# 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

## 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.

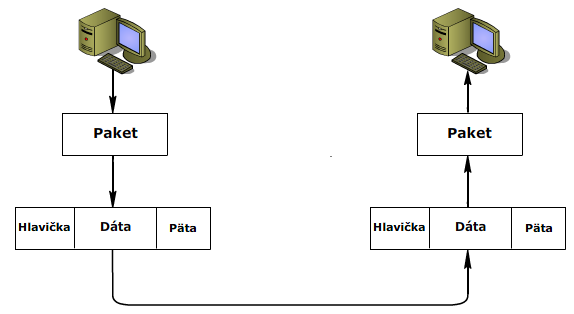
Linkovú vrstvu si môžeme predstaviť ako komunikáciu medzi dvomi susednými uzlami prenosového kanála. Hlavnou úlohou linkovej vrstvy je preto **poskytovanie mechanizmu na komunikáciu** medzi dvomi susednými uzlami. Jednotlivé systémy v sieti sa na tejto úrovni identifikujú adresami a komunikujú spôsobom „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.

## 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 pätu *(frame trailer)*, obr. 5.1*.*



Obr. 5.1 Rámec v linkovej vrstve

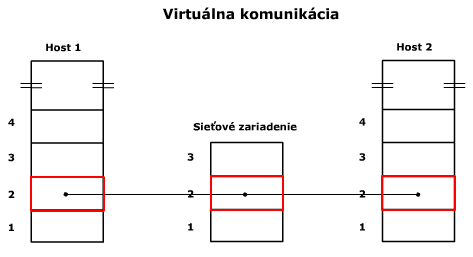
V niektorých technológiách nie sú na linkovej úrovni poskytované všetky vyššie uvedené funkcie. Ide hlavne o kontrolu chýb a kontrolu toku dát, ktoré sú presunuté do vyšších vrstiev. Princípy, ktoré budú vysvetľované v tejto časti sú platné aj pre ich uplatnenie v iných úrovniach.

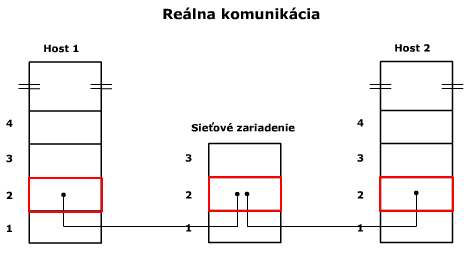
V lokálnych sieťach je linková vrstva rozdelená na dve podvrstvy:

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

## 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





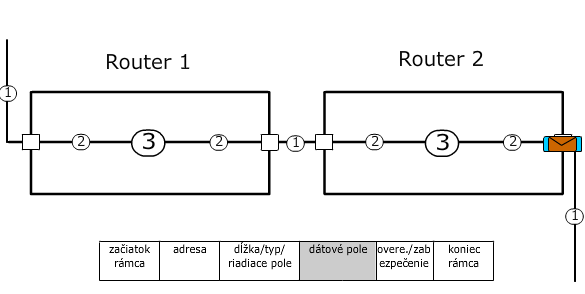
Obr. 5.2. Virtuálna a reálna komunikácia na linkovej úrovni

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.

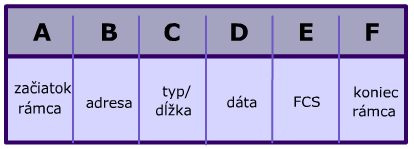
### Tvorba rámcov

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 použitom spôsobe zabezpečenia proti chybám.

### 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 poľa, 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.

### 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 synchrónny prenos, pri ktorom sa používa synchronizácia na fyzickej vrstve na úrovni znakov (*character synchronizationn*), 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.

## 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:

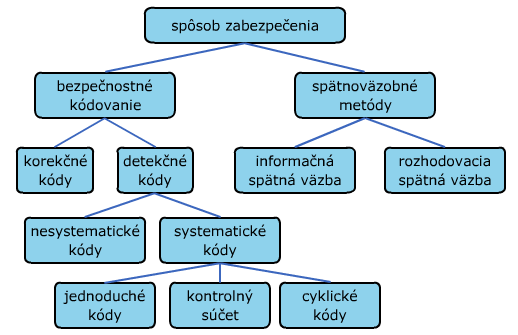
* bezpečnostné kódovanie,
* metódy so spätnou väzbou.

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 vysielacou 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

### Zabezpečenie paritou

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

(Sk, Sk-1, …… S1,**r1**)

kde Si sú binárne znaky zakódovanej správy,**r1 je zabezpečovací symbol**.

Hodnotu zabezpečovacieho symbolu určí kóder na vstupe kanála podľa rovnice:

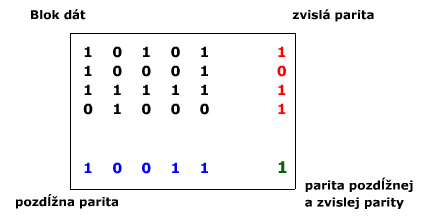
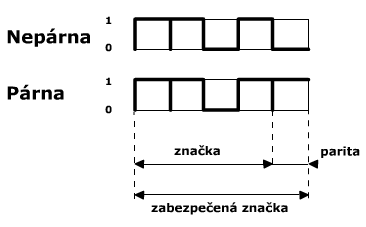
Sk + Sk-1 + …… + S1 +r1 = 0 pre párnu paritu

Sk + Sk-1 + …… + S1 +r1 = 1 pre nepárnu 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

### 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 vysielač 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 x16 + x12 + x5 + 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 1014 správne prenesených bitov.

## Prístup na spoločné komunikačné prostredie

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

* Rozdeliť celkovú kapacitu prenosového média na časti, ktoré sú prideľované jednotlivým prenosovým kanálom.
* Zabezpečiť rovnomerné prideľovanie 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 médiom. Komunikujúce zariadenia sú vzájomne prepojené spoločným médiom, 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 vysielať 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 prideľujú 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 médiom so zanedbateľnou bitovou chybovosťou, zaručuje prakticky ideálny priebeh riadenia siete.

Vlastné riadenie komunikácie môže byť:

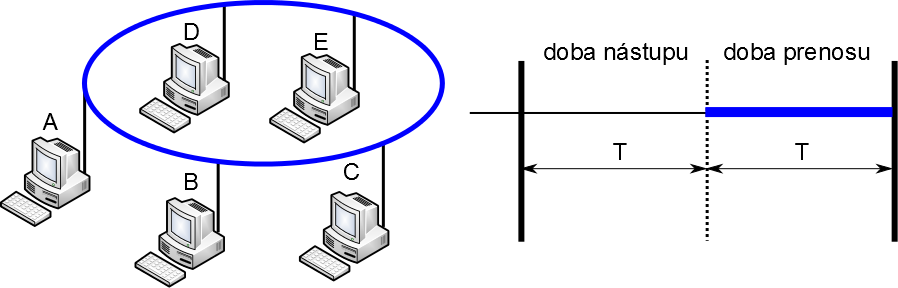
* Centralizované, kde jedno zariadenie je zvolené ako riadiace a prideľuje ostatným podriadeným zariadeniam kapacitu kanála na základe ich požiadavky.
* Decentralizované, ktoré odstraňuje závislosť na jednom riadiacom zariadení. V závislosti od použitej metódy sa zariadenie pripája k spoločnému kanálu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

**Stochastické prístupové metódy**

#### 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 vysielať 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 vysielať. Rovnako prijímacia strana zistí kolíziu a tiež prestane vysielať. 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 vysielať. 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 prenesie 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.

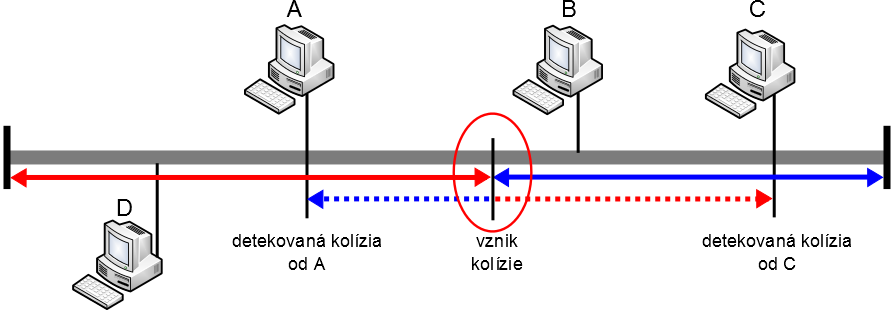
Riziko vzniku kolízie sa dá radikálne zmeniť, keď sa zariadeniam povolí vysielanie len v určitých časových okamžikoch. Prakticky to znamená prechod od spojitého času na čas diskrétny. Na tejto myšlienke je postavený princíp synchronizovanej Alohy *(Synchronus Aloha, Slotted Aloha, S-Aloha)*. Tým je zavedený deterministický prvok do stochastickej metódy. Pri S-Alohe zariadenie nemôže vysielať kedykoľvek, ale iba v tzv. synchronizačných okamžikoch, viď. 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

#### 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 vysielať 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

#### 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.

#### Token Passing

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

### Deterministické prístupové metódy

Deterministické metódy zabezpečujú bezkonfliktné prideľovanie 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:

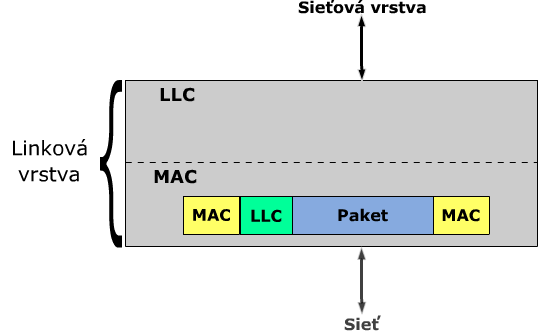
* **TDMA *(Time Division Multiple Access****),* kde sa dostupná prenosová kapacita delí v čase. Vychádza z časovo deleného - TDM princípu, ktorý je pre komunikáciu bod–multibod (*point to multipoint*) nutné doplniť o procedúry zabezpečujúce časovo delený prístup na prenosové médium (A- *access*), ktoré 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 priraďovaní kanála jednotlivým zariadeniam, musia byť WDM multiplexory preladiteľné.
* **CDMA *(Code Division Multiple Access)***priraďuje 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.

## 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. Znázornenie rozdelenia je na obrázku 5.8.

****

Obr. 5.10 Rozdelenie linkovej úrovne podľa IEEE 802.2

### Riadenie logického spoja - LLC

**LLC -** *Logical Link Control* **poskytuje služby sieťovým protokolom**, ktoré sú nad ňou, a súčasne využíva služby rôznych technológií fyzickej vrstvy. LCC sa podieľa na procese zapuzdrenia *(encapsulation).* Spracováva dáta sieťového protokolu, spravidla IP paketu, a pridá svoje riadiace informácie, aby sa paket dostal sa 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.

### 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. Prideľovanie adries riadi organizácioa 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.

## Riadenie toku

Riadenie toku dát na linkovej vrstve je mechanizmus, ktorý zabezpečuje, aby vysielacie zariadenie nezahltilo 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.

### 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 potvrdení o jeho prijatí. Vysielacie zariadenie čaká, kým nedostane potvrdenie. Až po prijatí tohto potvrdenia môže vysielacie zariadenie opäť vysielať.

### Protokol posuvného okna *(Sliding Window Protokols)*

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

Číslo vo vnútri "okna vysielača" predstavuje číslo vysielaného a doposiaľ nepotvrdeného rámca. Okno je rozdiel medzi množstvom vyslaných a potvrdených rámcov. Preto sa po príchode nového rámca, zväčší okno nepotvrdených rámcov o jednotku. Ako náhle príde potvrdenie o prijatí rámca okno sa o jednotku zmenší. Vysielač 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.

## Opravy prenosu rámcov

Chybne prenesená rámce sú opravované dvojakým spôsobom:

* Mechanizmami na opravu rámcov, ktoré sú založené na týchto princípoch:
  + detekcia bitových chýb zaisťovaná pomocou CRC (*Cyclic Redundancy Code*),
  + kladné potvrdzovanie prijatia rámca, čo znamená, že prijímač odosiela kladné potvrdenie pre bezchybne prijaté rámce,
  + opakovanie vysielania rámcov po uplynutí času, tj. ak do definovanej doby nedostane vysielač 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.

## Základné linkové protokoly

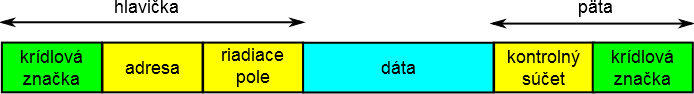
Protokoly linkovej vrstvy popisujú rámce, ktoré sú komunikačnou jednotkou linkovej vrstvy.

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

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

Protokol HDLC je ISO3309 linkový protokol pre synchrónny 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.

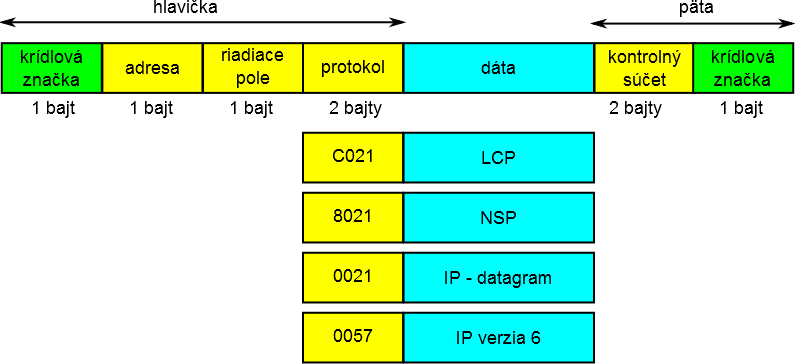
  
Obr. 5.11 Rámec protokolu HDLC

### 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 vlastní 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 protokomom IPV6, NCP protokol pre IPV6 má označenie 8057.

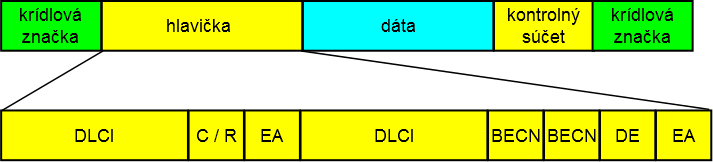
Na obr. 5.12 sú znázornené tvary rámcov protokolu PPP.



Obr. 5.12 Rámce protokolu PPP

### 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 informáciou 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

### 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.

Ethernet%20format%20ramca

Obr. 5.14 Formát rámca Ethernet

### 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.

Token%20Ring%20format

Obr. 5.15 Formát rámca Token Ring

### Protokol FDDI (Fiber Distributed Data Interface)

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

FDDI%20format%20ramca

Obr. 5.16 Formát rámca v FDDI

## 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.

### 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 prideľuje 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

### 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 zmenšuje 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.

### Rozbočovač (*HUB*)

***HUB***  umožňuje vetvenie siete a v principiálne je to opakovač. Všetky prijaté dáta z jedného zariadenia posiela 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 staších typoch sietí, postupne sú nahradzované prepínačmi (svitch).



Obr. 5.18 Hub

### 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

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

**Kontrolné otázky**

1. Ktorej 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 (*acknowleged 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 ja 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 podvrvrstvy 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 adries?
37. Kto prideľuje 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?