrstvu je tento mechanizmus neviditeľný – vyššia vrstva pracuje s predstavou prúdu jednotlivých bajtov.

Segment protokolu TCP má nasledujúcu štruktúru:

Zdrojový port (<i>source port</i>) 16 bitov				Cieľový port (<i>destination port</i>) 16 bitov			
Poradové číslo odosielaného bajtu (<i>sequence number</i>) 32 bitov							
Požadované číslo prijatého bajtu (<i>acknowledgement number</i>) 32 bitov							
Dĺžka hlavičky 4 bity	Rezerva 6 bitov	U R G	A C K	P S H	R S T	S Y N	F I N
Binárne nuly				Dĺžka okna (<i>window size</i>)			
Binárne nuly				Ukazovateľ naliehavých dát (<i>urgent pointer</i>) 16 bitov			
Voliteľné položky TCP hlavičky							
DATA							
Prípadná výplň na páry počet bajtov - binárne nuly							

- **Zdrojový port** – port odosielaťa TCP segmentu
- **Cieľový port** – port príjemcu TCP segmentu.
- **Poradové číslo odosielaného bajtu** – poradové číslo prvého bajtu v dátovej časti TCP segmentu v toku dát od odosielaťa k príjemcovi. Tok dát v opačnom smere má samostatné číslovanie svojich dát.
- **Poradové číslo prijatého bajtu** – vyjadruje číslo nasledujúceho bajtu, ktorý je príjemca pripravený prijať, t.j. príjemca potvrdzuje, že správne prijal všetko až do poradového čísla prijatého bajtu mínus jedna.
- **Dĺžka hlavičky** – vyjadruje dĺžku hlavičky TCP segmentu
- **Dĺžka okna** – vyjadruje maximálny objem dát, ktorý je príjemca naraz schopný prijať
- **Príznaky** – 6 príznakových bitov vyjadrujúcich osobitný príkaz alebo operáciu pre príjemcu segmentu
- **Ukazovateľ naliehavých dát** – využívaný veľmi zriedkavo. Umožňuje v segmente preniesť dáta, ktoré má jeho príjemca spracovať mimo poradia (prednostne).

7.3.1 Spôľahlivosť v protokole TCP

V protokole TCP sa spoľahlivosť dosahuje pomocou dvoch mechanizmov: **číslovania** a **potvrdzovania** segmentov.

TCP segmenty nesú poradové, takisto nazývané aj **sekvenčné** čísla. Sekvenčné číslo prvého segmentu začína od náhodnej hodnoty stanovenej pri otvorení spojenia. Sekvenčné číslo každého ďalšieho segmentu sa vypočíta ako sekvenčné číslo predchádzajúceho segmentu zvýšené o objem dát prenesených v tomto predchádzajúcom segmente. Pre príklad, ak boli za sebou odoslané 4 segmenty s veľkosťou 52, 1420, 68 a 512 bajtov, pričom úvodné poradové číslo bolo 2367, potom poradové číslo prvého segmentu je 2367, druhý segment má poradové číslo $2367+52=2419$, tretí segment má poradové číslo $2419+1420=3839$ a štvrtý segment má poradové číslo $3839+68=3907$. Piaty segment by mal poradové číslo

$3907+512=4419$. Pomocou tohto číslovania je jednak jednoznačne určené správne poradie segmentov (musia tvoriť neklesajúcu¹ postupnosť), jednak je možné zistiť, či nejaký úsek dát chýba. Ak by napríklad pri doručovaní vypadol tretí segment, príjemca by dostal prvý segment s poradovým číslom 2367, druhý segment s poradovým číslom 2419, avšak ďalší prijatý segment by mal číslo 3907. Pretože druhý segment má veľkosť 1420 bajtov, ďalší segment v poradí musí byť 3839 a nie 3907. Z tohto rozdielu je príjemcovi jasné, že mu chýba segment, ktorý obsahuje bajty 3839 až 3906.

Tu si treba povšimnúť, že poradové čísla segmentov sú v skutočnosti aj poradové čísla jednotlivých bajtov, ktoré boli odoslané. Hoci nemusia začínať od 0, ale od náhodného počiatočného čísla, predsa sa chápu ako očíslovanie jednotlivých odoslaných bajtov. Sekvenčné číslo segmentu je zároveň poradovým číslom prvého bajtu, ktorý prenáša.

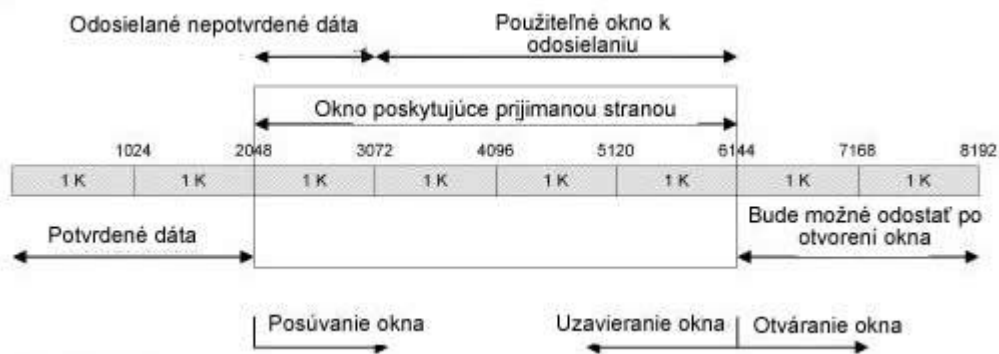
Potvrdzovanie v protokole TCP slúži na informovanie odosielateľa, že doposiaľ odoslané dáta boli buď prijaté v poriadku a je možné s vysielaním pokračovať, alebo niektoré dáta chýbajú a je potrebné ich odoslať znovu. Protokol TCP používa tzv. kladné potvrdzovanie (positive acknowledgement), čo znamená, že potvrdzuje úspešne prijaté dáta, a na chybné prijaté alebo úplne chýbajúce dáta nereaguje (tie potom odosielateľ znovu odošle po vypršaní časového limitu, v ktorom očakával ich kladné potvrdenie). Príjemca segmentov potvrdzuje ich prijatie tak, že odosielateľovi priebežne oznamuje, aké **d'alsie** sekvenčné číslo prijateho bajtu očakáva. Ak príjemca segmentov odosielateľovi zašle potvrdenie s hodnotou 3907, znamená to, že úspešne prijal všetky bajty až po bajt s poradovým číslom 3906 vrátane, a preto má odosielateľ pokračovať odosielaním práve od bajtu 3907. Príjemca vlastne potvrdením odosielateľovi oznamuje, od ktorého bajtu má v odosielaní pokračovať.

7.3.2 Metóda posuvného okna

Naivná implementácia protokolu TCP by mohla pracovať tak, že odosielateľ odošle segment, počká na potvrdenie od príjemcu, potom pošle ďalší segment, opäť počká na potvrdenie, a týmto spôsobom preniesie všetky dáta. Takýto prístup je však neefektívny práve pre spomenuté akcie na potvrdenia medzi jednotlivými segmentmi. TCP, ktoré by pracovalo týmto spôsobom, by síce pracovalo správne, ale dosiahnuteľné prenosové rýchlosti by boli hlboko pod úrovňou prenosovej kapacity siete.

TCP preto v skutočnosti odosiela určitý objem dát v predstihu, bez čakania na prijatie potvrdenia z druhej strany. Tento objem dát sa nazýva veľkosť okna. Samotné okno, takisto nazývané aj posuvné okno (sliding window), je jednoducho dvojica poradových čísel bajtov Od-Do, ktoré je možné odoslať bez čakania na potvrdenie z druhej strany.

¹ Je možné odosielať aj prázdne TCP segmenty obsahujúce iba hlavičku protokolu TCP. V takom prípade sa sekvenčné číslo segmentu nezvyšuje.



Dáta s poradovými číslami menšími ako „Od“ už boli odoslané a úspešne potvrdené. Dáta s poradovými číslami „Od“ až „Do“ sa práve odosielaajú a čakajú na potvrdenie. Dáta s poradovými číslami nad „Do“ sú ešte neodoslané dáta. Ak príjemca odošle potvrdenie prijatých dát, príjemca nastaví ľavý okraj okna, teda index „Od“, na prvý zatiaľ nepotvrdený bajt a index „Do“ zvýši tak, aby okno malo opäť svoju maximálnu veľkosť. Tým sa okno posunulo „doprava“ po odosielaných dátach a dostali sa doň nové, ešte neodoslané dáta, ktoré teraz TCP môže odoslať a čakať na ich potvrdenie. Tento proces sa neustále opakuje. Zvýšenie prenosového výkonu je pri využívaní posuvného okna daný tým, že namiesto čakania odosielateľ posiela ďalšie dáta, priebežne od príjemcu očakáva ich potvrdenia a na ich základe posúva okno po prenášaných dátach.

7.3.3 Riadenie toku dát

Informácia o maximálnej veľkosti okna je v TCP prenášaná spolu s potvrdeniami. Príjemca, ktorý odosiela potvrdenie o prijatých dátach, zároveň v potvrdení odosielateľovi aj oznamuje, najviac koľko dát môže odoslať v ďalšom kroku. Inými slovami, príjemca reguluje maximálnu veľkosť okna u odosielateľa. Čím menšie okno príjemca odosielateľovi predpíše, tým menej dát naraz môže odosielateľ odoslať, potom musí čakať na príchod potvrdenia. Príjemca dokonca môže odosielateľovi zmenšiť jeho dátové okienko až na nulovú veľkosť, a tým vlastne celkom zastaviť vysielanie akýchkoľvek dát.

Protokol TCP sa snaží predchádzať zahlcovaniu uzlov siete aj tým, že i odosielateľ si sám môže zmenšiť veľkosť svojho okna, a to v situácii, kedy sám predpokladá preťaženie komunikačnej siete. Každú stratu odoslaného dátového segmentu (t.j. keď nedorazí kladné potvrdenie do príslušného časového limitu) odosielateľ interpretuje ako dôsledok zahltenia komunikačnej siete. Reaguje na to tým, že si sám zúži svoje okno na polovicu a súčasne s tým predlžuje na dvojnásobok i časový limit, do ktorého očakáva kladné potvrdenie. Pri opakovaných stratách prenášaných segmentov tak veľkosť okienka exponenciálne klesá. Tým sa odosielateľ snaží odosielať dáta pomalšie a poskytnúť tak sieti priestor na zotavenie. Po skončení stavu zahltenia TCP opäť postupne veľkosť okna zvyšuje až na maximálnu veľkosť uvádzanú príjemcom.

7.3.4 Multiplexovanie (súbežný prenos a odlišenie) konverzácií a identifikácia komunikujúcich procesov

Keďže v protokolovom modeli TCP/IP neexistuje relačná vrstva, niektoré jej funkcie na seba preberá transportná vrstva. Medzi tieto funkcie patrí aj identifikácia a separácia komunikačných dialógov a adresovanie prenášaných dát konkrétnemu komunikujúcemu procesu. Pripomeňme, že na strane klienta môže bežať viacero klientských procesov – poštový klient, webový prehliadač, instant messaging klient a podobne. Na strane servera takisto môže bežať viacero služieb – poštový server, webový server, FTP server atď. Ako zabezpečiť, aby webový prehliadač adresoval svoju komunikáciu práve procesu webového servera, poštový klient komunikoval práve s procesom poštového servera, atď.?

Protokol TCP pre tento účel zavádza koncept tzv. **portov**. Port je 16-bitové číslo, ktoré je pridelené konkrétnemu bežiacemu procesu pre jednu konkrétnu sieťovú konverzáciu². Toto číslo pridčuje bežiacemu procesu operačný systém v momente, keď tento proces požiada o vytvorenie alebo akceptovanie sieťovej konverzácie. Pri vzájomnej komunikácii dvojice procesov na rôznych koncových sieťových uzloch sú jednotlivé segmenty konverzácie označované dvojicou čísel portov – zdrojový port (proces, ktorý segmenty odosiela) a cieľový port (proces, ktorému sú segmenty určené). Konverzácia medzi dvojicou uzlov je teda jednoznačne identifikovaná päťicou údajov [Adresa zdrojového uzla, Adresa cieľového uzla, Transportný protokol, Zdrojový port, Cieľový port].

Sieťové služby, teda procesy typu server, očakávajú konverzácie klientov na dopredu známych, spravidla rovnakých číslach portov. Vďaka tomu môžu klienti ľahko adresovať svoje segmenty konkrétnej službe na serveri. Medzi najbežnejšie služby a zodpovedajúce čísla portov patria:

- FTP: Porty 20 a 21
- Secure Shell: Port 22
- Telnet: Port 23
- SMTP: Port 25
- DNS: Port 53
- HTTP: Port 80
- POP3: Port 110
- IMAP: Port 143

Čísla portov, ktoré patria jednotlivým sieťovým službám, spravuje agentúra Internet Assigned Numbers Authority a aktuálny zoznam je možné nájsť na stránke

<http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml>

² Výnimku tvoria procesy typu server, ktoré na porte s tým istým číslom akceptujú viaceré konverzácie.

Čísla portov pridelované od operačného systému klientským procesom sú dynamické a trvajú len po dobu danej konverzácie, potom sa vrátia operačnému systému a môžu byť použité pre inú konverzáciu, či už tým istým alebo iným procesom.

Mohlo by sa javiť, že server, ktorý na tom istom porte obsluhuje všetkých klientov danej služby, nevie medzi nimi správne rozlíšiť, pretože jeden port servera už nie je unikátny pre jednu konkrétnu konverzáciu. Tu si však treba uvedomiť, že konverzácia je jednoznačne identifikovaná päticou [Adresa zdrojového uzla, Adresa cieľového uzla, Transportný protokol, Zdrojový port, Cieľový port]. Ak sa zmení čo len jeden údaj v tejto päťici, jedná sa o novú konverzáciu. Z pohľadu servera teda jednotlivých klientov odlišuje jednak ich adresa (z pohľadu servera je to adresa cieľového uzla), jednak číslo klientského portu (z pohľadu servera je to cieľový port). Aj keby bolo vytvorených niekoľko paralelných spojení od toho istého klienta na ten istý server, klient dostane pre svoje jednotlivé konverzácie od operačného systému rôzne klientské čísla portov, takže tieto konverzácie vždy budú od seba odlišiteľné.

7.4 Transportný protokol User Datagram Protocol

Transportný protokol UDP patrí medzi nespojovo orientované a nespoľahlivé protokoly bez riadenia toku dát. Pojem „nespoľahlivý“ treba chápať vo význame „bez garancie spoľahlivého prenosu dát“. To znamená, že UDP nebude riešiť prípadné straty, preusporiadanie alebo poškodenie prenesených segmentov, avšak neznamená to, že UDP bude cielene vnášať chyby do prenášaných dát. Zo všetkých služieb transportnej vrstvy UDP teda poskytuje iba segmentáciu a adresovanie dát konkrétnym komunikujúcim procesom.

Hlavička UDP segmentov je veľmi jednoduchá, obsahuje len štyri polia:

- **Zdrojový port** – port odosielaťľa UDP segmentu
- **Cieľový port** – port príjemcu UDP segmentu
- **Dĺžka** – celková dĺžka UDP segmentu
- **Kontrolný súčet** – overenie správnosti preneseného UDP segmentu

UDP teda rovnako ako TCP využíva čísla portov pre adresovanie komunikujúcich procesov. Tu sa však jeho podobnosť s protokolom TCP končí.

Mohlo by sa javiť, že pri kvalitných vlastnostiach protokolu TCP nemá existencia protokolu UDP vôbec význam. Nie je to tak. Predovšetkým, protokol TCP umožňuje len komunikáciu typu bod-bod, teda vždy medzi párom uzlov, medzi ktorými sa vytvorí TCP spojenie. TCP nedokáže realizovať hromadnú komunikáciu typu bod-multibod, na ktorej je založená napríklad internetová televízia (IPTV) – odosielanie dát z jedného zdroja mnohým príjemcom naraz. Ak je potrebné doručovať dáta technológiou multicast (od jedného odosielaťľa k viacerým príjemcom naraz) alebo broadcast (od jedného odosielaťľa ku všetkým príjemcom naraz), TCP nie je možné využiť.

Ďalšou vlastnosťou TCP, ktorá paradoxne môže byť i nevhodná, je jeho spoľahlivosť. Ak sa v TCP stratí počas doručovania dát segment, TCP nemôže v odosielaní pokračovať, kým sa

stratený segment nepodarí jeho opakovaným odoslaním doručiť k príjemcovi. Vyplýva to zo základnej techniky okna, ktorú TCP používa. Tento princíp nie je vhodný pre služby v reálnom čase, napríklad IP telefónia, internetový rozhlas, video či televízia, v ktorých je dôležitejší trvalý plynulý tok dát než občas stratený segment. Pre služby v reálnom čase sa teda TCP nehodí.

Naviac, pre niektoré služby je režia, ktorú TCP vkladá do prenosu, nepomerne veľká v porovnaní s objemom užitočnej prenesenej informácie. Pre príklad, protokol DNS je jednoduchý protokol typu otázka-odpoveď. Ak by sa však DNS konverzácia mala prenášať pomocou DNS, na dvojicu DNS správ otázka-odpoveď by celkovo pripadalo 10 TCP správ (3 TCP správy na otvorenie TCP spojenia, prenos otázky, potvrdenie, prenos odpovede, potvrdenie, 3 TCP správy na uzatvorenie TCP spojenia). V porovnaní s jednoduchosťou protokolu DNS je tento sled správ jednoducho hrubo neefektívny.

Všetky tieto fakty sú dôvodom, prečo potrebujeme aj protokol UDP.

Kvôli chýbajúcej spoľahlivosti sa aplikácie nad UDP musia zmieriť s prípadnými stratami segmentov, ich preusporiadaním, duplikáciou alebo chybami. Obvykle však aplikácie používajúce UDP podobný opravný mechanizmus nepotrebujú a dokonca ním môžu byť zdržované, prípadne si ho môžu implementovať sami na aplikačnej úrovni.

Aj keď celkové množstvo UDP prevádzky na typickej sieti je rádovo len niekoľko percent, UDP používa celý rad kľúčových služieb, vrátane DNS, SNMP, DHCP, RIP a služieb v reálnom čase.

Kľúčové slová:

1. Segmentácia, segment
2. End-to-end komunikácia
3. Spoľahlivý resp. nespoľahlivý prenos
4. Spojovo orientovaný resp. nepojovo orientovaný prenos
5. Riadenie toku dát
6. Posuvné okno
7. Sekvenčné číslo
8. Port
9. TCP
10. UDP

Kontrolné otázky:

1. Aké sú funkcie transportnej vrstvy?
2. Čo je to spojovo orientovaný typ komunikácie?
3. Čo je to nepojovo orientovaný typ komunikácie?
4. Čo je to riadenie toku dát?
5. Čo je to segmentácia?
6. Čo v kontexte transportnej vrstvy vyjadruje pojem spoľahlivosť?
7. Čo znamená pojem end-to-end komunikácia?
8. Ako transportná vrstva v protokolovom modeli TCP/IP oddeľuje medzi sebou jednotlivé konverzácie medzi klientom a serverom?

9. Ako transportná vrstva v protokolovom modeli TCP/IP umožňuje klientovi vybrať si konkrétnu službu, s ktorou chce na serveri komunikovať?
10. Čo je to transportný port?
11. Aký je dôvod riadenia toku dát na transportnej vrstve?
12. Aký je význam techniky okna na transportnej vrstve?
13. Aký je rozdiel medzi protokolmi TCP a UDP?
14. Prečo aplikácie v reálnom čase nepotrebujú spoľahlivú službu?

8 Prezentačná a relačná vrstva

Ciele

Čo by mal študent vedieť:

- Úlohy a funkcie prezentačnej a relačnej vrstvy spojené s problematikou spoločného formátu a významu prenášaných dát a riadenia komunikačných vzťahov – relácií
- Umiestnenie služieb prezentačnej a relačnej vrstvy v protokolovom modeli TCP/IP
- Vybrané spôsoby realizácie funkcií prezentačnej vrstvy v protokoloch TCP/IP

V kapitole o aplikačnej vrstve sme sa zaoberali tým, ako používateľské aplikácie pomocou aplikačných protokolov dokážu svojim používateľom sprostredkovať rôzne služby – WWW, elektronickú poštu, prenos súborov atď. Nehovorili sme pritom, ako sa dáta medzi komunikujúcimi aplikáciami prenesú. Jednoducho sme len predpokladali, že vieme dopraviť dáta, ktoré vytvorila odosielajúca aplikácia, cieľovej aplikácii, a že im bude cieľová aplikácia správne rozumieť. V skutočnom svete však nie je tento proces taký priamočiary.

Jedným z problémov, ktoré treba pri komunikácii dvojice rôznych aplikácií vyriešiť, je otázka spoločného formátu dát. Napríklad webový prehliadač je schopný zobraziť veľké množstvo druhov obrázkov. Pred tým, ako však môže obrázok vykresliť, musí rozpoznať jeho formát (BMP, JPG, GIF, PNG apod.). Podobne, webový prehliadač musí správne rozpoznať, prípadne i konvertovať znakovú sadu, v ktorej je HTML stránka napísaná, aby správne zobrazil národné znaky. Musí preto existovať mechanizmus, ktorým sa aplikácie navzájom informujú o formáte a význame dát, ktoré si posielajú.

Ďalšou úlohou, ktorú treba riešiť, je, aby dáta boli doručené správne procesu (bežiacей aplikácii) u príjemcu. Na počítači používateľa totiž môže súčasne bežať množstvo procesov – webový browser, poštový klient, nástroj pre instant messaging apod. Takisto na jednom serveri môže bežať niekoľko sieťových služieb súčasne. Potrebujeme preto mechanizmus, ktorý zabezpečí, aby sa aplikačné dáta doručili vždy správne procesu – aby webový browser komunikoval s webovým serverom, poštový klient s poštovým serverom apod.

Obom týmto úlohám sa v RM OSI venujú dve vrstvy – prezentačná a relačná.

8.1 Prezentačná vrstva

Prezentačná vrstva je 6. vrstva RM OSI. Svoje služby poskytuje priamo aplikačnej vrstve, pod ktorou sa nachádza. Úlohou prezentačnej vrstvy je zabezpečiť, aby komunikujúce aplikácie správne rozumeli významu a formátu údajov, ktoré si medzi sebou prenášajú, a v prípade potreby vedeli tento formát previesť (konvertovať) na iný. Povedané inými slovami, prezentačná vrstva sprostredkuje rovnaký formát dát, ktoré sa prenášajú medzi entitami aplikačnej vrstvy. Medzi jednotlivé operácie, ktoré prezentačná vrstva vykonáva, patria:

- Identifikácia významu a formátu prenášaných dát

- Konverzia formátu prenášaných dát
- Kompresia a dekompresia aplikačných dát
- Šifrovanie aplikačných dát

Autori protokolového modelu TCP/IP osobitnú prezentačnú vrstvu do svojho modelu nezahrnuli, preto v TCP/IP neexistuje osobitný prezentačný protokol. Funkcie prezentačnej vrstvy preto obvykle vykonáva samotná aplikácia. Napriek tomu sú funkcie prezentačnej vrstvy veľmi dôležité a mnohé aplikácie interne implementujú činnosti, ktoré zodpovedajú práve operáciám prezentačnej vrstvy.

Otázka výmeny dát v spoločnom formáte je veľmi obsiahla, budeme sa preto venovať len niektorým jej aspektom – kódovým stránkam, bajtovému poradiu v binárnych dátach a spôsobu identifikácie významu a formátu prenášaných dát v textových protokoloch.

8.1.1 Kódové stránky

Veľkú skupinu aplikačných programov tvoria nástroje pre spracovanie a zobrazenie textov. Sem patria rôzne editory, prezentačné nástroje, ale aj webové prehliadače, poštovní klienti a ďalšie aplikácie, ktoré umožňujú spracovať, zobraziť či prenášať textovú informáciu. Reprezentácia textu, najmä s ohľadom na špeciálne znaky v rôznych národných abecedách, však prešli pomerne dlhým vývojom.

Každý znak (písmeno abecedy) je v počítači reprezentované ako jeden alebo skupina viacerých bajtov. Historicky staršie počítače používali iba anglickú abecedu a vybrané špeciálne znaky. Každé písmeno a špeciálny znak tejto abecedy boli v počítači reprezentované unikátnou jednobajtovou číselnou hodnotou. Znak tejto abecedy boli teda v stanovenom poradí očíslované a konkrétne číslo v počítači reprezentovalo znak na danej pozícii v abecede. Tabuľka, ktorá definuje poradie a očíslovanie znakov tejto abecedy, sa nazýva kódová tabuľka alebo kódová stránka. Najpoužívanejšia kódová stránka so základnou anglickou abecedou a vybranými špeciálnymi znakmi sa nazýva **ASCII** (American Standard Code for Information Interchange). V tejto tabuľke sa nachádza 33 špeciálnych, tzv. riadiacich znakov, ktoré sú určené pre riadenie zobrazovacích alebo tlačových zariadení, a 95 alfanumerických znakov. Spolu teda ASCII tabuľka obsahuje 128 znakov, na očíslovanie ktorých stačí 7 bitov (hodnoty 0 až 127). Preto sa o ASCII tabuľke niekedy hovorí aj ako o 7-bitovom kódovaní. Samozrejme, počítače pracujú s 8-bitovými bajtmi. Najvyšší bit každého bajtu, ktorý v počítači reprezentuje text, je teda pri ASCII kóde nevyužitý – buď je nastavený na hodnotu 0, alebo ho rôzne aplikácie využívajú pre svoje interné, navzájom nekompatibilné účely.

Pre bežný anglický text je sústava písmen a znakov v ASCII tabuľke úplne dostatočná. ASCII tabuľka však neobsahuje žiadne neanglické písmená, takže pomocou nej nie je možné v počítači vyjadriť napríklad text v slovenčine s využitím mäkčeňov a dĺžňov (t.j. národných znakov). Preto začali vznikať pre jednotlivé jazyky a ich abecedy rôzne nové kódové tabuľky, ktoré jednotlivým hodnotám bajtov priradzovali znaky národných abecied. Aby bolo možné v jednej tabuľke vyjadriť čo najviac rôznych znakov, tabuľky pre národné jazyky už

využívajú všetkých 8 bitov v bajte, a teda obsahujú celkom 256 rôznych znakov vrátane riadiacich kódov.

Pre rôzne jazyky a rôzne abecedy teda vznikali rôzne kódové stránky, keďže v jednej kódovej stránke s 256 znakmi prirodzene nie je možné vyjadriť znaky všetkých existujúcich národných abecied. Navyše, v prvopočiatoch podpory národných jazykov neboli jednotliví tvorcovia kódových stránok koordinovaní. Napríklad pre slovenskú abecedu vznikli minimálne 4 rôzne kódové stránky (Windows 1250, DOS 852, ISO 8859-2, Kamenický) líšiace sa poradím i zastúpením jednotlivých národných znakov. Rôzne operačné systémy tak používali rôzne kódové stránky – DOS používal kódovú stránku 852 alebo Kamenický, systémy typu Unix využívali ISO 8859-2, zatiaľ čo Windows mali svoju kódovú stránku 1250. To veľmi znepríjemňovalo prenos textových dokumentov medzi rôznymi operačnými systémami. Obzvlášť viditeľné boli tieto rozdiely v začiatkoch služby WWW, kedy HTML dokument vytvorený pod jedným operačným systémom nebol korektne zobrazený v prehliadači pod iným operačným systémom. Napríklad rad písmen „řščťžýáíé“ v kódovaní ISO 8859-2 by prehliadač očakávajúci kódovanie Windows 1250 zobrazil ako „µaç»řýáíé“.

Ešte závažnejší problém než existencia rôznych kódových stránok pre tú istú abecedu však bol fakt, že žiadna kódová stránka neobsahovala všetky existujúce svetové abecedy a znaky. Neexistoval teda nijaký jednoduchý spôsob, ako vytvoriť textový dokument písaný v rôznych jazykoch či abecedách. Ak by dokument pozostával z častí písaných pod rôznymi kódovými stránkami, neexistoval by univerzálny spôsob, ako rozoznať, ktorá časť je písaná akou kódovou stránkou. Nedostatky plynúce z duplicity rôznych kódových stránok a neexistencie univerzálnej kódovej stránky viedli koncom 80. rokov 20. storočia ku vzniku iniciatívy, ktorú dnes poznáme pod názvom **Unicode**. Unicode je kódovací štandard, ktorým je možné konzistentne popísať 1 114 112 ($=2^{16} \cdot 17$) rôznych znakov. Keďže tento počet znakov je podstatne väčší, než je možné vyjadriť hodnotou jedného bajtu, Unicode zároveň definuje aj niekoľko spôsobov – formátov, ako jednotlivé znaky jednoznačne vyjadriť jednobajtovými alebo viacbajtovými hodnotami. Najpoužívanejším formátom je tzv. **UTF-8**, ktorý používa premenlivú dĺžku kódovania. Znaky starej ASCII tabuľky, ktorá bola bez zmeny prevzatá ako prvých 128 znakov kódu Unicode, UTF-8 kóduje do jednobajtových hodnôt, a národné znaky väčšiny abecied založených na latinke vrátane slovenských znakov kóduje ako dvojbajtové hodnoty. Využívanie Unicode a UTF-8 konečne odstraňuje problémy, ktoré boli spôsobené nekompatibilitou rôznych predchádzajúcich kódových stránok, a dovoľuje vytvárať skutočne viacjazyčné dokumenty bez obmedzení.

8.1.2 Kódovanie binárnych dát do textového tvaru

V predchádzajúcej časti sme uviedli, že staršie počítače využívali kódovú stránku ASCII so 128 znakmi. Pretože na popísanie 128 znakov stačí 7 bitov, mnohé staršie aplikácie určené na prenos textových informácií predpokladali, že prenášané bajty reprezentujúce text majú svoj najvyšší bit nevyužitý. Tento najvyšší bit potom tieto aplikácie ignorovali, prípadne nulovali či interne využívali na vlastné účely. Pokiaľ sa týmito aplikáciami naozaj prenášal iba text podľa ASCII tabuľky, všetko fungovalo správne. Len čo sa však pomocou týchto

aplikácií mal preniesť text podľa inej kódovej stránky, ktorá využívala viac než 128 hodnôt v bajte, prípadne binárne súbory, nastávali problémy – aplikácie buď nerešpektovali a strácali hodnotu najvyššieho bitu v bajte, prípadne si jeho hodnotu interne interpretovali po svojom a nepracovali korektne. Hoci v súčasnosti preferujeme kódovanie podľa štandardu Unicode, nie všetky aplikácie, sieťové protokoly či štandardy boli upravené na jeho využívanie. Namiesto toho využívame spôsob, ako všeobecné binárne dáta zapísať ako text podľa kódovania ASCII a späťne ho z tohto kódovania transformovať do pôvodných binárnych dát.

Najpoužívanejším spôsobom takéhoto prepisu binárnych dát na ASCII formát v súčasnosti je tzv. kód **Base64**. Základný princíp je jednoduchý:

1. Vstupné binárne dáta sa načítavajú v skupinách po 3 bajtoch, t.j. 24 bitoch
2. Načítaná 24-bitová skupina sa rozdelí na štyri 6-bitové podskupiny
3. Každá z týchto 6-bitových podskupín sa vyjadří vhodným ASCII alfanumerickým znakom a prenáša sa v ASCII kódovaní

Pretože 6-bitová podskupina môže nadobúdať hodnoty v rozsahu od 0 po 63, zatiaľ čo kód ASCII obsahuje až 95 alfanumerických znakov, ku každej 6-bitovej podskupine je teda možné ľahko priradiť alfanumerický znak z ASCII tabuľky, ktorý je určite 7-bitový. Týmto postupom je teda možné vstupné binárne dáta transformovať do kódovania ASCII za cenu mierneho zväčšenia ich objemu – na každé tri vstupné bajty pripadajú štyri výstupné bajty. Konkrétne priradenie ASCII znakov hodnotám 6-bitových podskupín v Base64 je takisto jednoduché:

- **Hodnoty 0 až 25:** Znaký **A až Z** anglickej abecedy
- **Hodnoty 26 až 51:** Znaký **a až z** anglickej abecedy
- **Hodnoty 52 až 61:** Znaký **0 až 9**
- **Hodnota 62:** Znak **+**
- **Hodnota 63:** Znak **/**

Názov Base64 vyjadruje skutočnosť, že vstupné dáta sú po transformácii vyjadrené v číselnej sústave so základom 64 (každá 6-bitová podskupina reprezentuje jednu číslicu v rozsahu hodnôt 0-63).

Pre príklad si demonštrujeme kódovanie reťazca bajtov s hodnotami **197, 146, 51, 211, 97, 254** do ASCII podľa algoritmu Base64

1. Vstupné dáta načítavame po trojiciach bajtov. Prvá trojica je teda 197, 146, 51, binárne **11000101, 10010010, 00110011**. Druhá trojica je 211, 97, 254, binárne **11010011, 01100001, 11111110**.
2. Prvá trojica rozdelená na 6-bitové skupiny je **110001, 011001, 001000, 110011**, dekadicky **49, 25, 8, 51**. Druhá trojica rozdelená na 6-bitové skupiny je **110100, 110110, 000111, 111110**, dekadicky **52, 54, 7, 62**.
3. Hodnotám 49, 25, 8, 51 zodpovedajú podľa vyššie uvedeného mapovania ASCII alfanumerické znaky **x, Z, I, z**. Hodnotám 52, 54, 7, 62 zodpovedajú ASCII

alfanumerické znaky **0, 2, H, +**. Touto transformáciou teda zo šiestich vstupných bajtov vznikol osemznakový ASCII reťazec „**xZlZ02H+**“.

Spätná transformácia sa deje v opačnom poradí operácií, t.j. alfanumerickým znakom v kóde Base64 sa najprv priradia zodpovedajúce 6-bitové hodnoty a po načítaní štyroch 6-bitových hodnôt sa tieto prepíšu na tri 8-bitové hodnoty, čím sa získajú dáta v pôvodnom tvare.

Kódovanie pomocou Base64 je veľmi obľúbené v aplikáciách elektronickej pošty. Prakticky všetky binárne prílohy správ elektronickej pošty sú transformované do ASCII práve pomocou Base64. Takisto diakritika v mene odosielateľa, príjemcu správy či v jej predmete je v konkrétnej kódovej stránke konvertovaná pomocou Base64 do ASCII, aby ju bolo možné bez problémov preniesť aj poštovými systémami, ktoré správne pracujú len so 7-bitovým textovým kódom.

8.1.3 Systémy typu „big-endian“ a „little-endian“

Doposiaľ sme sa zaoberali prenosom textových dát medzi počítačmi, prípadne prepisom binárnych dát do textového tvaru. Samozrejme, binárne dáta je možné pomocou vhodných protokolov a aplikačných služieb prenášať medzi počítačmi v pôvodnom binárnom tvare. I tu však číha jedno nebezpečenstvo, ktorého pôvod sa v angličtine označuje pojmami „**big-endian**“ resp. „**little-endian**“.

Predstavme si obyčajnú celočíselnú premennú, ktorú by sme v jazyku C definovali príkazom `int i;`. Takáto celočíselná premenná má v pamäti vyhradené 4 bajty. Nezávisle od toho, či do nej uložíme hodnotu napríklad 0, 7632 alebo 1 072 790 071, vždy bude v pamäti zaberat' 4 bajty.

Všimnime si konkrétne hodnotu 1 072 790 071. Jej zápis v hexadecimálnej sústave je **0x3ff17a37**, čo znamená, že jednotlivé bajty tejto 4-bajtovej premennej majú hodnotu **0x3f**, **0xf1**, **0x7a**, **0x37**. Bajt 0x3f úplne vľavo sa označuje ako **najvyšší** bajt (Most Significant Byte), bajt 0x37 úplne vpravo sa označuje ako **najnižší** bajt (Least Significant Byte). Otázkou však je – v akom poradí sú tieto jednotlivé 4 bajty uložené v pamäti nášho počítača?

Spontánnou odpoveďou by bolo – „predsa v tom poradí, v akom sme ich práve uviedli!“. Táto odpoveď však vôbec nie je samozrejماً. Skutočné poradie bajtov viacbajtových premenných, v akom sú uložené v pamäti počítača v smere rastúcich pamäťových adries, totiž veľmi silne závisí od architektúry CPU. Procesory Intel či AMD patria medzi procesory, ktoré do pamäti ukladajú viacbajtové premenné v poradí **od najnižšieho bajtu po najvyšší**, t.j. v presne opačnom, než by sme očakávali. Číslo 0x3ff17a37 je pri týchto procesoroch uložené do pamäti v poradí 0x37, 0x7a, 0xf1, 0x3f. Keďže viacbajtové premenné sa pri týchto procesoroch ukladajú do pamäti v poradí od svojho najnižšieho bajtu po najvyšší, tieto procesory sa nazývajú v angličtine pojmom „**little-endian**“. Takisto sa niekedy uvádza označenie **LSB First**.

Procesory označované ako „**big-endian**“ ukladajú viacbajtové premenné do pamäti v poradí **od najvyššieho bajtu po najnižší**, teda MSB First. Medzi tieto procesory patria SPARC, PowerPC či Itanium.

Táto zdanlivá nuansa sa veľmi rýchlo prejaví ako problém, ak medzi dvojicou počítačov chceme prenášať binárne dáta. Ak totiž aplikácia prikáže odoslať napríklad hodnotu celočíselnej premennej druhému počítaču, operačný systém odošle hodnotu premennej v presne takom tvare, v akom je uložená v pamäti. Ak prijímajúci operačný systém beží na počítači, ktorý používa iné poradie bajtov než odosielaajúci počítač, prenesená viacbajtová hodnota sa vyhodnotí nesprávne.

Riešením tohto problému je stanoviť dohodnuté poradie bajtov viacbajtových premenných počas ich prenosu cez sieť, nezávisle od toho, aké poradie používa odosielaajúca a prijímajúca strana. Ak toto poradie je inakšie, pri odoslaní resp. prijatí dát si musíme realizovať ich zodpovedajúcu konverziu, no môžeme sa aspoň spoľahnúť na dohodnuté poradie bajtov pri ich prenose cez sieť. **Pre protokoly v protokolovom modeli TCP/IP je týmto dohodnutým poradím bajtov poradie od MSB, t.j. „big-endian“.** Toto poradie sa v anglickej literatúre často označuje aj pojmom „**network byte order**“.

8.1.4 Identifikácia a konverzia formátu prenášaných dát v textových protokoloch

Existuje veľa spôsobov, ako si komunikujúce aplikácie vedia oznámiť význam a formát prenášaných dát. Nasledujúci text treba preto chápať ako ukážku vybraných možností, nie ako vyčerpávajúci zoznam.

Všimnime si jeden z najbežnejších aplikačných protokolov – HTTP. Hoci tento protokol má svoju veľmi špecifickú úlohu – umožňuje prenos dát medzi webovým prehliadačom a serverom – tieto dáta môžu byť rôzneho významu a formátu. Pomocou HTTP môžeme preniesť HTML, XHTML či XML stránku, obrázkov v rôznych formátoch, obraz CD/DVD, spustiteľný súbor, archív, video či audio záznam a mnohé ďalšie druhy súborov. HTTP preto význam, prípadne i formát prenášaného obsahu vždy identifikuje v odpovedi servera niekoľkými textovými riadkami. Všimnime si HTTP dialóg, ktorý sme už raz použili v kapitole o aplikačných protokoloch:

```
GET /kt/pozdrav.html HTTP/1.1
Host: www.kis.fri.uniza.sk
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:6.0.2) Gecko/20100101
Firefox/6.0.2
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: sk,cs;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Accept-Charset: ISO-8859-2,utf-8;q=0.7,*;q=0.7
```


Connection: close

HTTP/1.1 200 OK

Date: Fri, 25 Nov 2011 09:01:42 GMT

Server: Apache/2.2.16

Last-Modified: Fri, 25 Nov 2011 08:55:33 GMT

Content-Length: 61

Connection: close

Content-Type: text/html

<HTML>

<BODY>

Ukazkova HTML stranka.

</BODY>

</HTML>

Tučným podčiarknutým písmom sú vysádzané riadky HTTP protokolu, ktoré medzi prehliadačom a serverom sprostredkujú činnosti prezentačnej vrstvy.

Riadok **Accept** v žiadosti od WWW prehliadača uvádza, aké formáty dokumentov prehliadač akceptuje. V zobrazenej žiadosti WWW prehliadač najviac preferuje dokumenty HTML a XHTML+XML. Ak dokument tohto formátu nie je na serveri k dispozícii, WWW prehliadač ďalej preferuje dokument typu XML, a ak ani ten na serveri neexistuje, potom akýkoľvek iný formát. Poradie preferencie určuje atribút „q“³ v rozsahu od 0 po 1. Ak nie je pri konkrétnom formáte uvedený, automaticky sa berie hodnota 1 (najviac preferovaný).

Riadok **Accept-Language** v žiadosti od WWW prehliadača uvádza preferované jazykové mutácie stránky. Ak má server tú istú stránku k dispozícii v rôznych jazykoch, môže klientovi ponúknuť ten jazyk, ktorý klient preferuje. V zobrazenej žiadosti WWW prehliadač najviac preferuje jazyky v poradí slovenský, český, v americkej angličtine, v ľubovoľnej angličtine. Toto poradie zodpovedá preferovaným jazykom, ktoré si používateľ nastavil vo vlastnostiach svojho prehliadača.

Riadok **Accept-Encoding** uvádza, či WWW prehliadač podporuje kompresiu a dekompresiu⁴ obsahu prenášanej stránky v reálnom čase. Rozsiahle WWW stránky je možné v momente odosielania zo servera komprimovať a tým zmenšiť ich veľkosť, preniesť ku klientovi za kratší čas a u klienta opäť dekomprimovať do pôvodného tvaru. Keďže

³ Pôvodne pochádza zo slov „quality factor“ – čím vyššia hodnota faktora, tým vyššia predpokladaná kvalita obsahu.

⁴ Pojmy „kompresia“ a „dekompresia“ tu označujú operácie nad dátami, ktoré ich umožnia prenášať v skrátenej tvare, aby ich prenos trval kratší čas (typické kompresné/dekompresné programy sú napríklad ZIP alebo RAR).

kompresných algoritmov existuje niekoľko, WWW prehliadač tu uvádza, ktoré z týchto algoritmov pozná.

Nakoniec, riadok **Accept-Charset** vymenúva preferované znakové sady klienta, teda kódové stránky alebo kódovanie národných znakov. Ak sa na serveri nachádza požadovaný obsah vo viacerých kódových stránkach, server môže klientovi poskytnúť stránku v preferovanom kódovaní. V našom príklade je najprv preferované kódovanie ISO 8859-2 a po ňom kódovanie UTF-8.

V odpovedi servera sa nachádzajú dva riadky, ktoré súvisia s funkciami prezentačnej vrstvy. Riadok **Content-Length** informuje prehliadač o veľkosti odovzdaného dokumentu – v našom prípade 61 bajtov. Riadok **Content-Type** informuje o význame preneseného dokumentu, ktorým je textový dokument vo formáte HTML. Touto dvojicou riadkov webový server informoval prehliadač o veľkosti správy a o jej formáte.

V nasledujúcich ukážkach sa nachádza niekoľko rôznych žiadostí webového prehliadača o obsah rôzneho formátu a odpoveď servera. Nepodstatné riadky zo žiadostí sú kvôli prehľadnosti odstránené a telá dokumentov sú zámerne vynechané.

```
GET / HTTP/1.1
Host: www.kis.fri.uniza.sk
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
```

```
HTTP/1.1 200 OK
Server: Apache/2.2.16
Content-Type: text/html; charset=utf-8
```

V tejto konverzácii WWW prehliadač požiadal o hlavnú webovú stránku sídla www.kis.fri.uniza.sk. Server odpovedá textovým dokumentom typu HTML v kódovaní UTF-8.

```
GET /images/Logos/logo_kis_120x750.png HTTP/1.1
Host: www.kis.fri.uniza.sk
Accept: image/png,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
```

```
HTTP/1.1 200 OK
Server: Apache/2.2.16
Content-Length: 17575
Content-Type: image/png
```

V tejto konverzácii WWW prehliadač požiadal server `www.kis.fri.uniza.sk` o súbor `logo_kis_120x750.png` v priečinku `/images/Logos`. Server odosiela tento súbor a informuje, že sa jedná o obrázok (image/png) formátu PNG.

```
GET /~peterp/ROUTE/ROUTE%20IS-IS.ppt HTTP/1.1
Host: frix.fri.uniza.sk
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
```

```
HTTP/1.1 200 OK
Server: Apache/2.2.19 (Debian)
Content-Length: 977920
Content-Type: application/vnd.ms-powerpoint
```

V tejto konverzácii WWW prehliadač požiadal server `frix.fri.uniza.sk` o dokument s názvom `ROUTE IS-IS.ppt` (zápis `%20` v pôvodnej žiadosti predstavuje hexadecimálny ASCII kód znaku medzera). Server odosiela tento dokument a informuje, že sa jedná o prezentáciu programu Microsoft PowerPoint.

```
GET /debian-cd/6.0.6/amd64/iso-cd/debian-6.0.6-amd64-netinst.iso
HTTP/1.1
Host: hammurabi.acc.umu.se
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
```

```
HTTP/1.1 200 OK
Server: Apache/2.2.22 (Unix)
Content-Length: 176160768
Content-Type: application/octet-stream
```

V tejto konverzácii WWW prehliadač požiadal server `hammurabi.acc.umu.se` o súbor s názvom `debian-6.0.6-amd64-neinst.iso`. Server odosiela tento súbor, pričom uvádza, že sa jedná o bližšie nešpecifikované binárne dáta (application/octet-stream).

Veľmi podobný princíp popisu formátu obsahu sa používa aj v správach elektronickej pošty. Všimnime si túto hlavičku správy elektronickej pošty (telo správy je odstránené):

```
Message-ID: <50C5E75A.3050003@fri.uniza.sk>
Date: Mon, 10 Dec 2012 14:44:58 +0100
From: =?UTF-8?B?UGV0ZXIgaUGFsw7pjaA==?= <Peter.Paluch@fri.uniza.sk>
Organization: =?UTF-8?B?xb1pbGluc2vDoSB1bml2ZXJ6aXRhLCBLSVMgRlJJ?=?
MIME-Version: 1.0
To: =?UTF-8?B?TWYydGluIMSMZWNodmFsYQ==?= <martin@cechvala.eu>
```

```
Subject: Ako bolo? :)
```

```
Content-Type: text/plain; charset=UTF-8; format=flowed
```

```
Content-Transfer-Encoding: 7bit
```

Riadok Content-Type informuje, že samotná správa je bežný text (text/plain) v kódovaní UTF-8. Častou alternatívou je formát HTML (text/html). Riadok Content-Transfer-Encoding informuje, že samotné telo správy je vyjadrené v 7-bitovom ASCII kódovaní (t.j. ak má prenášať špeciálne znaky, potom používa napr. Base64). Všimnime si tiež, že položky From, Organization a To obsahujú reťazec, ktorý je zapísaný v Base64 kódovaní a po prevode nazad do binárneho formátu sa jedná o text v kódovaní UTF-8. V skriptovacom jazyku Python je možné veľmi ľahko zistiť obsah pôvodných textov:

```
>>> import base64
>>> print (base64.decodestring('UGV0ZXIgaUGFsw7pjaA=='))
Peter Palúch
>>> print
(base64.decodestring('xb1pbGluc2vDoSB1bml2ZXJ6aXRhLCBLSVMgR1JJ'))
Žilinská univerzita, KIS FRI
>>> print (base64.decodestring('TWFyYdGluIMSMZWNodmFsYQ=='))
Martin Čechvala
```

8.2 Relačná vrstva (Session layer)

Relačná vrstva je piatou vrstvou modelu RM OSI. Úlohou relačnej vrstvy je **riadenie komunikačných vzťahov, tzv. relácií** alebo dialógov, medzi komunikujúcimi aplikáciami. Medzi jednotlivé činnosti, ktoré relačná vrstva vykonáva, patria:

- Doručovanie dát konkrétnym komunikujúcim aplikáciám
- Identifikácia a rozlíšenie jednotlivých komunikačných dialógov
- Riadenie dialógov (ktorá aplikácia má kedy právo odosielať dáta)
- Stanovovanie významných momentov v dialógu a možnosť vrátiť sa k nim (checkpointing)

Zámerom autorov RM OSI bolo, aby relačná vrstva v sebe združovala všetky operácie, ktoré sa týkajú samotného riadenia relácií (dialógov, konverzácií) medzi komunikujúcimi aplikáciami. Jednou z prirodzených úloh je zabezpečenie, aby konverzáciu spracovala tá aplikácia, pre ktorú je konverzácia určená. Ak medzi klientom a serverom prebieha niekoľko konverzácií súčasne, napríklad prenos WWW stránky aj elektronickej pošty, potom si určite želáme, aby HTTP dialóg prebiehal medzi WWW prehliadačom a serverom, zatiaľ čo POP3 dialóg má prebiehať medzi poštovým klientom a serverom. To isté platí aj o situácii, kedy aj v jednej službe (napr. WWW) prenášame súbežne niekoľko nezávislých obsahov, napr. sťahujeme viaceré DVD obrázky z jedného WWW servera. Jednotlivé konverzácie alebo

dialógy musia byť jasne identifikované a oddelené od seba, inak by došlo k neželanému zmiešaniu prenášaných dát a k ich znehodnoteniu.

Ďalšie očakávané funkcie prezentačnej vrstvy sú menej bežné. Jednou z nich je schopnosť definovať počas dialógov význačné momenty, ku ktorým je neskôr možné sa vrátiť, čím sa celý dialóg vráti na stav, v ktorom sa nachádzal v danom momente (efektívne sa jedná o UNDO operáciu). Pomocou tejto schopnosti malo riadenie dialógov nadobudnúť tzv. transakčnú povahu. Pojmom transakcia predstavuje všeobecne istý sled operácií, ktoré sa buď vykonajú všetky s trvalým výsledkom, alebo je možné ich účinok úplne odvolať a vrátiť sa do stavu pred vykonaním prvej z nich. Príkladom môže byť napr. finančná transakcia spočívajúca v odpísaní určitej čiastky z jedného účtu a pripísanie tejto čiastky na účet iný. Určite by nebolo správne, ak by prebehla len jedna časť transakcie – odpísanie čiastky z jedného účtu – a ostatné časti, napríklad pripísanie na iný účet, by sa už nevykonali, bez možnosti celú transakciu odvolať a vrátiť účty do pôvodného stavu. Pretože však mnohé aplikácie natoľko precízne operácie nad dialógmi nevyžadujú, nebýva relačná vrstva v celej svojej úplnosti implementovaná. V protokolovom modeli TCP/IP nie je táto vrstva uvažovaná vôbec. Jej funkcie – ak sú potrebné – sú vykonávané v samotných aplikáciách. Preto sa v popise relačnej vrstvy sústredíme len na princípy, ale nebudeme sa zaoberať ich implementáciou.

8.2.1 Funkcie relačnej vrstvy

Medzi základné **funkcie relačnej vrstvy** sú:

- Nadviazanie, udržiavanie a ukončovanie relácií
- Riadenie obojsmerného dialógu – zaistenie správneho striedania komunikačných systémov pri vysielaní
- Synchronizácia – zaistenie súladu medzi dátami vysielanými odosielateľom a prijímanými príjemcom

8.2.2 Nadviazanie, udržiavanie a ukončovanie relácií

Samozrejmovou vlastnosťou relačnej vrstvy je samotné vytvorenie, udržiavanie a **ukončenie relácie** čiže komunikačného vzťahu medzi komunikujúcimi aplikáciami na vzdialených uzloch prepojených komunikačnou sieťou. Súčasťou vytvorenia relácie je aj informácia, medzi ktorými bežiacimi aplikáciami (procesmi) sa relácia vytvára. Tým je zaistené, že konverzácia dvoch konkrétnych procesov bude vždy doručená práve im a nebude spracovaná inými bežiacimi aplikáciami na cieľových komunikujúcich uzloch.

Dôležitým predpokladom na to, aby bolo možné reláciu vytvoriť, je schopnosť doručovať dáta medzi koncovými komunikujúcimi uzlami. Ak nemôžeme doručiť dáta cieľovému uzlu, nemôžeme s ním viesť dialóg. Hoci na tomto mieste ešte detaily tohto procesu nepoznáme, môžeme poznamenať aspoň toľko, že na úrovni doručovania dát medzi koncovými uzlami môže dôjsť k prechodným stratám správ, prípadne k rozpadom spojenia. Jednou z úloh relačnej vrstvy je, aby voči aplikáciám vytvárala ilúziu trvalého komunikačného vzťahu.

V prípade, že dôjde na nižších vrstvách k rozpadu komunikačného spojenia medzi koncovými uzlami, relačná vrstva ho v prípade potreby obnoví, a to spôsobom, ktorý je pre komunikujúce aplikácie neviditeľný.

8.2.3 Riadenie dialógu – zaistenie pravidelného striedania uzlov pri vysielaní

Ďalšou, menej využívanou funkciou relačnej vrstvy, je **riadenie dialógov** medzi komunikujúcimi procesmi. Väčšina aplikačných protokolov svojou samotnou povahou a špecifikáciou stanovuje, kedy a ako si klient a server môžu odosielať dáta. Je zrejmé, že napríklad webový server nemôže začať klientovi odosielať webovú stránku skôr, než mu klient vôbec stihne oznámiť, o akú stránku má záujem. Takisto je zrejmé, že ak webový klient odošle serveru niekoľko žiadostí za sebou, a to i počas prebiehajúceho prenosu jednej webovej stránky, znamená to, že postupne žiada o ďalšie a ďalšie dokumenty, ktoré sa majú postupne za sebou preniesť. Osobitné riadenie dialógov v tomto prípade nie je potrebné.

Podľa druhu sieťovej služby však môžu existovať také aplikácie, ktoré vyžadujú koordinované striedanie oboch zúčastnených strán pri komunikácii – keď záleží na tom, v akom vzájomnom slede si jednotlivé procesy odosieltajú dáta. Ak je potrebné realizovať takéto koordinovanie komunikujúcich aplikácií, používa sa na to spravidla princíp vyžiadania a odovzdania povolenia, tzv. tokenu, pre právo odoslať ďalšie dáta.

Na úrovni relačnej vrstvy rozlišujeme tri spôsoby vedenia dialógu:

- **Plne duplexné** (full duplex, Two-Way-Simultaneous, TWS) – komunikujúce procesy môžu navzájom komunikovať v ktoromkoľvek momente a poradí
- **Poloduplexné** (half duplex, Two-Way-Alternate TWA) – komunikujúce procesy môžu navzájom komunikovať, avšak ich vzájomná komunikácia musí byť koordinovaná, napr. pomocou tokenov
- **Simplexné** (simplex, One-Way) – komunikácia je možná iba v jednom smere

8.2.4 Synchronizácia (synchronization)

Ďalšou službou relačnej vrstvy je synchronizácia. Jej význam súvisí s transakčnou povahou riadenia dialógov, t.j. schopnosťou viesť dialóg po ucelených sekvenciách, ktoré buď budú spracované u príjemcu naraz a správne, alebo je možné celú sekvenciu odvolať.

Mechanizmus použitý pri synchronizácii je nazývaný checkpointing a spočíva v definovaní tzv. kontrolných bodov (check point) do prenášaných dát. Tým umožňuje relačná vrstva možnosť vrátiť sa v dialógu k určitému „kontrolnému bodu“ a pokračovať od neho odznova. Takýchto kontrolných bodov môže existovať viac a v relácii je možné pokračovať od ktoréhokoľvek z nich. Častým užívateľom transakčného prístupu sú rôzne databázové či rezervačné systémy.

Kľúčové slová

1. Kódová stránka, kódová tabuľka
2. ASCII
3. Unicode, UTF-8

4. Base64
5. Little-endian, Least Significant Byte First
6. Big-endian, Most Significant Byte First
7. Network byte order
8. Prezentačná vrstva
9. Relácia (session)
10. Riadenie dialógu v relácii
11. Full duplex, Two-Way-Simultaneous, TWS
12. Half duplex, Two-Way-Alternate, TWA
13. Synchronizácia na relačnej vrstve
14. Checkpointing

Kontrolné otázky

1. Medzi ktorými vrstvami sa nachádza prezentačná vrstva?
2. Akej vrstve poskytuje prezentačná vrstva svoje služby?
3. Aké sú služby resp. úlohy prezentačnej vrstvy?
4. Čo je to kódová stránka a prečo ich existuje niekoľko?
5. Aká je v súčasnosti odporúčaný univerzálny štandard pre kódovanie znakov národných abecied?
6. Čo je to kód Base64 a kde sa využíva?
7. Čo označujú pojmy „big-endian“ a „little-endian“?
8. Čo je to „network byte order“?
9. Akým spôsobom protokol HTTP poskytuje služby prezentačnej vrstvy?
10. Medzi ktorými vrstvami sa nachádza relačná vrstva?
11. Aké sú služby resp. úlohy relačnej vrstvy?
12. Čo predstavuje pojem relácia v relačnej vrstve?
13. Čo zabezpečuje funkcia riadenie dialógu v relačnej vrstve?
14. Aký je rozdiel medzi plne duplexným a poloduplexným dialógom v relačnej vrstve?
15. Na čo slúži synchronizácia v relačnej vrstve?
16. Čo znamená pojem checkpointing?

9 Aplikačná vrstva

Ciele učenia

Čo by mal študent vedieť:

- Úlohy a funkcie aplikačnej vrstvy
- Odlišnosti v pohľade na aplikačnú vrstvu medzi referenčným modelom OSI a protokolovým modelom TCP/IP
- Vlastnosti a rozdiely architektúry klient-server a peer-to-peer
- Vybrané služby a protokoly implementované na aplikačnej vrstve

9.1 Úvod

Ľudia ako používatelia počítačov a informačno-komunikačných technológií pri svojej práci s výpočtovou technikou využívajú najrôznejšie softvérové produkty, neraz nazývané aj aplikačné programové vybavenie. Medzi ne patria aj programy, ktoré sú schopné komunikovať prostredníctvom sietí a poskytovať či sprostredkovať používateľovi sieťové služby – elektronickú poštu, web, instant messaging, telefonovanie či dokonca videohovory cez internet, zdieľanie súborov a tlačiarňí, vzdialené ovládanie zariadení a mnohé ďalšie. Tieto programy z pohľadu referenčného modelu OSI patria do tzv. aplikačnej vrstvy.

Aplikačná vrstva je najvyššou vrstvou RM OSI a vo voľnejšom poňatí zahŕňa v sebe všetky sieťovo dostupné služby a prostriedky určené na ich využívanie ľuďmi ako koncovými používateľmi. Aplikačná vrstva teda poskytuje svoje možnosti priamo používateľom výpočtovej techniky, alebo – presnejšie povedané – aplikačnému programovému vybaveniu, s ktorým používatelia pracujú. Každý aplikačný softvér, ktorý dokáže spolupracovať so sieťou, v sebe implementuje alebo využíva prostriedky ponúkané aplikačnou vrstvou. Aplikačná vrstva teda predstavuje komponenty aplikačného programového vybavenia, ktoré sa týkajú sieťovej komunikácie. Samotná aplikačná vrstva neposkytuje svoje služby žiadnej ďalšej formálnej vrstve, ale priamo aplikačnému programovému vybaveniu a prostredníctvom neho samotným používateľom.

9.2 Aplikácia, program a proces

Pod pojmom aplikácia resp. aplikačný softvér sa v informatike rozumie softvérové vybavenie počítača, ktoré umožňuje alebo pomáha používateľom vykonávať na počítači isté aktivity. Patrí sem teda používateľský softvér ako webové prehliadače, poštovní klienti, kancelárske balíky, grafické nástroje, integrované prostredia pre vývoj nových programov, informačné systémy, nástroje pre podporu elektronického vzdelávania či hry. Okrem toho medzi aplikácie môžeme zaradiť ale aj databázové, poštové, webové, súborové, aplikačné a mnohé iné druhy serverov a ďalších softvérových komponentov, s ktorými používateľ ani nemusí prísť do bezprostredného kontaktu, no napriek tomu ich využíva ako súčasť väčšieho softvérového produktu.

Aplikácia pozostáva z jedného alebo viacerých programov. Pojmom program sa označuje postupnosť inštrukcií, ktoré môže procesor počítača vykonávať a vykonanie ktorých vedie k získaniu určitého výsledku. Obvykle sú programy na počítači uložené vo forme súborov na pamäťových médiách, odkiaľ ich je možné spustiť.

Samotný program môže spotrebovávať úložné miesto, ale pokiaľ sa nevykonáva, nevyužíva iné systémové zdroje – procesorový čas, pamäť, periférie – a samozrejme, neprodukuje nijaké výsledky. Až po svojom spustení dostáva každá konkrétna spustená kópia (tzv. inštancia) programu svoj procesorový čas, pamäťové miesto a ďalšie systémové prostriedky. Každá spustená inštancia programu, ktorej operačný systém prideliť systémové prostriedky, sa nazýva proces. Jeden program môže bežať v mnohých procesoch a na počítači môže bežať mnoho rôznych procesov rôznych programov. Súčasné operačné systémy realizujú tzv. multitasking – striedavé pridelovanie a odoberanie procesora jednotlivým procesom tak, aby vznikol dojem, že všetky procesy bežia súčasne a paralelne. Na viacprocesorových počítačoch aj skutočne bežia viacero procesov naraz, na jednoprocessorových počítačoch sa môže v každom momente vykonávať najviac jeden proces.

9.3 Funkcie aplikačnej vrstvy a ich vývoj

Svet aplikačného softvéru je mimoriadne pestrý a neustále sa vyvíja vrátane nových sieťových služieb. Úlohou aplikačnej vrstvy je napriek tejto obrovskej variabilite poskytnúť softvérovým aplikáciám a ich tvorcom spoločné základné nástroje, pomocou ktorých bude možné aplikáciám dať schopnosť komunikovať prostredníctvom informačných sietí. Nie je pritom snahou aplikačnej vrstvy predpripraviť množinu všetkých možných sieťových služieb – to by realisticky ani nebolo možné – ale ponúknuť stavebné kamene, z ktorých je možné tieto sieťové služby vystavať, aby nemuseli v každej aplikácii byť implementované odznovu. Všímnime si tieto základné, spoločné nástroje bližšie.

Prvým z týchto spoločných základných nástrojov je vôbec umožniť jednej aplikácii bežiacej na jednom počítači kontaktovať prostredníctvom informačnej siete druhú aplikáciu na inom počítači, t.j. **vytvoriť komunikačný vzťah medzi dvomi procesmi bežiacimi na rôznych počítačoch**. Proces musí mať možnosť, ako vytvoriť komunikačné spojenie s iným procesom (otvorenie spojenia), ako spojenie ukončiť (uzatvorenie spojenia), prípadne ako byť informovaný, že spojenie bolo uzatvorené z druhej strany alebo nemohlo vôbec byť zostavené (informácia o priebehu a stave spojenia). Samozrejmom súčasťou tohto procesu musí byť aj možnosť vybrať si, voči ktorej aplikácii na cieľovom počítači sa komunikačné spojenie vytvára. Je prirodzené, že napríklad poštový program (MS Outlook, Mozilla Thunderbird atď.) komunikuje len s poštovými službami, zatiaľ čo webový prehliadač komunikuje iba s webovou službou, hoci obe služby môžu bežať na tom istom serveri. Takisto by komunikujúce aplikácie pri vytváraní komunikačného vzťahu mali mať možnosť deklarovať, akú úroveň kvality služby od siete očakávajú (napr. spoľahlivé resp. nespoľahlivé doručovanie dát). Proces, ktorý vytvára komunikačný vzťah, sa tradične nazýva klient, zatiaľ

čo proces, voči ktorému sa komunikačný vzťah vytvára, sa nazýva server. Pre samotný komunikačný vzťah je zaužívaný pojem asociácia alebo jednoducho spojenie.

Druhým zo základných nástrojov aplikačnej vrstvy je **zabezpečenie spoľahlivého doručenia správ prenášaných medzi jednotlivými aplikáciami**. Nad týmto tvrdením by sa pozorní čitatelia mali pozastaviť s komentárom, že spoľahlivé doručovanie dát nad komunikačnou sieťou je predsa starosťou transportných protokolov – a mali by úplnú pravdu. Treba si však uvedomiť, že spoľahlivý transportný protokol garantuje len doručenie dát cez sieť na cieľový počítač, avšak nerieši situácie, kedy sa dáta poškodia alebo stratia po ich úspešnom doručení na cieľový počítač pred tým, ako ich aplikácia sama korektne spracuje. Predstavme si napríklad situáciu, kedy počas prenosu súboru a jeho ukladania na USB kľúč predčasne kľúč odpojíme. Dáta boli až do aplikácie doručené správne a transportná vrstva si teda svoju úlohu splnila – aplikácia však nebola schopná korektne dokončiť svoju vlastnú činnosť. Práve na ochranu proti chybám, ktoré sa môžu vyskytnúť na cieľovom uzle počas spracovávania doručených dát, je potrebný nástroj, ktorý poskytuje spoľahlivosť pri komunikácii jednotlivých aplikácií.

Tretím základným nástrojom aplikačnej vrstvy je **mechanizmus tzv. vzdialeného volania procedúr**. Pod týmto názvom sa skrýva mechanizmus, na ktorom môžu byť postavené tzv. distribuované aplikácie. Jednotlivé procedúry a funkcie, z ktorých takéto aplikácie pozostávajú, budú sieťovo dostupné a proces bežiaci na jednom počítači môže volať procedúry a funkcie procesu na inom počítači, ako keby boli lokálne.

Štvrtý základný nástroj súvisí so všetkými predchádzajúcimi. Ak môžu viaceré počítače na sieti využívať zdieľané zdroje (napríklad prístup k súborom, k spoločnému pamäťovému priestoru apod.), vzniká otázka, ako riadiť a synchronizovať prístup rôznych procesov k tomu istému sieťovému zdroju. Pri nekoordinovanom prístupe napríklad k súboru na centrálnom serveri hrozí, že doň budú viacerí klienti zapisovať a čítať z neho v domnení, že každý z nich je jediný, kto so súborom pracuje. Výsledkom však bude, že súbor bude obsahovať zmes údajov zapísaných všetkými klientmi, ba čo viac, každý klient bude pracovať nad údajmi, ktoré zo súboru načítal, ale ktoré sa v ňom už nemusia nachádzať. Pri distribuovaných sieťových aplikáciách je preto potrebné mať k dispozícii **nástroj na vzájomnú koordináciu aplikácií, ktoré pracujú so spoločnými sieťovo dostupnými zdrojmi**.

Využívaním týchto štyroch spoločných základných nástrojov môže softvérový inžinier vytvárať sieťové aplikácie, ktoré vedia komunikovať prostredníctvom komunikačnej siete. Tieto nástroje však nepredstavujú hotovú sieťovú službu (napríklad elektronickú poštu či web). Aplikácia musí tieto nástroje využívať a pridaním vlastných súčastí vytvárať konkrétne sieťové služby. Súčasti, ktoré aplikácia pridá, sú už špecifické pre konkrétnu sieťovú službu. Iné špecifické súčasti sú potrebné pre zdieľanie súborov a tlačiarní, iné sú potrebné pre elektronickú poštu, zasa iné pre IP telefóniu atď. Veľká variabilita sieťových aplikácií a služieb sa skrýva práve vo voľnosti, ktorú softvérový inžinier má pri vytváraní vlastných špecifických komponentov, z ktorých tvorí novú sieťovú aplikáciu.

Môžeme teda povedať, že každá sieťová aplikácia z pohľadu aplikačnej vrstvy vnútorne využíva dva druhy súčastí: špecifické, ktoré aplikácii dávajú schopnosť poskytovať alebo využívať konkrétne sieťové služby, a súčasti spoločné, ktoré aplikáciu vôbec uschopňujú na sieťovú komunikáciu.

V terminológii RM OSI sa tieto súčasti nazývajú elementy aplikačnej služby – Application Service Elements. Spoločné elementy sa označujú názvom Common Application Service Elements alebo Common ASE (CASE), špecifické elementy majú názov Specific Application Service Elements alebo Specific ASE (SASE).

Keď organizácie ISO a ITU-T vytvárali špecifikáciu RM OSI, podľa tohto istého RM vytvárali aj jednotlivé protokoly zodpovedajúce jednotlivým jeho vrstvám a požadovaným funkciám. V rodine protokolov vytvorených podľa RM OSI existuje niekoľko protokolov, ktoré zabezpečujú už popísané štyri základné CASE nástroje:

1. Nástroj pre vytváranie a správu asociácií (spojení) medzi aplikáciami. V rodine protokolov podľa RM OSI tieto funkcie zabezpečuje protokol Association Control Service Element, ACSE
2. Nástroj pre zabezpečenie spoľahlivého doručovania správ medzi komunikujúcimi aplikáciami. V rodine protokolov podľa RM OSI tieto funkcie zabezpečuje protokol Reliable Transfer Service Element, RTSE
3. Nástroj pre zabezpečenie volania vzdialených procedúr. V rodine protokolov podľa RM OSI tieto funkcie zabezpečuje protokol Remote Operation Service Element, ROSE
4. Nástroj pre riadenie súčasného prístupu k sieťovým prostriedkom. V rodine protokolov podľa RM OSI tieto funkcie zabezpečuje protokol Commitment, Concurrence and Recovery Service Elements, CCRSE

V architektúre protokolov TCP/IP bol zvolený iný prístup. Hoci sa všeobecne uznáva, že všetky vymenované funkcie aplikačnej vrstvy sú potrebné, v TCP/IP neexistujú žiadne prísne stanovené CASE elementy a formálne stanovené, predpripravené protokoly. To, čo je aplikáciám k dispozícii, je len tzv. aplikačné programové rozhranie (Application Programming Interface, API) dané nástrojmi operačného systému, pomocou ktorých môže aplikácia vytvárať alebo akceptovať sieťové spojenia. Všetky ostatné funkcie si má aplikácia zabezpečiť sama. Tvorcovia aplikácií v TCP/IP majú teda voľnosť v tom, akým spôsobom si jednotlivé CASE funkcie zabezpečia. Samozrejme, časom vzniklo i v TCP/IP množstvo protokolov, ktoré zabezpečujú jednotlivé CASE funkcie podobne ako v protokoloch podľa RM OSI (ACSE, RTSE, ROSE, CCRSE). Rozdiel je v tom, že v RM OSI sú jednotlivé CASE protokoly predpísané (tvorcovia aplikácií sú viazaní používať ich), zatiaľ čo v architektúre TCP/IP majú softvéroví inžinieri voľnosť vo výbere nástrojov, ktoré použijú. V aplikačných protokoloch rodiny TCP/IP preto často nebude osobitné vyčlenenie CASE elementov viditeľné, v mnohých prípadoch dokonca vôbec tieto elementy nebudú prítomné, pretože aplikácia ich nebude potrebovať.

9.4 Porovnanie aplikačnej vrstvy RM OSI a TCP/IP

Prirodzenou snahou veľkých štandardizačných organizácií, medzi ktoré patrí aj ISO a ITU-T, je tvoriť čo najúplnejšie štandardy a pokryť v nich čo najväčšiu časť problematiky, na ktorú sa ich štandardy zameriavajú. Tento prístup pripomína spôsob, akým v čase vzniku RM OSI pracovali mnohé IT firmy – každá sa snažila poskytnúť kompletne riešenie celej IT infraštruktúry. Štandardy ISO a ITU-T týkajúce sa sieťovej komunikácie podľa RM OSI sa podobne snažia vyčerpávajúco popísať na jednotlivých vrstvách všetky činnosti, ktoré sa pri prenose informácie komunikačnými sieťami musia vykonávať. Takto vytvárané štandardy majú prirodzene veľmi široký záber, pretože vopred počítajú so všetkými typickými scenármi sieťovej komunikácie. Výhodou je, že sa v týchto štandardoch myslí na prakticky každú spoločne potrebnú činnosť, proces či službu vrátane jej presnej špecifikácie. Tvorca sieťového aplikačného softvéru má teda veľmi veľa prostriedkov už vopred hotových – špecifikácie služieb, procesov, funkcií, rozhraní, formátov správ i celých protokolov, a môže sa teda sústrediť na tvorbu samotnej aplikácie. Podrobnosti sieťovej komunikácie si softvérový inžinier nemusí navrhovať sám, pretože na takmer každú jeho požiadavku, ktorú môže mať, už štandardy ISO a ITU-T myslia dopredu a ponúkajú presný popis, ako ju splniť. Prirodzenou nevýhodou takéhoto prístupu je, že štandardy musia byť veľmi rozsiahle, komplexné a mnohokrát v záujme univerzálnosti aj veľmi abstraktné. To komplikuje ich implementáciu i neskoršie využívanie. Takisto je nevýhodou tohto prístupu menšia efektívnosť – mnohé štandardy v snahe byť čo najviac univerzálne môžu požadovať rôzne čiastkové činnosti, ktoré konkrétna sieťová aplikácia nemusí využívať, no napriek tomu sa musia realizovať.

Protokolový model TCP/IP vznikol viac z praktických skúseností a potrieb. Jeho aplikácie začínali ako relatívne jednoduché, postupom času sa ich funkcie a schopnosti zväčšovali a začali sa zavádzať nové, náročnejšie druhy aplikácií. Sieťový model TCP/IP vychádza z predpokladu, že jednotlivé aplikácie nebudú mať veľa spoločného, aby sa tieto ich spoločné časti vyplatilo osamostatniť do samostatných protokolov. Na rozdiel od referenčného modelu ISO/OSI sa preto očakávalo, že každá aplikácia si sama zaistí to, čo potrebuje a čo jej nižšie vrstvy neposkytujú. Až v poslednej dobe sa i v rámci protokolového modelu TCP/IP začínajú niektoré podporné mechanizmy v rámci aplikačnej vrstvy osamostatňovať, napríklad volanie vzdialených procedúr.

Tu je treba uvedomiť si rozdiel medzi referenčným modelom OSI a protokolovým modelom TCP/IP. Referenčný model OSI abstraktne popisuje najmä procesy, ktoré sa v sieťach vykonávajú, zatiaľ čo protokolový model TCP/IP popisuje istú konkrétnu sadu protokolov, ktorými sa sieťová komunikácia zabezpečuje. Keďže oba modely sa týkajú toho istého problému – sieťovej komunikácie, sú si podobné, avšak OSI a TCP/IP vznikali nezávisle na sebe a nie sú navzájom koordinované. Na protokoly rodiny TCP/IP preto nie je správne pozeráť sa cez prizmu RM OSI a násilne v nich hľadať princípy, ktoré RM OSI stanovuje, pretože tvorcovia TCP/IP sa nikdy nesnažili byť s RM OSI kompatibilní. RM OSI a TCP/IP možno len porovnať a komentovať ich rozdielne prístupy k tým istým problémom.

Z pohľadu aplikačnej vrstvy RM OSI zaraďuje medzi transportnú vrstvu a vrstvu aplikačnú ešte dve ďalšie vrstvy, relačnú a prezentačnú, ktoré tiež poskytujú služby vlastným aplikáciám. Protokolový model TCP/IP však nemá žiadnu analógiu relačnej a prezentačnej vrstvy. Tieto funkcie si v prostredí TCP/IP musia zaistiť jednotlivé aplikácie.

9.5 Architektúry klient-server a peer-to-peer

Pojmom klient-server sa označuje taký spôsob poskytovania sieťovej služby, v ktorom jedna z dvoch komunikujúcich strán službu poskytuje, zatiaľ čo druhá strana túto službu využíva. Poskytovateľ služby sa nazýva server, používateľ služby sa nazýva klient. Server je teda producentom služby, klient je jej konzumentom. Pojmy klient a server pritom neoznačujú priamo počítač ako fyzickú jednotku, ale skôr aplikačný program, ktorý buď o službu žiada (klient) alebo túto službu poskytuje (server).

Toto striktné rozdelenie komunikácie na producenta a konzumenta služby vychádza z prirodzenej motivácie sprístupniť výpočtový výkon, prípadne i špecializované funkcie jedného zariadenia (servera) mnohým klientom naraz. Výpočtový výkon klientov nie je v architektúre klient-server až taký podstatný. Zrejmovou výhodou architektúry klient-server je špecializácia – možnosť optimalizovať činnosť a výkon servera podľa druhu vybranej sieťovej služby, ktorú ponúka. Ďalšou výhodou je centralizácia – sústredenie poskytovania danej sieťovej služby na jeden alebo niekoľko serverov. Centralizované poskytovanie služby z jedného miesta veľmi uľahčuje jej údržbu, riešenie prístupových práv, ochranu, zabezpečenie, opravy, aktualizácie či iné aktivity súvisiace s jej poskytovaním. Vďaka tomu sú služby v architektúre klient-server vhodné pre nasadenie i vo veľmi veľkých sieťach s obrovským počtom klientov. Väčšina sieťových služieb používaných v súčasnosti je práve typu klient-server.

V architektúre klient-server komunikáciu vždy začína klient. Server čaká na požiadavky od klientov a reaguje na ne, avšak sám sa klientom nevnučuje. Ukončenie komunikácie však môže iniciovať aj server, aj klient.

S nárastom výpočtového výkonu používateľských počítačov sa objavila prirodzená snaha navzájom si zdieľať ich výpočtový výkon, úložné miesto či periférie. Pri tomto prístupe každý počítač môže využívať služby iných počítačov a v tom istom momente môže sám poskytovať vlastné služby svojej okoliu. V tejto architektúre neexistuje striktné rozdelenie na konzumenta a producenta služby – každý počítač môže byť súčasne serverom i klientom. Takúto architektúru nazývame peer-to-peer. Architektúra peer-to-peer je veľmi obľúbená najmä v menších sieťach, kde nemá význam prevádzkovať vyhradený server alebo kde sa poskytovanie služby rozprestiera cez väčšinu počítačov siete. Zrejmovou nevýhodou tejto architektúry je náročnosť údržby – čím viac uzlov, ktoré službu poskytujú, tým náročnejšie je celú sieť udržať pod kontrolou.

9.6 Protokol Domain Name System

9.7 Predchodcovia systému DNS

V kapitole o sieťovej vrstve sme vysvetlili, že jednotlivé uzly siete, ktoré pracujú na sieťovej a vyššej vrstve, majú svoje vlastné unikátne sieťové adresy. Protokol IP prideluje uzlom siete (presnejšie, ich rozhraniam) číselné sieťové adresy vo formáte štvorbajtových čísel. Komunikácia medzi uzlami IP siete potom prebieha s využitím týchto IP adries – odosielateľ i príjemca každého paketu sú identifikovaní v jeho záhlaví práve pomocou svojich IP adries. Ak má počítač odoslať cez IP sieť správu inému počítaču, musí poznať jeho IP adresu.

Používatelia sieťových aplikácií však s IP adresami prichádzajú do kontaktu iba zriedkavo. Je to pochopiteľné – spravidla si totiž lepšie pamätáme slovný názov počítača, napr. `www.kis.fri.uniza.sk`, než jeho IP adresu, v tomto prípade `158.193.152.2`. Tým však vzniká problém: pre IP protokol, ktorý je zodpovedný za doručenie dát na príjemcov uzol, sú slovné mená uzlov nepoužiteľné. Jedinou adresovou informáciou pre IP protokol je štvorbajtová IP adresa. Používatelia zasa chcú uzlom siete dávať slovné mená a o IP adresy sa nezaujímajú. Je to podobné ako s telefónnymi číslami – telefónna sieť sa riadi iba telefónnymi číslami, zatiaľ čo ľudia sa navzájom poznajú pod svojimi menami. Bez telefónneho zoznamu by používanie telefónnej služby bolo veľmi nepraktické.

Podobný systém „telefónneho zoznamu“ preto potrebujú aj komunikačné siete.

V prvých operačných systémoch, ktoré už podporovali sieťovú komunikáciu, bolo možné vo vhodnom systémovej priečinku vytvoriť textový súbor s názvom `HOSTS5`. Do tohto súboru sa vpisovali mená počítačov a ich číselné adresy. Keď sa neskôr na tomto počítači v sieťových aplikáciách používali mená počítačov, operačný systém sa k zadanému menu automaticky pokúsil nájsť v súbore `HOSTS` príslušnú číselnú adresu. Tento proces sa nazýva preklad mena na číselnú adresu.

Riešenie pomocou súboru `HOSTS` síce splnilo svoj účel v prvopočiatkoch komunikačných sietí, ale trpelo niekoľkými zásadnými nedostatkami:

- Súbor `HOSTS` platil iba pre počítač, na ktorom bol vytvorený. Neexistovala žiadna jednoduchá možnosť, aby sa o jeden súbor `HOSTS` mohli deliť viaceré počítače.
- Tým, že za obsah súboru `HOSTS` zodpovedal administrátor daného počítača, mohol súbor `HOSTS` obsahovať aj nepravdivé alebo neúplné informácie.
- Súbory `HOSTS` sa na rôznych počítačoch mohli líšiť

5 Súbor `HOSTS` alebo `HOSTS.TXT` sa začal používať od začiatku 70. rokov 20. storočia. V tom čase ešte IP protokol neexistoval, adresy v tomto súbore preto pôvodne zodpovedali adresovaniu v predchodcoch IP.

- Meno, ktoré nebolo v súbore HOSTS zapísané, sa na danom počítači nedalo preložiť na IP adresu. Poznať všetky počítače na internete teda znamenalo mať ich všetky zapísané v tomto súbore vrátane ich IP adries.
- S rastúcim počtom sieťovo dostupných počítačov bolo prakticky nemožné súbor HOSTS ručne udržiavať správny, aktuálny a úplný.
- Mená počítačov v súbore HOSTS nemali nijakú záväznú vnútornú štruktúru, ktorá by ich umožňovala istým spôsobom triediť alebo zoskupovať.

Tieto nevýhody boli zrejme pomerne skoro. Aby sa aspoň niektoré z nich odstránili, vznikla dohoda, že o obsah súboru HOSTS sa bude centrálne starať Stanford Research Institute (SRI). Centrálne spravovaný súbor HOSTS bol umiestnený na verejne prístupnom serveri SRI, odkiaľ si ho ktorýkoľvek počítač mohol nahrať. Základný princíp používania súboru HOSTS sa však nezmenil a bolo zrejme, že bude potrebný od základu iný prístup.

9.8 Princípy systému DNS

Vývoj nového systému, ktorý poznáme pod menom Domain Name System (DNS), prebiehal od roku 1981. Základ verzie, ktorú používame dnes, pochádza z roku 1987. Návrh systému DNS sa riadil týmito kritériami:

- Mená počítačov majú mať systematickú hierarchickú (stromovú) štruktúru, ktorá vyjadruje ich príslušnosť k vlastníkovi
- Databáza systému DNS musí byť distribuovaná. Znamená to, že každý DNS server bude obsahovať iba časť obsahu pôvodného súboru HOSTS, nie jeho úplný obsah. Žiaden DNS server teda nebude musieť udržiavať databázu všetkých existujúcich mien a adries, ale bude spravovať iba istú zónu – časť množiny všetkých mien. Zároveň musí existovať mechanizmus, aby každý DNS server vedel kontaktovať ďalšie DNS servery so žiadosťou o preklad mena, ktoré sám nepozná.
- Obsah zóny, ktorú spravuje jeden konkrétny DNS server, musí byť kedykoľvek možné ďalej rozdeliť a časť z nej delegovať na ďalší DNS server. Týmto spôsobom bude možné zväčšujúcu sa zónu rozdeliť na menšie podzóny a presunúť zodpovednosť za ich správu na iné DNS servery.
- Databáza DNS systému by nemala byť obmedzená iba na záznamy, ktoré k slovným názvom asociujú ich číselné adresy. K menu sa môžu viazať záznamy rôznych typov: prezývky, meno obsluhujúceho poštového servera, meno obsluhujúceho DNS servera, textový popis, prípadne i ďalšie – zatiaľ neznáme – informácie, ktoré budú potrebné v nových sieťových aplikáciách v budúcnosti.
- Klienti systému DNS môžu na zodpovedanie svojej otázky kontaktovať akýkoľvek DNS server. Systém DNS sa postará o správne zodpovedanie otázky aj vtedy, ak sa hľadaný záznam nachádza na inom DNS serveri.

Základným pojmom v systéme DNS je doména. Slovom doména sa všeobecne označuje sféra vplyvu alebo rozhodujúca oblasť pôsobenia. V systéme DNS sa pod slovom doména

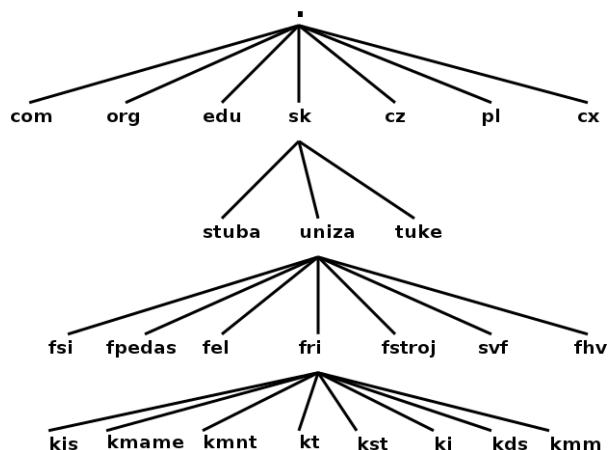
rozumie časť slovného názvu, ktorý vyjadruje príslušnosť nositeľa tohto názvu do istej oblasti. Touto oblasťou môže byť krajina, štát, typ organizácie, jej meno, vnútorné členenie a podobne. Úplné meno objektu v DNS obsahuje aspoň jednu, spravidla však niekoľko hierarchicky usporiadaných domén, zoradených od najviac špecifických po veľmi všeobecné. Pre príklad, názov `www.kis.fri.uniza.sk` obsahuje 6 domén, ktoré popíšeme v poradí sprava doľava:

- Symbol „.“ na konci názvu predstavuje tzv. koreňovú doménu (angl. root domain) v systéme DNS, ktorá je doménou najvyššej úrovne. Pod koreňovou doménou sa nachádzajú, priamo či pod ďalšími doménami, všetky existujúce slovné názvy. Táto doména je teda najmenej špecifická. Symbol „.“ sa na konci doménových názvov píše len zriedkakedy, pretože ho automaticky v prípade potreby doplní operačný systém. Ďalšie symboly „.“ v doménovom mene už nepredstavujú koreňovú doménu, ale iba oddeľujú jednotlivé domény medzi sebou.
- Doména „**sk**“ je tzv. vrcholovou doménou alebo doménou prvej úrovne (angl. Top Level Domain, TLD). Pod vrcholovou doménou „sk“ sa nachádzajú názvy objektov, ktoré istým spôsobom súvisia so Slovenskom.
- Doména „**uniza**“ je tzv. doménou druhej úrovne. Pod doménou „uniza“ sa nachádzajú názvy objektov, ktoré súvisia so Žilinskou univerzitou.
- Doména „**fri**“ je tzv. doménou tretej úrovne. Pod doménou „fri“ sa nachádzajú názvy objektov, ktoré súvisia s Fakultou riadenia a informatiky.
- Doména „**kis**“ je tzv. doménou štvrtej úrovne a patria pod ňu názvy objektov, ktoré súvisia s Katedrou informačných sietí.
- Doména „**www**“ je vlastné meno webového servera.

Celý názov `www.kis.fri.uniza.sk` sa nazýva aj úplné doménové meno (angl. Fully Qualified Domain Name, FQDN). Doména „www“ na začiatku tohto mena sa niekedy zvykne nazývať aj meno hostiteľa alebo vlastné meno (angl. hostname).

Množinu všetkých doménových mien môžeme graficky znázorniť ako strom, v ktorom budú jednotlivé domény usporiadané podľa svojej úrovne. Tento strom nazývame doménový strom.

Na obr. Obr. 9.1 sa nachádza malá časť celého doménového stromu. Na najvyššej úrovni sa nachádza koreňová doména „.“. Pod ňou sa nachádzajú TLD – domény prvej úrovne, nazývané tiež vrcholové domény. V USA sa ako TLD najčastejšie používajú názvy odvodené od typu organizácie, ktorá si chce pod TLD registrovať svoju vlastnú doménu druhej úrovne. Medzi najbežnejšie vrcholové domény patria:



Obr. 9.1 Časť doménového stromu v systéme DNS

- com: komerčné organizácie (v súčasnosti ľubovoľné organizácie)
- org: neziskové organizácie
- edu: školstvo
- gov: vláda
- mil: armáda

Mimo USA sa najčastejšie používajú TLD odvodené od skratky mena štátu.

Pod každou TLD sa nachádzajú domény druhej úrovne. Ich presné znenie si navrhuje ich vlastník sám – obvykle podľa vlastného obchodného mena alebo druhu podnikania. Na obr. Obr. 9.1 sú pod TLD „sk“ naznačené tri domény druhej úrovne: „stuba“ (Slovenská technická univerzita), „uniza“ (Žilinská univerzita) a „tuke“ (Technická univerzita v Košiciach). Na vytvorenie novej domény druhej úrovne a jej vloženie pod konkrétnu TLD má právo len správca konkrétnej TLD. Záujemca, ktorý si chce v systéme DNS nechať zriadiť vlastnú doménu druhej úrovne, musí o jej vytvorenie požiadať správcu tej TLD, pod ktorou sa chce zaregistrovať. Správcom slovenskej vrcholovej domény „sk“ je spoločnosť SK-NIC.

Po tom, čo vlastník získal vlastnú doménu druhej úrovne, jej obsah – domény tretej a vyššej úrovne – si už určuje a vytvára sám podľa vlastného uváženia. Menším organizáciám obvykle stačí vytvoriť jednu alebo niekoľko bežných domén tretej úrovne, napríklad www.vlastnik.sk (názov webového servera firmy), mail.vlastnik.sk (názov poštového servera firmy), ftp.vlastnik.sk (názov FTP servera firmy) a podobne.

Ak je vlastník veľkou spoločnosťou, ktorá sa vnútorne člení na časti, môže každej z nich prideliť vlastnú doménu tretej úrovne. Každá časť firmy si potom pod svojou doménou tretej úrovne môže vytvárať vo vlastnej rézii názvy štvrtej úrovne. Pre príklad, Žilinská univerzita pod doménou „uniza.sk“ vytvorila pre každú zo svojich fakúlt doménu tretej úrovne, ako je vidno na obr. Obr. 9.1. Každá fakulta je teda vlastníkom svojej vlastnej domény tretej úrovne a opäť má plnú moc nad názvami, ktoré vytvorí pod svojou doménou tretej úrovne.

Tento proces, keď vlastník domény nižšej úrovne (prvej, druhej, tretej, ...) vytvorí doménu vyššej úrovne (druhej, tretej, štvrtej, ...) a zverí jej spravovanie ďalšiemu subjektu, sa v terminológii systému DNS nazýva delegovanie – presunutie zodpovednosti. Delegovaním sa vlastne presúva zodpovednosť za istú časť DNS stromu na ďalší a ďalší subjekt, a teda ďalší a ďalší DNS server. Súvislá časť DNS stromu (t.j. istý jeho podstrom), ktorá je delegovaná – zverená jednému subjektu, sa nazýva zóna. V DNS sa teda delegujú zóny.

Zóny je vždy možné delegovať ďalej – z danej časti DNS stromu vyčleniť novú vetvu alebo vetvy a zveriť ich administráciu ďalšiemu subjektu. Práve delegovanie zón je jednou z najdôležitejších vlastností, vďaka ktorej systém DNS dokáže dodnes bez obmedzení obsluhovať obrovský počet domén na internete.

Doména a zóna nie sú to isté, i keď sú si významovo veľmi blízke. Doména je len súčasť slovného názvu počítača. Zóna je súvislá, ucelená časť celého DNS stromu, môže teda obsahovať aj viacero domén, ktoré hierarchicky patria pod seba. Hranice zón stanovujú administrátori systému DNS vždy pri delegovaní zón.

Pozrime sa, ako doposiaľ popísané princípy pracujú v praxi. V koreni DNS stromu sa nachádza už spomenutá koreňová doména „.“. Táto doména tvorí samostatnú zónu. Jej obsah sa v súčasnosti replikuje medzi 348 DNS servermi⁶ (tzv. root DNS servers) po celom svete. V koreňovej zóne existujú iba záznamy o tom, ktoré konkrétne TLD domény (domény prvej úrovne) existujú a ktoré ďalšie DNS servery ich spravujú. Nijaké iné informácie koreňová zóna neobsahuje. Inými slovami, z koreňovej zóny sú delegované TLD domény na DNS servery jednotlivých správcov vrcholových domén. Informácie obsiahnuté v koreňovej zóne slúžia na to, aby bolo možné zistiť, či daná TLD doména vôbec existuje, a ak áno, na ktorý ďalší DNS server je delegovaná. Koreňová zóna však nič nehovorí o tom, aký obsah sa pod jednotlivými existujúcimi TLD nachádza. Servery koreňovej zóny vedia teda s určitosťou vyhlásiť, že napr. TLD doména „qwe“ neexistuje, že TLD doména „sk“ existuje a nachádza sa na inom mieste, ale nevedia nič povedať o tom, aké domény sa nachádzajú pod TLD „sk“.

Z koreňovej zóny je týmto spôsobom delegovaná aj slovenská vrcholová doména „sk“, ktorá tiež tvorí samostatnú zónu. V súčasnosti je obsah zóny „sk“ obsluhovaný 8 DNS servermi. V zóne „sk“ sú vytvorené záznamy o existujúcich doménach druhej úrovne pod TLD „sk“, ktorými sa tieto domény delegujú na ďalšie DNS servery. Rovnako ako pri koreňovej zóne, ani v zóne „sk“ nie sú informácie o tom, čo sa nachádza vo vnútri jednotlivých domén druhej úrovne. Zóna „sk“ iba udržiava zoznam existujúcich slovenských domén druhej úrovne a delegujúce záznamy, ale zodpovednosť za ich obsah presúva na ďalšie DNS servery.

Zo zóny „sk“ je týmto spôsobom delegovaná aj doména druhej úrovne „uniza.sk“, a to na 3 DNS servery s identickým obsahom. Obsah DNS zóny „uniza.sk“ si stanovuje Žilinská univerzita sama. Pod názvom „uniza.sk“ sa na týchto DNS serveroch jednak nachádzajú mená s celouniverzitnou platnosťou – napr. www.uniza.sk, i-smtp-01.uniza.sk a i-smtp-02.uniza.sk (centrálne poštové servery pre prichádzajúcu poštu) a mnohé ďalšie, a jednak sa tu nachádzajú delegácie domén tretej úrovne pre jednotlivé fakulty.

Analogickým postupom je zo zóny „uniza.sk“ delegovaná zóna „fri.uniza.sk“, obsah ktorej si vytvára a udržiava Fakulta riadenia a informatiky. Na úrovni Fakulty riadenia a informatiky sú následne delegované zóny štvrtej úrovne pre jednotlivé jej katedry alebo pracoviská.

Delegovanie zóny má v DNS dôležitú vlastnosť: DNS server, na ktorom je zaznamenané delegovanie zóny, obsahuje iba odkaz na DNS servery v delegovanej zóne, ktoré poznajú jej obsah. Nijaké ďalšie informácie o obsahu delegovanej zóny DNS server v nadradenej (delegujúcej) zóne neobsahuje. Postupné delegovanie zón preto nezvyšuje záťaž na DNS servery, práve naopak – jednotlivé servery sú zodpovedné za menšie časti DNS stromu.

9.9 Záznamy v systéme DNS

Na systém DNS sa teda môžeme pozerat' ako na databázu údajov, ktoré nie sú uložené na jedinom centrálnom mieste, ale sú rozložené po častiach (distribuované) na rôznych DNS serveroch. Údaje sa v DNS vyhľadávajú pomocou svojich úplných doménových mien – k zadanému doménovému menu sa vyhľadáva záznam istého typu. Opýtaný DNS server buď hľadané doménové meno a záznam k nemu pozná, alebo aspoň obsahuje inštrukcie, ako ho v doménovom strome medzi rôznymi DNS servermi vyhľadať.

Jednotlivé položky databázy v DNS sa nazývajú zdrojové záznamy (angl. Resource Records). Zdrojové záznamy sú viacerých typov – k vyhľadávanému doménovému menu uchovávajú rôzne druhy informácií. Typy zdrojových záznamov sa označujú písmenovou skratkou. Najčastejšie využívané typy zdrojových záznamov sú:

- A – IP adresa patriaca danému doménovému menu
- AAAA – IPv6 adresa patriaca danému doménovému menu
- MX – meno poštového servera pre danú doménu
- CNAME – prezývka (alias) daného počítača
- PTR – reverzný záznam – doménové meno príslušné danej IP adrese
- NS – meno autoritatívneho DNS servera pre dané doménové meno (práve pomocou tohto záznamu sa realizujú odkazy – delegácie)

Nie všetky uvedené typy záznamov sú povinné – k doménovému menu administrátor vkladá do DNS databázy len tie záznamy, ktoré bude využívať. Niektoré typy záznamov k danému doménovému menu vôbec nemusia v DNS databáze existovať, iné môžu byť prítomné aj viackrát. Pozrime sa teraz na jednotlivé typy záznamov bližšie a využijeme pritom nástroj nslookup dostupný v príkazovom riadku operačného systému MS Windows.

9.9.1 Záznamy typu A a AAAA

Záznam typu A (Address) je najviac využívaným záznamom v DNS – k slovnému doménovému menu priradzuje IP adresu. Pomocou neho systém DNS realizuje svoju najdôležitejšiu funkciu – preklad slovných mien na číselné adresy. Vždy, keď v aplikačnom programe, či je to už WWW prehliadač, poštový program, ICQ alebo iný nástroj, zadáme slovné meno, operačný systém na pozadí kontaktuje prednastavený DNS server a vyhľadá v ňom k zadanému slovnému menu záznam typu A. Ak záznam neexistuje, toto meno nie je možné preložiť na IP adresu a program oznámi chybu. Pomocou programu nslookup v príkazovom riadku operačného systému MS Windows je možné z DNS systému získať záznam typu DNS jednoduchým zadaním príkazu nslookup a slovného mena servera:

```
C:\> nslookup www.kis.fri.uniza.sk
Server:   castor.kis.fri.uniza.sk
Address:  158.193.152.2

Name:     www.kis.fri.uniza.sk
Address:  158.193.152.2
```

```
C:\> nslookup www.google.com
Server:   castor.kis.fri.uniza.sk
Address:  158.193.152.2

Non-authoritative answer:
Name:     www.google.com
Addresses: 173.194.35.147, 173.194.35.148, 173.194.35.144,
173.194.35.145, 173.194.35.146
```

Príkaz nslookup automaticky pri zadaní mena hľadá v DNS záznamy typu A. V tomto výpise si môžeme všimnúť, že k menu `www.kis.fri.uniza.sk` je v DNS systéme uložený záznam A s hodnotou `158.193.152.2`. K menu `www.google.com` je v systéme DNS uložených päť záznamov A s hodnotami `173.194.35.144` až `173.194.35.148`. To znamená, že pod týmto menom sa nachádza niekoľko rôznych serverov a klient môže kontaktovať ktorýkoľvek z nich. Pretože klienti si z tohto zoznamu vyberú konkrétny server náhodne, rôzni klienti budú komunikovať s rôznymi servermi a záťaž sa tak rozkladá medzi tieto jednotlivé servery.

Ak je možné k doménovému menu získať v DNS záznam typu A s IP adresou, môžeme ho použiť v akomkoľvek programe, ktorý komunikuje cez sieť. Ako ukážku tu použijeme príkaz ping, ktorý posielá serveru daného doménového mena krátke správy so žiadosťou o okamžitú odpoveď a tým overuje, či server pracuje:

```
C:\> ping www.kis.fri.uniza.sk

Pinging www.kis.fri.uniza.sk [158.193.152.2] with 32 bytes of data:

Reply from 158.193.152.2: bytes=32 time<1ms TTL=64
Reply from 158.193.152.2: bytes=32 time<1ms TTL=64
Reply from 158.193.152.2: bytes=32 time=1ms TTL=64
Reply from 158.193.152.2: bytes=32 time<1ms TTL=64

Ping statistics for 158.193.152.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\> ping www.google.com

Pinging www.google.com [173.194.35.145] with 32 bytes of data:

Reply from 173.194.35.145: bytes=32 time=25ms TTL=54
Reply from 173.194.35.145: bytes=32 time=25ms TTL=54
Reply from 173.194.35.145: bytes=32 time=25ms TTL=54
Reply from 173.194.35.145: bytes=32 time=25ms TTL=54

Ping statistics for 173.194.35.145:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 25ms, Maximum = 25ms, Average = 25ms
```

Všimnime si, že príkazu ping sme zadali meno servera, nie jeho IP adresu. Príkaz ping však na pozadí využil DNS na preklad tohto mena na IP adresu, čiže z DNS vyžiadal k tomuto menu záznam typu A. IP adresy, ktoré sú v tomto výpise viditeľné, sú tie isté, ako zobrazil príkaz nslookup.

Zdrojový záznam typu AAAA má veľmi podobnú funkciu ako záznam typu A, avšak k doménovému menu priraduje IPv6 adresu. Názov AAAA je odvodený od faktu, že IPv6 adresa je štyrikrát dlhšia ako IP adresa (16 bajtov). Ak chceme pomocou príkazu nslookup získať zo systému DNS záznam typu AAAA, je potrebné výslovne to uviesť na príkazovom riadku:

```
C:\> nslookup -type=aaaa www.kis.fri.uniza.sk  
Server: castor.kis.fri.uniza.sk  
Address: 158.193.152.2
```

```
kis.fri.uniza.sk  
primary name server = ns.kis.fri.uniza.sk  
responsible mail addr = hostmaster.kis.fri.uniza.sk  
serial = 201211170  
refresh = 10800 (3 hours)  
retry = 3600 (1 hour)  
expire = 604800 (7 days)  
default TTL = 3600 (1 hour)
```

```
C:\> nslookup -type=aaaa www.google.com  
Server: castor.kis.fri.uniza.sk  
Address: 158.193.152.2
```

```
Non-authoritative answer:  
www.google.com AAAA IPv6 address = 2a00:1450:4016:800::1012
```

```
google.com nameserver = ns1.google.com  
google.com nameserver = ns3.google.com  
google.com nameserver = ns2.google.com  
google.com nameserver = ns4.google.com
```

Všimnime si, že k menu www.kis.fri.uniza.sk odpoveď neobsahuje nijakú IPv6 adresu, hoci príkaz nslookup zobrazil isté technické informácie o zóne kis.fri.uniza.sk, do ktorej meno www.kis.fri.uniza.sk patrí. Tým nslookup potvrdzuje, že samotné doménové meno www.kis.fri.uniza.sk existuje, avšak nie je k nemu evidovaný záznam typu AAAA. K menu www.google.com však príkaz nslookup zobrazuje IPv6 adresu, keďže k tomuto menu v DNS

existuje aj AAAA záznam. Existencia resp. neexistencia záznamu typu AAAA pre konkrétne doménové meno sa v príkaze ping prejaví nasledovne:

```
C:\> ping -6 www.kis.fri.uniza.sk
Ping request could not find host www.kis.fri.uniza.sk. Please check the
name and try again.
```

```
C:\> ping -6 www.google.com

Pinging www.google.com [2a00:1450:4016:800::1012] from
2001:4118:300:121:64b:80ff:fe80:8003 with 32 bytes of data:

Reply from 2a00:1450:4016:800::1012: time=25ms
Reply from 2a00:1450:4016:800::1012: time=25ms
Reply from 2a00:1450:4016:800::1012: time=26ms
Reply from 2a00:1450:4016:800::1012: time=25ms

Ping statistics for 2a00:1450:4016:800::1012:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 25ms, Maximum = 26ms, Average = 25ms
```

Prepínač -6 v príkaze ping znamená, že na test komunikácie chceme použiť sieťový protokol IPv6. Všimnime si, že pri teste konektivity so serverom www.kis.fri.uniza.sk príkaz ping zareagoval, ako keby meno neexistovalo – dôvodom je, že ho nedokázal preložiť v DNS na IPv6 adresu. Test konektivity so serverom www.google.com prebehol v poriadku i s využitím protokolu IPv6.

9.9.2 Záznam typu MX

Záznam typu MX – Mail eXchanger – obsahuje meno poštového servera, ktorý je zodpovedný za prevzatie elektronickej pošty pre príjemcu v danej doméne. Pre príklad predpokladajme, že odosielame e-mail príjemcovi dekan@fri.uniza.sk. Túto správu na začiatku prevezme poštový server odosielateľa a je zodpovedný za jej doručenie na poštový server príjemcu. Ktorý server to však je? Meno fri.uniza.sk môže byť len názov domény, avšak nie meno žiadneho konkrétneho servera, preto nemusí k nemu byť v DNS zaznačený žiaden A ani AAAA záznam. V skutočnosti sa pri doručovaní tejto správy bude najprv v DNS vyhľadávať zdrojový záznam typu MX k doménovému menu fri.uniza.sk a pošta sa doručí na tento konkrétny server. Až v prípade, že by k tomuto doménovému menu neexistoval žiaden MX záznam, sa pošta bude doručovať na server, ktorého meno je priamo fri.uniza.sk.

Príkaz nslookup umožňuje z DNS vyžiadať i MX záznam:

```
C:\> nslookup -type=mx fri.uniza.sk
Server: castor.kis.fri.uniza.sk
```

```
Address: 158.193.152.2
```

```
Non-authoritative answer:
```

```
fri.uniza.sk MX preference = 10, mail exchanger = relay.uniza.sk  
fri.uniza.sk MX preference = 20, mail exchanger = smtp3.uniza.sk
```

```
fri.uniza.sk nameserver = nic.uniza.sk  
fri.uniza.sk nameserver = kinfo.fri.uniza.sk  
fri.uniza.sk nameserver = pd.uniza.sk  
pd.uniza.sk internet address = 194.160.135.33  
nic.uniza.sk internet address = 158.193.48.33  
nic.uniza.sk AAAA IPv6 address = 2001:4118:300:48::33  
kinfo.fri.uniza.sk internet address = 158.193.138.7
```

Podľa tohto výpisu sú za preberanie elektronickej pošty pre príjemcov v doméne fri.uniza.sk zodpovedné až dva servery – relay.uniza.sk a smtp3.uniza.sk. Číslo, ktoré je v tomto výpise označené ako „preference“, vyjadruje, v akom poradí majú tieto servery byť kontaktované. Pri doručovaní elektronickej pošty sa vždy najprv pošta doručuje na server s najnižšou hodnotou čísla „preference“. Ak by neodpovedal, pošta sa bude doručovať na server s druhou najnižšou hodnotou čísla „preference“, atď. K doméne je takto ľahko možné v DNS evidovať niekoľko rôznych poštových serverov s rôznou preferenciou.

O poštu pre príjemcov v obľúbenej doméne gmail.com sa stará až päť rôznych serverov:

```
C:\> nslookup -type=mx gmail.com  
Server: castor.kis.fri.uniza.sk  
Address: 158.193.152.2
```

```
Non-authoritative answer:
```

```
gmail.com MX pref = 10, mail exchanger = alt1.gmail-smtp-in.l.google.com  
gmail.com MX pref = 20, mail exchanger = alt2.gmail-smtp-in.l.google.com  
gmail.com MX pref = 30, mail exchanger = alt3.gmail-smtp-in.l.google.com  
gmail.com MX pref = 40, mail exchanger = alt4.gmail-smtp-in.l.google.com  
gmail.com MX pref = 5, mail exchanger = gmail-smtp-in.l.google.com
```

```
gmail.com nameserver = ns4.google.com  
gmail.com nameserver = ns2.google.com  
gmail.com nameserver = ns3.google.com  
gmail.com nameserver = ns1.google.com
```

9.9.3 Záznam typu CNAME

Záznam typu CNAME (Canonical NAME) vyjadruje, že hľadané doménové meno je len prezývkou pre iné, už existujúce (tzv. kanonické) doménové meno. Pre príklad, meno www.uniza.sk je v skutočnosti prezývkou a skutočné, kanonické meno je www3.uniza.sk. Ak systém DNS pri hľadaní záznamu ľubovoľného typu k istému doménovému menu narazí na záznam CNAME, v ďalšom hľadaní pokračuje od skutočného, kanonického mena. Záznam CNAME teda spôsobí „presmerovanie“ hľadania v DNS z pôvodného doménového mena na

nové meno. V našom príklade, hľadanie záznamu typu A či AAAA k menu `www.uniza.sk` sa zmení na hľadanie záznamu A alebo AAAA k menu `www3.uniza.sk`, pretože sa k menu `www.uniza.sk` počas vyhľadávania nájde záznam typu CNAME, ktorý hovorí, že meno `www.uniza.sk` je prezývkou kanonického mena `www3.uniza.sk`.

```
C:\> nslookup www.uniza.sk
Server:   castor.kis.fri.uniza.sk
Address:  158.193.152.2

Non-authoritative answer:
Name:     www3.uniza.sk
Address:  158.193.48.211
Aliases:  www.uniza.sk
```

Všimnime si, že príkazu `nslookup` sme tu prikázali vyhľadať záznam typu A k doménovému menu `www.uniza.sk`. O existencii záznamu typu CNAME sme sa pri spustení programu nezmienili (nakoniec, dopredu sa ani nedá vedieť, či je hľadané meno prezývkou alebo nie). Vo výpise sa však objavuje informácia, že skutočné meno je `www3.uniza.sk`, ktorého IP adresa je `158.193.48.211`, a riadok, ktorý hovorí, že meno `www.uniza.sk` je „aliasom“ kanonického mena `www3.uniza.sk`. Spracovanie záznamu typu CNAME sa teda udialo v systéme DNS úplne automaticky, bez toho, aby sme dopredu museli vedieť, že `www.uniza.sk` je len prezývkou. Vďaka tomu sú mená `www.uniza.sk` a `www3.uniza.sk` z pohľadu vyhľadávania informácií v DNS systéme rovnocenné. Príkaz `ping` pri teste konektivity so serverom `www.uniza.sk` automaticky použije IP adresu, ktorá je pridelená menu `www3.uniza.sk`:

```
C:\> ping www.uniza.sk

Pinging www3.uniza.sk [158.193.48.211] with 32 bytes of data:

Reply from 158.193.48.211: bytes=32 time<1ms TTL=124
Reply from 158.193.48.211: bytes=32 time=48ms TTL=124
Reply from 158.193.48.211: bytes=32 time=1ms TTL=124
Reply from 158.193.48.211: bytes=32 time<1ms TTL=124

Ping statistics for 158.193.48.211:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 48ms, Average = 12ms
```

Veľmi často sa prezývky využívajú pri tzv. virtuálnych serveroch, ktoré sa líšia svojimi doménovými menami, ale všetky bežia na jednom hardvérovom zariadení a majú tú istú IP adresu. Výhodou používania CNAME záznamov je, že ak sa v budúcnosti zmení záznam typu A alebo AAAA pre kanonické meno (napríklad dôjde k zmene IP adresy servera), zmena sa

prejaví i na všetkých prezývkach tohto kanonického mena bez toho, aby bolo potrebné akokoľvek upravovať záznamy CNAME. Stačí upraviť A alebo AAAA záznam kanonického mena.

9.9.4 Záznam typu PTR

Doposiaľ sme sa na systém DNS pozerali ako na databázu, v ktorej sme k doménovým menám vyhľadávali záznamy istého typu, teda vstupom hľadania bolo doménové meno a výstupom bol záznam zvoleného typu – napríklad IP adresa. Systém DNS dovoľuje i opačný smer hľadania – k zadanej IP adrese vyhľadá doménové meno, ktoré k tejto IP adrese patrí. Zvláštnosťou systému DNS je, že preklad z IP adresy na doménové meno sa nerealizuje pomocou existujúcich záznamov typu A alebo AAAA, ale pomocou samostatných zdrojových záznamov typu PTR (PoinTeR). Dôvodom je, že DNS používa na prehľadávanie svojej databázy doménový strom, avšak ten je tvorený slovnými doménami, nie IP adresami. Ak je potrebné vyhľadať v DNS istú IP adresu a jej spätný preklad na doménové meno, musíme i IP adresu prepísať do tvaru slovných domén, aby ju bolo možné vyhľadať v existujúcom doménovom strome.

Prepis IP adresy do tvaru doménového mena sa realizuje tým, že jednotlivé oktety (bajty) IP adresy zapíšeme v opačnom poradí, než v akom sa nachádzajú v IP adrese, a na koniec tohto prepisu doplníme umelú doménu in-addr.arpa. K takto vytvorenému doménovému menu potom v DNS vyhľadávame záznam typu PTR. Pre príklad, pri spätnom preklade IP adresy 158.193.138.40 na doménové meno ju najprv treba prepísať do tvaru doménového mena:

158.193.138.40 → 40.138.193.158.in-addr.arpa

K menu 40.138.193.158.in-addr.arpa je teraz potrebné v DNS vyhľadať záznam typu PTR. Použijeme na to opäť príkaz nslookup:

```
C:\> nslookup -type=ptr 40.138.193.158.in-addr.arpa
Server:   castor.kis.fri.uniza.sk
Address:  158.193.152.2

Non-authoritative answer:
40.138.193.158.in-addr.arpa      name = frix.fri.uniza.sk

138.193.158.in-addr.arpa        nameserver = nic.uniza.sk
138.193.158.in-addr.arpa        nameserver = kinfo.fri.uniza.sk
nic.uniza.sk                     internet address = 158.193.48.33
nic.uniza.sk                     AAAA IPv6 address = 2001:4118:300:48::33
kinfo.fri.uniza.sk              internet address = 158.193.138.7
```

V tomto výpise sa uvádza, že hľadaná IP adresa patrí serveru s názvom frix.fri.uniza.sk.

9.9.5 Záznam typu NS

Posledným zdrojovým záznamom, ktorému sa budeme v tejto kapitole venovať, je záznam typu NS (Name Server). Záznam typu NS informuje, kto je autoritatívnym DNS serverom pre danú doménu. Prívlastok „autoritatívny“ znamená, že práve tento DNS server je ten, ktorý pozná obsah danej domény alebo jej časti (zóny) a má právo vyhlásiť, či nejaké doménové meno v jeho zóne existuje alebo neexistuje. Pomocou záznamu NS sa realizujú už spomínané delegovania zón – vlastnosť DNS, ktorá ho robí takým robustným a rozšíriteľným.

Význam záznamu typu NS je najlepšie demonštrovať na príklade. Pozrime sa na to, ako vlastne systém DNS realizuje vyhľadanie mena od úplného koreňa doménového stromu. Použijeme na to príkaz `nslookup`, ktorý budeme opakovane používať podľa potreby.

Predpokladajme, že potrebujeme preložiť meno `www.kis.fri.uniza.sk` na IP adresu. Znamená to, že v DNS vyhľadáваме k tomuto doménovému menu záznam typu A. Tentoraz však príkaz `nslookup` spustíme tak, aby nám opytovaný DNS server odpovedal len svojou momentálnou vedomosťou a nedal nám úplne rozriešenú odpoveď. Na každej úrovni doménového stromu nám teda príslušný DNS server odpovie len istou delegáciou – posunutím na vhodný DNS server na ďalšej úrovni doménového stromu, kým sa nedopracujeme k DNS serveru, ktorý je autoritatívnym serverom pre zónu, v ktorej sa hľadané meno nachádza. Táto delegácia bude vyjadrená pomocou NS záznamov, ktorými nám jednotlivé nadržané DNS servery odpovedia.

Keďže doménový strom začína doménou „.“, položíme našu otázku najprv DNS serveru, ktorý je zodpovedný za túto najvyššiu koreňovú doménu. Stanovenou dohodou sú to servery, ktoré sa volajú `a.root-servers.net` až `m.root-servers.net`. My sa opýtame DNS servera `a.root-servers.net` (nasledujúce výpisy budú zámerne skrátené, aby sme vynechali nepodstatné informácie):

```
C:\> nslookup -norecurse www.kis.fri.uniza.sk a.root-servers.net
Server: UnKnown
Address: 198.41.0.4

Name: www.kis.fri.uniza.sk
Served by:
- sns-pb.isc.org
    192.5.4.1
    sk
- ns.uu.net
    137.39.1.3
    sk
- a.tld.sk
    194.0.45.1
    sk
- c.tld.sk
    217.75.72.157
    sk
- ns.eunet.sk
    217.75.73.242
```

```

        sk
- ns.sk-nic.sk
    195.12.159.2
    sk
- ns1.sk-nic.sk
    195.12.159.3
    sk
- ns3.sk-nic.sk
    217.75.67.234
    sk

```

Čo tento výpis znamená? Všimnime si, že hľadanú odpoveď zatiaľ neobsahuje. Nachádza sa v ňom však výpis 8 rôznych serverov, ktoré sú zodpovedné za vrcholovú doménu sk. V DNS databáze sú tieto záznamy uložené ako NS záznamy k doménovému menu sk. Servery, ktoré spravujú koreňovú doménu „“, nevedia o vrcholovej doméne sk ani o menách pod ňou nič okrem jediného faktu: ktoré DNS servery za vrcholovú doménu sk zodpovedajú. Práve zoznam týchto serverov sme získali v tomto prvom kroku.

V ďalšom kroku si teda vyberieme ľubovoľný jeden DNS server z tohto zoznamu, napríklad ns.uu.net, a položíme mu tú istú otázku:

```

C:\> nslookup -norecurse www.kis.fri.uniza.sk ns.uu.net
Server:      UnKnown
Address:     137.39.1.3

Name:        www.kis.fri.uniza.sk
Served by:
- nic.uniza.sk
    158.193.48.33
    uniza.sk
- sun.uakom.sk
    192.108.131.11
    uniza.sk
- proxy.uniza.sk
    158.193.1.10
    uniza.sk

```

Tento výpis nás informuje, že opýtaný server opäť nedokáže našu otázku úplne zodpovedať, avšak ako jeden z autoritatívnych DNS serverov pre vrcholovú doménu sk aspoň vie, že existuje doména druhej úrovne uniza.sk a že autoritatívnymi servermi pre ňu sú nic.uniza.sk, sun.uakom.sk a proxy.uniza.sk. Tieto tri servery sú v DNS databáze na ns.uu.net zaznamenané ako trojica záznamov typu NS k doméne uniza.sk. Server ns.uu.net nevie, čo konkrétne sa nachádza vo vnútri domény uniza.sk, ale vie nám povedať, ktoré DNS servery to vedia – deleguje nás na niektorý z týchto serverov práve pomocou trojice záznamov typu NS.

Položme teda túto otázku opäť jednému z týchto serverov, napríklad sun.uakom.sk:

```
C:\> nslookup -norecurse www.kis.fri.uniza.sk sun.uakom.sk
Server: sun.uakom.sk
Address: 192.108.131.11

Name: www.kis.fri.uniza.sk
Served by:
- kinfo.fri.uniza.sk
    158.193.138.7
    fri.uniza.sk
- nic.uniza.sk
    158.193.48.33
    fri.uniza.sk
```

Postupujeme postupne hlbšie a hlbšie do doménového stromu. Hoci ani server sun.uakom.sk nedokáže úplne zodpovedať našu otázku, odkazuje nás pomocou dvojice NS záznamov na dva autoritatívne servery pre doménu fri.uniza.sk.

Opýtajme sa servera nic.uniza.sk:

```
C:\> nslookup -norecurse www.kis.fri.uniza.sk nic.uniza.sk
Server: nic.uniza.sk
Address: 158.193.48.33

Name: www.kis.fri.uniza.sk
Served by:
- frix.fri.uniza.sk
    158.193.138.40
    kis.fri.uniza.sk
- ns.kis.fri.uniza.sk
    158.193.152.2
    kis.fri.uniza.sk
- kinfo.fri.uniza.sk
    158.193.138.7
    kis.fri.uniza.sk
```

Tento server nás pomocou troch NS záznamov odkazuje na autoritatívne servery pre doménu kis.fri.uniza.sk. Skúsme položiť tentoraz otázku serveru ns.kis.fri.uniza.sk:

```
C:\> nslookup -norecurse www.kis.fri.uniza.sk ns.kis.fri.uniza.sk
Server: castor.kis.fri.uniza.sk
Address: 158.193.152.2

Name: www.kis.fri.uniza.sk
Address: 158.193.152.2
```

Tentoraz sme konečne položili otázku serveru, ktorý je autoritatívnym serverom pre doménu kis.fri.uniza.sk a ktorý dokázal zodpovedať, že k menu www.kis.fri.uniza.sk patrí A záznam s IP adresou 158.193.152.2.

Takúto „pochôdzku“ po doménovom strome realizujú DNS servery vždy, keď majú vyhľadať záznam v DNS databáze. Aby klient nemusel celú túto procedúru realizovať sám, DNS servery ju obvykle vyriešia medzi sebou a klientovi vrátia hotovú odpoveď (niekedy ju nazývame aj rekurzívnou odpoveďou). Práve prepínač -norecurse v príkaze nslookup použitie tejto rekurzívie vypol a umožnil nám vidieť, ako vyzerá v DNS vyhľadávanie úplného doménového mena pomocou čiastkových výsledkov, ktoré si DNS servery na jednotlivých úrovniach doménového stromu vrátia.

9.10 Hyper Text Transfer Protocol

Služba World Wide Web (WWW) je v súčasnosti zrejme najviac využívanou aplikačnou službou v komunikačných sieťach. V službe WWW sa využíva veľmi pestrý rad rôznych jazykov a technológií pre tvorbu samotného obsahu WWW stránok (od jednoduchých statických stránok vytvorených v základnom jazyku HTML cez skriptovacie jazyky ako Java či PHP až po dynamické interaktívne stránky s využitím technológií AJAX, SOAP, Adobe Flash atď.), avšak z pohľadu sieťovej komunikácie sa vždy jedná len o dáta, ktoré je potrebné preniesť sieťou medzi WWW prehliadačom a serverom.

Prenos dát medzi WWW prehliadačom a serverom je sprostredkovaný pomocou aplikačného protokolu HTTP (Hyper Text Transfer Protocol). Tento protokol patrí medzi najbežnejšie textové protokoly – všetky jeho príkazy sú tvorené textovými riadkami, ktorým je možné rozumieť i bez špecializovaného sieťového analyzátoru. Ukážka komunikácie webového prehliadača a servera je v nasledujúcom výpise:

```
GET /kt/pozdrav.html HTTP/1.1
Host: www.kis.fri.uniza.sk
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:6.0.2) Gecko/20100101
Firefox/6.0.2
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: sk,cs;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Accept-Charset: ISO-8859-2,utf-8;q=0.7,*;q=0.7
Connection: close

HTTP/1.1 200 OK
Date: Fri, 25 Nov 2011 09:01:42 GMT
Server: Apache/2.2.16
Last-Modified: Fri, 25 Nov 2011 08:55:33 GMT
Content-Length: 61
Connection: close
Content-Type: text/html
```

<HTML>

```
<BODY>
  Ukazkova HTML stranka.
</BODY>
</HTML>
```

Prvý odsek červenej farby sú príkazy, ktoré odoslal webový prehliadač na server. Prvý riadok obsahuje tzv. metódu GET a cestu k požadovanému webovému dokumentu. Touto metódou si klient vyžiada konkrétny dokument zo servera. Ďalšie riadky sú pomocné informácie o tom, na akom WWW serveri sa požadovaný dokument má nachádzať, informácie o samotnom prehliadači, preferovaných formátoch dokumentov, preferovaných jazykoch, kódových stránkach a ďalšie špecifické informácie.

Druhý odsek vyznačený modrou farbou je odpoveď WWW servera. Prvý riadok odseku je návratový kód, ktorý informuje o úspechu alebo neúspechu vykonania príkazu zadaného klientom (v tomto prípade metódy GET). V ďalších riadkoch poskytuje webový server informácie o sebe a o vyžiadanom dokumente. Nakoniec, v poslednom odseku zelenej farby server odošle klientovi samotný požadovaný dokument. V tomto príklade je to kód jednoduchej HTML stránky.

Hoci je protokol HTTP obsiahlejší než to, čo je možné v tejto ukážke vidieť, jeho základný princíp je veľmi jednoduchý – klient zadá serveru príkaz a poskytne doplnkové informácie o sebe. Server sa pokúsi príkaz vykonať, klienta informuje o úspechu alebo neúspechu a odovzdá mu výsledok vykonania tohto príkazu. Po prijatí odpovede môže prehliadač spojenie ukončiť, alebo požiada o vykonanie ďalšej metódy. HTTP si neuchováva žiadnu informáciu o stave komunikácie s klientom a ku každej požiadavke pristupuje individuálne. Preto sa niekedy HTTP nazýva aj bezstavový protokol.

Jednotlivé riadky žiadosti majú nasledujúci význam:

- GET – príkaz (tzv. metóda) protokolu HTTP. Obsahuje časť URI bez mena servera (/kt/pozdrav.html – reprezentuje cestu k žiadanému dokumentu na serveri) a použitú verziu HTTP protokolu.
- Host – riadok hlavičky HTTP, ktorý hovorí, na ktorom webovom serveri sa hľadá dokument uvedený v metóde GET. Spojením tohto mena a cesty z metódy GET sa získava úplné URI, t.j. <http://www.fri.uniza.sk/kt/pozdrav.html>. Dôvod, prečo sa meno servera uvádza v samostatnom poli, je ten, že na jednom fyzickom serveri (IP adrese) môže bežať množstvo WWW serverov (virtuálne WWW servery). Každý z nich má však unikátne meno, ktoré je plne špecifikované v tomto riadku žiadosti.
- User-Agent – Riadok, ktorý identifikuje typ a verziu webového prehliadača.
- Accept – Riadok, v ktorom webový prehliadač oznamuje, aké typy dokumentov preferuje. Váha jednotlivých typov sa uvádza parametrom "q" (quality). Ak parameter q nie je uvedený, berie sa implicitná hodnota 1. V tomto prípade prehliadač najviac preferuje HTML a XHTML dokumenty, menej preferuje XML dokumenty a ešte menej iné typy dokumentov
- Accept-Language – Riadok, v ktorom klient uvádza preferované jazyky s označením preferencií (rovnakým spôsobom ako v riadku Accept). Predpokladá sa, že server

poskytne klientovi stránku v čo najviac preferovanom jazyku, ak je taká k dispozícii. V tomto prípade prehliadač najviac preferuje slovenčinu, potom češtinu, potom americkú angličtinu a potom angličtinu bez udania pôvodu.

- Accept-Encoding – Riadok, v ktorom klient uvádza, v akom dátovom formáte je ochotný akceptovať prenesenú stránku. Obvykle sa jedná o online kompresiu a dekompresiu dát. V tomto prípade klient uvádza dve podporované kompresné metódy: gzip a deflate
- Accept-Charset – Riadok, v ktorom klient uvádza preferované znakové sady pre HTML dokumenty. V tomto prípade klient preferuje ISO-8859-2 (stredoeurópske jazyky), potom UTF-8 alebo hocijakú inú znakovú sadu (preferuje sa však presná zhoda, t.j. ak by server nemal ISO8859-2, ale UTF-8 aj Win1250, preferovanejšia je UTF-8, lebo o nej sa prehliadač vyjadril explicitne, i keď aj UTF-8, aj Win1250 majú podľa prehliadača rovnakú preferovanú váhu)
- Connection – Riadok, v ktorom klient hovorí, či sa po vybavení jeho žiadosti má spojenie uzatvoriť. Staršie verzie HTTP vedeli v jednom spojení vybaviť iba jednu HTTP transakciu ("close"), novšie HTTP verzie môžu v jednom spojení realizovať niekoľko transakcií ("Keep-Alive")

Modrý text je odpoveď servera, presnejšie, hlavička odpovede. Jednotlivé riadky:

- HTTP/1.1 200 OK – Riadok informuje o verzii HTTP protokolu používanej serverom, číselný návratový kód odpovede a slovný popis. Kód 200 znamená úspešné vybavenie odpovede.
- Date – uvádza aktuálny čas na serveri, v ktorom sa realizuje vybavenie klientovej žiadosti
- Server – informuje o verzii servera (názov softvéru, verzia, prípadne iné informácie)
- Last-Modified – informuje, kedy bol vyžiadaný dokument naposledy zmenený
- Content-Length – informuje o veľkosti prenášaného dokumentu (v bajtoch)
- Connection – informuje o stave spojenia po vybavení tejto žiadosti
- Content-Type – informuje o type vyžiadaného dokumentu

Nakoniec, zelený text je takisto súčasťou odpovede servera a nasleduje ihneď za hlavičkou odpovede. V tomto prípade obsahuje text vyžiadanej webovej stránky v jednoduchom HTML kóde.

Hoci sú jednotlivé parametre hlavičiek HTTP žiadostí a odpovedí rozmanité, základný HTTP protokol má vždy dva základné druhy správ – príkazy, tzv. metódy, a odpovede resp. návratové kódy. Príkazy posielajú klientovi server, návratové kódy posielajú server klientovi. Metóda i návratový kód sú jednoriadkové textové správy. Obe bývajú doplnené pomocnými textovými hlavičkami, no samotné metódy i návratové kódy sú veľmi jednoduché.

Najčastejšie používané metódy (príkazy od klienta) sú:

- GET – žiadosť o zaslanie dokumentu zo servera na prehliadač

- POST – odoslanie formulára vyplneného v prehliadači na server a žiadosť o zaslanie výsledku jeho spracovania
- PUT – odoslanie dokumentu z prehliadača na server

Metóda GET je najvyužívanejšia – pomocou nej si webový prehliadač vyžiada zo servera konkrétny dokument. Pomocou metódy POST sa na server odovzdávajú položky tzv. formulára čiže webovej stránky, na ktorej mal používateľ vyplniť isté údaje a odoslať ju na server. Metóda PUT je relatívne zriedkavá – predpokladá sa totiž, že pomocou nej bude klient modifikovať súbory na serveri, čo v drvivej väčšine prípadov nie je povolené.

Najbežnejšie návratové kódy zo servera sú:

- 200 až 299 – indikujú úspešné vykonanie metódy
- 300 až 399 – indikujú tzv. presmerovanie – požadovaný dokument sa nachádza na inom URI než na tom, ktoré uviedol prehliadač
- 400 až 499 – neúspešné vykonanie metódy kvôli neexistujúcemu dokumentu, nedostatočným prístupovým právam a podobne

Návratový kód 200 je typický pre úspešné vykonanie metódy, ktorú klient požadoval. Obvykle sa tento kód objavuje pri správne vyžiadanych stránkach, ktoré server odosiela klientovi. I v príklade HTTP komunikácie v tejto kapitole sa objavuje kód 200.

Kódy 3xx sú využívané pri presmerovaní klienta na inú lokalitu. Predstavme si napríklad, že klient požiada o webovú stránku lokality `java.sun.com`. Keďže spoločnosť Sun bola pred niekoľkými rokmi odkúpená spoločnosťou Oracle, stránka `java.sun.com` je v súčasnosti presťahovaná na webové sídlo spoločnosti Oracle. Aby však staré URI zostalo funkčné, i keď pôvodné webové sídlo už neexistuje, webový server na lokalite `java.sun.com` presmeruje klienta na nové platné URI:

```
GET / HTTP/1.1
Host: java.sun.com
Connection: close

HTTP/1.0 301 Moved Permanently
Location: http://www.oracle.com/technetwork/java/index.html
Server: BigIP
Connection: close
Content-Length: 0
```

Všimnime si, ako server odpovedal klientovi odpoveďou 301 Moved Permanently. Tým klientovi oznamuje, že požadované URI je trvale presťahované na novú lokalitu, ktorá je uvedená v nasledujúcom riadku Location. Klient teraz automaticky stiahne stránku z tejto novej lokality.

Návratové kódy 4xx sú použité, ak požadovaná stránka neexistuje alebo klient k nej nemá prístup. V nasledujúcom príklade je zobrazená reakcia servera na žiadosť o neexistujúcu stránku:


```

GET /nonexistent.html HTTP/1.1
Host: st.fri.uniza.sk
Connection: close

HTTP/1.1 404 Not Found
Server: Apache/2.2.16 (Debian) PHP/5.3.3-7+squeezel3 with Suhosin-Patch
Vary: Accept-Encoding
Content-Length: 336
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL /nonexistent.html was not found on this server.</p>
<hr>
<address>Apache/2.2.16 (Debian) PHP/5.3.3-7+squeezel3 with Suhosin-Patch
Server at st.fri.uniza.sk Port 80</address>
</body></html>

```

Odpoveď servera je charakterizovaná návratovým kódom 404 Not Found. HTML kód zobrazený v zelenom odseku je len vysvetľujúca stránka, ktorá sa zobrazí klientovi v prehliadači. Niektoré prehliadače (napríklad MS Internet Explorer) dokonca namiesto tejto stránky zobrazia vlastné hlásenie, že požadované URI neexistuje – stačí, aby server odpovedal návratovým kódom 404.

V súvislosti s protokolom HTTP sa niekedy spomínajú tzv. cookies. Cookie je jednoduchá premenná, ktorá má svoj názov a hodnotu. Táto premenná je uložená u klienta a vytvára sa na príkaz servera. Cookie sa viaže ku konkrétnemu URI: ak webový server pri prístupe k istému URI prikázal klientovi vytvoriť si cookie istého názvu a hodnoty, webový prehliadač túto cookie vytvorí, zapíše na disk klienta a pri každom ďalšom prístupe k tomuto URI ju opätovne priloží do komunikácie s webovým serverom. Úlohou tejto cookie je umožniť serveru rozpoznať, že sa jedná o klienta, ktorý už predtým k danej URI pristupoval, prípadne si o tomto klientovi aj zaznamenať isté údaje, ktoré sú známe v danej HTTP transakcii a vďaka cookie sa tieto údaje prenesú aj do ďalších HTTP transakcií. Cookies teda pomáhajú z HTTP vytvoriť protokol, ktorý si môže s využitím prostriedkov samotného klienta pamätať o klientovi a jeho vzťahu k serveru isté stavové informácie. Cookies sú veľmi dôležitou funkciou, ak webové sídlo využíva napríklad prihlásenie sa používateľa menom a heslom. Samotné HTTP si nedokáže zapamätať, že používateľ sa správne autentifikoval – zadaním mena a hesla a ich odoslaním (metódou POST) sa totiž daná HTTP transakcia ukončí a v HTTP sú transakcie od seba nezávislé. Ak si však po úspešnom prihlásení HTTP server u klienta uloží cookie, v ktorej si zaznamená, že tento klient sa prihlásil úspešne, pri každom ďalšom prístupe k zabezpečenému URI klient priloží aj túto cookie a server ho môže identifikovať ako úspešne prihláseného.

V nasledujúcom prepise HTTP komunikácie je zobrazené nastavenie cookie pri prístupe na zabezpečenú lokalitu:

```
POST /mailman/admindb/ngn HTTP/1.1
Host: mailman.kis.fri.uniza.sk
Connection: close
Content-Length: 44

adminpw=VelmiTajneHeslo&admlogin=Vpust+ma...

HTTP/1.1 200 OK
Server: Apache/2.2.16
Set-Cookie: ngn+admin=2802000000692d6dce; Path=/mailman/; Version=1
Connection: close
[ Zostávajúca časť správy odstránená ]
```

Táto dvojica správ zobrazuje použitie metódy POST, ktorá serveru z vyplneného formulára odovzdáva dve formulárové polia – pole „adminpw“ nastavené na hodnotu „VelmiTajneHeslo“ a pole „admlogin“ nastavené na hodnotu „Vpust+ma...“. Ak server súhlasí s takýmito prihlasovacími údajmi, v odpovedi obsahuje riadok Set-Cookie, ktorým prikazuje prehliadaču, aby si na disku klienta uložil cookie s názvom „ngn+admin“ a s hodnotou „2802000000692d6dce“. Túto cookie má prehliadač priložiť pri každom ďalšom prístupe k lokalite mailman.kis.fri.uniza.sk/mailman/, aby server vedel, že sa jedná o klienta, ktorý sa už prihlásil úspešne. Ak teraz klient požiadajú o nejakú stránku pod touto lokalitou, vo svojej žiadosti priloží hodnotu tejto cookie v riadku Cookie:

```
GET /mailman/admindb/ngn HTTP/1.1
Host: mailman.kis.fri.uniza.sk
Connection: close
Cookie: ngn+admin=2802000000692d6dce

HTTP/1.1 200 OK
Server: Apache/2.2.16
Connection: close
[ Zostávajúca časť správy odstránená ]
```

Hoci sa o bezpečnosti cookies dlhodobo vedú polemiky, cookies samy osebe nie sú kód, ktorý by sa vykonával na počítači klienta, jedná sa len o dáta, ktoré si na disku klienta ukladá webový server. Diskusia o bezpečnostných rizikách spojených s používaním cookies však presahuje rámec tejto publikácie.

9.10.1 Poštové protokoly SMTP a POP

Služba elektronickej pošty patrí medzi ďalšie notoricky známe a široko využívané služby komunikačných sietí. Základný princíp elektronickej pošty je veľmi jednoduchý – odosielateľ vytvorí v poštovom programe správu, ktorú adresuje príjemcovi, a tá sa prostredníctvom

poštových serverov doručuje až do poštovej schránky príjemcu. Tam čaká, kým si ju vyzdvihne jej adresát.

Doručovací reťazec správ elektronickej pošty obsahuje niekoľko stavebných prvkov. Prvým, používateľsky najzrejmším prvkom je samotný poštový program, v ktorom používateľ pracuje so svojou elektronicou poštou: číta si ju, píše nové správy, organizuje si prijaté správy atď. Používateľských poštových programov existuje množstvo – MS Outlook, Mozilla Thunderbird, Evolution, The Bat! a ďalšie. V architektúre služby elektronickej pošty sa používateľské poštové programy označujú pojmom Mail User Agent – MUA. Hoci je v poslednej dobe veľmi populárne používať webové rozhranie pre prístup k elektronickej pošte bez nutnosti čokoľvek inštalovať na používateľov počítač, aj toto webové rozhranie slúži na ovládanie istého MUA, ktoré beží na vzdialenom serveri.

Ďalším stavebným prvkom doručovacieho reťazca sú samotné poštové servery, teda programové vybavenie bežiacie na vyhradených počítačoch, ktoré od MUA prevezme správu elektronickej pošty a stará sa o jej doručenie do adresátovho poštového priechinka. Tento priechinok sa môže nachádzať na tom istom serveri, ktorý prevzal poštu od odosielateľa, avšak môže sa nachádzať i na úplne inom serveri, ku ktorému treba správu elektronickej pošty dopraviť. Poštové servery takisto existujú viaceré – pre operačný systém MS Windows je to najmä MS Exchange, pre systémy unixového typu je to Postfix, Exim, Sendmail a iné. Poštové servery sa v architektúre služby elektronickej pošty označujú pojmom Mail Transfer Agent – MTA. Správa, ktorú používateľ vytvorí a odošle použitím svojho MUA, môže prejsť viacerými MTA, kým sa dostane na server, na ktorom sa nachádza poštový priechinok adresáta. Medzi MUA a MTA i medzi MTA navzájom prebieha sieťová komunikácia pomocou aplikačného protokolu Simple Mail Transfer Protocol, s ktorým sa zoznámime neskôr.

Posledným stavebným prvkom doručovacieho reťazca je tzv. Mail Delivery Agent – MDA. Tento komponent sa stará o všetky činnosti, ktoré súvisia s uložením prijatej správy elektronickej pošty do priechinka adresáta na cieľovom poštovom serveri, napríklad triedenie správ do rôznych priechinkov používateľa podľa zadaných kritérií alebo automatická odpoveď v prípade dlhodobej neprítomnosti adresáta. MDA vlastne odbreňuje MTA na cieľovom poštovom serveri od nutnosti poznať detaily toho, ako si používateľ praje uložiť prijatú poštu do svojich poštových priechinkov. Pretože MDA rieši iba lokálne uloženie prijatej správy, nezúčastňuje sa sieťovej komunikácie. MDA buď môže byť vstavanou súčasťou programového vybavenia poštového servera (napr. MS Exchange), alebo sa môže jednať o dodatočný softvér (napr. Procmail alebo Maildrop pre systémy unixového typu). S MDA používatelia obvykle nepracujú priamo.

Pri doručovaní správy elektronickej pošty správa vznikne v odosielateľovom MUA, ktorý ju odovzdá na doručenie svojmu prednastavenému serveru odchádzajúcej pošty – prvému MTA. Správa môže prejsť cez niekoľko ďalších MTA podľa toho, kde sa nachádza príjemca, až bude doručená na server, na ktorom sa nachádzajú poštové priechinky adresáta. Na tomto serveri MTA odovzdá prijatú správu MDA, ktorý ju podľa svojich nastavení uloží do vhodného priechinka adresáta. Odtiaľ si ju adresát neskôr môže vyzdvihnúť pomocou svojho

vlastného MUA. Poznamenajme, že správa sa považuje za doručенú už vtedy, keď ju MDA uloží do príjemcovho priečinka. Jej prevzatie a prečítanie v MUA adresáta je už dodatočná činnosť, ktorá sa nepovažuje za súčasť doručovania správy, ale len za prístup k už doručенým správam elektronickej pošty.

Doručovanie elektronickej pošty sa líši od prístupu k už doručenej pošte. Pri doručovaní elektronickej pošty je potrebné zaujímať sa o to, kde sa nachádza adresát, ako sa vôbec v správe vyjadrí, kto je jej odosielateľ a kto sú zamýšľaní príjemcovia, cez aké poštové servery sa má správa doručiť, ako oznámiť prípadnú nedoručiteľnosť a podobne. Prístup k doručenej elektronickej pošte má inú povahu – je potrebné adresáta autentifikovať (overiť jeho identitu) a umožniť mu manipulovať s individuálnymi správami: preniesť ich do MUA, presunúť či zmazať ich, označiť ako čítané či neprečítané atď. To je dôvod, prečo sa v systéme elektronickej pošty používajú viaceré protokoly: protokol Simple Mail Transfer Protocol (SMTP) pre doručovanie pošty a protokoly Post Office Protocol (POP) resp. IMAP (Internet Mail Access Protocol) pre prístup k doručenej pošte.

9.10.2 Protokol SMTP

Protokol SMTP (Simple Mail Transport Protocol) sa používa na doručovanie elektronickej pošty do priečinka adresáta. Pomocou protokolu SMTP poštový program (Outlook, Thunderbird a i.) odovzdá hotovú správu elektronickej pošty svojmu prednastavenému serveru odchádzajúcej pošty. Server odchádzajúcej pošty takisto pomocou SMTP odovzdáva túto správu ďalej cieľovému poštovému serveru, na ktorom sa nachádza poštový priečinok adresáta správy.

Priebeh odosielania správy elektronickej pošty je zaznamenaný na nasledujúcom výpise:

```
220 mail.kis.fri.uniza.sk ESMTP Postfix
EHLO [158.193.152.140]
250-mail.kis.fri.uniza.sk
250-PIPELINING
250-SIZE 10240000
250-VERFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
MAIL FROM:<Peter.Paluch@fri.uniza.sk> SIZE=629
250 2.1.0 Ok
RCPT TO:<Michal.Bruncko@fri.uniza.sk>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>. <CR><LF>
Message-ID: <4B59BB6B.60B0401@fri.uniza.sk>
Date: Fri, 22 Jan 2010 12:26:32 +0100
From: Peter Paluch <Peter.Paluch@fri.uniza.sk>
Organization: Zilinska univerzita, KIS FRI
User-Agent: Thunderbird 2.0.0.23 (Windows/20090812)
```

```
MIME-Version: 1.0
To: Michal Bruncko <Michal.Bruncko@fri.uniza.sk>
Subject: Ukazka prenosu spravy elektronickej posty
Content-Type: text/plain; charset=ISO-8859-1; format=flowed
Content-Transfer-Encoding: 7bit
```

Ahoj, Miso,

Tuto spravu, prosim, ignoruj - len si potrebujem odchytit priebeh SMTP dialogu medzi postovym programom a serverom a Ty si mi padol za obet :-)

Pozdravuje

Peter

.

```
250 2.0.0 Ok: queued as B29762010C65
```

```
QUIT
```

```
221 2.0.0 Bye
```

Červená farba znázorňuje dáta odoslané z poštového programu (klienta) na server, modrá farba označuje dáta odoslané z poštového servera poštovému programu.

Na začiatku spojenia sa v prvom riadku s kódom 220 poštový server predstaví svojim menom. Klient následne odosiela príkaz EHLO (Extended HelLO), v ktorom popisuje svoju identitu (v tomto príklade svoju IP adresu) a zároveň uvádza, že podporuje pokročilé (extended) vlastnosti protokolu SMTP. Na tento príkaz server odosiela sériu riadkov s kódom 250, v ktorých uvádza jednotlivé pokročilé vlastnosti protokolu SMTP, ktoré podporuje.

Klient pokračuje dvojicou príkazov MAIL FROM a RCPT TO, ktorými uvádza odosielateľa a príjemcu správy elektronickej pošty. Poštový server každú z týchto správ overí na formálnu správnosť a môže aj skontrolovať, či má odosielateľ právo cez tento server odosielať poštu danému príjemcovi. Ak je príjemcov správy viac, príkaz RCPT TO sa zopakuje pre každého z nich.

Klient ďalej pokračuje príkazom DATA, ktorým uvádza, že skončil s vymenovávaním príjemcov a ide odovzdať samotné telo správy elektronickej pošty. Server klienta v riadku s kódom 354 informuje, že koniec tela správy má oznámiť znakom bodky na samostatnom prázdnom riadku.

Klient následne odovzdá obsah celej elektronickej správy, v ktorom vidno jednak hlavičky identifikujúce odosielajúci poštový program, informácie o odosielateľovi a príjemcovi, predmet správy, informácie o jej formáte a samotný text. Správa je ukončená bodkou na samostatnom riadku.

V posledných troch riadkoch server potvrdí úspešné prevzatie správy na ďalšie doručovanie, klient odošle príkaz QUIT na ukončenie spojenia a server potvrdí jeho prijatie.

Doručovanie správy prebieha analogickým spôsobom aj medzi samotnými poštovými servermi, až pokiaľ správa nebude doručená do poštového priečinka adresáta.

Začiatok konverzácie pri odovzdávaní správy elektronickej pošty až po príkaz DATA sa nazýva tzv. obálka správy (message envelope). Osobitný význam tu má príkaz RCPT TO, pretože ten určuje, kto je skutočným príjemcom správy. Hlavičky, ktoré sa objavujú po príkaze DATA, sa nazývajú telo správy (message body) a nemajú už nijaký vplyv na to, komu bude táto správa doručená – používa ich len príjemcov MUA na zobrazenie zdanlivého odosielateľa a príjemcu správy. Pretože sa adresy v obálke môžu líšiť od adres uvedených v tele správy, je možné v SMTP protokole veľmi ľahko odosielať aj správy s podstrčenými, prípadne utajenými príjemcami a odosielateľom. V nevyžiadanej pošte (spam) je typické, že adresy odosielateľa a príjemcu v tele správy sú vymyslené, aby nebolo ľahké späťne odosielateľa vystopovať.

9.10.3 Protokol POP

Protokol Post Office Protocol (POP) sa používa na prístup k doručenej pošte. Pomocou tohto protokolu získava MUA adresáta po správnom overení mena a hesla (autentifikácii) prístup k priečinkom s doručenou poštou, môže si zobrazit' zoznam doručených správ, ich veľkosti, môže vyžiadať prenos jednotlivých správ na adresátov počítač, prípadne zvolené správy z priečinkov na serveri odstrániť. Môže sa zdať, že protokol POP je popri protokole SMTP zbytočný, ale nie je to tak. Protokol SMTP má prostriedky na hľadanie príjemcu správy a jej doručenie správne mu poštovému serveru. Uložením správy do poštovej schránky príjemcu sa však starosť SMTP o doručovanie správy skončila – správa sa považuje za doručenú. Adresát potrebuje pri práci so svojou poštovou schránkou iné nástroje – potrebuje vedieť, koľko správ sa momentálne v schránke nachádza, každú zo správ musí vedieť individuálne preniesť, ponechať v schránke alebo vymazať a podobne. Práve tieto prostriedky SMTP nemá a namiesto neho ich ponúka protokol POP.

Priebeh konverzácie MUA s poštovým serverom pri prístupe k doručenej pošte pomocou protokolu POP je zobrazený v nasledujúcom výpise.

```
USER brunckom
+OK Password required.
PASS TotoJeT4jn3H3510
+OK logged in.
STAT
+OK 1 1423
LIST
+OK POP3 clients that break here, they violate STD53.
1 1423
UIDL
+OK
1 1264159592.19491_0.castor
RETR 1
+OK 1423 octets follow.
Return-Path: <Peter.Paluch@fri.uniza.sk>
Delivered-To: Michal.Bruncko@fri.uniza.sk
Received: from [158.193.152.140] (unknown [158.193.152.140])
```

.by mail.kis.fri.uniza.sk (Postfix) with ESMTP id B29762010C65
.for <Michal.Bruncko@fri.uniza.sk>; Fri, 22 Jan 2010 12:26:32 +0100
(CET)

Message-ID: <4B59BB6B.60B0401@fri.uniza.sk>
Date: Fri, 22 Jan 2010 12:26:32 +0100
From: Peter Paluch <Peter.Paluch@fri.uniza.sk>
Organization: Zilinska univerzita, KIS FRI
User-Agent: Thunderbird 2.0.0.23 (Windows/20090812)
MIME-Version: 1.0
To: Michal Bruncko (Michal.Bruncko@fri.uniza.sk)
Subject: Ukazka prenosu spravy elektronickej posty
Content-Type: text/plain; charset=ISO-8859-1; format=flowed
Content-Transfer-Encoding: 7bit

Ahoj, Miso,

Tuto spravu, prosim, ignoruj - len si potrebujem odchytiť priebeh SMTP dialogu medzi postovym programom a serverom a Ty si mi padol za obeť :-)

Pozdravuje

Peter

.

DELE 1

+OK Deleted.

QUIT

+OK Bye-bye.

Červená farba znázorňuje dáta odoslané z poštového programu (klienta) na server, modrá farba označuje dáta odoslané z poštového servera poštovému programu.

Klient po otvorení spojenia s poštovým serverom odosiela príkaz USER a prihlasovacie meno používateľa. Server si následne vyžiada heslo, ktoré klient odosiela v ďalšom príkaze PASS. Príkazom STAT klient požiada o informáciu, koľko doručených správ sa celkovo nachádza v schránke a aká je ich úhrnná veľkosť. Ďalšími príkazmi LIST a UIDL si klient vyžiada informácie o veľkosti individuálnych správ v schránke a ich identifikátory. Príkazom RETR klient následne vyzdvihne správu zo schránky, príkazom DELE ju po prenesení zo schránky zmaže a príkazom QUIT ukončí spojenie.

Protokol POP je veľmi jednoduchý, no má isté obmedzenia, ktoré sa týkajú najmä schopností používať viaceré poštové priečinky na serveri a práce s doručenými správami priamo na serveri. Tieto obmedzenia odstránil nový protokol s názvom Internet Mail Access Protocol (IMAP), ktorý je však podstatne zložitejší a nebudeme sa mu v tejto publikácii venovať.

Kľúčové slová

1. Aplikačná vrstva
2. Aplikácia
3. Program

4. Proces
5. Základné funkcie aplikačnej vrstvy
6. Application Service Elements (ASE)
7. Common Application Service Element (CASE)
8. Specific Application Service Element (SASE)
9. Domain Name System (DNS)
10. Doména
11. Koreňová doména
12. Vrcholová doména
13. Zdrojový záznam
14. Hyper Text Transfer Protocol (HTTP)
15. Metódy a návratové kódy HTTP
16. Cookies
17. Elektronická pošta
18. Mail User Agent (MUA)
19. Mail Transfer Agent (MTA)
20. Mail Delivery Agent (MDA)
21. Simple Mail Transfer Protocol (SMTP)
22. Post Office Protocol (POP)

Kontrolné otázky:

1. Na ktorej úrovni sa nachádza aplikačná vrstva v RM OSI?
2. Na ktorej úrovni sa nachádza aplikačná vrstva v protokolovom modeli TCP/IP?
3. V akom vzájomnom vzťahu sú aplikačné vrstvy v RM OSI a TCP/IP?
4. Čo sú základné funkcie aplikačnej vrstvy?
5. Aké dátové jednotky sú používané na aplikačnej úrovni?
6. Čo vyjadruje pojem aplikácia?
7. Aký je rozdiel medzi aplikáciou, programom a procesom?
8. Čo sú to Application Service Elements v aplikačnej vrstve?
9. Aké typy Application Service Elements sú špecifikované na aplikačnej vrstve?
10. Čo znamená označenie CASE – Common Application Service Element?
11. Čo znamená označenie SASE – Specific Application Service Element?
12. Aký je rozdiel medzi architektúrou klient-server a peer-to-peer?
13. Pre aký účel je používaný systém DNS (Domain Name System) ?
14. Akú hierarchiu využíva DNS pri vytváraní domén?
15. Čo sú to zdrojové záznamy v DNS?
16. Aké typy zdrojových záznamov v DNS existujú?
17. Ako je označovaná najvyššia úroveň doménovej hierarchie v DNS?
18. Ktorý je základný protokol komunikácie v službe World Wide Web?
19. Aká je úloha protokolu HTTP (Hypertext Transfer Protocol)?
20. Aké metódy používa protokol HTTP?
21. Aký je význam protokolu SMTP (Simple Mail Transfer Protocol) v službe elektronickej pošty?
22. Aký je význam protokolu POP (Post Office Protocol) v službe elektronickej pošty?
23. Ktorý typ záznamu v DNS sa využíva pri doručovaní správ elektronickej pošty a ako?

10 Komunikačné siete a ich technológie

Ciele učenia

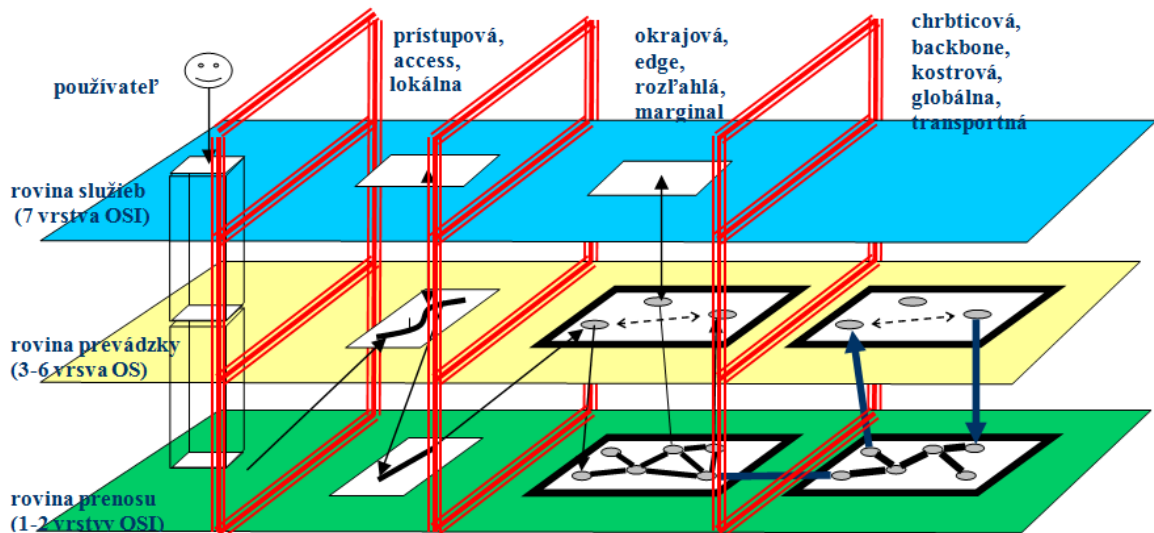
Po štúdiu tejto kapitoly by ste mali vedieť:

- Potreby vzdialených prístupov ku komunikačným sieťam
- Princípy prístupu cez
 - cez telefónne siete (PSTN, ISDN, GSM, UMTS)
 - rádiové siete (WiFi, WiMAX)
 - optické prístupové siete
 - CATV.
- Úlohu edge sietí.
- Základné technológie transportných sietí
 - časový multiplex - TDM
 - plesiochrónnu digitálnu hierarchiu - PDH
 - synchronnú digitálnu hierarchiu – SDH
 - vlnový multiplex – WDM, DWDM, CWDM
 - optickú digitálnu hierarchiu OTH.

10.1 Úvod

Kapitoly 1 až 9 sú venované princípom vrstvomého členenia komunikačných technológií, ktoré sú špecifikované vrstvomým modelom komunikácie, odporúčanie ISO OSI 74910. Tento model je základom teoretických princípov a vyjadrením podmienok vzájomnej komunikácie rôznych technológií. Realizácia komunikačných sietí predstavuje vzájomné prepojenie rôznych technológií, ktorých principiálne riešenie je všeobecne vyjadrené úrovňovým modelom komunikačnej siete, znázornenom na obr. 10.1, ktorého stručné vysvetlenie je v kapitole 2. V tejto kapitole sa budeme venovať konkrétnym technológiám, ktoré sú používané v jednotlivých typoch sietí.

Účelom každej technológie komunikačných sietí je poskytovanie služieb, ktoré zabezpečuje rovina služieb, riadi rovina prevádzky a samotný prenos informácie je poskytovaný rovinou prenosu. Približné prepojenie s vrstvomým OSI modelom vzájomnej komunikácie je nasledovné. Rovinu služieb predstavuje aplikačná vrstva OSI modelu, rovinu prevádzky vrstvy 3-6, sieťová, transportná relačná a prezentačná, rovinu prenosu vrstvy 1-2, fyzická a linková. Ak všeobecný vrstvomý model, rozčleníme vertikálne, dostávame priestorový pohľad, ktorý na obrázku 10.1 znázorňujú typy sietí podľa polohy v prenosovom reťazci.

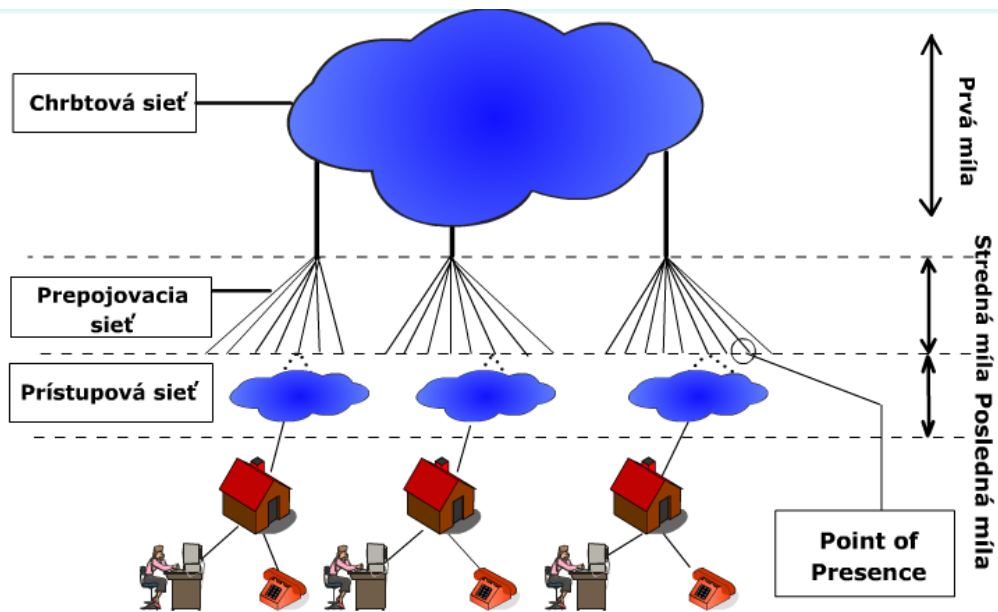


Obr. 10.1 Vertikálne členenie úrovňového modelu komunikačnej siete

Podľa vertikálneho členenia úrovňového modelu sa komunikačné siete delia na tri základné typy:

- Prístupové siete (*Access Network*), označované aj ako lokálne siete, v minulosti miestne siete.
- Okrajové siete (*Edge siete*), niekedy označované aj ako rozľahlé siete alebo *marginal networks*.
- Transportné siete (*Backbone networks*), označované aj ako chrbticové, kostrové, alebo globálne siete.

Aj z hľadiska takejto hierarchie je na oboch koncoch komunikačného kanálu koncový používateľ služieb elektronickej komunikačnej siete, ktorý je vlastníkom koncového zariadenia KZ. Prístupovou sieťou je nazývaná sieť, ktorá zabezpečuje prístup koncových zariadení na transportnú komunikačnú sieť. Medzi uvedenými dvoma typmi sietí je vložená okrajová – *edge* sieť. Dôvodom pre špecifikáciu *edge* sietí, respektíve *edge* uzlov, je prispôbenie požiadaviek prenosu z prístupových sietí na prenos po transportných sieťach. Hierarchické usporiadanie siete, označované často aj ako architektúra siete je na obrázku 10.2.

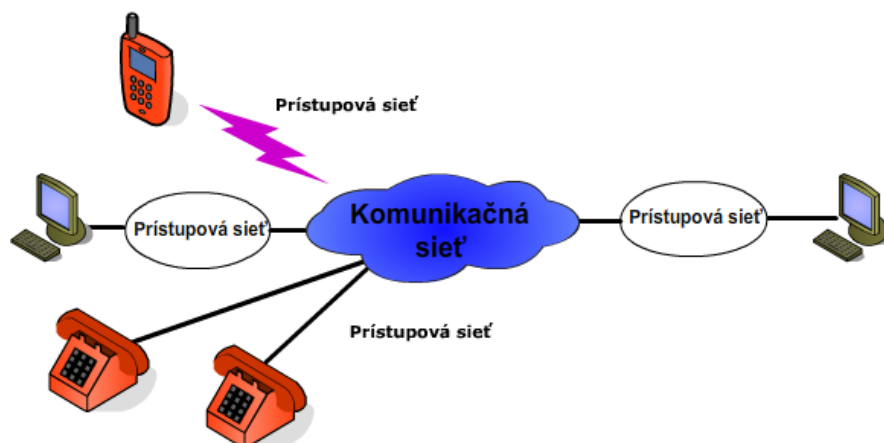


Obr. 10.2 Hierarchické usporiadanie siete

10.2 Prístupové siete

Prístupová sieť je prvou časťou komunikačnej infraštruktúry smerom od používateľa. Služi pre určitú oblasť, organizačnú, mestskú alebo vidiecku, ktorej koncoví používatelia sú cez prístupové body pripájaní do komunikačnej siete. Prístupové body prvého komunikačného uzla poskytujú prepojenia do vyšších úrovní siete. Ako marketingový pojem je pre prístupovú sieť používané označenie „posledná míľa“.

Problematika prístupu k sieti sa vyskytovala už i v analógovej sieti, kde používateľské koncové zariadenia boli, a ešte aj sú, pripojené k sieti metalickými prípojnými vedeniami. Tie boli zoskupované do kábla a vytvárali sieť, ktorá sa nazývala „miestna sieť“. Takýmto spôsobom sú dnes ešte pripojené koncové zariadenia pevnej telefónnej siete PSTN (*Public Switched Telephone Network*). Tento spôsob pripojenia je príkladom priestorového multiplexu. Vytváranie prístupových sietí vzniklo v súvislosti s digitalizáciou komunikačných sietí. Digitalizácia spojovacích a prenosových systémov umožnila vyššie prenosové rýchlosti a tým možnosti pripojenia väčšieho počtu koncových zariadení k uzlom siete. Problémom sa vtedy stali metalické miestne siete, ktorých nízke prenosové rýchlosti bránili poskytovaniu širokopásmových služieb. Pozornosť komunikačného trhu sa sústredila na „poslednú míľu“. Dôsledkom vytvárania prístupových sietí bola decentralizácia miestnych sietí na časť koncových zariadení a časť prístupovej siete. Koncové zariadenia boli ako prvé v elektronických komunikačných sieťach liberalizované a ich pripojenie na sieť je dnes na používateľovi alebo poskytovateľovi služby. Často sa v tejto súvislosti používa pojem „sieť koncových zariadení“, aj keď sa jedná o sieť len v niektorých prípadoch a to len veľmi obmedzenú. Znárodnenie pripojenia troch najčastejšie používaných koncových zariadení na komunikačnú sieť je na obr. 10. 3.



Obr. 10.3 Pripojenie koncových zariadení na komunikačnú sieť

Z obrázku vyplýva, že pripojenie cez prístupovú sieť je rôzne podľa typu koncového zariadenia. V praxi je možné pripájať rozličné koncové zariadenia cez rozličné typy prístupových sietí, ale v mnohých prípadoch je potrebná dodatočná technológia, ktorá využije existujúce sieťové prvky a umožní pripojenie rôznych zariadení.

Dôvodom prístupu k elektronickej komunikačnej sieti je potreba komunikácie z rôznych pracovných aj osobných dôvodov, získavanie informácií z centralizovaných miest, posielanie rôznych dát a dokumentov a využívanie poskytovaných služieb po elektronických komunikačných sieťach. Prístup k sieti je rozdielny podľa potrieb jednotlivých kategórií používateľov. Používateľské segmenty sa delia na:

- privátnych používateľov a
- biznis používateľov.

Ich potreby sú brané do úvahy, pri riešení prístupu ku komunikačnej sieti a výbere prístupovej siete, alebo prístupovej technológii.

Používatelia prístupujú v súčasnosti k rôznym typom elektronických komunikačných sietí, podľa povahy využívanej služby. Najčastejšie sú využívané prístupy k:

- telefónnym sieťam pevným,
- telefónnym sieťam mobilným,
- sieti internet,
- verejnej dátovej sieti,
- sieťam distribúcie televíznych a rozhlasových programov,
- LAN sieťam (aj keď pre vzdialený prístup môžu byť siete LAN prístupovými sieťami).

Najčastejšie využívané služby elektronických komunikačných sietí, kvôli ktorým používatelia potrebujú prístup ku komunikačnej sieti sú:

- telefónna služba,
- služby siete internet (www, e-mail,..),

- iné webové služby,
- televízne a rozhlasové služby,
- telefaxová služba,
-

10.2.1 Funkcie prístupových sietí

Prístupové siete poskytujú pre prenos informácie nasledujúce funkcie:

- zber prevádzky z koncových zariadení v danej oblasti k uzlu na vyššej úrovni siete,
- zabezpečenie štandardného rozhrania prístupu k sieti medzi koncovým zariadením a prvým uzlom v sieti, označovaným ako *service node*,
- prístup vyššími prenosovými rýchlosťami od koncového zariadenia po prvý uzol v sieti,
- prenos informácie na krátke a stredné vzdialenosti,
- napájanie koncových zariadení,
- zabezpečenie signalizácie,
- konverzie signálov (modulácie),
- riadenie prístupu k sieti,
-

Funkciu prístupovej siete môžu poskytovať rôzne technológie. Výber technológie závisí od hierarchického usporiadania siete, od typu koncového zariadenia a od požadovanej služby používateľom. Iné funkcie sú požadované pre telefónnu službu, iné pre prenos dát a iné pre rôzne informačné služby. Preto jednotlivé funkcie prístupových sietí sú spojené s príslušnými prístupovými sieťami alebo ich technológiami.

Všeobecne možno funkcie prístupu ku komunikačnej sieti je rozdeliť do dvoch častí:

- funkcie prístupu z koncového zariadenia,
- funkcie prenosovej časti, ktorá poskytuje pripojenie k príslušnej sieti.

Funkcie prístupu z koncového zariadenia sa rozlišujú podľa charakteru služby a typu siete, ktorou prístup realizujeme. V telefónnej službe je prístup realizovaný podľa toho, či sa je požiadavka pripojenia cez telefónnu sieť PSTN, ISDN, alebo mobilnú telefónnu sieť. Iný prístup je pre využívanie telefónnej služby VoIP/hlas po internete, ktorý je spojený s prístupmi v dátových prenosoch. Každá technológia má špecifikovaný postup prístupu ku sieti.

Klasická telefónna služba používa pre riadenie prístupu funkcie signalizácie, pri dátových prenosoch sú využívané metódy vzdialeného prístupu. Príkladom použitia je služba vzdialeného prístupu RAS (*Remote Access Services*), ktorá umožňuje vzdialený prístup k nástrojom alebo informáciám, ktoré sú na dátovej sieti alebo iných IT zariadeniach. Pre dátovú prevádzku je možné použiť aj telefónne prístupy, ale vtedy sú potrebné ďalšie doplnujúce technológie.

Prenosová časť prístupu k sieti je rôzna podľa charakteru pripojenia a použitej technológie. Princiálne rozlišujeme:

- analógové pripojenie cez analógové prístupové siete PSTN/ISDN, používané pre hlasovú službu (v súčasnosti málo používané),
- digitálne pripojenie cez pôvodne analógové prístupové siete, kde sa doplnujúcimi technológiami vytvorí digitálne pripojenie, napríklad xDSL v PSTN alebo káblový modem v CATV.
- digitálne pripojenie cez digitálne siete, napríklad ISDN, GSM.

Podľa použitého prenosového média sa rozlišujú prístupové siete :

- drôtové
 - metalické - krútená dvojlinka a koaxiálny kábel
 - optické vlákna/káble
- bezdrôtové
 - mobilné
 - pevné.

Prístup na prenosovú časť komunikačnej sieť nemusí vždy tvoriť sieť. V niektorých prípadoch sú to iba prístupové systémy, alebo prístupové technológie použité na prípojnom vedení, ktoré je pripojené priamo k uzlu siete. Podľa prístupu k sieti rozlišujeme:

- technológie s komutovaným prístupom,
- technológie s permanentným prístupom.

Technológie s komutovaným prístupom sú vhodné pre časovo obmedzené spojenia alebo ako záloha technológii s permanentných spojením pre prípad výpadku. Komutovaný prístup je poskytovaný cez verejné komunikačné siete ako služba prístupu, často s použitím prídavných technológií. Dial Up, xDSL, 3G,... Základným prvkom pripojenia tohto typu je modem pripojený k sieti. Spojenie je vytvárané na základe potreby a to buď automaticky (*Dial on Demand*) alebo na základe vyžiadania používateľom.

Technológie s permanentným spojením sú vhodné pre komunikácie, kde je komutované pripojenie nevýhodné, alebo vyžadujú vyššiu kvalitu pripojenia. Spôsoby permanentného spojenia tvoria:

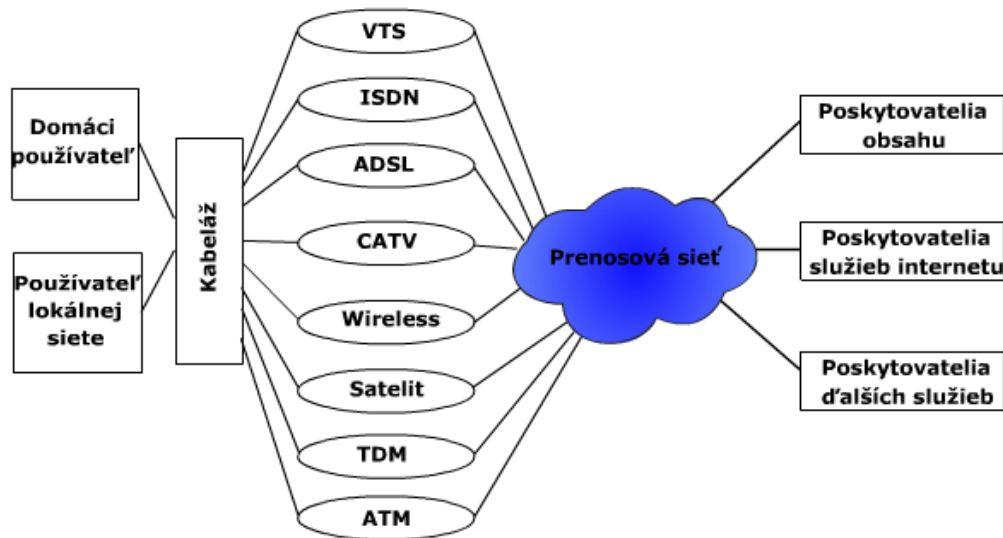
- prenajaté okruhy (*Leased Line*) a
- sieťové technológie, ktoré vytvárajú samostatné prístupové siete.

Najpoužívanejšie služby prístupu cez verejné telefónne siete sú v súčasnosti známe pod týmito marketingovými označeniami:

- 3G, čo je skratka tretej generácie mobilných technológií. Umožňuje v mobilných sieťach renos hlasu aj dát (telefónny hovor) i dáta (st'ahované dáta, e-mail, správy).
- ADSL (*Asymmetrical Digital Subscriber Line*) umožňuje vysokorýchlostné dátové prenosy po metalických telefónnych linkách.

- Chello je služba poskytovania širokopásmového internetu cez rozvody káblovej televízie.
- Edge (*Enhanced Data rates for GSM Evolution*) je služba mobilných dátových technológií, pôvodné označenie GPRS. EDGE je nadmnožinou GPRS.
- Flarion, je služba mobilných dátových technológií. Ponúkaná je iba vtedy, ak v danej lokalite nie je minimálne 3G pokrytie.

Niektoré príklady prístupových technológií sú na obr. 10. 4. Vybrané prístupové technológie a služby sú popísané v ďalšej kapitole.



Obr. 10. 4 Príklady prístupových technológií (prístupy)

10.2.2 Technológie prístupových sietí

10.2.2.1 PSTN (Public Switched Telephone Network) - Verejná telefónna sieť VTS

PSTN alebo verejná telefónna sieť - VTS je najväčšou komunikačnou sieťou s viac než 700 miliónmi používateľov. VTS bola dlho jedinou sieťou poskytujúcou službu prenosu hlasu a bola to jediná služba, ktorú poskytovala. V priebehu svojej histórie prešla VTS radom technických a iných zmien. Z analógovej siete sa stala sieť digitalizovaná, zmenila sa štruktúra siete i jej využitie. Nezmenil sa však princíp prepojovania okruhov. Aj keď sa nezmenilo pôvodné poslanie hlasových sietí, prenášať hlas, nastali ďalšie zmeny. Sieť sa využíva aj na iné služby, napríklad telefaxová služba, prístup k sieti internet, prenos dát. Rozšírili sa doplnkové služby zvyšujúce komfort pre používateľa a ďalšie rozšírenie vzniklo poskytovaním služieb inteligentnej siete. Tým sa nezmenili ani ekonomické a funkčné vlastnosti hlasových sietí. Preto tieto siete dokážu vyhovieť pomerne náročným požiadavkám, kladeným na kvalitu prenosových služieb. Tie sú vyjadrené napríklad parametrami oneskorenia či premenlivosti tohto oneskorenia. Základné charakteristiky sú:

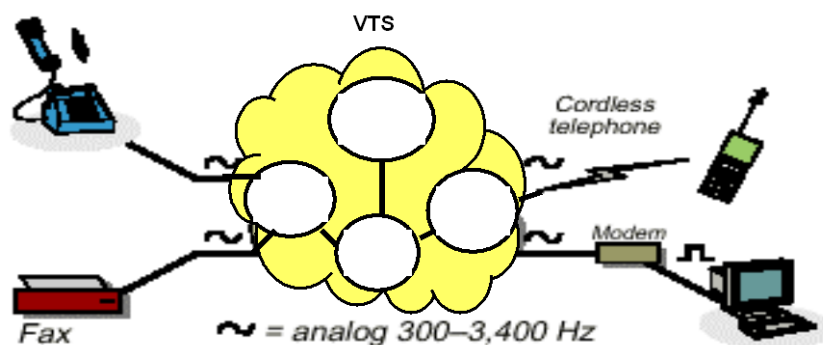
- pôvodne analógový prístup,
- obojsmerné spojenie,
- princíp prepájania okruhov,

- prepojovaná šírka pásma 300-3400 Hz (64 kbit/s),
- digitalizácia siete (prenos a spojovanie),
- riadenie prístupu k sieti,
- imobilita používateľov, resp. obmedzená mobilita, mobilita iba cez bezšnúrové koncové zariadenie.
- prístup po pevných metalických vedeniach, v niektorých prípadoch rádiový prístup, hlavne v málo obývaných územiach,
- niekedy sa používa pripojenie prostredníctvom pobočkových ústrední, alebo koncentrátorov,
- prístupová sieť je využívaná alternatívnymi operátormi, ktorí nemajú vybudovanú vlastnú pevnú prístupovú sieť.

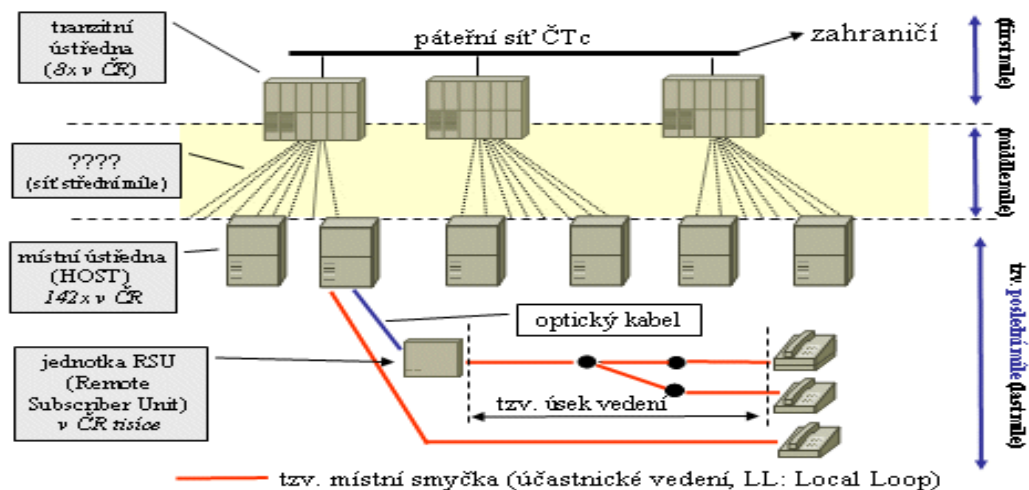
Architektúra siete je tvorená usporiadaním technických prostriedkov do hierarchie tvorenej kategóriou uzlov. Rozlišujú sa nasledujúce kategórie uzlov:

- lokálne (miestne), pre pripojenie používateľov,
- tranzitné, na tranzitovanie prevádzky,
- medzinárodné, na tranzitovanie prevádzky medzi rôznymi štátmi.

Znázornenie architektúry verejnej telefónnej siete je na obr. 10.5.



Obr. 10.5 Usporiadanie verejnej telefónnej siete



Obr. 10.5 Hierarchické usporiadanie

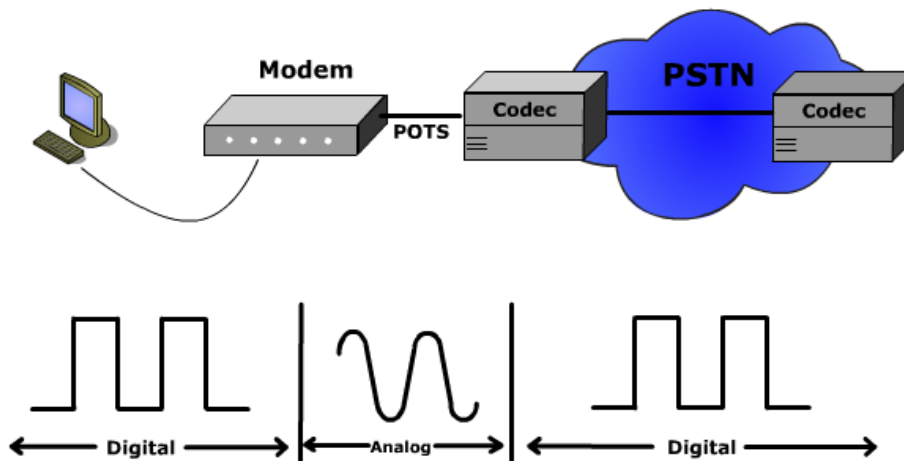
Časť prístupu na obrázku 10.5, označená ako posledná míľa (*lastmile*), je kritickou časťou prístupových sietí. Pôvodné miestne siete, aj keď sú veľmi dobre vybudované, sú prevažne riešené ako medené krútené dvojlinky. Preto prevádzkovatelia sietí vytvárané rôzneslužby, ako prístupové siete čo najlepšie využiť. Najčastejšie je to nasadzovaním iných technológií, ktoré využijú vyššie frekvenčné spektrum nad 4kHz a tak sa posúva prístupový bod - RSU (*Remote Subscriber Unit*) bližšie ku koncovému používateľovi.

PSTN poskytuje nasledovné služby:

POTS - *Plain Old Telephone Service*, v doslovnom preklade "stará prostá telefónna služba" je označenie pre analógové pripojenie k verejnej telefónnej sieti. Takéto pripojenie je možné využiť iba pre nižšie prenosové rýchlosti, pretože šírka prenášaného pásma je iba od 300 až 3400 Hz. Kvôli obmedzeniu šírky pásma je obmedzená aj rýchlosť dátových prenosov. Dátové prenosy sú realizované veľmi jednoduchou službou označovanou ako **dial-up**. Aj keď pre využívanie širokopásmových prístupov je perspektíva v iných prístupových sieťach, vysvetlíme princíp dial-up. Dôvodom sú dve skutočnosti:

5. V niektorých prípadoch nie je možné iné pripojenie, alebo používateľ využíva pripojenie k dátovým službám tak málo, že sa mu neoplatí.
6. Princíp, použitý u dial-up služby je veľmi podobný s inými princípmi komutovaného pripojenia.

Princíp služby dial-up je na obrázku 10.6. Digitálny signál z koncového zariadenia je prístupovou sieťou prenášaný k prístupovému uzlu siete ako analógový, použitím niektorého spôsobu analógovej modulácie (kľúčovania).



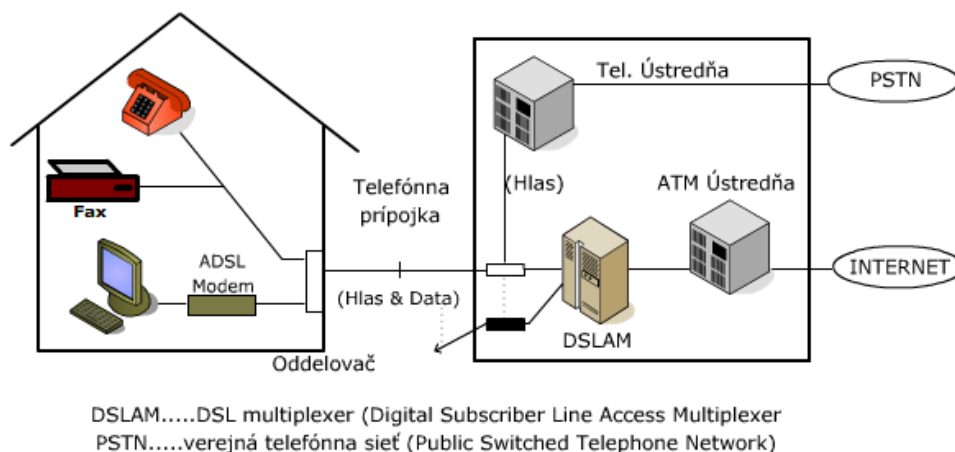
Obr. 10.6 Princíp Dial-up služby

xDSL (*xDigital Subscriber Line*) je technológia, ktorá umožňuje digitálne pripojenie po metalických vedeniach, používaných pre analógové prenosy. Po prípojných metalických vedeniach je tak možné prenášať okrem telefónneho signálu aj vysokorýchlostné dátové služby. Technológie xDSL sú kompromisom medzi prenosovou rýchlosťou v oboch smeroch prenosu a vzdialenosťou, do ktorej je možné tieto technológie použiť. Podľa charakteru dopredného (*upstream*) a spätného (*downstream*) prenosu sa xDSL technológie delia na:

- symetrické, ktoré poskytujú v oboch smeroch rovnakú prenosovú rýchlosť,
- nesymetrické, ktoré majú rozdielne prenosové rýchlosti dopredného a spätného prenosu.

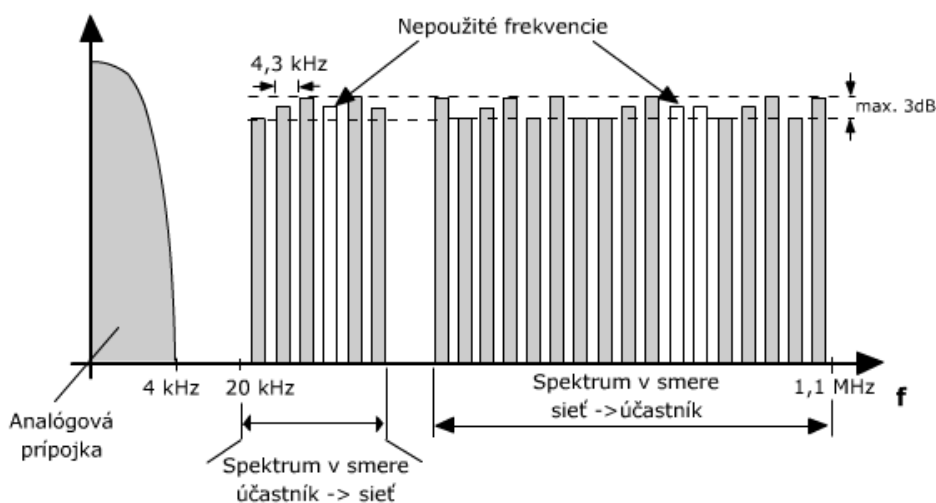
Podľa charakteru prenosu sú ponúkané nasledovné služby prístupu:

ADSL (Asymmetrical Digital Subscriber Line) - Asymetrická digitálna účastnícka prípojka je v súčasnosti najviac používanou xDSL technológiou. V spätnom smere prenosu, (*downstream*), umožňuje prenosovú rýchlosť do 8 Mbit/s a v doprednom smere, (*upstream*), 768 kbit/s. Takáto prenosová rýchlosť je možná len pri relatívne malých dĺžkach účastníckych prípojných vedení, asi do 2 km. Pri menších rýchlostiach, *downstream* 2 Mbit/s a *upstream* 192 kbit/s, môže byť dĺžka vedenia až do 5 km. Pripojenie používateľa do PSTN použitím technológie ADSL je na obr. 10.6



Obr. 10.6 Pripojenie k PSTN použitím ADSL

Pripojenie sa realizuje prostredníctvom ADSL modemu, ktorý rozdeľuje dostupné frekvenčné pásmo medzi hlas a dáta, čím umožňuje súčasný prístup používateľa k hlasovej i dátovej službe, obr. 10.7.



Obr. 10.7 Frekvenčné spektrum ADSL

Iné DSL technológie sa odlišujú v prenosových rýchlostiach a v dĺžkach prípojných vedení.

VDSL (Very high-bit rate DSL) - Vysokorýchlostné DSL umožňuje prenosovú rýchlosť downstream až do 52 Mbit/s, ale iba pri dĺžke účastníckeho vedenia do cca 500 m. Preto je potrebná taká architektúra, pri ktorej je koaxiálny alebo optický kábel dovedený až k distribučnému miestu, ktorého vzdialenosť od účastníckeho zariadenia nie je väčšia ako 1 km.

HDSL (High-bit rate DSL) na rozdiel od iných DSL technológií, umožňuje symetrickú prenosovú rýchlosť, rovnakú pre obidva smery prenosu. V USA je prenosová rýchlosť 1,544 Mbit/s, v Európe, 2048 Mbit/s. HDSL predstavuje technológiu, ktorá je používaná predovšetkým v podnikových sieťach na vzájomné prepojenie LAN a prístup k internetu.

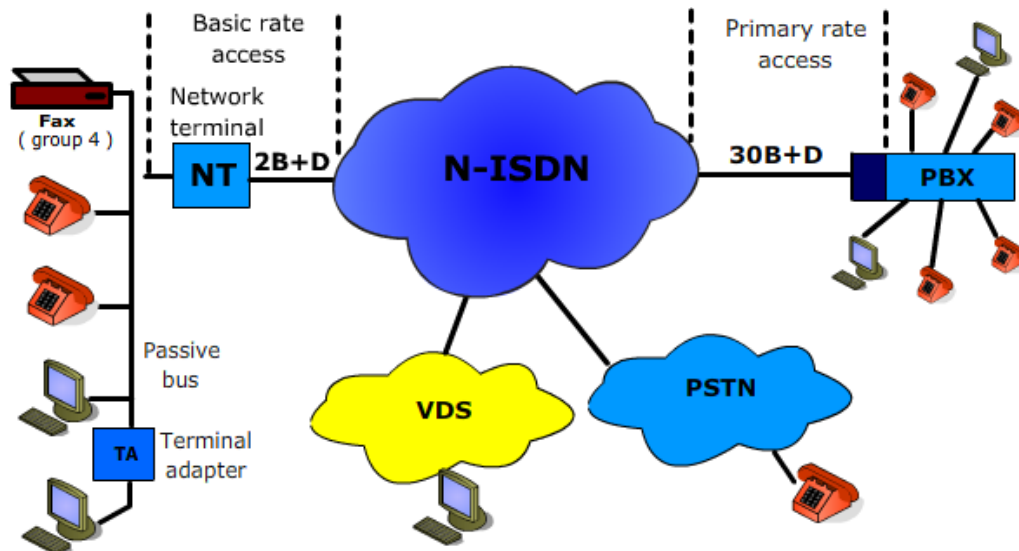
Veľmi dobre spolupracuje s inými technológiami, ako ISDN a klasické telefónne alebo prenajaté okruhy.

10.2.2.2 ISDN (Integrated Services Digital Network) – Digitálna sieť integrovaných služieb

ISDN je jedna z vývojových etáp telekomunikačných sietí. Viac ako sto rokov bola hlavnou komunikačnou infraštruktúrou telefónna sieť, vytvorená s ohľadom na potreby analógového prenosu ľudského hlasu a telegrafná sieť na prenos textu. I keď po oboch sieťach bolo možné poskytovať aj službu prenosu dát, ani jedna zo sietí nebola nikdy vhodným prostriedkom pre prenos dát. Preto boli vytvárané špecializované dátové siete, určené iba na prenos dát. Od týchto špecializovaných sietí pokračoval vývoj ku spoločnej digitálnej sieti, v ktorej je integrované široké spektrum služieb rôznych informačných typov – ISDN, štandardizovanej organizáciou ITU (*International Telecommunication Union*) a ETSI ako Euro ISDN. Základné charakteristiky ISDN sú:

- digitálna sieť,
- prenos je digitálny už od koncového zariadenia,
- základná prenosová rýchlosť 64 kbit/s,
- poskytuje prepojenie okruhov i prepojenie paketov,
- prístup cez drôtové prípojné vedenia cez definované štandardizované rozhranie,
- signalizácia, účastnícka aj sieťová,
- poskytuje integrované služby všetkých informačných typov.

Základom architektúry siete sú ústredne ISDN, vzájomne spolupracujúce prostredníctvom signalizačného systému SS č.7. Na ústredne sú pripojené pobočkové ústredne buď dvojdrôtovými digitálnymi okruhmi, alebo štvordrôtovým vedením s multiplexným zariadením. Koncové zariadenia sú pripojené buď cez pobočkové ústredne, alebo priamo pomocou prípojných digitálnych okruhov. Na konci účastníckej prípojky je umiestnené ukončujúce zariadenie siete, označované ako NT (*Network Termination*). Analógové koncové zariadenie, alebo dátové koncové zariadenie s iným než ISDN rozhraním, je pripojené prostredníctvom terminálových adaptérov TA ISDN. Ústredne ISDN bývajú prepojené s prepojovacími uzlami verejných dátových sietí VDS a ústredňami verejnej telefónnej siete. Znázornenie koncepcie je na obr. 10.10.



Obr. 10.8 Konceptia riešenia siete ISDN

ISDN poskytuje používateľom rôzne druhy prenosových kanálov resp. okruhov. Dva základné majú nasledujúce označenie:

7. B - digitálny kanál s prenosovou rýchlosťou 64 kbit/s. Umožňuje prenosi s prepojaním okruhov aj prepojaním paketov. Je určený na prenos digitálnych telefónnych a dátových signálov.
8. D - digitálny kanál na služobné účely, s prenosovou rýchlosťou 16 alebo 64 kbit/s. Je označovaný ako D_{16} a D_{64} . Slúži predovšetkým na prenos riadiacej signalizácie a používa paketovú komunikáciu. Keď nie je použitý na prenos signalizácie, môže slúžiť na prenos používateľských informácií paketovým prepojaním.

Odporúčanie ITU štandardizuje dve základné kombinácie týchto kanálov, označované ako IDSL (*Integrated Digital Subscriber Line*) prístupy, ktoré patria do skupiny prístupov DSL – *Digital Subscriber Line*. Sú to:

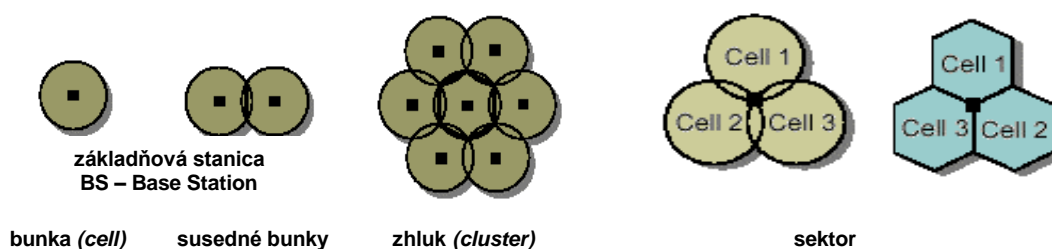
Základný prístup ISDN BRA (*Basic Rate Access*), ktorý poskytuje prístup prenosovou rýchlosťou 64 kbit/s v jednom používateľskom B kanáli, resp. 128 kbit/s pri dvoch používateľských B kanáloch v základnom prístupe BRA. Je označovaný aj ako 2B + D prístup. Využíva sa pre pripojenie privátnych používateľov.

Primárny prístup ISDN PRA (*Primary Rate Access*) je najčastejšie používaný na pripojenie pobočkových ústrední. V tomto prípade je súčasne k dispozícii v Európe 30 kanálov B a jeden kanál D_{64} , (v USA a Japonsku 23 kanálov B a 1 kanál D). Je označovaný ako prístup 30B + D. Celková prenosová rýchlosť je 2 Mbit/s a má rovnakú štruktúru ako 30-kanálový multiplexný prenosový systém PCM 32/30. Spojenie medzi používateľským zariadením a ústredňou je štvordrôtové. Pripojenie je uskutočňované cez rozhranie skupiny NT2.

ISDN má obmedzenie v konečnej rýchlosti a tiež v dosahu. ISDN sieť po štandardných prípojných vedeniach umožňuje prenos približne do vzdialenosti 5 až 10 km, čo je najväčším obmedzením pre rozvoj sietí ISDN v podmienkach vidieka.

10.2.2.3 Mobilné telefónne siete

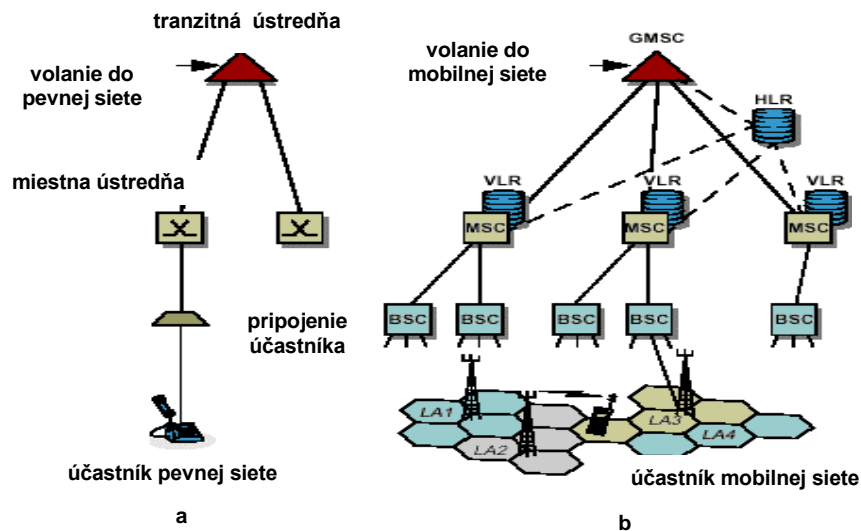
Mobilné telefónne siete majú odlišnú architektúru oproti pevným telefónnym, alebo dátovým sieťam. Celé územie, ktoré má byť pokryté signálom, napríklad územie jedného štátu, je rozdelené na menšie časti, bunky (*cells*). Odtiaľ je tiež názov celulárne alebo bunkové systémy. Priemery jednotlivých buniek sa pohybujú od stoviek metrov do desiatok kilometrov, v závislosti od očakávanej prevádzky. Bunka je najmenšie rozlíšiteľné územie, ktoré má svoj prijímač a vysielač a pridelenú vlastnú frekvenciu. Susedné bunky majú pridelené rôzne frekvencie, ale bunky, ktoré sú od seba dostatočne vzdialené, môžu mať pridelené rovnaké frekvencie, pretože pri pomerne malom výkone na území bunky sa frekvencie pri dostatočnej vzdialenosti nerušia. Použitie rôznych frekvencií pre susedné bunky a identických frekvencií pre vzdialené bunky vedie k rozdeleniu územia na zhľuky (*clusters*). Zhľuk je skupina buniek v rámci ktorých sa nesmú opakovať pridelené frekvencie. Frekvencie sa môžu opakovať v bunkách patriacich do rôznych zhľukov. Zhľuky obsahujú spravidla 4,7, alebo 12 buniek. Príklady rozdelenia územia v mobilných sieťach sú na br. 10.9.



Obr. 10.9. Rozdelenie územia v mobilných sieťach

Obvykle uprostred každej bunky sú umiestnené základňové stanice, označované ako BS (*Base Station*), alebo BTS (*Base Transceiver Station*). Počet BS sa môže redukovať tak, že BS sa neumiestni do stredu každej bunky, ale do priesečníka dvoch, troch alebo štyroch buniek. Vtedy je BS so smerovými anténami umiestnená tak, aby každá anténa pokryla územie jednej bunky. Takto je územie delené na iné útvary, nazývané sektory. Keď je použité sektorovanie, predstavuje sektor v podstate bunku.

Takto zostavená architektúra používa hierarchickú štruktúru, znázornenú na obr. 10.10.aj s porovnaním architektúry pevnej telefónnej siete.



Obr. 10.10 Architektúra pevnej a mobilnej telefónnej siete

Funkcie jednotlivých blokov architektúry:

BTS (Base Transceiver Station) resp. Base Station BS - základňová rádiová stanica predstavuje najnižšiu úroveň relatívne neinteligentných viackanálových vysielačov a prijímačov a antény. Základňové stanice zaisťujú rádiové spojenie s mobilnými koncovými zariadeniami cez rádiové rozhrania. Základnú funkciu BTS možno zhrnúť do nasledujúcich bodov:

- pokrýva územie bunky,
- má pridelené určité frekvencie,
- kóduje, dekoduje a komprimuje prenášaný signál,
- uskutočňuje rádiovú komunikáciu s mobilným koncovým zariadením.

BTS je spojená digitálne s ďalšou hierarchickou úrovňou, ktorou je úroveň riadenia BSC.

BSC (Base Station Controller) riadenie základňovej stanice riadi prevádzky niekoľkých základňových staníc BTS. Najdôležitejšia funkcia riadenia základňových staníc BSC je riadenie frekvencií pridelených skupine BTS a riadenie a koordinácia *handovera*. **Handover** označuje funkciu neprerušenej komunikácie pri prechode používateľa z územia jednej bunky do územia inej bunky. Predstavuje odovzdávanie používateľa medzi jednotlivými BTS. Všetky BTS, sú prepojené na spojovací podsystem MSC.

MSC (Mobile Switching Centre) mobilná ústredňa zaisťuje všetky funkcie prepínania a spojovania. Je spravidla dimenzovaná pre zaistenie prevádzky napríklad pre oblasť veľkého mesta a jeho okolia. Jej úlohou je riadiť reláciu so všetkými potrebnými činnosťami, zostavovanie spojenia, dohľad a rozpojenie mobilných používateľov, prípadne mobilného používateľa a používateľa pevnej siete. Jedna MSC riadi viac BTS a obvykle postačuje jedna MSC na územie s približne miliónom obyvateľov. Ak je ústredňa prepojená s externými sieťami, s pevnou telefónnou sieťou PSTN, označuje sa GMSC (*Gateway MSC*). BTS sú pripojené k MSC, buď rádiovými okruhmi, alebo pevnými telefónnymi okruhmi. Skupina

základňových staníc pripojených k jednej MSC vytvára zväzok – servisnú oblasť SA (*Service Area*), ktorá môže byť rozdelená na niekoľko suboblastí TA (*Traffic Area*). Ústredne MSC sú vzájomne prepojené, pričom jedna z nich má funkciu hlavnej ústredne HMSC (*Home MSC*). Tá obsahuje databázu všetkých používateľov systému označovanú ako domovský lokačný register HLR.

HLR (*Home Location Register*) je databáza, v ktorej sú uložené dôležité informácie o všetkých vlastných používateľoch a ďalej informácie o službách, ku ktorým majú používatelia prístup. Napríklad aktuálna poloha, identifikační údaje, predplatené služby, atď.. Register HLR môže byť využitý jednou alebo niekoľkými ústredňami MSC. Každý používateľ je registrovaný len v jednom registri HLR.

Ostatné ústredne obsahujú návštevnícky lokačný register VLR.

VLR (*Visitor Location Register*) je databáza, v ktorej sú dočasne uložené aktuálne údaje o mobilných používateľoch, ktorí sa práve pohybujú v oblasti príslušnej ústredne MSC. Ak používateľ opustí oblasť ústredne, údaje z registra sú vymazané. Register VLR je súčasťou každej ústredne. Tak, ako sa používateľ pohybuje so svojim mobilným koncovým zariadením, menia sa jeho údaje v týchto registroch.

Ďalšie bloky mobilnej siete sú napríklad:

- Strediská pre riadenie prevádzky krátkych správ **SMSC (*Short Message Service Centre*)**.
- Centrum autentizácie **AuC (*Authentication Centre*)**, ktorý je súčasťou registra HLR a využíva sa k overeniu každého používateľa pred zahájením komunikácie.
- Identifikačný register mobilných staníc **EIR (*Equipment Identity Register*)**, ktorý zaznamenáva dáta o odcudzených alebo neoprávnene používaných mobilných koncových zariadeniach. Je tesne prepojený s AuC a je len jeden v celej sieti jedného operátora.

Funkcie mobilného koncového zariadenia: Identifikácia používateľa

Identifikáciu používateľa zabezpečuje systém SIM karte cez štvormiestne číslo PIN (*Personal Identification Number*). Pri troch chybných zadaniach čísla PIN sa SIM karta zablokuje a možno ju odblokovať len použitím čísla PUK (*Personal Unblocking Key*). Číslo PIN možno ľubovoľne často meniť. Na SIM karte sú uložené dôležité údaje potrebné pre utajenie prenášaných informácií a pre zaistenie anonymity používateľa v sieti.

Anonymita v sieti je používateľovi zaručená jednoznačne identifikovaným číslom IMSI (*International Mobile Subscriber Identification*), ktoré je uložené v pamäti mobilného zariadenia. Aby používateľ nemusel toto číslo posielat' cez rádiové rozhranie pri každej žiadosti o nejakú službu, priradí mu systém dočasnú identifikáciu TMSI (*Temporary Mobile Subscriber Identification*). Číslo TMSI je uložené na SIM karte a v registri VLR mobilnej ústredne. Pokiaľ sa používateľ s mobilným zariadením presunie na územie pod kontrolou inej ústredne, pošle mu táto ústredňa nové číslo TMSI a predchádzajúce číslo je zrušené, ako v SIM karte, tak i vo VLR predchádzajúcej ústredne. Len v prípadoch, kedy sa používateľ hlási

do systému po zapnutí mobilného koncového zariadenia, posiela do ústredne identifikáciu IMSI.

Overenie totožnosti používateľa môže byť uskutočnené až vtedy, keď systém pozná IMSI alebo TMSI. V niektorých prípadoch pri znalosti tejto identifikácie môže systém použiť aj ďalšie tajné informácie potrebné k príslušným výpočtom. Jedná sa o kontrolu totožnosti používateľa, ktorá sa realizuje špeciálnou technikou. Tá môže byť použitá ku kontrole pri zostavovaní spojenia. Uskutočňuje sa v niekoľkých krokoch. Najskôr MSC-VLR žiada u mobilného koncového zariadenia identifikáciu IMEI a po spätnom zaslaní identifikácie je táto odovzdaná do registra EIR, ktorý vykoná kontrolu, prípadne zaradí koncové mobilné zariadenie do jedného z troch zoznamov.

9. Biely zoznam obsahuje čísla IMEI všetkých platne registrovaných mobilných koncových zariadení.
10. Čierny zoznam obsahuje čísla IMEI všetkých nahlásených odcudzených mobilných koncových zariadení.
11. Šedý zoznam obsahuje čísla IMEI všetkých poškodených mobilných koncových zariadení.

Technológie mobilných telefónnych systémov sú nasledovné:

GSM (Global System for Mobile Communication)

GSM je najrozšírenejší mobilný štandard. Predstavuje 2. generáciu mobilných systémov, ktorá sa orientuje hlavne na hlasové služby. Obidva kanály, komunikačný i kontrolný sú digitálne. Pre prístup sú najčastejšie používané FDD s TDMA systémami, alebo kombinované FDMA/TDMA systémy.

GSM spolupracuje s ostatnými telekomunikačnými sieťami - PSTN, ISDN a družicové telekomunikácie. Dôležitý je i pokročilý spôsob zabezpečenia informácií. Systém GSM poskytuje štyri základné spôsoby zabezpečenia informácií:

12. identifikácia používateľa prostredníctvom SIM (*Subscriber Identity Module*) karty,
13. anonymitu použitím TMSI (*Temporary Mobile Subscriber Identity*),
14. overenie totožnosti cez IMSI (*International Mobile Subscriber Identification*),
15. ochranu signalizačných a hovorových dát šifrovaním.

Tri štandardy, ktoré vznikli počas vývoja GSM sa líšia predovšetkým použitím frekvenčných pásiem a počtom kanálov:

- GSM 900 pracujúce v pásme 900 MHz, maximálne 2x124 kanálov, šírka pásma 2x25 MHz,
- GSM 1800 pracujúce v pásme 1800 MHz, maximálne 2x374 kanálov, šírka pásma 2x75 MHz,

- GSM 1900 pracujúce v pásme 1900 MHz, maximálne 2x298 kanálov, šírka pásma 2x75 MHz.

Vývoj GSM pod označením generácie 2,5 možno chápať ako modifikáciu existujúcej techniky implementáciou nových technológií a služieb. Generácia 2,5 poskytuje tieto zlepšenia:

GPRS (General Packet Radio Service)

Systém GPRS bol prvý systém, ktorý umožnil rozšíriť existujúci systém GSM a umožnil tak paketový prenos cez rádiové rozhranie s teoretickou prenosovou rýchlosťou až 171,2 kbit/s. Aplikácia technológie GPRS, založená na paketovom prenose dát, umožnila prvý mobilný prístup do siete internet. GSM systém ako aj mobilné koncové zariadenia bolo nutné doplniť o ďalšie bloky. Paketový prenos systémom GPRS je realizovaný medzi MS a BTS, ale v BSC sú pakety smerované do jednotky PCU (*Packet Controller Unit*), ktorá identifikuje a riadi paketovú prevádzku na rádiovom rozhraní. Konceptia i prevedenia PCU sú rôzne podľa výrobcu, podobne ako rozhranie medzi BSC a PCU.

EDGE (Enhanced Data for GSM Evolution)

Systém EDGE umožnil ďalšie zvyšovanie prenosových rýchlostí. Používa princíp prepojovania paketov, podobne ako GPRS, reálna prenosová rýchlosť je trojnásobne vyššia ako u GPRS. Je považovaný za technológiu generácie 2,75. Maximálna rýchlosť 384 kbit/s závisí od viacerých faktorov - pridelenej kódovacej schémy, aktuálneho stavu používateľa a siete, počtu podporovaných kanálov. Použité princípy:

- Modulačná technika 8-PSK čo je osemstavové fázové kľúčovanie.
- Vylepšený mechanizmus pre detekciu a opravu stratených a poškodených paketov.
- Kódovacie schémy MCS1-MCS9.

Flarion

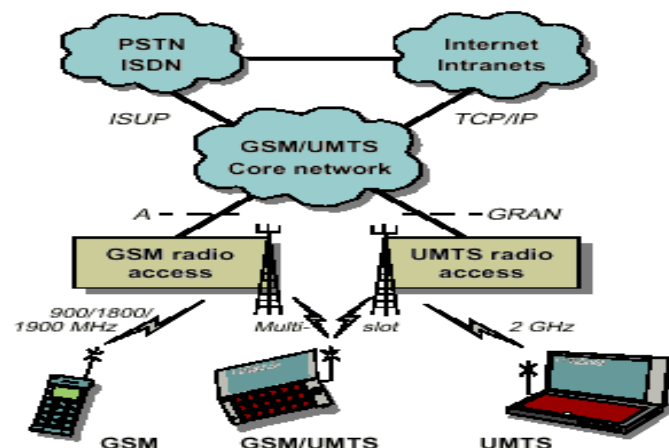
Flarion je oveľa rýchlejší oproti GPRS a EDGE. Možno ho používať aj v husto zastavaných mestách. Používa OFDM (*Orthogonal Frequency Division Multiplexing*) a *Seamless Handoff*, čo znamená neprerušované spojenie medzi BS a mobilným koncovým zariadením.

Technológie GPRS a EDGE a Flarion sa vzdialili pôvodnej sieti GSM, lebo využívajú predovšetkým jej prístupovú rádiovú časť a poskytujú služby dátových sietí.

Systém UMTS (Universal Mobile Telecommunication System)

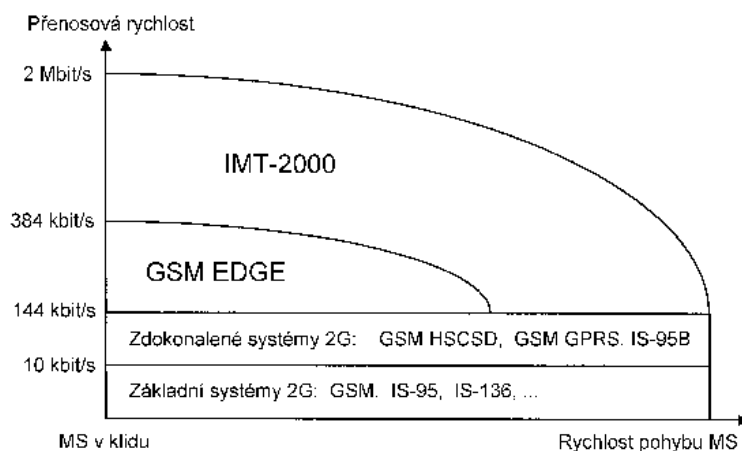
Systém UMTS bol vyvinutý ako európsky variant IMT-2000. Podľa ITU je systém IMT-2000 definovaný ako „otvorený, zastrešujúci medzinárodný štandard pre mobilné telekomunikačné systémy tretej generácie 3G s vysokou kapacitou a vysokou prenosovou rýchlosťou, zahŕňujúci pozemné i družicové rádiokomunikačné prostriedky, spolupracujúci s pozemskými pevnými sieťami“. Ide o systém, pracujúci v 2 GHz pásme a ktorý zjednocuje rôzne bezdrôtové prístupové technológie súčasnosti do jednej pružnej a výkonnej infraštruktúry, schopnej ponúknuť široký rozsah multimediálnych služieb s garantovanou

kvalitou. Rovnako kvalitný je aj prenos hovorových signálov. Spolupráca UMTS s inými systémami je na obr. 10.11.



Obr. 10.11 UMTS spolupráca s inými systémami

Prenosová rýchlosť signálu závisí na rýchlosti pohybu mobilného zariadenia, čo umožní okrem hlasových služieb i prístup k pokročilým službám, ako sú videokonferencie, dátové prenosy 384 kbit/s s plnou mobilitou v dopravných prostriedkoch do 120 km/hod a až 2 Mbit/s s obmedzenou mobilitou pri pohybe chôdze menej ako 10 km/hod. Znáznornenie závislosti prenosových rýchlostí na rýchlosti pohybu rôznych mobilných systémov je na obr. 10.12.



Obr. 10.12 Závislosť prenosovej rýchlosti od rýchlosti pohybu

Systém podporuje rýchle paketové prepojenie (*Fast Packet Switching*), ale aj prepojenie okruhov. Na rozhraní medzi mobilným koncovým zariadením a sieťou využíva pre prístup princíp CDMA (*Code Division Multiple Access*). V niektorých aplikáciách je prenos výrazne asymetrický, tj. prenosová rýchlosť signálu v jednom smere (väčšinou *downlink*) bude výrazne vyššia ako prenosová rýchlosť signálu v opačnom smere. S tým súvisí i princíp pridelenia šírky pásma podľa potreby, ktorý výrazne zvýši efektivitu využitia kmitočtového pásma. Jednotlivé pásma frekvenčného spektra sú v tabuľke 10.1.

Tab. 10.1: Frekvenčné spektrum vyhradené pre UMTS

Pásmo	Rozsah [MHz]	Šírka [MHz]
pásmo 1	1885 – 1900	15
pásmo 2	1900 - 1920	20
pásmo 3	1920 - 1980	60
pásmo 4	1980 - 2010	30
pásmo 5	2010 - 2025	15
pásmo 6	2110 - 2170	60
pásmo 7	2170 - 2200	30

LTE (*Long Term Evolution*) je súbor 3GPP štandardov označovaných ako mobilná technológia štvrtej generácie - 4G, ktorá je nástupcom sietí UMTS (3G) a GSM EDGE. Je v súčasnosti najnovšou mobilnou technológiou, umožňujúcou prenos hlasu, dát, aj HD videa. Rýchlosti prenosu sa pohybujú teoreticky až 172,8 Mbit/s (*downlink*) a odosielanie 57,6 Mbit/s (*uplink*). Technológia LTE je určená pre vysokorýchlostný internet v mobilných sieťach.

LTE používa ortogonálny frekvenčný multiplex OFDM (*Orthogonal Frequency Division Multiplexing*). Signál je pomocou OFDM rozdelený do určitého počtu signálov a každý signál prenáša určitú časť dát. Tieto signály sú maximálne blízko seba, aby bolo čo najlepšie využité dostupné frekvenčné spektrum. Tým sa veľmi efektívne dokáže prenos prispôbiť podmienkam prenosu. Čím sú tieto frekvenčné kanály širšie, tým prenesú väčšie množstvo signálov a dosiahnu tak vyššiu prenosovú rýchlosť v sieti. Siete s technológiou LTE majú oproti 3G sieti menej technologických prvkov a oveľa väčší výkon. Maximálna odozva (*Ping*) je v sieti 4. generácie cca 23 ms.

Prvé LTE siete na komerčné účely vybudovala spoločnosť Telia Sonera v roku 2009 vo Švédsku a v Nórsku. V roku 2010 bolo spustených ďalších 15 LTE sietí, za začiatok budovania týchto sietí môžeme označiť rok 2011. Najväčšou prekážkou budovania siete s LTE bola v začiatkoch pre operátorov malá dostupnosť koncových zariadení s podporou pre túto technológiu. Na druhej strane inteligentné mobilné telefóny (*Smartphone*) neboli dostatočne využité. Rok 2012 mal byť posunom vo výrobe smartfónov alebo tabletov používaných v tejto technológii.

Technológia LTE odstraňuje aj nedostatok 3G siete, kde aktualizácie aplikácií nadmerne zaťažovali batérie koncových zariadení. Efektívnym a úsporným prístupom sledovania signalizačných správ dokáže LTE optimálne redukovať nárok na batériu.

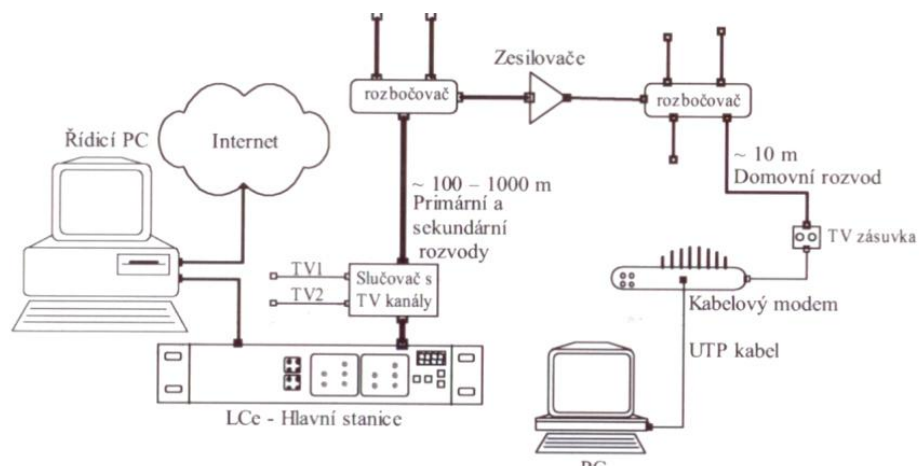
10.2.2.4 CATV (Cable TV)

CATV - sieť káblovej televízie bola v začiatkoch navrhnutá len na prenos a distribúciu TV a audio programu k domácim používateľom. Neskôr boli vyvinuté metódy, ktoré umožňujú aj interaktívnu službu prenosu hlasu, dát a služieb internetu. Prenos dát sa riadi štandardom **DOCSIS** (*Data Over Cable Service Interface Specification*) alebo jeho európskym ekvivalentom **euroDOCSIS**. Ide o pevné nie komutované pripojenie. Zapnutím PC je realizované trvalé pripojenie k sieti.

Prenosové médium je zdieľané všetkými aktívnymi používateľmi pomocou časového multiplexu - TDM. Používa sa viac typov modulácií, najpoužívanejšia je QAM - kvadrátová amplitúdová modulácia a QPSK - štvorstavové kľúčovanie s posunom fázy. QPSK je pomalšia než QAM, ale je viac odolná proti vonkajším rušeniam. Pre prenos dát sa obvykle vyhradzuje jeden 6 MHz *downstream* kanál z pásma 50 až 750 MHz a jeden *upstream* kanál z rozsahu 5-42 MHz. Tieto hodnoty sú pri jednotlivých štandardoch a riešeniach odlišné. DOCSIS, verzia 2.0, umožňuje využitím 6 MHz kanála *downstream* pri 256-stavovej QAM zabezpečiť rýchlosť až 42 Mbit/s. V smere *upstream* je možné používať rôzne šírky pásma (až 2 MHz), čo pri 16-stavovej QAM znamená rýchlosť až 10 Mbit/s. Prenosová rýchlosť, ktorá je k dispozícii koncovým používateľom, je však podstatne nižšia než vyššie uvedené maximálne hodnoty.

Pôvodne sa v sieťach CATV používali koaxiálne káble, neskôr sa začali používať optické vlákna. Úprava infraštruktúry CATV má zmysel hlavne v oblasti veľkých miest, kde je veľký počet zákazníkov. Typické riešenia v súčasnosti kombinujú použitie drahších optických a lacnejších koaxiálnych káblov. Na väčšie vzdialenosti a v chrbticových častiach rozvodov bývajú použité optické káble a pre rozvody do jednotlivých domácností je používaný takmer výhradne koaxiálny kábel. Sieť káblových rozvodov má stromovú štruktúru.

Riešenie je veľmi jednoduché. Stačí inštalácia ľubovoľnej Ethernet karty, ktorá sa pripojí ku káblovému modemu. Pokiaľ je počítač vybavený USB portom, odpadá aj inštalácia sieťovej karty. Káblový modem je pomocou rozbočovača zapojený na káblovú TV zásuvku a následne prepojený so sieťovou kartou počítača. Pripojenie je zdieľané spolu s TV signálom, ich oddelenie je cez rozbočovač. Princíp pripojenia je na obr. 10.12.



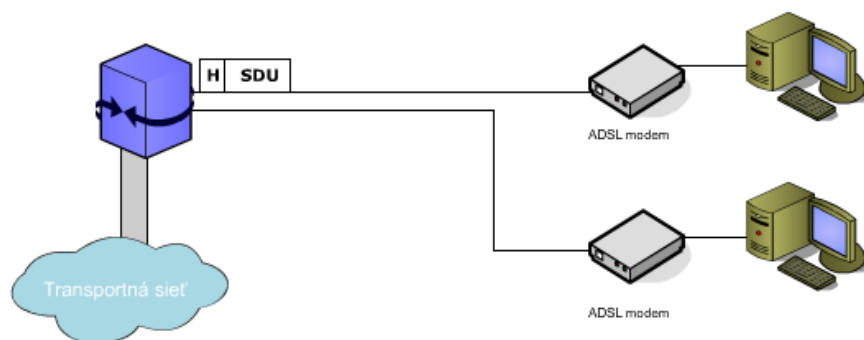
Obr. 10.12 Pripojenie PC ku CATV

10.2.2.5 Optické prístupové siete

Optické prístupové siete sú najvhodnejším prenosovým médium pre širokopásmové služby. Optická prístupová sieť využíva rôzne typy optických káblov, ktorými sú koncoví používatelia pripájaní k elektronickej komunikačnej sieti. V prístupových sieťach sa využíva profil 1, 2, 4, 8, 12, 24, 48, 72 optických jednovidových vlákien s priemerom 9/125 μ m. Topológia optickej siete môže byť vytvorená ako stromová, hviezdicová alebo kruhová.

V prístupových sieťach sa používajú pasívne optické siete PON (*Passive Optical Networks*). Sú vytvárané z pasívnych optických prvkov a optických káblov. Okrem pasívnych optických sietí sú ešte aktívne optické siete AON (*Active Optical Network*), ktoré prepojujú optické sieťové jednotky ONU (*Optical Network Unit*) prostredníctvom aktívnych sieťových prvkov, ako sú napríklad elektricky napájané opakovače, rozbočovače, multiplexory, demultiplexory, ktoré rozdeľujú a v opačnom smere združujú signály medzi jednotlivými časťami optickej siete. Výhodou optických sietí AON voči PON je zaistenie podstatne väčších dosahov, nevýhodou u AON sú vyššie náklady na ich budovanie. Budovanie optických prístupových sietí je najviac známe pod označením **FTTx** (*Fibre to the x*). Sú to pasívne optické siete dostupné až ku koncovému používateľovi s dostupnosťou transportných optických sietí. Označenie x znamená niekoľko typov riešení, príklady niektorých sú uvedené ďalej.

FTTEx (*Fibre to the Exchange*) je založené na zakončení optického vlákna v miestnej telefónnej ústredni, kde je umiestnený účastnícky multiplexor DSLAM a cez hlavný rozvod ústredne sú účastníci pripojení prostredníctvom metalického vedenia a prípojok ADSL, SHDSL, prípadne VDSL. Príklad zapojenia je na obr. 10.13.



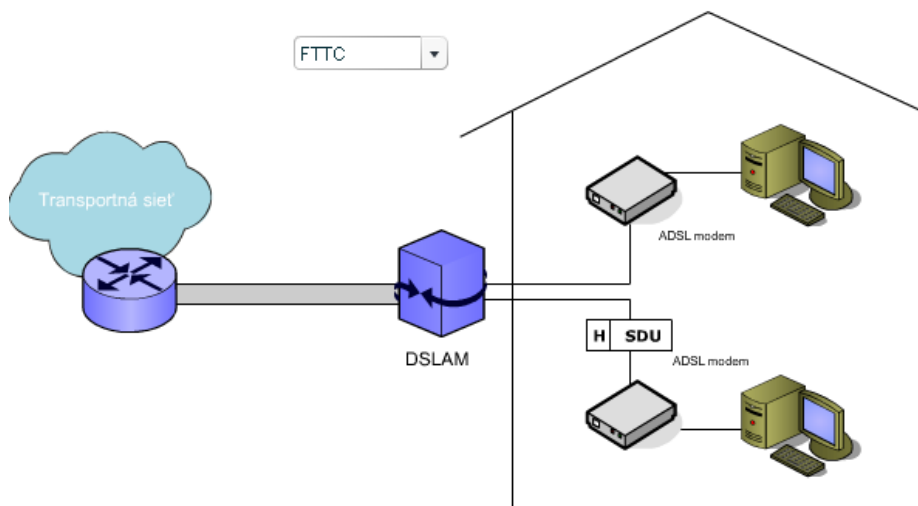
Obr. 10.13 FTTEx

Riešenie FTTEx je využíva existujúce metalické vedení, nie je to však optická prístupová sieť v pravom slova zmysle. Prenosová rýchlosť je tu závislá od vzdialenosti od ústredne. Vyššie prenosové rýchlosti v prístupových sieťach zaistí privedenie optického vlákna čo najbližšie ku koncovému používateľovi. Označujú sa ako hybridné riešenia.

Hybridné riešenia optických prístupových sietí sú:

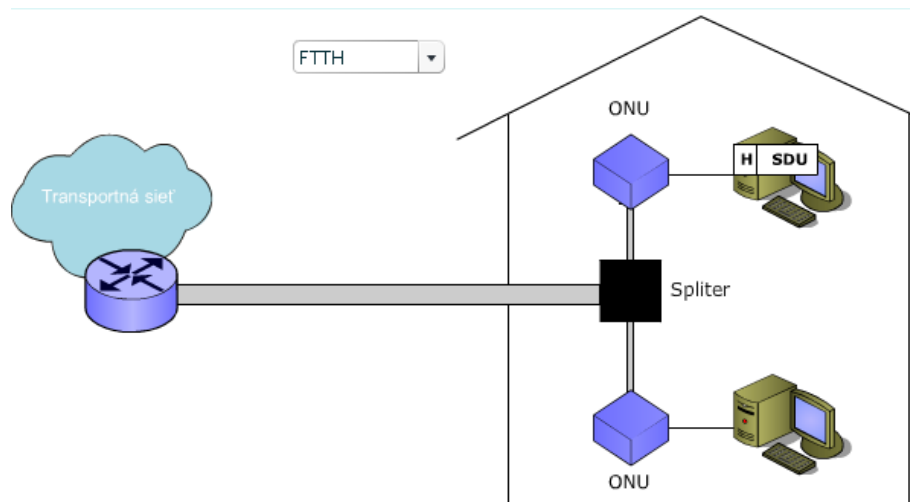
- **FTTCab** (*Fibre to the Cabinet*), kde je optické vlákno privedené do rozvádzača v teréne,
- **FTTC** (*Fibre to the Curb*), kde je optické vlákno privedené k okraji chodníka do blízkosti skupiny domov,
- **FTTB** (*Fibre to the Building*), kde je optické vlákno privedené až do budovy, a ďalej sú použité metalické vedenia, alebo bezdrôtová komunikácia.

Hybridné riešenie je vhodným kompromisom medzi optickým prístupom a technológiami ADSL a VDSL, prípadne aj koaxiálne rozvody CATV. Znázornenie je na obr. 10.14.



Obr. 10.14 FTTCab

FTTH (Fibre To the Home), optický kábel do domácnosti, znázornený na obr. 10.15.



Obr. 10.15. FTTH

Riešenie je vytvorené medzi dvomi bodmi (*point-to-point - PTP, P2P*), s individuálnymi optickými vláknami z centrálnej jednotky prevádzkovateľa, kde na vetvenie je použitý aktívny odbočovač, alebo pri mnohobodovej architektúre (*point-to-multipoint - PTMP, P2MP*) s použitím pasívneho odbočovača. Obidve riešenia môžu využívať buď dve vlákna, každé pre jeden smer prenosu, alebo jedno vlákno, s vyhradenými vlnovými dĺžkami pre každý smer prenosu.

FTTO (Fibre to the Office) je celo optické riešenie, kde je optické vlákno, podobne ako u FTTH privedené až do sieťovej zásuvky. Pripojenie je určené pre používateľov s vysokými nárokmi na prenosovú kapacitu.

10.2.2.6 Bezdrôtové prístupové siete

Wi-Fi (*Wireless Fidelity*), je skupina špecifikácie IEEE 802.11 navrhnutá pre bezdrôtové zariadenia a lokálne siete WLAN (*Wireless Local Area Network*). Principiálne môžu byť realizované dvomi spôsobmi:

WLAN, kde komunikuje drôtová LAN s pripojenými koncovými zariadeniami cez prístupový bod AP (*Access Point*), ktorý ma funkciu smerovača - *routera* alebo s rozširujúcim bodom EP (*Extension Point*). Takéto riešenie sa označuje ako PoE (*Power over Ethernet*) alebo *Wireless Ethernet*.

Ad-hoc LAN nemá centrálny bod, komunikácia je typu bod-bod (*Point-to-Point*).



Obr. 10.16 WiFi hotspot s prístupovým bodom v strede a rôznymi koncovými zariadeniami

Základné charakteristiky:

- Používaná metóda prístupu na spoločné médium je CSMA/CA.
- Podporuje rozličné stupne kryptovania, čím je zaručená bezpečnosť komunikácie. Šifrovacia metóda algoritmus WEP (*Wired Equivalent Privacy*).
- Dosah maximálne 1500 m vo voľnom priestore, 1000 metrov v budovách pri použití externých antén.
- Parametre v nelicencovaných rádiových pásmach 2,4 a 5 GHz s prenosovými rýchlosťami podľa tabuľky 10.2.

Tabuľka 10.2. Parametre špecifikácií WiFi

Špecifikácia	Rýchlosť	Frekvencia	Pásmo
802.11b	11 Mbit/s	2.4 GHz	b
802.11a	54 Mbit/s	5 GHz	a
802.11g	54 Mbit/s	2.4 GHz	b, g
802.11n	100 Mbit/s	2.4 GHz	b, g, n

Rýchlosť závisí od

- typu a kvality kódovania

- kvality spojenia
- rušenia - ak je veľké rušenie musia sa často opravovať pakety a tým sa znižuje rýchlosť.

Využíva nelicencované rádiové pásmo a nepotrebuje používateľské licencie miestnych úradov.

Dosah max 1500 m vo voľnom priestore, 1000 metrov v budovách pri použití externých antén.

Podporuje *roaming* - prechod medzi *hotspotmi*, na koncového používateľa.

Vo Windows XP existuje funkcia nulová konfigurácia (*zero configuration*), ktorá umožňuje používateľovi vidieť všetky dostupné siete a pripojiť sa ku ktorejkoľvek z nich.

Nedostatky Wi-Fi

- Nelicencované pásmo 2.4 GHz, je využívané aj inými zariadeniami, napríklad Bluetooth, mikrovlnné rúry, bezdrôtové telefóny, čo môže spôsobiť zníženie výkonu, ktorý je pod limitom 100 mW.
- Kryptovací štandard WEP je prelomiteľný, v mnohých prípadoch je potrebné dodatočné kryptovanie. Anonymný útok, sa nedá vyhľadať za majiteľom prístupového bodu.

Certifikované produkty môžu používať oficiálne logo Wi-Fi, ktoré označuje produkty spolupracujúce s akýmkoľvek iným certifikovaným produktom.



WiMax (*Worldwide Interoperability for Microwave Access*) - celosvetová interoperabilita pre mikrovlnný prístup, je bezdrôtová komunikačná technológia, štandard IEEE 802.16, verzie 802.16 a, b, c, d, e. Niekedy je označovaná aj ako WirelessMAN, pretože je určená ako prístupová technológia poslednej míle a alternatíva ku káblovým prístupovým technológiám. Architektúra je podobná bunkovým štruktúram sietí. Prístupový bod je označovaný ako bazová stanica BS. Jedna bazová stanica môže pokrývať maximálne šesť sektorov. WiMax možno charakterizovať z pohľadu troch parametrov: prenosová rýchlosť, dosah a viditeľnosť na bazovú stanicu, ktoré musia byť v rovnováhe.

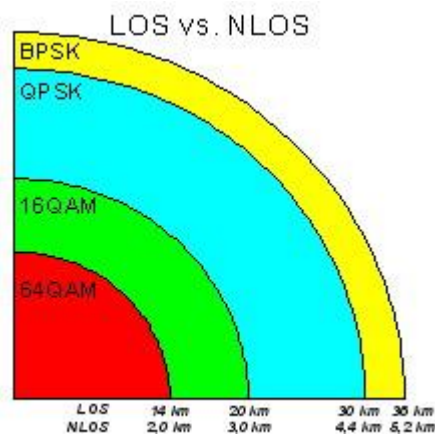
Prenosová rýchlosť je závislá od šírky frekvenčného pásma a od modulácie. WiMAX používa adaptívne modulácie, ktoré umožňujú meniť typ modulácie podľa kvality spojenia. Vie pracovať so 64 QAM, 16 QAM, QPSK a BPSK. Prehľad jednotlivých modulácií je uvedený v tabuľke 10.3.

Tabuľka 10.3 Modulácie siete WiMax

modulácia	počet stavov	počet bitov	rýchlosť Mbit/s kódované/nekód.

64 QAM	64	6	70/50
16 QAM	16	4	46/34
QPSK	4	2	22/17
BPSK	2	1	11/8

Použitie modulácie závisí od ďalších dvoch faktorov priamej alebo nepriamej viditeľnosti BS a od vzdialenosti od básovej stanice BS. Ak je viditeľnosť slabá a vzdialenosť od DS vysoká zhoršuje sa pomer signál-šum (SNR) a vtedy bude použitá s menším počtom stavov, aspoň tri sektorové antény, takže prenosové kapacity sa týmto spôsobom zvyšujú. **Viditeľnosť básovej stanice** môže byť priama LOS (*Line Of Sight*) alebo nepriama NLOS (*Non Line Of Sight*). Ak však nie je priamy výhľad na BS znižuje sa dosah signálu. Riešením je budovanie básových staníc hustejšie a používať viac sektorových antén. Porovnanie LOS a NLOS prístupu je na obr. 10.17. Nižšie verzie normy vyžadujú priamu viditeľnosť, verzie c a vyššie podmienku priamej viditeľnosti nepožadujú.



Obr. 10.17. Porovnanie modulácií, viditeľnosti BS a dosahu technológie WiMax

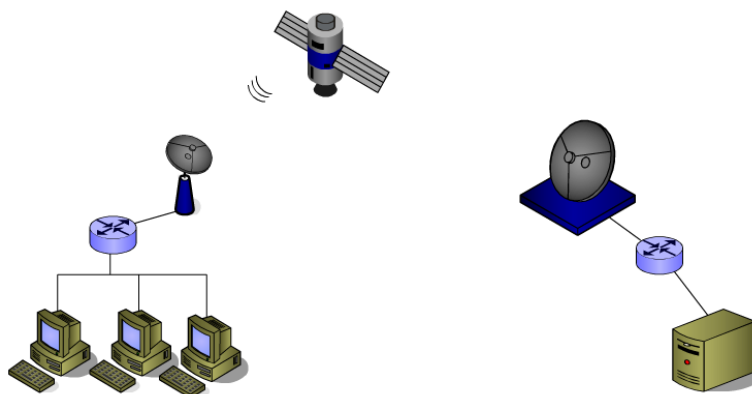
Základné charakteristiky:

- V niektorých štátoch sa WiMax využíva v bezlicenčnom pásme 2,4 GHz, u nás WiMax využíva frekvenciu **3,5 GHz** a je **potrebná licencia**.
- Frekvenčné rozpätie od 2 do 11 GHz.
- Využíva OFDM. (*Orthogonal Frequency Division Multiplexing*). OFDM rozdeľuje širokopásmový signál do 256 úzkopásmových kanálov, z ktorých každý prenáša asi 50 kbit/s.
- Frekvenčné pásmo môže byť rozdelené rôznymi spôsobmi. Rozstup frekvenčných pásiem závisí od nosnej frekvencie – pre WiMax v slovenských podmienkach je to 100 MHz, pričom šírka jedného kanála je 3,5 MHz.
- Prenos sa realizuje v niekoľkých frekvenčných pásmach, čo minimalizuje možnosť rušenia s inými rádiovými aplikáciami. Kanály aj keď sú pomerne blízko vo frekvenčnom pásme, neprekrývajú sa a tak nehrozí ich vzájomné rušenie. Zanedbateľný je aj útlm signálu vo vonkajšom prostredí.
- Dosah a maximálna rýchlosť prenosu závislosti od voľby frekvenčného spektra a od použitej verzie štandardu.

- Prenosová rýchlosť básovej stanice sa pohybuje na úrovni 76,194 Mb/s. Najvyššia prenosová rýchlosť kanála pri frekvencii 3,5 GHz je 12,699 Mbit/s. Jedna básová stanica môže pokrývať maximálne šesť sektorov.
- Frekvenčné pásmo môže byť rozdelené rôznymi spôsobmi. V závislosti od šírky kanála môže byť k jednej básovej stanici pripojených 750 používateľov, pričom každý z nich bude mať pridelené pásmo v šírke 0,5 Mb/s. Prevádzkovateľ sa však môže rozhodnúť zväčšiť šírku kanála, a tak môže poskytovať 375 používateľom pásmo v šírke 1 Mb/s. V extrémnych situáciách sa tiež môže rozhodnúť celé pásmo rozdeliť niekoľkým firmám, ktoré sa podelia o rýchlosť 75 Mb/s.
- Podporuje kvalitu služby QoS (Quality of Services).
- Fyzická vrstva používa princíp FDD (*Frequency Division Duplex*), čo znamená, že na prenos smerom od používateľa je použitá jedna frekvencia a iná frekvencia sa používa na prenos v opačnom smere.
- Na druhej vrstve OSI modelu používa protokol MAC (*Media Access Control*). V smere od používateľa využíva protokol TDMA (*Time-Division Multiple Access*). V opačnom smere je prenos prostredníctvom TDM (*Time-Division Multiplex*) s centralizovaným plánovačom, ktorého úlohou je efektívne a prednostné pridelenie šírky pásma.
- Autentifikácia a autorizácia koncového zariadenia je na základe digitálneho certifikátu X.509 a certifikátu výrobcu, ktorý sa zariadeniu prideli pri výrobe.
- Na ochranu dát sa využíva zlepšený šifrovací protokol PKM (*Privacy Key Management*). Komunikácia v bezpečnom kanáli šifruje prenášané dáta podľa štandardu DES (*Data Encryption Standard*).

Najväčšou výhodou technológie WiMax oproti káblovým technológiám je práve adaptívna modulácia a možnosť rozdelenia pásma na menšie pásma, prípadne rozdelenie vyťaženého sektora na dva menšie sektory. Poskytovateľ môže rozhodnúť na čo použije frekvenčné pásmo a ako ho rozdelí, aby čo najefektívnejšie využil jeho celú šírku. Rovnako významným prínosom je zabezpečenie QoS.

VSAT (*Very Small Aperture Terminal*) je pozemská stanica skladajúca sa z parabolickej antény s vonkajšou jednotkou a vnútornej jednotky (satelitného modemu), ktoré sú navzájom prepojené systémovými káblami. Rozmery parabolickej antény závisia od jej účelu a prenosových rýchlostí. Priemery sú spravidla od 0,55 m až do 3,7m. Terminál je vybavený dátovým rozhraním (RS232, X.21, V.35, a pod.) schopný prenášať všetky bežné protokoly podľa aplikácie používateľa. VSAT sieť ponúka široké spektrum služieb, prístup k internetu, telefón a fax, videokonferencie, a iné. Znázornenie satelitnej komunikácie je na obr. 10.110.



Obr. 10. 18 Znáozornenie satelitnej komunikácie

Topologicky môže spájať dve miesta (*point to point*), centrálnu stanicu so vzdialenými miestami (*half meshed network*), alebo každé vzdialené miesto so všetkými ostatnými uzlami siete (*full meshed network*). V každom prípade je duplexný prenos. Pri špeciálnych aplikáciách napríklad distribúcia dát je prenos iba jednosmerný. Technologicky môže satelitná telekomunikácia prebiehať viacerými spôsobmi, medzi základné patrí:

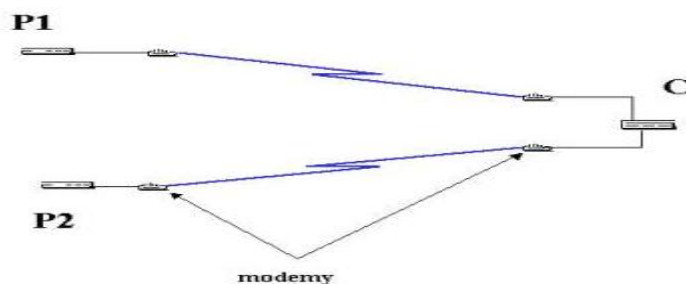
- FDMA (*Frequency Division Multiple Access*) je spojenie, ktoré sa realizuje pridelením trvalého komunikačného kanála na družici bez časového obmedzenia.
- TDMA (*Time Division Multiple Access*) je spojenie VSAT sieťami, ktoré sa uskutočňuje na spoločných kanáloch, s pridelovaním časových slotov pre jednotlivých používateľov. Tento spôsob je výhodnejší k prenosu menších objemov dát, napr. na transakčné operácie.
- Kombinácia FDMA - TDMA, ktorou sa dosahuje lepšie využitie pridelovaných kanálov v rámci VSAT siete, uskutočňuje sa na viacerých spoločných kanáloch, s pridelovaním časových slotov pre jednotlivých používateľov. Tento spôsob je vhodný napríklad na dynamické pridelovanie kanálov - dátových alebo hlasových služieb.

10.2.2.7 Permanentné pripojenia ku komunikačnej sieti

Prenajaté okruhy (*Leased Lines*) sú spojenia typu bod-bod (*Point-to-Point*). Na oboch koncoch je modem a zariadenia pre prístup. Tým môže byť smerovač, koncentrátor RAC (*Remote Access Contretator*) alebo sériový port počítače. Z koncentrátora sa používa multikanálové pripojenie E1, ktoré odpovedá PCM multiplexom.

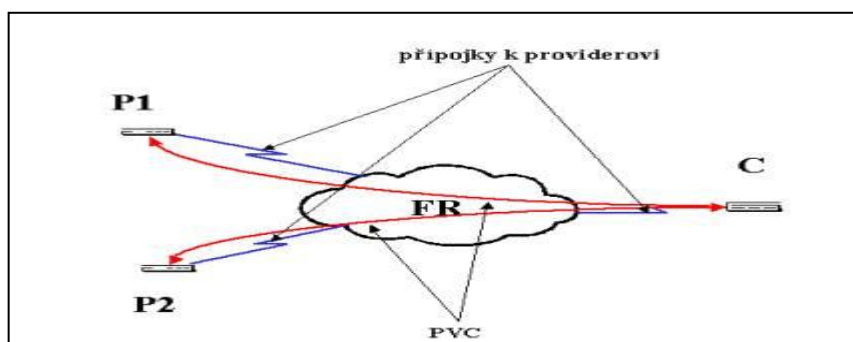
Rýchlosť spojenia je závislá od vzdialenosti a použitého prenosového média. Môže byť viac ako 2 Mbit/s. Pre spojenie možno použiť rôzne WAN protokoly. Často je používaný protokol PPP (*Point-to-Point*).

Predstava tohto spojenia je na obr. 10.19.



Obr. 10.19 Pevné pripojenie ku komunikačnej sieti

Frame Relay (FM) je služba poskytovaná poskytovateľmi siete Frame Relay. Frame Relay je technológia, prepojovania paketov na linkovej vrstve. Efektivita protokolu je lepšia ako protokol PPP (*Point-to Point*). Na obrázku 10.20 je znázornené pripojenie dvoch LAN - P1 a P2 ku koncentrátoru C. Každý z uzlov je pripojený k prístupovému bodu poskytovateľa a medzi vybranými koncami je vytvorený permanentný virtuálny kanál PVC (*Permanent Virtual Channel*). PVC môžu byť vytvárané ľubovoľne, každý s každým. LAN - P1 a P2 spolu komunikujú prostredníctvom koncentrátora C.



Obr. 10.20 Pripojenie cez Frame Relay

Digitálna elektrická prípojka (DPL-Digital Power Line / PLC- Power Line Communication) je technológiou o ktorej sa dlhodobo diskutuje a ktorá v Európe nie je veľmi používaná. Na prenos informácie využíva elektrické vedenie. Výhodou tejto technológie je to, že každá domácnosť je pripojená k rozvodovej sieti elektrickej energie. Na prenos dát môžu byť využívané podľa štandardizačnej organizácie CENELEN iba frekvencie z rozsahu 3 až 148,5 kHz pre úzkopásmové PCL a 2 až 30 MHz pre širokopásmové PCL. Frekvenčné pásma patria medzi bezlicencované pásma. Úzko pásmové PLC modemy pracujú v pásmach B a C normy CENELEC, čo sú frekvencie od 95 do 140 kHz, prenosové rýchlosti sú niekoľko kbit/s. Využívajú sa hlavne v budovách a na správu zariadení v domácnostiach. Širokopásmové PLC modemy pracujú na frekvenciách od 2 do 30 MHz. Prenosové rýchlosti závisia od typu prostredia. V otvorených priestoroch (vysoké a veľmi vysoké napätie) dosahujú prenosové rýchlosti 2 Mbit/s, v uzavretých priestoroch (*in home systems*) je to až 12 Mbit/s.

Vysokonapäťové PLC technológie sú realizované pre spojenie typu point to point na vzdialenosť niekoľko stoviek metrov. Využíva sa na prepojenie antén a základňových staníc a na vytváranie sietí medzi budovami.

Nízkonapäťové PLC technológie sa využívajú ako telekomunikačné prístupové siete. Môžu sa využívať na vysokorýchlostné prenosy dát, prenos audio a video signálov a podobne.

Použitím najnovších modulačných techník a systémov detekcie chýb umožňujú technológie PLC dosiahnuť prenosové rýchlosti až 100 – 200 Mbit/s.

Fast Ethernet alebo Ethernet in the First Mile (EFM) je prístupová technológia, ktorá je rozšírením štandardov Ethernet. Štandardy umožňujú symetrické rýchlosti 100 Mbit/s až 1 Gbit/s po existujúcich telefónnych linkách, alebo po optických vláknach. V skutočnosti je však maximálna využiteľná rýchlosť menšia, pretože časť prenosovej kapacity sa spotrebuje na riadenie.

Štandardy definujú prístupové siete využívajúce optické vlákna, aj klasické medené páry. V oboch prípadoch sa používa protokol CSMA/CD s hviezdnicovou topológiou. Protokol sa všeobecne označuje ako 100BASE-X, kde X je všeobecný symbol pre prenosové médium. Napríklad TX je krútená dvojlinka, FX je optické vlákno. Číslo 100 v názve protokolu označuje prenosovú rýchlosť 100 Mbit/s. Označení BASE znamená, že sa jedná o Ethernet. Príklad jednej špecifikácie:

100BASE-FX je verzia *Fast Ethernetu* cez optické káble. Používa vlnovú dĺžku 1300 nm.. Pre prenos sa používajú 2 vlákna, jedno pre príjem a druhé pre vysielanie. Maximálna dĺžka je 400 metrov pre *half-duplex* pripojenie a 2 km pre *full-duplex* po viac vidovom optickom vlákne.

Výhodou technológie Ethernet in the First Mile je oproti iným používaným širokopásmovým technológiám jednoduché zvyšovanie rýchlosti podľa pribúdajúcich náročnejších aplikácií alebo krátkodobých nárokov na vyššiu rýchlosť (*Bandwidth on Demand*).

10.3 Edge (okrajové)siete

Dôvodom pre špecifikáciu **edge sietí**, respektíve *edge* uzlov je prispôbenie požiadaviek prenosu z prístupových sietí na prenos po transportných sieťach. Riešenia edge sietí/uzlov sú spojené s vývojom elektronických komunikačných sietí, ktorý je v súčasnosti spojený hlavne s riešením sietí novej generácie, označovaných NGN (*Next Generation Networks*). Problematikou NGN sa zaoberajú rozhodujúci poskytovatelia telekomunikačných služieb, výrobcovia a dodávatelia technológií. Vychádzajú z predpokladu, že používatelia chcú používať multimediálne služby s jedným spoločným koncovým zariadením – telefónom a počítačom v jednom, kdekoľvek a kedykoľvek. Navyše zákazníci nechcú byť obmedzovaní ani výberom jedného operátora a okrem toho chcú, aby boli služby lacnejšie.

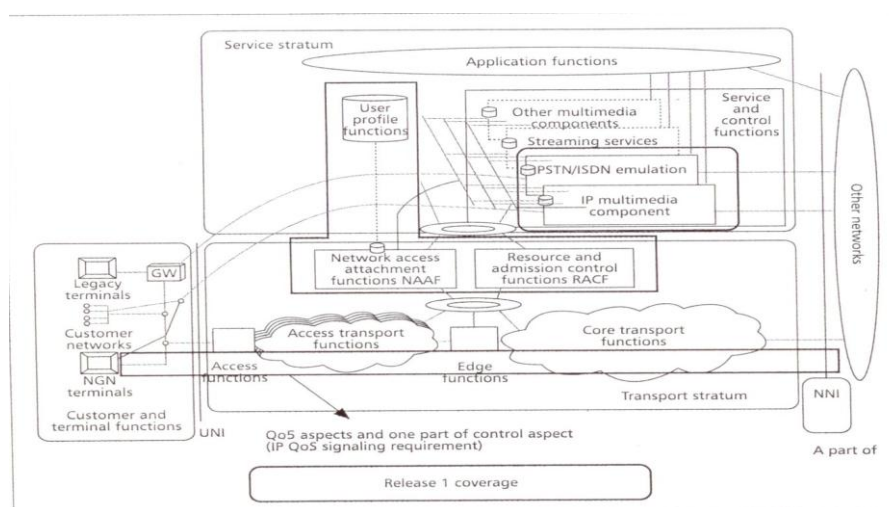
Základnou myšlienkou NGN je vytvorenie jedinej siete, ktorá prenáša všetky typy informácie a služieb. Je výsledkom konverencie telefónnych a dátových sietí a zlučuje ich vlastnosti do jednej spoločnej siete. Hlavnými znakmi NGN je paketový prenos informácie a poskytovanie všetkých typov služieb (telefónne, textové, obrazové, audio, video a dáta) elektronických komunikačných sietí.

Formálna definícia NGN vydaná organizáciou ITU (ITU-T Y.2001) je:

"Next Generation Network (NGN): a packet-based network able to provide telecommunication services and able to make use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies. It offers unrestricted access by users to different service providers. It supports generalized mobility which will allow consistent and ubiquitous provision of services to users."

Tato definícia vyjadruje, že NGN je vysokorýchlostná paketová sieť, ktorá zaručuje kvalitu poskytovaných telekomunikačných služieb (QoS). Služby sú nezávislé na prenosovej technológii a môžu byť ponúkané rôznymi poskytovateľmi. To znamená, že ak chce poskytovateľ kedykoľvek implementovať novú službu, môže tak urobiť priamo v servisnej vrstve bez ohľadu na prenosovú vrstvu, teda **služby sú nezávislé od prenosových častí**.

Architektúra NGN je založená na oddelených vrstvách: prístupovej a transportnej vrstve – vrstva prenosu, riadiacej vrstve a vrstve sieťových služieb (vrstva manažmentu). Edge siete v NGN nepredstavujú samostatné rozľahlé siete. Sú tvorené uzlami, ktoré prispôbujú prevádzku v prístupových sieťach prevádzke po transportných sieťach. Preto je možné edge siete považovať za časť celkovej prenosovej siete, aj keď ich realizácia je v jednom mieste celkovej siete. Znáznomenie edge funkcií je v obr. 10.21.



Obr. 10.21 Architektúra NGN podľa projektu TISPAN riešeného v ETSI

Aj keď NGN koncepcia nie je zatiaľ v plnej miere implementovaná, vyvíjajú sa technológie, ktoré patria do koncepcie NGN. Technológie, ktoré riešia aj problematiku edge sietí/uzlov zabezpečujú dve základné funkcie:

1. prispôsobenie multimediálnych prenosov na paketový prenos,
2. signalizáciu.

K nim sa pridružuje ďalšia dôležitá funkcia edge sietí a tou je zabezpečenie kvality služby.

Protokoly spojené s EDGE sieťami sú:

SIP (*Session Internet Protocol*) je primárne určený pre vytvorenie udržanie a rušenie telefonických a videokonferenčných prenosov po IP sieťach, ale môžu ho využívať aj iné aplikácie. Je využívaný iba v signalizačnej časti komunikácie. Signalizačné informácie sú prenášané v transportných protokoloch UDP alebo TCP.

H323 je štandard nazvaný *Packet-based multimedia communications systems* je určený pre multimediálne prenosy cez IP siete. Prvé verzie boli hlavne pre videokonferencie, ďalšie verzie sú pre VoIP. Ide o skupinu protokolov, ktoré špecifikujú multimediálnu komunikáciu cez rôzne typy sietí.

MPLS (*Multiprotocol Label Switching*), ktorý je ďalšou vývojovou etapou riadenia prevádzky v elektronických komunikačných sieťach. Riadenie obsahuje prvky QoS (*Quality of Service*) a CoS (*Class of Service*). Motivácia k jeho vytvoreniu bola hlavne v tom, aby doplnil nedostatky IP protokolu, ktorý nezabezpečoval QoS. Pracuje na 2. a 3. Vrstve OSI modelu.

Príkladom ponúkaných služieb, ktoré požadujú edge funkcie sú Voice over IP a TriplePlay.

10.4 Transportné siete

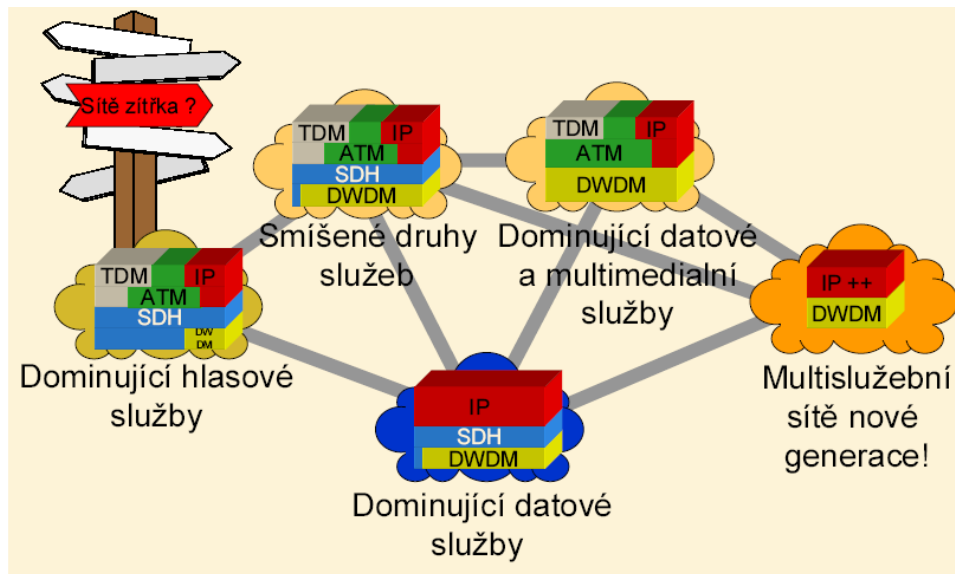
Transportné siete tvoria najvyššiu architektonickú úroveň elektronických komunikačných sietí. Zabezpečujú prenos informácie na veľké vzdialenosti. Ich charakteristické funkcie sú:

- Prenos signálov medzi jednotlivými uzlami siete.
- Prenos veľkého objemu dát prenosovými rýchlosťami rádovo stovky Mbit/s až stovky Gbit/s.
- Zabezpečenie spoľahlivosti prenosu.

Spoľahlivosť prenosu sa v transportných sieťach zabezpečuje:

- dimenzovaním prenosových kapacít podľa očakávaného zaťaženia,
- zabezpečením siete centrálnym riadiacim systémom označovaným TMN (*Telecommunications Management Network*).

Technológie transportných sietí prešli v posledných desaťročiach veľkým vývojom, ktorý je znázornený na obrázku 10.22.



Obr. 10.22 Technologické transportních sítí

Dominantní technologie v současnosti sú:

- TDM (*Time Division Multiplex*)
- SDH (*Synchronous Transfer Mode*)
- WDM (*Wavelength Division Multiplex*)

Ich princípy stručne vysvetlíme.

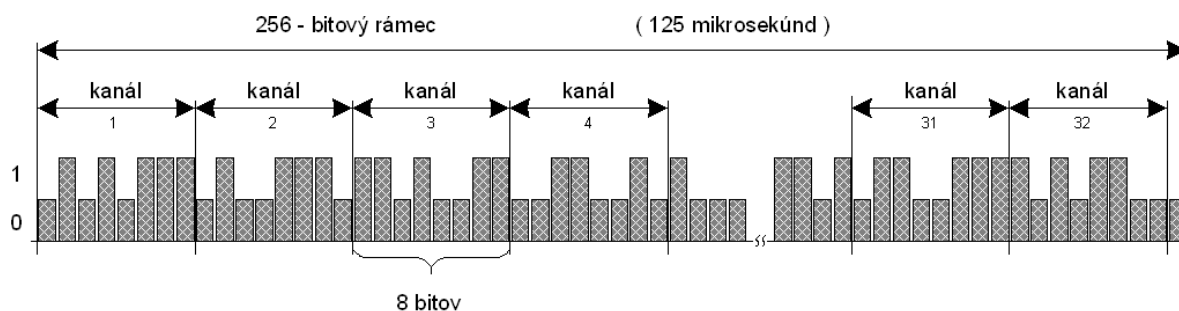
10.4.1 Časový multiplex – TDM

Princíp časového multiplexu bol vysvetlený v kapitole 4. Z hľadiska spôsobu komunikácie môžeme časový multiplex rozdeliť na dve kategórie:

- Synchronný prenosový mód STM (*Synchronous Transfer Mode*).
- Asynchronný prenosový mód ATM (*Asynchronous Transfer Mode*).

Výhodou asynchronného prenosového módu je možnosť štatistického multiplexovania STDM (*Statistic Time Division Multiplex*), kedy sú prenosové prostriedky siete pridelované iba v prípade aktívneho využitia prenosového kanála, čo spôsobuje jeho efektívnejšie využitie. Štatistický multiplex umožňuje realizovať prenosy s premenlivou prenosovou rýchlosťou, a tak pružne reagovať na požiadavky používateľa. ATM je všeobecný princíp prenosu informácie, ale táto skratka sa používa tiež v konkrétnej technológii.

Typickým predstaviteľom STM je PCM 1. rádu/stupňa, kde pravidelne, vždy v rovnakom časovom intervale 8 bitov tvorí vzorku telefónneho alebo dátového signálu rôznych kanálov, ktoré sa prenášajú v jednom rámci s prenosovou rýchlosťou 64 kbit/s. Rámec PCM 1. rádu je na obrázku 10.23.



Obr. 10.23 Rámec PCM 1. rádu

Charakteristika rámca európskej normy je nasledovná:

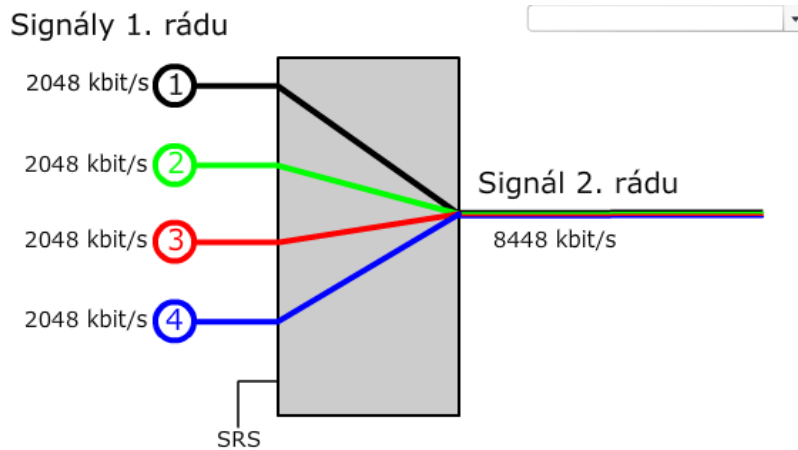
- Rámec má celkom $8 \times 32 = 256$ bitov.
- Prenáša 32 nezávislých kanálov.
- Frekvencia vzorkovania 2×4 kHz, t.j. 8 kHz.
- Prenosová rýchlosť pre jeden kanál: $8 \times 8000 = 64$ kbit/s.
- Pre 256 bitov v rámci je prenosová rýchlosť $256 \times 8000 = 2,048$ Mbit/s.
- 0. kanál tvorí rámcovú synchronizáciu (synchroskupina 0011011).
- 16. kanál prenáša signalizáciu pre všetky kanály.

Americký a japonský štandard je odlišný.

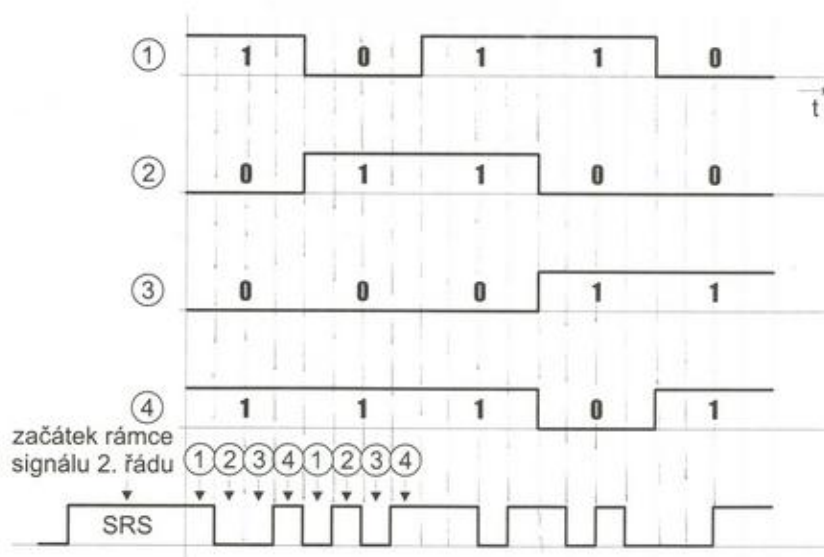
Na združovanie väčšieho počtu kanálov, než dokáže multiplexovať zariadenie PCM 1. rádu, prípadne na prenos dát vyšších prenosových rýchlostí, bola vytvorená celá sústava zariadení a im odpovedajúcich signálov vyšších rádov. Podľa metódy združovania rozoznávame digitálne systémy PDH a SDH.

Plesiochrónna digitálna hierarchia PDH (*Plesionus Digital Hierarchy*) združuje signály PCM prvého stupňa, do vyšších hierarchických stupňov. Jednotlivé združované signály sú bit po bite vkladané do rámca signálu vyššieho rádu bez toho, aby bol akokoľvek definovaný vzťah medzi rámcom signálu nižšieho rádu a rámcem signálu vyššieho stupňa.

Princíp multiplexu je zjednodušene znázornený na obr. 10.24. Združovacie zariadenie multiplexuje štyri signály nižšieho stupňa (platí pre európsky štandard) a vkladá pomocné informácie, najmä skupinu rámcovej synchronizácie a vyrovnávanie prenosových rýchlostí. Výsledkom multiplexovania je signál druhého stupňa. Časové priebehy multiplexovaných signálov sú zjednodušene na obr. 10.254.



Obr. 10.24 Princíp multiplexu v PDH



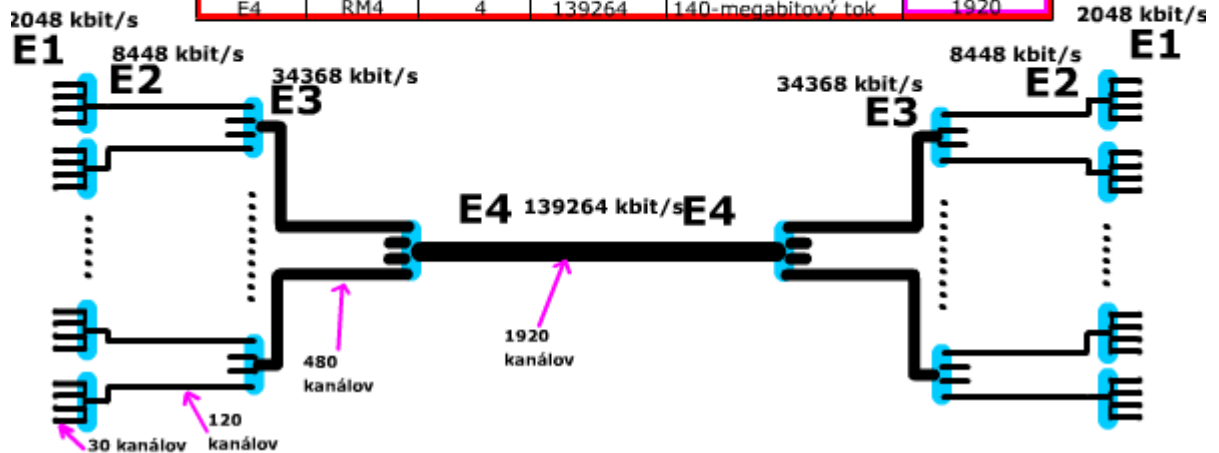
Obr. 10.25 Časové priebehy pri združovaní 1. rádu

Signály vyšších tried sa vytvárajú podobne. Štyri signály prvého rádu sa združujú a vytvárajú signál druhého rádu. Prenosová rýchlosť v_p signálu n -tého rádu sa počíta podľa vzťahu $v_{pn} = p * v_{p(n-1)} + m * 64$, kde $v_{p(n-1)}$ je prenosová rýchlosť jedného príspevkového signálu, p je počet združovaných dátových tokov (u PDH je vždy 4), m je multiplikatívny koeficient. Pre PDH 2. rádu platí $v_{pn} = 4 * 2048 + 4 * 64 = 8448$ kbit/s.

Tabuľka 10. 4 uvádza prehľad až do 4. rádu s uvedeným maximálnym počtom kanálov s prenosovou rýchlosťou 64 kbit/s. Obrázok 10.28 znázorňuje princíp vytvorenia jednotlivých rádo PDH.

Tabuľka Hierarchické stupne PDH je na obr. 3.26.

HIERARCHICKÉ STUPNE PDH					
Označenie	Označenie rozhrania	Násobok	Prenosová rýchlosť [kbit/s]	Skrátené označenie	Počet kanálov 64 kbit/s
E1	RM0		64		1
E2	RM1	30	2048	2-megabitový tok	30
E3	RM2	4	8448	8-megabitový tok	120
E4	RM3	4	34368	34-megabitový tok	480
	RM4	4	139264	140-megabitový tok	1920



Obr. 10.26 Princíp vytvárania PDH rámcov

Signály nižšieho rádu sa získajú demultiplexovaním na prijímajúcej strane komunikačného kanála.

Mnohonásobne opakované operácie multiplexovania a demultiplexovania na rôznych hierarchických úrovniach a v rade po sebe nasledujúcich uzloch siete, môžu viesť k degradácii signálu a vzniku chýb. Systémy PDH majú nasledovné nedostatky:

- Dohľadacie a monitorovacie funkcie sú limitované.
- Ťažkopádne multiplexovanie a demultiplexovanie v uzle.
- Nekompatibilita medzi USA, Japonskom a EU.
- Žiaden štandard nad 140 Mbit/s.
- Nedostatočné možnosti manažovania.

Preto pre vyššie prenosové rýchlosti bol vytvorený systém SDH.

Synchrónna digitálna hierarchia SDH (*Synchronous Digital Hierarchy*) bola prirodzeným pokračovaním prudkého nárastu požiadaviek prenosu dát, ktoré PDH nebola schopná realizovať. Pridávanie ďalších hierarchických stupňov nebolo efektívne a technicky ťažko realizovateľné. Preto vznikla v roku 1988 principiálne nová, podľa ITU celosvetovo štandardizovaná synchrónna digitálna hierarchia SDH. Vychádza z amerického štandardu SONET (*Synchronous Optical Network*) a jej charakteristiky sú nasledovné:

- Poskytuje vysoké prenosové rýchlosti. Najnižší stupeň SDH začína približne v oblasti kde PDH končí (140-155 Mbit/s)
- Všetky signály sa multiplexujú synchrónne s pevným časovým vzťahom medzi signálmi vyššieho a nižšieho rádu.
- Medzi hierarchickými stupňami používa riadené prekladanie po celých bajtoch.

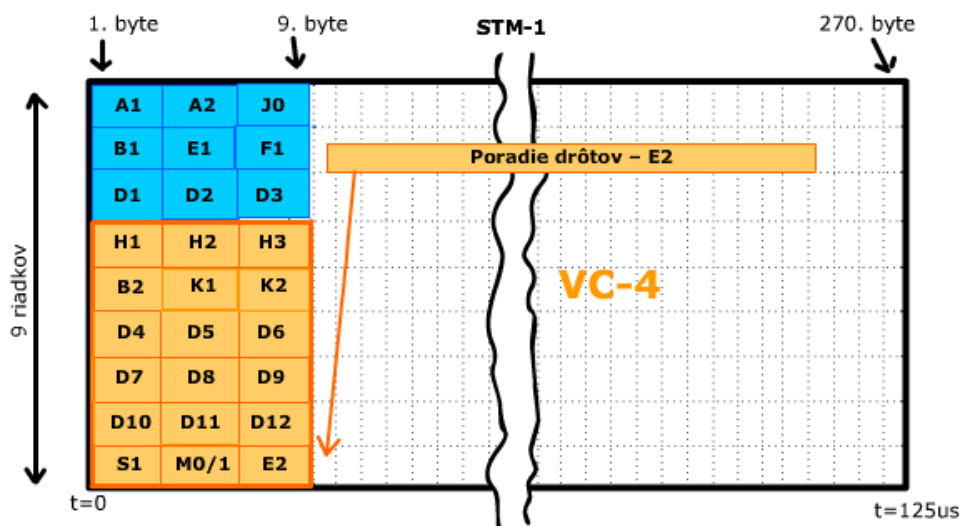
- Štandardizovaným prenosovým médiom je optické vlákno, ktoré dovoľuje vysoké prenosové rýchlosti, rádovo Gbit/s až Tbit/s.
- Zaisťuje bezchybnú prevádzku aj pri poruchách v sieti.

Základné signály synchronnej digitálnej hierarchie sa nazývajú synchronne transportné moduly STM-N, kde N vyjadruje hierarchický stupeň. Najnižšie v hierarchii je STM-1, ďalšie sa tvoria združovaním vždy štyroch signálov nižšieho rádu, z ktorých sú vytvárané STM-4, STM-16, STM-64. Číslo N určuje, do koľkých signálov STM-1 môžeme STM-N demultiplexovať.

Príspevkové signály STM môžu byť:

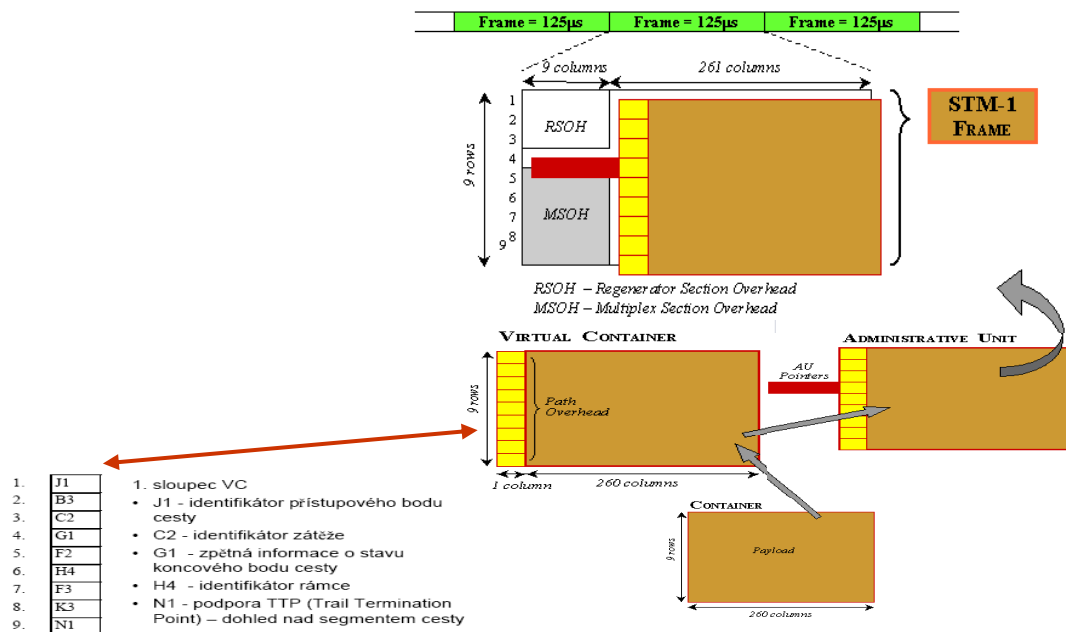
- PDH signály
- ATM bunky
- IP pakety
- Ethernet rámce.

Rámec STM-1 sa kreslí v tvare tabuľky podobne ako rámce signálov vyšších rádov PDH. Známenie tabuľky STM-1 je na obrázku 10.27.



Obr. 10.27 Rámec STM-1

Jednotlivé bajty v tabuľke nasledujú za sebou po riadkoch zľava do prava. Pri STM-1 je 9 riadkov po 270 bajtoch, Prvých 9 bajtov každého riadku nesie pomocnú informáciu - hlavičku, synchronizáciu, zabezpečenie, Zvyšok každého riadku tvorí informačné pole určené na prenos signálu, ktorý nesie užitočnú informáciu. Toto pole sa označuje aj ako virtuálny kontajner VC-4. Kontajner sa v SDH nazýva rámec, ktorý je určený na prenos signálov. Virtuálny je preto lebo nemá v informačnom poli STM stabilnú polohu ale môže začínať kdekoľvek v informačnom poli. Jeho začiatok je označený smerníkom. Kontajner v SDH je rámec, ktorý je určený na prenos užitočnej informácie. Signály nižších stupňov sa prekladajú synchronne po bajtoch do signálu vyššieho stupňa. Spôsob prekladania je na obr. 10.210.



Obr. 10.28 Princíp vytvárania SDH

Vo všetkých hierarchických stupňoch a multiplexných jednotkách SDH je dôsledne dodržiavaná dĺžka rámca 125 μ s, tak ako pri PCM prvého rádu. Prenosová rýchlosť v sa vypočíta ako súčin rozmerov tabuľky, počtu bitov v bajte a vzorkovacej frekvencie rámcov. Dosadením za rozmer tabuľky 270x9, počtu bitov v bajte 8 a vzorkovacej frekvencie 8 kHz dostávame prenosovú rýchlosť prvého stupňa $v_p = 270 \cdot 9 \cdot 8 \cdot 8000 = 15552$ Mbit/s. Tabuľka má v každom stupni 9 riadkov a počet bajtov v riadku sa zvyšuje štvornásobne. Prenosové rýchlosti signálov vyšších stupňov budú na rozdiel od PDH vždy presným štvornásobkom. Prenosové rýchlosti hierarchických stupňov PDH sú v tabuľke 10.4.

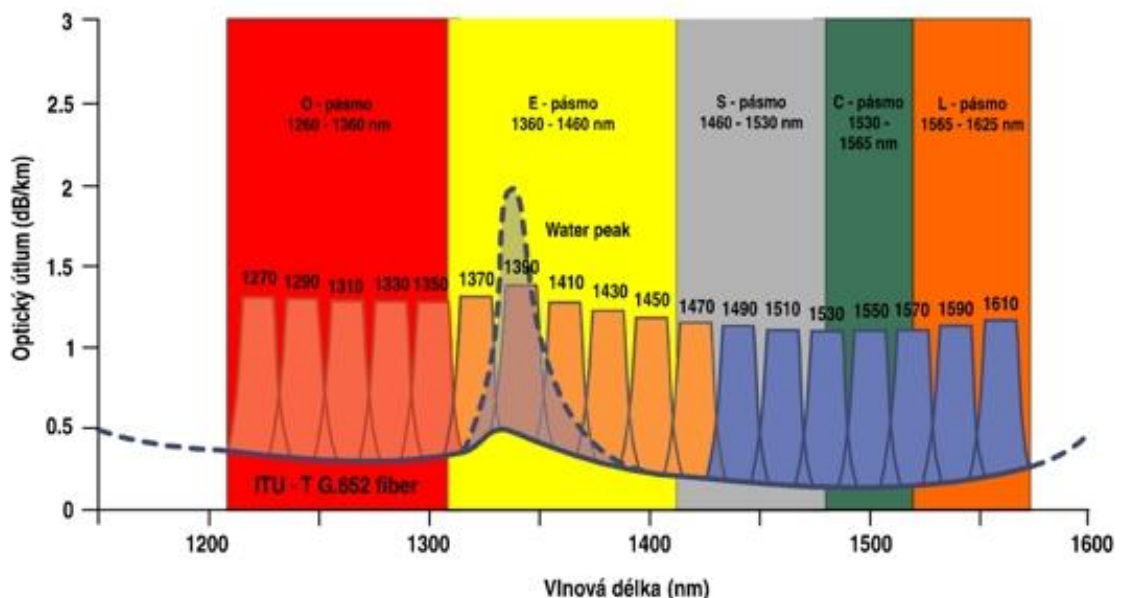
Tabuľka 10.4. Prenosové rýchlosti STM

Stupeň SDH	Synchrónne transportné moduly STM	Označenie SONET	Prenosová rýchlosť v Mbit/s
0	STM - 0	STS-1 OC-1	51,84 (platí len pre SONET)
1	STM - 1	STS-3 OC-3	155,52
2	STM - 4	STS- 2 OC-12	622,08
3	STM - 16	STS-48 OC-48	2 488,32
4	STM - 64	STS-192 OC-192	9 953,28
5	STM - 256	STS-768 OC-768	39 813,12
7	STM-512	STS-1536 OC- 1536	79 626,120
8	STM-1024	STS-3072 OC-3072	159 252,240

10.4.2 Vlnový multiplex

Vlnový multiplex WDM (Wavelength Division Multiplexing) je multiplexná technológia pre optické siete. Princíp vlnového multiplexu bol vysvetlený v kapitole 4. Vo WDM každá vlnová dĺžka prenáša signály rôzneho formátu rôznou prenosovou rýchlosťou. WDM sa používa v dvoch variantách:

- DWDM (*Dense WDM*) – husté vlnové delenie, ktoré má rozstupy optických vlnových dĺžok pod 1 nm. Počet paralelných vlnových dĺžok v jednom vlákne môže byť 32, 64 alebo 96. Každé z nich prenáša signál rýchlosťou až 40 Gbit/s, čím sa dá v jednom vlákne dosiahnuť prenosová rýchlosť až v Tbit/s. Odporúčanie ITU-T G.694.1 "Spectral grids for WDM applications: DWDM frequency grid" špecifikuje jednotlivé prenosové kanály v oblasti vlnových dĺžok v rozsahu od 1490 nm (200,95 THz) do 1620 nm (186,00 THz), označované ako S, C a L pásmo. Ich znázornenie je na obr. 10.31.
- CWDM (*Coarse WDM*) – hrubé vlnové delenie, ktoré má rozstupy optických nosných nad 10 nm. Jednotlivé vlnové dĺžky CWDM technológie sú definované v rozsahu 1270 nm až 1610 nm so vzájomným odstupom 20 nm. Každý zo signálov môže byť tiež prenášaný v rozdielnom formáte s rôznou rýchlosťou prenosu. CWDM systémy sú používané v nízko nákladových prevádzkach kvôli nízkej energetickej náročnosti a nákladom na prevádzku a údržbu. Kanály podľa odporúčania ITU-T G.694.2 sú na obrázku 410.



Obr. 48 CWDM kanály podľa ITU-T G.694.2

Systémy CWDM sú lacnejšie a uplatňujú sa v prístupových a metropolitných sieťach. Systémy DWDM sú využívané pre veľké vzdialenosti. Dosah signálu z CWDM systému je až 100km bez zosilňovania. Pre dlhšie trasy je potrebné signál u oboch systémov priebežne zosilňovať, prípadne obnovovať jeho tvar.

DWDM siete sa naďalej rozvíjajú, pribúdajú rôzne nové funkcionality rozširiteľnosti, integrácie sieťových a prenosových vrstiev, dokonalejšie plánovacie nástroje pre správu a dohľad, až k službám typu „pásma na vyžiadanie“ (*Bandwith on Demand*). Často používajú len jednoduché označenie WDM.

Optická prenosová hierarchia OTH (*Optical Transport Hierarchy*) je vytvorenie spoločnej platformy pre rôzne typy sieťových technológií - SDH, ATM, IP, s podporou monitorovania a manažmentu siete. Je založená na technológii WDM. Podľa doporučenia ITU-T G.692. používa pre vlnové delenie DWDM pásmo 196,1 – 192,1 THz, tj. 1528,77 až 1560,61 nm. Základné signály optickej prenosovej hierarchie sa nazývajú optické transportné moduly OTM (*Optical Transport Module*). Moduly majú všeobecné označenie OTM-n.m, kde n je počet vlnových dĺžok a m vyjadruje aké typy signálov sa prenášajú. Znárodnenie je v tabuľke 10.5, pre tri rýchlosti CBR (*Constant Bit Rate*), 2,5; 10; 40 Gbit/s.

Tabuľka 10.5 Optické hierarchických stupňov OTH

Hierarchický stupeň	Užitočná prenosová rýchlosť v_p [Mbit/s]	Prenášané signály
OMT – n.1	$n \cdot 2488,32$	$n \cdot$ STM - 16
OMT – n.2	$n \cdot 9953,28$	$n \cdot$ STM - 64
OMT – n.3	$n \cdot 39813,12$	$n \cdot$ STM - 256

10.5 Záver

V prístupových sieťach nastali v posledných dvadsiatich rokoch najväčšie technologické zmeny. Prístupové siete boli liberalizované, čo podnietilo výrobcov technológií k vývoju rozličných možností hlavne širokopásmového – vysokorýchlostného prístupu. Širokopásmové prístupy sú poskytované:

- V existujúcich, pôvodne miestnych sieťach po metalických vedeniach technológiami xDSL (*Digital Subscriber Line*), alebo *Fast Ethernet*.
- Optické siete poskytujú rôzne možnosti prístupu cez FTTx (*Fibre To The x*).
- Mobilné telefónne siete, poskytujú služby širokopásmových prístupov cez technológie EDGE, Flarion a 3G, 4G.
- Bezdrôtový prístup umožňujú technológie WiFi (*Wireless Fidelity*) a WiMax, prípadne VSAT.

Edge siete alebo iba edge uzly sú technológie pre prispôbenie prístupových a transportných sietí, ktoré sú potrebné hlavne pri vytváraní koncepcie NGN sietí.

Transportné siete reagovali na rozvoj prístupových sietí a od technológie PDH prešli k technológiám SDH. Poslednou vývojovou technológiou sú optické multiplexy WDM.

Kľúčové slová

1. *Prístupové siete*
2. *Miestne siete*
3. *Posledná míľa*
4. *Používateľské segmenty*
5. *Technológie prístupu*
6. *Služby prístupu*
7. *Komutovaný prístup*
8. *Permanentný prístup*
9. *Drôtové prístupové siete*
10. *Bezdrôtové prístupové siete*
11. *PSTN (Public Switched Telephone Network)*
12. *Verejná telefónna sieť VTS*
13. *POTS, Plain Old Telephone Service*
14. *Dial-up*
15. *xDSL (xDigital Subscriber Line)*
16. *ADSL - Asymmetrical Digital Subscriber Line*
17. *VDSL (Very high-bit rate DSL)*
18. *HDSL (High-bit rate DSL)*
19. *IDSL - Integrated Digital Subscriber Line*
20. *ISDN (Integrated Services Digital Network)*
21. *BRA (Basic Rate Access)*
22. *PRA (Primary Access Rate)*
23. *Prenajaté okruhy (Leased Lines)*
24. *Frame Relay (FM)*
25. *Cable TV- CATV*
26. *FTTx (Fibre to the x)*
27. *FTTH (Fibre To the Home)*
28. *FTTEx (Fibre to the Exchang)*
29. *FTTC (Fibre to the Curb)*
30. *FTTCab (Fibre to the Cabinet)*
31. *FTTB (Fibre to the Building)*
32. *BTS (Base Transceiver Station)*
33. *BSC (Base Station Controller)*
34. *MSC (Mobile Switching Centre)*
35. *HLR (Home Location Register)*
36. *VLR (Visitor Location Register)*
37. *GSM (Global System for Mobile Communication)*
38. *GPRS (General Packet Radio Service)*
39. *UMTS (Universal Mobile Telecommunication System)*
40. *Wi-Fi (Wireless Fidelity)*
41. *WiMax (Worldwide Interoperability for Microwave Access)*
42. *VSAT (Very Small Aperture Terminal)*
43. *Edge siete*
44. *NGN(Next Genetration Network)*
45. *PDH (Plesionous Digital Hierarchy)*
46. *SDH (Synchronus Digital Hierarchy)*
47. *WDM(Wavelength Digital Multiplex)*
48. *DWDM (Dense WDM)*
49. *CWDM (Coarse WDM)*
50. *OTH (Optical Transport Hierarchy)*

Kontrolné otázky

1. Ako sa označuje časť komunikačnej siete, ktorá je najbližšie ku koncovému používateľovi?
2. Aké je označenie siete, ktorou sa koncový používateľ pripája k prvému uzlu komunikačnej siete?
3. Kedy a prečo vznikol pojem prístupová sieť?
4. Aké segmenty používateľov sa pripájajú ku komunikačnej sieti?
5. Prečo je potrebné poznať používateľské segmenty používajúce prístupové siete?
6. K akým sieťam sa najčastejšie pripájajú koncoví používatelia?
7. Aký je účel používateľov pre pripojovanie sa do komunikačnej siete?
8. Ktoré z vymenovaných typov sú typické prístupové siete?

9. Ktoré z vymenovaných komunikačných sietí slúžia ako prístupy k iným sieťam?
10. Ktoré z vymenovaných názvom patria službám prístupu ku komunikačnej sieťi?
11. Ako je možné rozdeliť prístup ku komunikačnej sieťi?
12. Čím je charakteristický vlastný prístup ku komunikačnej sieťi v telefónnych sieťach?
13. Čím je charakteristický vlastný prístup v počítačových a dátových sieťach?
14. Aké typy pripojení môžu byť vytvárané v prenosovej časti prístupu ku komunikačným sieťam?
15. Čo znamená označenie komutovaný prístup ku komunikačnej sieťi?
16. Čo znamená permanentný prístup ku komunikačnej sieťi?
17. Ktoré z vymenovaných pôsobov patria ku komutovanému prístupu ku komunikačnej sieťi?
18. Ktoré z vymenovaných spôsobov patria k permanentnému prístupu?
19. Ktoré z vymenovaných funkcií sú funkciami prístupových sietí?
20. Prečo je PSTN dôležitá ako prístupová sieť?
21. Ktorá kategória uzlov VTS je najdôležitejšia pre prístupové siete?
22. Ktorá časť PSTN je označovaná ako posledná míľa?
23. K akému účelu je v PSTN využívané zariadenie RSU (*Remote Subscriber Unit*)?
24. Čo znamená označenie POTS - *Plain Old Telephone Service*?
25. V čom spočíva princíp služby dial-up?
26. Prečo je služba dial-up už málo využívaná?
27. Ktoré z vymenovaných technológií nahradili službu dial-up?
28. V čom je princíp xDSL odlišný od služby dial-up?
29. Ktoré z uvedených charakteristík sú rozdielne v jednotlivých DSL technológiách?
Odpovede (symetria smerov prenosu, vzdialenosť prenosová rýchlosť, pripojenia k rôznym typom sietí, typ prenosového média)
30. V čom sa odlišuje PSTN od ISDN?
31. Ktoré z vymenovaných kanálov sú použité v ISDN?
32. Aké typy prístupov umožňuje ISDN?
33. Ako je vytvorený prístup PRA (*Primary Rate Access*)?
34. Pre aký účel je využívaný prístup PRA (*Primary Rate Access*)?
35. Čo označuje pojem prenajaté okruhy (*Leased Lines*)?
36. Ktoré z vymenovaných technológií sa využívajú ako typické prístupové siete pre lokálne siete? (Odpovede správne FR, ATM Fast ethernet)
37. Aký je princíp prístupu k sieťi cez CATV?
38. Čo znamená označenie FTTx (*Fibre to the x*)?
39. Aké typy FTTx sú rozlišované?
40. V čom sa líšia jednotlivé typy FTTx?
41. Čo znamená pojem bunka (cell) v bunkových rádiových systémoch?
42. K čomu slúži BTS (*Base Transceiver Station*) v bunkových rádiových systémoch?
43. Aká je najdôležitejšia funkcia riadenia základňových staníc (*BSC - Base Station Controller*) pre mobilitu prístupu?
44. Čo označuje pojem generácia v bunkových rádiových systémoch?
45. V čom je odlišnosť systému GSM od GPRS (*General Packet Radio Service*)?
46. V čom je odlišnosť systému GSM UMTS (*Universal Mobile Telecommunication System*)?
47. K akej kategórii patrí prístupová sieť Wi-Fi (*Wireless Fidelity*)?
48. K akej kategórii patrí prístupová sieť WiMAX (*Worldwide Interoperability for Microwave Access*)?
49. V čom odlišnosť v prístupových sieťach WiFi a WiMAX?

50. Kedy je vhodné použiť prístupovú sieť VSAT - VSAT Very Small Aperture Terminal?
51. Aký je rozvojový trend v prístupových sieťach?
52. Prečo boli špecifikované edge siete/edge uzly?
53. Aká je hlavná úloha edge sietí?
54. Čo znamená označenie NGN (*Next Generation Networks*)?
55. Prečo vznikla potreba vytvorenia sietí NGN – Next Generation Network?
56. Ktoré sú hlavné znaky siete NGN – Next Generation Network?
57. Aká je výhoda NGN v to, že služby sú nezávislé od prenosových častí?
58. Ktoré dva typy prenosových sietí sú špecifikované v NGN – Next Generation Networks?
59. Ako je vnímaný pojem Edge siete?
60. Ktoré dve základné funkcie riešia edge technológie?
61. Čo podnecuje dynamický vývoj transportných sietí?
62. Označte charakteristické vlastnosti transportných sietí.
63. Patrí optické prenosové médium medzi charakteristické vlastnosti transportných sietí?
64. Metalické vedenie patrí medzi charakteristické vlastnosti transportných sietí.
65. Čím sa zaisťuje spoľahlivosť transportných sietí?
66. Ktoré technológie majú v súčasnosti najväčší vplyv na rozvoj transportných sietí?
67. Vymenujte dominantné technológie používané v transportných sieťach.
68. Používa sa TDM – časový multiplex v transportných sieťach?
69. Typickým predstaviteľom STDM je rámec PCM 1. rádu?
70. Základná výhoda asynchrónneho prenosového módu spočíva v možnosti štatistického multiplexovania (STDM).
71. Čím je charakteristická plesiochrónna digitálna hierarchia (PDH)?
72. V plesiochrónnej hierarchii kladieme jednotlivé združované signály bit po bite do rámca signálu vyššieho rádu?
73. Aké sú vlastnosti synchronnej digitálnej hierarchie (SDH)?
74. Prenosová rýchlosť najnižšieho stupňa synchronnej digitálnej hierarchie začína približne od 55 Mbps?
75. Napíšte skratku pre americký štandard Synchronous Optical Network, z ktorého vychádza aj SDH.
76. Napíšte skratku pre základnú jednotku SDH (bez očíslovania).
77. Koľko základných jednotiek prenosu (STS-1) sa spája v základnej jednotke SDH (STM-1)?
78. Koľko signálov nižšieho rádu združujeme vo vyšších rádoch STM?
79. Je možné začleniť signály PDH do SDH?
80. Aký je význam systémov DWDM a CWDM?
81. Na čo slúži optická prenosová hierarchia (OTH)?