1. DESCRIEREA TOPOLOGIILOR REȚELELOR DE DATE

1.1 Transmisia datelor în rețelele de calculatoare

O rețea de calculatoare este alcătuită dintr-un ansamblu de echipamente interconectate între ele prin intermediul unor echipamente de rețea, cu scopul transmisiei de date şi partajării resurselor.

O rețea poate partaja diverse tipuri de resurse:

- Servicii – cum ar fi imprimarea sau scanare;
- Spații de stocare pe suporturi externe – cum ar fi hard-diskurile;
- Aplicații – cum ar fi bazele de date

Echipamentele interconectate pot fi sisteme de calcul (desktop sau laptop) sau echipamente periferice (imprimante, scannere etc)

Conectivitatea este asigurată de echipamente de rețea (hub-uri, switch-uri, rutere, puncte de acces wireless)

Transmisia datelor se realizează prin medii de transmisie care pot fi:

- Conductoare de cupru – pentru transmisia datelor sub formă de semnale electrice;
- Fibră optică – din fibre de sticlă sau materiale plastice – pentru a transporta datele sub formă de impulsuri luminoase;
- Medii de transmisie a datelor fără fir – transmit datele sub formă de unde radio, microunde, raze infraroşii sau raze laser - în cadrul conexiunilor fără fir (wireless);

În timpul transmisiei de la un calculator sursă la un calculator destinație, datele suferă o serie de modificări:

- Înainte de a fi transmise în rețea, datele sunt transformate în flux de caractere alfanumerice, apoi sunt împărțite în segmente, care sunt mai uşor de manevrat şi permit mai multor utilizatori să transmită simultan date în rețea;
- Fiecărui segment i se ataşează apoi un antet (header), care conține o serie de informații suplimentare cum ar fi:
    - un semnal de atenționare, care indică faptul că se transmite un pachet de date;
    - adresa IP a calculatorului-sursă;
    - adresa IP a calculatorului-destinație;
    - informații de ceas pentru sincronizarea transmisiei) şi un postambul care

este de obicei o componentă de verificare a erorilor (CRC). Segmentul, astfel modificat se numeşte pachet, pachet IP sau datagramă;

- Fiecărui pachet i se ataşează apoi un al doilea antet care conține adresele MAC ale calculatorului-sursă, respectiv ale calculatorului-destinație. Pachetul se transformă astfel în cadru (frame);

Cadrele circulă prin mediul de transmisie sub formă de şiruri de biți. Există mai multe tipuri de cadre, în funcție de standardele folosite la descrierea lor (cadru Ethernet, cadru FDDI, etc.).

Odată ajunse la calculatorul-destinație, şirurile de biți suferă procesul invers de transformare. Li se detaşează antetele, segmentele sunt apoi reasamblate, li se verifică integritatea şi numărul, apoi sunt aduse la o formă care poate fi citită de utilizator.

Procesul de împachetare a datelor se numeşte încapsulare, iar procesul invers, de detaşare a informațiilor suplimentare se numeşte decapsulare. Trebuie menționat că în timpul încapsulării, datele propriu-zise rămân intacte

Sunt definite două tehnologii de transmisie a datelor: transmisia prin difuzare (broadcast) şi transmisia punct-la-punct.

- Transmisia prin difuzare utilizează de cele mai multe ori un singur canal de comunicație care este partajat de toate stațiile din rețea. Orice stație poate trimite pachete, care sunt primite de toate celelalte stații, operațiunea numindu-se difuzare. Stațiile prelucrează numai pachetele care le sunt adresate şi le ignoră pe toate celelalte. În unele rețele cu difuzare este posibilă transmisia simultană de pachete către mai multe stații conectate la rețea, operațiune ce poartă numele de trimitere multiplă. Această tehnică se utilizează cu precădere în rețelele de mici dimensiuni, localizate în aceeaşi arie geografică.
- Transmisia punct-la-punct se bazează pe conexiuni pereche între stații, cu scopul transmiterii de pachete. Pentru a parcurge traseul de la o sursă la destinație intr-o rețea de acest tip, un pachet va „călatori" prin una sau mai multe maşini intermediare. Pot exista mai multe trasee între o sursă şi o destinație motiv pentru care în aceste situații este necesara implementarea unor algoritmi specializați de dirijare. Tehnica punct-la-punct este caracteristică rețelelor mari

Cantitatea de informație care poate fi transmisă în unitatea de timp este exprimată de o mărime numită lățime de bandă (bandwidth), şi se măsoară în biți pe secundă (bps). Adeseori în aprecierea lățimii de bandă se folosesc multiplii cum ar fi:

- Kbps – kilobiți pe secundă;
- Mbps – kilobiți pe secundă;

O rețea suportă trei moduri de transmisie a datelor: simplex, half-duplex şi full-duplex:

- Simplex- întâlnit şi sub numele de transmisie unidirecțională, constă în transmisia datelor într-un singur sens. Cel mai popular exemplu de transmisie simplex este transmisia semnalului de la un emițător (stația TV) către un receptor(televizor);
- Half-duplex – constă în transmiterea datelor în ambele direcții alternativ. Datele circulă în acest caz pe rând într-o anumită direcție. Un exemplu de transmisie half-duplex este transmisia datelor între stațiile radio de emisie-recepție. Sistemele sunt formate din două sau mai multe stații de emisie-recepție dintre care una singură joacă rol de emițător, în timp ce celelalte joacă rol de receptor;
- Full-duplex – constă în transmisia datelor simultan în ambele sensuri. Lățimea de bandă este măsurată numai într-o singură direcție (un cablu de rețea care funcționează în full-duplex la o viteză de 100 Mbps are o lățime de bandă de 100 Mbps). Un exemplu de transmisie full-duplex este conversația telefonică.

1.2. Tipuri de rețele

1.2.1. Rețele de tip LAN, WAN şi WLAN

O clasificare a rețelelor după criteriul răspândirii pe arii geografice, al modului de administrare si al mediului de transmisie a datelor ar evidenția, printre altele , următoarele trei tipuri de rețele: rețele locale de calculatoare (LAN – Local Area Network); rețele de întindere mare (WAN – Wide Area Network); rețele fără fir (WLAN – Wireless Local Area Network).

- Rețele LAN

Rețeaua locală de calculatoare este o rețea de echipamente interconectate răspândite pe o suprafață de mici dimensiuni (încăpere, clădire, grup de clădiri apropiate).

Conceptul de LAN face referire la o rețea de calculatoare interconectate şi supuse aceloraşi politici de securitate şi control a accesului la date, chiar dacă acestea sunt amplasate în locuri diferite (clădiri sau chiar zone geografice). În acest context, conceptul de local se referă mai degrabă la controlul local decât la apropierea fizică între echipamente. Transmisia datelor în rețelele LAN tradiționale se face prin conductoare de cupru.

- Rețele WAN

O rețea de întindere mare este alcătuită din mai multe rețele locale (LAN-uri) aflate în zone geografice diferite. Rețelele de întindere mare acoperă arii geografice extinse, o rețea WAN se poate întinde la nivel național sau internațional.

În mod specific în aceste rețele calculatoarele se numesc gazde (host), termen care se extinde şi la rețelele LAN care fac parte din acestea. Gazdele sunt conectare printr-o subrețea de comunicație care are sarcina de a transporta mesajele de la o gazdă la alta. Subrețeaua este formată din două componente distincte: liniile de transmisie şi elementele de comutare. Elementele de comutare, numite generic noduri de comutare, sunt echipamente specializate, folosite pentru a interconecta două sau mai multe linii de transmisie.

Unele rețele WAN aparțin unor organizații a căror activitate se desfăşoară pe o arie largă şi sunt private. Cel mai popular exemplu de rețea WAN este Internetul, care este format din milioane de LAN-uri interconectate cu sprijinul furnizorilor de servicii de comunicații (TSP-Telecommunications Service Providers).

- Rețele WLAN

Sunt rețele locale care transmisia datelor se face prin medii fără fir. Într-un WLAN, stațiile, care pot fi echipamente mobile – laptop – sau fixe – desktop - se conectează la echipamente specifice numite puncte de acces. Stațiile sunt dotate cu plăci de rețea wireless. Punctele de acces, de regulă routere, transmit şi recepționează semnale radio către şi dinspre dispozitivele wireless ale stațiilor conectate la rețea.

Punctele de acces se conectează de obicei la rețeaua WAN folosind conductoare de cupru. Calculatoarele care fac parte din WLAN trebuie să se găsească în raza de acțiune a acestor puncte de acces, care variază de la valori de maxim 30 m în interior la valori mult mai mari în exterior, în funcție de tehnologia utilizată.

Primele transmisii de date experimentale în rețele rețele wireless au avut loc în anii 70 si au folosit ca agent de transmisie a datelor in rețea undele radio sau razele infraroşii. Între timp, tehnologia a evoluat şi s-a extins până la nivelul utilizatorilor casnici..

În prezent există mai multe moduri de a capta datele din eter: Wi-Fi, Bluetooth, GPRS, 3G ş.a. Acestora li se adaugă o nouă tehnologie care poate capta datele de şapte ori mai repede şi de o mie de ori mai departe decât populara tehnologie Wireless Fidelity (Wi-Fi), numită WiMAX. În timp ce rețelele Wi-Fi simple au o rază de acțiune de aproximativ 30 m, WiMax utilizează o tehnologie de microunde radio care măreşte distanța la aproximativ 50 km. Astfel, se pot construi rețele metropolitane WiMAX.

Avantaje:

- Simplitate in instalare;
- Grad ridicat de mobilitate a echipamentelor – tehnologia s-a popularizat cu precădere pentru conectarea la rețea a echipamentelor mobile;
- Tehnologia poate fi utilizată în zone în care cablarea este dificil sau imposibil de realizat;
- Costul mai ridicat al echipamentelor wireless este nesemnificativ raportat la costul efectiv şi costul manoperei în cazul rețelelor cablate;
- Conectarea unui nou client la o rețea wireless nu implică folosirea unor echipamente suplimentare.

Dezavantaje:

- Securitate scăzută;
- Raza de acțiune în cazul folosirii echipamentelor standart este de ordinul zecilor de metrii. Pentru extinderea ei sunt necesare echipamente suplimentare care cresc costul;
- Semnalele transmise sunt supuse unor fenomene de interferențe care nu pot fi controlate de administratorul de rețea şi care afectează stabilitatea şi fiabilitatea rețelei– motiv pentru care serverele sunt rareori conectate wireless;

- Lățimea de bandă mică (1-108 Mbit/s) în comparație cu cazul rețelelor cablate (până la câțiva Gbit/s);

1.2.2. Rețele peer-to-peer (P2P) şi rețele client-server

Într-o rețea de calculatoare comunicarea are loc între două entități: clientul care emite o cerere prin care solicită o anumită informație şi serverul care primeste cererea, o prelucreaza iar apoi trimite clientului informatia solicitată. Dacă ar fi să clasificăm rețelele după ierarhia pe care o au într-o rețea echipamentele conectate, ar trebui să facem referire la două tipuri de rețele: rețele de tip peer-to-peer şi rețele de tip client-server.

- Rețele peer-to-peer

Într-o rețea peer-to-peer, toate calculatoarele sunt considerate egale (peers), fiecare calculator îndeplineşte simultan şi rolul de client şi rolul de server, neexistînd un administrator responsabil pentru întreaga rețea. Un exemplu de serviciu care poate fi oferit de acest tip de rețele este partajarea fişierelor. Acest tip de rețele sunt o alegere bună pentru mediile în care: există cel mult 10 utilizatori, utilizatorii se află într-o zonă restrânsă, securitatea nu este o problemă esențială, organizația şi rețeaua nu au o creştere previzibilă în viitorul apropiat:

Neajunsuri ale rețelelor peer-to-peer sunt următoarele:

- Nu pot fi administrate centralizat;
- Nu poate fi asigurată o securitate centralizată, ceea ce înseamnă că fiecare calculator trebuie să folosească măsuri proprii de securitate a datelor;
- Datele nu pot fi stocate centralizat, trebuie menținute backup-uri separate ale datelor, iar responsabilitatea cade în sarcina utilizatorilor individuali;
- Administrarea rețelelor peer-to-peer este cu atât mai complicată cu cât numărul calculatoarelor interconectate este mai mare.

- Rețele client-server

Rețele client-server, în care un calculator îndeplineşte rolul de server, în timp ce toate celelalte îndeplinesc rolul de client. De regulă, serverele sunt specializate (servere dedicate) în efectuarea diferitelor procesări pentru sistemele-client, cum ar fi:

- Servere de fişiere şi imprimare – oferă suport sigur pentru toate datele şi gestionează tipărirea la imprimantele partajate în rețea pot fi administrate centralizat;
- Servere web – găzduiesc pagini web;
- Servere pentru aplicații – cum ar fi serverele pentru baze de date;
- Servere de mail – gestionează mesaje electronice;
- Servere pentru gestiunea securității – asigură securitatea unei rețele locale când aceasta este conectată la o rețea de tipul Internetului – exemple: firewall, proxy-server;
- Servere pentru comunicații – asigură schimbul de informații între rețea şi clienții din afara acesteia.

Rețelele client-server se folosesc cu precădere pentru comunicarea de date în rețea, marea majoritate a aplicațiilor software dezvoltate au la bază acest model. Printre avantajele rețelelor de tip client-server se numără:

- administrarea centralizată, administratorul de rețea fiind cel asigură back-up-urile de date ervere de fişiere şi imprimare – oferă suport sigur pentru toate datele şi gestionează tipărirea la imprimantele partajate în rețea pot fi administrate centralizat;
- implementarea măsurile de securitate şi controlul accesul utilizatorilor la resurse;
- funcționarea cu sisteme-client de capabilități diverse;
- securitate ridicată a datelor;
- controlul accesului exclusiv la resurse a clientilor autorizați;
- întretinere usoară.

- Rețelele hibride – sunt o combinație a modelului client-server cu modelul peer-to-peer. Stațiile (peers) depozitează resursele partajate iar serverul păstrează informații în legătură cu stațiile (adresa lor, lista resurselor deținute de acestea) şi răspunde la cererea de astfel de informații. Un exemplu de serviciu oferit de o astfel de rețea este descărcarea de fişiere de pe site-urile torrent.

1.3. Topologii de rețele de calculatoare

Topologia este un termen care desemnează maniera de proiectare a unei rețele. Există două tipuri de topologii: topologia fizică şi topologia logică:

1.3.1. Topologia logică

Topologia logică descrie metoda folosită pentru transferul informațiilor de la un calculator la altul.

Cele mai comune două tipuri de topologii logice sunt broadcast şi pasarea jetonului (token passing)

- Într-o topologie broadcast, o stație poate trimite pachete de date în rețea atunci când rețeaua este liberă (prin ea nu circulă alte pachete de date). În caz contrar, stația care doreşte să transmită aşteaptă până rețeaua devine liberă. Dacă mai multe stații încep să emită simultan pachete de date în rețea, apare fenomenul de coliziune. După apariția coliziunii, fiecare stație aşteaptă un timp(de durată aleatoare), după care începe din nou să trimită pachete de date. Numărul coliziunilor într-o rețea creşte substanțial odată cu numărul de stații de lucru din rețeaua respectivă, şi conduce la încetinirea proceselor de transmisie a datelor în rețea, iar dacă traficul depăşeşte 60% din lățimea de bandă, rețeaua este supraîncărcată şi poate intra în colaps.
- Pasarea jetonului controlează accesul la rețea prin pasarea unui jeton digital secvențial de la o stație la alta. Când o stație primeşte jetonul, poate trimite date în rețea. Dacă stația nu are date de trimis, pasează mai departe jetonul următoarei stații şi procesul se repetă.

1.3.2. Topologia fizică

Topologia fizică defineşte modul în care calculatoarele, imprimantele şi celelalte echipamente se conectează la rețea.

Topologii fizice fundamentale sunt: magistrală, inel, stea, plasă (mesh), arbore.

- Topologia magistrală

Foloseşte un cablu de conexiune principal, la care sunt conectate toate calculatoarele vezi figura 1.1.

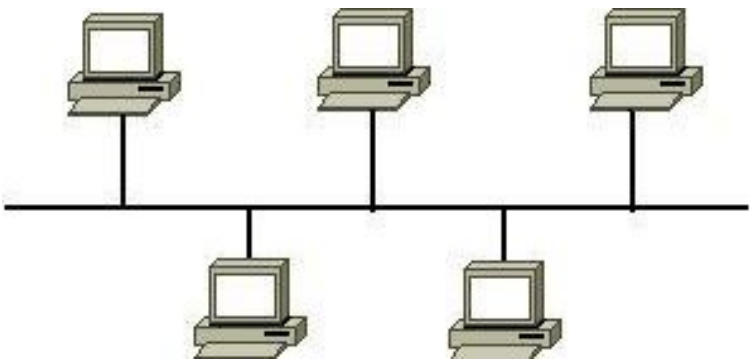

Fig. 1.1 Topologia magistrală

Cablul principal are la capete instalate capace (terminatoare) care previn fenomenul de reflexie a semnalelor, fenomen care poate genera erori în transmisia datelor.

Topologia magistrală are avantajul consumului redus de cablu si al conectării facile a calculatoarelor. În schimb, identificarea defectelor de rețea este dificilă, dacă apar întreruperi în cablu, rețeaua nu mai funcționează şi este nevoie de terminatori la ambele capete ale cablului.

Această topologie nu este practică decât pentru cele mai mici rețele peer-to-peer ieftine, care asigură o conectivitate elementară. Aceste produse sunt destinate utilizării casnice şi în birourile mici, însă o excepție al modului de transmitere de informații al acestui tip de topologie îl reprezintă standardul IEEE 802.4 Token Bus LAN, care îi oferea utilizatorului un grad înalt de control în determinarea perioadei maxime în care poate fi transmis un cadru de date.

- Topologia inel

Într-o topologie inel (ring), fiecare dispozitiv este conectat la următorul, de la primul până la ultimul, ca într-un lanț.

A început ca simplă topologie peer-to-peer. Fiecare stație de lucru din rețea avea două conexiuni: câteuna cu fiecare dintre vecinii cei mai apropiați.

Interconectarea trebuia să formeze un cerc, sau inel (ring), prin care datele erau transmise unidirecțional vezi figura 1.2. Fiecare stație de lucru avea rolul de repetor, acceptând şi răspunzând pachetelor de date care îi erau adresate şi transmițând celelalte pachete stației următoare din inel.

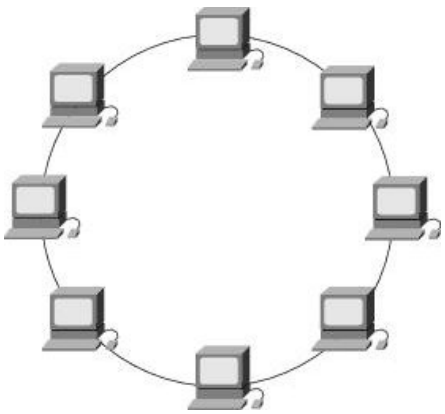

Fig. 1.2 Topologie de tip inel

Topologia inel inițială avea între stațiile de lucru conexiuni peer-to-peer, ce trebuiau să fie închise, adică să formeze un inel. Avantajul acestor rețele LAN era că timpul de răspuns era destul de previzibil. Cu cât erau mai multe dispozitive în inel, cu atât creşteau întârzierile rețelei. Dezavantajul era că, la început, rețelele în inel puteau fi complet dezactivate dacă una dintre stațiile de lucru se defecta.

Aceste inele primitive au fost depaşite odată cu apariția sistemului Token Ring al firmei IBM, care a fost standardizat prin specificația 802.5 a standardului IEEE. Acest sistem utilizează o sevență de biți specială, cunoscută ca jeton (token), pentru a controla accesul la mediul de transmisie. Un jeton conține câmpurile de delimitare a începuturilor de cadru, de control al accesului şi de delimitare a sfârşitului şi are rolul de a trece într-o sevență circulară pe la toate punctele de capăt din rețea.

Token Ring a deviat de la interconectarea peer-to-peer în favoarea unui concentrator repetor (hub), ceea ce a eliminat vulnerabilitatea rețelelor în inel la căderea stațiilor, prin eliminarea construcției peer-to-peer în inel. În ciuda numelui, rețelele Token Ring sunt implementate cu o topologie în stea şi o metodă circulară de acces.

- Topologia stea

Are un punct de conectare central, care este de obicei un echipament de rețea, precum un hub, switch sau router vezi figura 1.3.

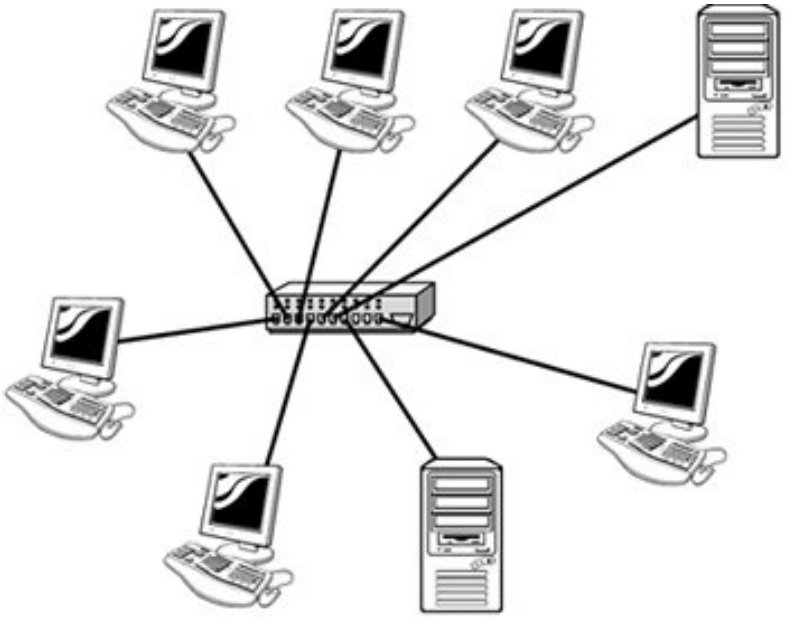

Fig. 1.3 Topologie de tip stea

Fiecare stație din rețea se conectează la punctul central prin câte un segment de cablu, fapt care conferă acestei toplogii avantajul că se depanează uşor. Dacă un segment de cablu se defectează, acest defect afectează numai calculatorul la care este conectat, celelalte stații rămânând operaționale.

Topologia stea are dezavantajul costului ridicat şi al consumului ridicat de cablu. În plus, dacă un hub se defectează, toate echipamentele din acel nod devin nefuncționale. În schimb, calculatoarele se conectează uşor, rețeaua nu este afectată dacă sunt adăugate sau deconectate calculatoare şi detectarea defectelor este simplă.

- Topologia plasă (mesh)

Într-o topologie mesh, fiecare echipament are conexiune directă cu toate celelalte. Dacă unul din cabluri este defect, acest defect nu afectează toată rețeaua ci doar conexiunea dintre cele două stații pe care le conectează. Altfel spus, dacă o parte a infrastructurii de comunicație sau a nodurilor devine nefuncțională, se găseşte oricând o noua cale de comunicare.

Topologia plasă se foloseşte în cadrul rețelelor WAN care interconectează LAN-uri. În plus, datorita fiabilității ridicate aceste topologii sunt exploatate in cazul aplicațiilor spațiale, militare sau medicale unde întreruperea comunicației este inacceptabilă.

- Topologia arbore (tree)

Combină caracteristicile topologiilor magistrală şi stea. Nodurile sunt grupate în mai multe topologii stea, care, la rândul lor, sunt legate la un cablu central vezi figura 1.4.

Topologia arbore prezintă dezavantajul limitării lungimii maxime a unui segment. În plus, dacă apar probleme pe conexiunea principală sunt afectate toate calculatoarele de pe acel segment. Avantajul topologiei arbore constă în faptul că segmentele individuale au legături directe

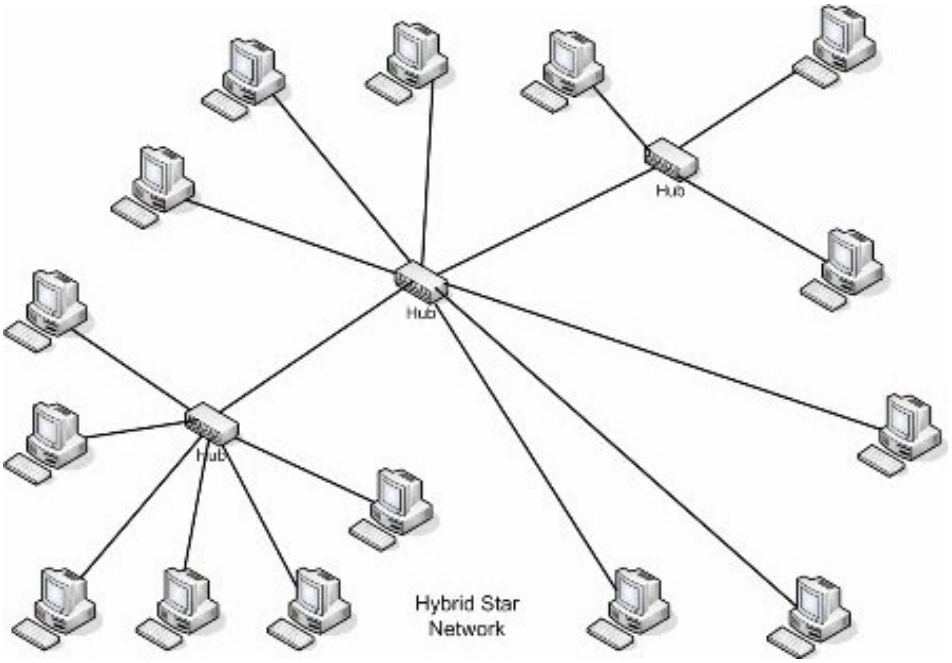

Fig 1.4 Topologie de tip arbore

În practică se întâlnesc de multe ori topologii compuse rezultate din combinarea topologiilor fundamentale, cum ar fi, spre exemplu este topologia magistrală-stea: mai multe rețele cu topologie stea sunt conectate la un cablu de conexiune principal.

2. ARHITECTURA REȚELELOR DE CALCULATOARE

Arhitecturile pentru LAN descriu atât topologiile fizice cât şi pe cele logice folosite într-o rețea

2.1 Arhitectura Ethernet

Ethernet este denumirea unei familii de tehnologii de rețele de calculatoare, bazate pe transmisia cadrelor (frames) şi utilizate la implementarea rețelelor locale de tip LAN. Ethernetul se defineşte printr-un şir de standarde pentru cablare şi semnalizare aparținând primelor două nivele din Modelul de Referință OSI - nivelul fizic şi legătură de date.

Numele ethernet provine de la cuvântul "eter" ilustrând faptul că mediul fizic (de exemplu cablurile) transportă biți către toate stațiile de lucru într-un mod asemănător cu străvechiul "luminiferous ether", despre care se credea odată că este mediul prin care se propagă undele eletromagnetice

Ethernetul a fost inventat pe baza ideii că pentru a lega computerele între ele astfel ca să formeze o rețea este nevoie de un mediu de transmisie central cum ar fi un cablu coaxial partajat. Conceptul şi implementarea Ethernetului s-au dezvoltat permanent, ajungându-se azi la tehnologiile de rețea complexe, care constituie fundamentul majorității LAN-urilor actuale. În loc de un mediu (cablu) central, tehnologiile moderne utilizează legături de tipul punct-la-punct, hub, switch (comutator), bridge (punte) şi repeater, bazate pe fire de cupru torsadate care reduc costurile instalării, măresc fiabilitatea şi înlesnesc managementul şi reparațiile rețelei.

Arhitectura Ethernet foloseşte:

- O topologie logică de tip broadcast şi o topologie fizică de tip magistrală sau stea.

Vitezele de transfer standard sunt de 10 Mbps şi 100 Mbps, iar noile standarde specifice pentru arhitectura Gigabit Ethernet permit viteze de până la 1000 MbpsConductoare de cupru – pentru transmisia datelor sub formă de semnale electrice;

- Metoda de control a accesului CSMA/CD (Carrier Sense Multiple Access Collision Detection = Acces multiplu cu detecția purtătoarei şi coliziunii).

Conform acestei metode, dacă o stație din rețea doreşte să transmită date trebuie ca înainte să "asculte" mediul de transmisie, proces similar cu a aştepta tonul înainte de a forma un număr pe linia telefonică. Dacă nu detectează nici un alt semnal, atunci poată să trimită datele. Dacă nici una din celelalte stații conectate la rețea nu transmite date în acel moment, datele transmise vor ajunge în siguranță la calculatorul destinație, fără nici o problemă. Dacă, însă, în acelaşi moment cu primul calculator, şi alt calculator din rețea decide că mediul de transmisie este liber şi transmite datele în acelaşi moment cu primul, va avea loc o coliziune. Prima stație din rețea care a depistat coliziunea, adică dublarea tensiunii pe mediul de transmisie, va transmite către toate stațile un semnal de jam, care le avertizează să oprească transmisia şi să execute un algoritm de încetare a comunicației pentru un timp (backoff algorithm). Acest algoritm generează un timp aleator de una, două milisecunde sau chiar mai scurt, de circa o miime de secundă, interval de timp după care stațiile să reînceapă transmisia. Algoritmul este repetat ori de câte ori apare o coliziune în rețea

- Cablu coaxial (la primele retele Ethernet) torsadat sau fibre optice ca mediu de transmisie a datelor.
- Cadrul Ethernet, ce constă dintr-un set standardizat de biți utilizat la transportul datelor şi al cărui structură este ilustrată în figura 2.1

PRE	START	A D	A S	TIP/LUNGIME	DATE	CRC
7 byte	1 byte	6 byte	6 byte	4 byte	46-1500 byte	4 byte

Fig. 2.1. Structura unui cadru Ethernet

Informațiile dintr-un asemena cadru sunt următoarele:

- PRE - Preambulul constă într-o secvență alternantă de 1 şi 0 ce indică stațiilor receptoare sosirea unui cadru
- START - Delimitatorul de start al cadrului - conține o secvență alternantă de 1 şi 0 şi care se termină cu doi de 1 consecutivi, indicând faptul că următorul bit constituie începutul primului octet din adresa destinație ;
- AD - Adresa destinație - identifică stația ce trebuie să recepționeze cadrul.
- AS - Adresa sursă - adresa stației ce a emis cadrul ;
- TIP/LUNGIME- indică numărul de biți de date conținuți în câmpul de date al cadrului.
- DATE - o secvență de date de maxim 1500 de octeți. Dacă lungimea cadrului de date este inferioară valorii de 46 de octeți, este nevoie să se completeze restul biților până se ajunge la valoarea minimă impusă de standard (tehnică cunoscută sub numele de padding) ;
- CRC - semnalizează apariția unor eventuale erori în cadrul de transmisie.

Cu toate progresele făcute, formatul cadrelor nu s-a schimbat, astfel încât toate rețelele Ethernet pot fi interconectate fără probleme. Fiecare calculator echipat Ethernet poartă denumirea de stație.

Arhitectura Ethernet este o arhitectură populară deoarece oferă echilibru între viteză, preț şi instalare facilă.

2.2. Arhitectura Token Ring

Este integrată în sistemele mainframe, dar şi la conectarea calculatoarelor personale în rețea. Foloseşte o tehnologie fizică stea-cablată inel numită Token Ring. Astfel, văzută din exterior rețeaua pare a fi proiectată ca o stea, calculatoarele fiind conectate la un hub central, numit unitate de acces multiplu (MAU sau MSAU- Multi Station Access Unit), iar în interiorul echipamentului cablajul formează o cale de date circulară, creând un inel logic.

Arhitectura foloseşte topologia logică de pasare a jetonului. Inelul logic este creat astfel de jetonul care se deplasează printr-un port al MSAU către un calculator. Dacă respectivul calculator nu are date de transmis, jetonul este trimis înapoi către MSAU şi apoi pe următorul port către următorul calculator. Acest proces continuă pentru toate calculatoarele, dând astfel impresia unui inel fizic.

Foloseşte ca mediu de transmisie a datelor cablul torsadat, cablul coaxial sau fibra optică.

2.3. Arhitectura FDDI

Arhitectura FDDI (Fiber Distributed Data Interface), bazată pe topologia logică Token Ring, foloseşte fibra optică şi funcționează pe o topologie fizică de tip inel dublu. Inelul dublu este alcătuit dintr-un inel principal, folosit pentru transmiterea datelor, şi un inel secundar, folosit în general pentru back-up (linie de siguranță).

Prin aceste inele, traficul se desfăşoară în sensuri opuse. În mod normal, traficul foloseşte doar inelul primar. În cazul în care acesta se defectează, datele o să circule în mod automat pe inelul secundar în direcție opusă. Un inel dublu suportă maxim 500 de

calculatoare pe inel. Lungimea totală a fiecărui inel este de 100 km şi se impune amplasarea unui repetor care să regenereze semnalele la fiecare 2 km. Inelul principal oferă rate de transfer de până la 100 Mbps, iar dacă cel de-al doilea inel nu este folosit pentru backup, capacitatea de transmisie poate fi extinsă până la 200 Mbps.

În FDDI se întâlnesc două categorii de staţii, fiecare având două porturi prin care se conectează la cele două inele:

- staţii de clasă A, ataşate ambelor inele
- staţii de clasă B ataşate unui singur inel

2.4. Standarde Ethernet

Standardizarea asigură compatibilitatea echipamentelor care folosesc aceeaşi tehnologie. Există numeroase organizaţii de standardizare, care se ocupă cu crearea de standarde pentru rețelele de calculatoare.

IEEE (The Institute of Electrical and Electronic Engineers) este o asociaţie profesională tehnică nonprofit fondată în 1884, formată din peste 3777000 de membrii din 150 de ţări, cu ocupaţii diferite – ingineri, oameni de ştiinţă, studenţi. IEEE este foarte cunoscut pentru dezvoltarea standardelor pentru industria calculatoarelor şi electronicelor în particular.

Pentru a asigura compatibilitatea echipamentelor într-o rețea Ethernet, IEEE a dezvoltat o serie de standarde recomandate producătorilor de echipamente Ethernet. Au fost elaborate astfel:

- Standarde pentru rețele cu cabluri
- Standarde pentru rețele cu fir

2.4.1. Standarde pentru rețele cu cabluri

În cazul rețelelor cu arhitectură Ethernet şi mediu de transmisie a datelor prin cablu, a fost elaborat standardul IEEE 802.3.

Au fost implementate o serie de tehnologii care respectă standardul Ethernet 802.3. dintre acestea cele mai comune sunt:

- 10BASE-T;
- 100 BASE-TX (cunoscută şi sub numele de Fast Ethernet deoarece dezvoltă o lăţime de bandă mai mare decât precedenta);
- 1000BASE-T (cunoscută şi sub numele de Gigabit Ethernet);
- 10BASE-FL;
- 100BASE-FX;
- 1000BASE-SX;
- 1000BASE-LX.;

Numărul din partea stângă a simbolului ilustrează valoarea în Mbps a lăţimii de bandă a aplicaţiei

Termenul BASE ilustrează faptul că transmisia este baseband – întreaga lăţime de bandă a cablului este folosită pentru un singur tip de semnal

Ultimele caractere se referă la tipul cablului utilizat (T-indică un cablu torsadat, F, L şi S indică fibra optică)

Avantajele şi dezavantajele tehnologiilor Ethernet dezvoltate în medii de transmisie prin cablu sunt ilustrate în tabelul 2.1.

Tabelul 2.1

Tehnologia	Avantaje	Dezavantaje
10BASE-T	Costuri de instalare mici în comparație cu fibra optică Sunt mai uşor de instalat decât cablurile coaxiale Echipamentul şi cablurile sunt uşor de îmbunătățit	Lungimea maximă a unui segment de cablu este de doar 100 m Cablurile sunt susceptibile la interferențe electromagnetice
100BASE-TX	Costuri de instalare mici în comparație cu fibra optică Sunt mai uşor de instalat decât cablurile coaxiale Echipamentul şi cablurile sunt uşor de îmbunătățit Lățimea de bandă este de 10 ori mai mare decât în cazul tehnologiilor 10BASE-T	Lungimea maximă a unui segment de cablu este de doar 100 m Cablurile sunt susceptibile la interferențe electromagnetice
1000BASE-T	Lățimea de bandă de până la 1 GB Suportă interoperabilitatea cu 10BASE-T şi cu 100BASE-TX	Lungimea maximă a unui segment de cablu este de doar 100 m Cablurile sunt susceptibile la interferențe electromagnetice Cost ridicat pentru plăci de rețea şi switch-uri Gigabit Ethernet Necesită echipament suplimentar

2.4.2. Standarde Ethernet pentru rețele fără fir

În cazul rețelelor cu arhitectură Ethernet şi mediu de transmisie a datelor fără fir, IEEE a elaborat standardul IEEE 802.11 sau Wi-Fi. Acesta este compus dintr-un grup de standarde , pentru care sunt specificate frecvența semnalelor de transmisie radio, lățimea de bandă , raza de acoperire şi alte capabilități ce sunt ilustrate în tabelul 2.2.

Tabelul 2.2

	Lățime bandă	Frecvență	Raza de acțiune	Interoperabilitate
IEEE 802.11a	Până la 54 Mbps	5 GHz	45,7 m	Incompatibil cu IEEE 802.11b, IEEE 802.11g, IEEE 802.11n
IEEE 802.11b	Până la 11 Mbps	2,4 GHz	91 m	Compatibil cu IEEE 802.11g
IEEE 802.11g	Până la 54 Mbps	2,4 GHz	91 m	Compatibil cu IEEE 802.11b
IEEE 802.11n	Până la 540 Mbps	2,4 GHZ	250 m	Compatibil cu IEEE 802.11b şi cu IEEE 802.11g

3. MODELUL ARHITECTURAL OSI

Elaborarea standardelor pentru rețele a devenit necesară datorită diversificării echipamentelor şi serviciilor, care a condus la apariția de rețele eterogene din punctul de vedere al tipurilor de echipamente folosite. În plus, multitudinea de medii fizice de comunicație a contribuit la decizia de a defini reguli precise pentru interconectarea sistemelor. ISO a elaborat un model arhitectural de referință pentru interconectarea calculatoarelor, cunoscut sub denumirea de modelul arhitectural ISO-OSI (Open System Interconnection).

OSI (Open System Interconnection) a fost emis in 1984 şi este un model în şapte straturi dezvoltat de ISO (International Standardization Organization) pentru descierea modului în care se pot combina diverse dispozitive pentru a comunica intre ele.

Modelul nu precizează cum se construiesc straturile, dar insistă asupra serviciilor oferite de fiecare şi specifică modul de comunicare între ele prin intermediul interfețelor. Fiecare producator poate construi straturile aşa cum doreşte, însă fiecare strat trebuie să furnizeze un anumit set de servicii. Proiectarea arhitecturii pe straturi determină extinderea sau îmbunătățirea facilă a sistemului. De exemplu, schimbarea mediului de comunicație nu determină decât modificarea nivelului fizic, lăsând intacte celelalte straturi.

Astfel, OSI a fost elaborat pentru a furniza producătorilor de echipamente de comunicație un set de standarde, respectarea cărora asigurând compatibilitatea şi interoperabilitatea între diverse tehnologii furnizate de firme diferite. Însuşi termenul de Open din denumire semnifică faptul că utilizarea standardelor este publică şi gratuită spre deosebire de sistemele «proprietary» a căror folosire trebuie licențiată de firma care le-a produs şi distribuit.

3.1 Structura modelului OSI

Modelul OSI defineşte un cadru general pentru rețelele de calculatoare prin implementarea protocoalelor de rețea în şapte straturi. În figura 3.1 este prezentată structura modelului OSI.

Fig.3.1. Structura modelului OSI

Modelul OSI împarte arhitectura retelei în şapte straturi (niveluri), construite unul deasupra altuia, adaugând funcţionalitate serviciilor oferite de nivelul inferior (mai exact un anumit set de funcţii). Aceste şapte straturi formeaza o ierarhie plecand de la stratul cel mai de sus 7 – Aplicaţie (Application) şi până la ultimul din partea de jos a stivei startul 1 – Fizic (Physical).

Se consideră că OSI este cel mai bun mijloc prin care se poate face înţeles modul în care informaţia este trimisă şi primită. În concluzie, în modelul OSI sunt şapte straturi care fiecare au funcţii diferite în reţea, aceasta repartiţie purtând numele de stratificare (layering). Se pot enunţa câteva dintre avantajele folosirii OSI:

- Descompunerea fenomenul de comunicare în reţea în părţi mai mici şi implicit mai simple;
- Standardizarea componentelor unei reţele permiţând dezvoltarea independentă de un anumit producator;
- Permite comunicarea între diferite tipuri de hardware şi software;
- Permite o înţelegere mai uşoară a fenomenelor de comunicare.

În cazul unui model architectural, un nivel nu defineşte un singur protocol—el defineşte o funcţie de comunicaţie a datelor ce va fi folosită de mai multe protocoale. Datorită faptului că fiecare nivel defineşte o anume funcţie, el poate conţine mai multe protocoale, fiecare dintre acestea oferind un serviciu potrivit cu respectiva funcţie a stratului.

Ca şi între oameni, pentru a putea să comunice între ele, calculatoarele trebuie să vorbească aceeaşi limbă sau altfel spus să folosescă acelaşi protocol. Aşadar un protocol este un set de reguli pe care fiecare calculator trebuie să-l respecte pentru a comunica cu un alt calculator.

În modelul OSI, la transferul datelor, se consideră că acestea traversează virtual de sus în jos straturilor modelului OSI al calculatorului sursă şi de jos în sus straturile modelului OSI al calculatorului destinaţie. Controlul este transferat de la un nivel la următorul, plecând de la nivelul aplicaţie într-unul din dispozitive spre nivelul de bază, cel fizic, de-a lungul canalului de comunicaţie către celălalt dispozitiv de reţea şi înapoi la nivelul aplicaţie în ierarhia pe nivele.

La fiecare nivel, datele inter-schimbate în reţea (ce se numesc generic PDU – Protocol Data Unit) au o anumită structură (un anumit format) şi poartă o anumită denumire în funcţie de nivelul la care se regăsesc.

3.2. Funcţiile straturilor asociate modelului OSI

Funcţiile principale ale fiecărui strat (nivel) asociat modelului OSI sunt prezentate în tabelul 3.1.

Tabelul 3.1

Modelul OSI	**Stratul (Nivelul)**	**Descriere**
Aplicaţie	7	Asigură interfaţa cu utilizatorul
Prezentare	6	Codifică şi converteşte datele
Sesiune	5	Construieşte, gestionează şi închide o conexiune între o aplicaţie locală şi una la distanţă
Transport	4	Asigură transportul sigur şi menţine fluxul de date dintr-o reţea
Reţea	3	Asigură adresarea logică şi domeniul de rutare
Legătură de date	2	Pachetele de date sunt transformate în octeţi şi octeţii în cadre. Asigură adresarea fizică şi procedurile de acces la mediu
Fizic	1	Mută şiruri de biţi între echipamente Defineşte specificaţiile electrice şi fizice ale echipamentelor

- **Stratul Aplicație**

Acest nivel oferă suport aplicațiilor (de rețea) şi proceselor utilizator. Sunt identificați partenerii de comunicație, calitatea serviciilor (QoS), autentificarea utilizatorilor şi restricții legate de sintaxa datelor. Tot ce are legătură cu acest nivel este legat de aplicațiile de rețea. Nivelul oferă servicii de aplicații pentru transfer de fişiere (FTP), e-mail, chat, conexiune la distanță (telnet sau ssh–secure shell).

La acest nivel PDU au denumirea generică de *date.*

- **Stratul Prezentare**

Acest nivel oferă independență cu privire la diferențele de reprezentare a datelor în diverse formate prin translatarea de la aplicație la formatul rețelei şi invers. Nivelul Prezentare are rolul de a aduce datele într-o formă convenabilă nivelului aplicație. Acest nivel formatează şi criptează datele transmise de-a lungul rețelei, oferind libertate de exprimare fără probleme de compatibilitate.Acest nivel poartă şi numele de nivelul sintaxei.

La acest nivel PDU au denumirea generică de *date.*

- **Stratul Sesiune**

Acest nivel asigură stabilirea, gestionarea şi închiderea sesiunilor de comunicație între utilizatorii de pe două stații (calculatoare gazdă) diferite. Prin sesiune se înțelege dialogul între două sau mai multe entități. Nivelul Sesiune sincronizează dialogul între straturile sesiune ale entităților şi gestionează schimbul de date între acestea. În plus, acest nivel oferă garanții în ceea ce priveşte expedierea datelor, clase de servicii şi raportarea erorilor.

Ca şi în cazul celorlalte două starturi superioare (Aplicație şi Prezentare), la nivelul Sesiune PDU- urile inter-schimbate în rețea poartă numele generic de *date*.

- **Stratul Transport**

Acest nivel are rolul de a oferi o modalitate transparentă de transfer al datelor între sisteme (calculatoare gazdă). De asemenea, nivelul Transport este responsabil cu corectarea erorilor şi controlul fluxului de date, asigurând complet transferul de date.

Este nivelul aflat în mijlocul ierarhiei, asigurând straturilor superioare o interfață independantă de tipul rețelei utilizate. Granița dintre acest strat şi cel de deasupra lui este foarte importantă pentru că delimitează straturile care se ocupă cu procesarea locală a informației (Aplicație, Prezentare şi Sesiune) şi pe cele care au ca funcție definirea modului în care trebuie să circule datele între echipamente (Transport, Rețea, Legătură de date şi Fizic).

Nivelul Transport este de asemenea nivelul la care are loc segmentarea încapsularea şi posibila reasamblare a datelor

La nivelul Transport PDU sunt organizate sub forma de *segmente*.

Functiile principale ale nivelului Transport sunt:

- inițierea transferului;
- controlul fluxului de date;
- se asigură că datele au ajuns la destinație;
- detectarea şi remedierea erorile care au aparut în procesul de transport;
- închiderea conexiunii.

Protocoale cele mai utilizate utilizate sunt TCP si UDP.

- TCP, Transmision Control Protocol este un protocol bazat pe conexiune, în care pentru fiecare pachet transmis se aşteaptă o confirmare din partea echipamentului de destinație. Transmisia următorului pachet nu se realizează dacă nu se primeşte confirmarea pentru pachetul transmis anterior;
- UDP, User Datagram Protocol este folosit în situațiile în care eficiența şi viteza transmisiei sunt mai importante decât corectitudinea datelor, de exemplu în rețelele multimedia, unde pentru transmiterea către clienți a informațiilor de voce sau imagine este mai importantă viteza (pentru a reduce întreruperile în transmisie) decât calitatea. Este un

protocol fără conexiuni, semnalarea erorilor sau reluărilor fiind asigurată de nivelul superior.

- **Stratul Rețea**

Acest nivel asigură dirijarea unităților de date între nodurile sursă şi destinație, trecând eventual prin noduri intermediare (routing). Este foarte important ca fluxul de date să fie astfel dirijat încât să se evite aglomerarea anumitor zone ale rețelei (congestionare). Interconectarea rețelelor cu arhitecturi diferite este o funcție a nivelului Rețea.

În concluzie, acest nivel are două mari functii:

- rezolvă adresarea între sisteme (calculatoare gazdă);
- identifică cele mai bune căi pe care informația trebuie să o parcurgă

pentru a junge la destinație.

Acest nivel oferă tehnologii de comutare şi rutare, creând rute logice (cunoscute sub denumirea de circuite virtuale) pentru transmiterea datelor de la un nod la altul. Rutarea şi redirectarea sunt funcțiile de bază ale acestui nivel, precum şi adresarea logică (prin utilizarea adreselor IP – Internet Protocol), comunicarea inter-rețelelor, administrarea erorilor, controlul congestiilor şi secvențierea pachetelor.

La acest nivel PDU sunt organizate sub forma de *pachete*.

- **Stratul Legăturii de Date**

La acaest nivel se corectează erorile de transmitere apărute la nivelul fizic, realizând o comunicare corectă între două noduri adiacente ale rețelei. Mecanismul utilizat în acest scop este împartirea pachetelor în cadre (frame), cărora le sunt adaugate informații de control. Cadrele sunt transmise individual, putând fi verificate şi confirmate de către receptor. Alte funcții ale nivelului se referă la fluxul de date (astfel încât transmitatorul să nu furnizeze date mai rapid decât le poate accepta receptorul) şi la gestiunea legăturii (stabilirea conexiunii, controlul schimbului de date şi desființarea conexiunii).

Nivelul legătură de date este împărțit în două sub-nivele:

- MAC (Media Access Control) – Control al Accesului la Mediu;
- LLC (Logical Link Control) – Legatura Logica de Date.

Subnivelul MAC controlează modul în care un dispozitiv de rețea obține acces la date şi cum le poate transmite.

Subnivelul LLC controlează sincronizarea frame-urilor, controlul fluxului şi verificarea/controlul erorilor.

La acest nivel PDU sunt organizate sub forma de *frame-uri*.

- **Stratul Fizic**

Acest nivel are rolul de a transmite datele de la un calculator la altul prin intermediul unui mediu de comunicație. Datele sunt văzute la acest nivel ca un şir de biți.

Problemele tipice sunt de natura electrică:

- nivelele de tensiune corespunzatoare unui bit 1 sau 0;
- durata impulsurilor de tensiune;
- inițializarea şi oprirea transmiterii semnalelor electrice;
- asigurarea păstrării formei semnalului propagat.

Astfel, se defineşte la nivel electric, mecanic, procedural şi funcțional legătura fizică între calculatoarele care comunică. Mediul de comunicatie nu face parte din nivelul fizic.

La acest nivel se definesc:

- tipul de transmitere şi recepționare a şirurilor de biți pe un canal de

comunicații;

- opologiile de rețea;
- tipurile de medii de transmisiune : cablu coaxial, cablu UTP, fibră optică,

linii închiriate de cupru etc;.

- modul de transmisie: simplex, half-duplex, full-duplex;
- standardele mecanice şi electrice ale interfețelor;

- modul de codificare şi decodificare a şirurilor de biți;
- modularea şi demodularea semnalelor purtătoare (modem-uri).

La acest nivel PDU sunt organizate sub forma de *biți*.

Modelul OSI nu este implementat în întregime de producatori, nivelele Sesiune si Prezentare putând să lipsească (unele din funcțiile atribuite acestora în modelul OSI sunt îndeplinite de alte straturi). Modelul OSI este un model orientativ, strict teoretic, realizările practice fiind mai mult sau mai putin diferite.

3.3. Realizarea transferului de date

Înainte ca datele să fie transmise, ele trec printr-un proces numit încapsulare. Încapsularea adaugă informații specifice fiecărui nivel prin adăugarea unui antet şi a unui trailer la fiecare nivel. Acest proces este vital în comunicare.

Prin încapsulare, protocoalele de pe fiecare nivel pot comunica între sursă şi destinație independent de celelalte niveluri. Fiecare nivel îşi adaugă informații specifice pe parcursul încapsulării. Astfel, în cadrul procesului de decapsulare, protocoalele de pe un anumit nivel pot primi aceste date la destinație şi pot da informații nivelurilor superioare în funcție de aceste date.

Se creează în acest fel o comunicare între nivelurile analoge de la sursă şi de la destinație; această comunicare nu are loc prin legături fizice, ci este posibilă datorită procesului de încapsulare/decapsulare a datelor.

Fiecare nivel comunică cu nivelurile analoge prin intermediul unor unități de date proprii (PDU = Protocol Data Unit). Aceste unități de date sunt constituite din datele primite de la nivelurile superioare, încadrate de un antet şi un trailer specifice nivelului respectiv.

Fiecare tip de PDU pentru nivelurile 2, 3 şi 4 (Legătură de Date, Rețea şi Transport) au semnificații deosebite şi poartă nume consacrate.

Nivelurile Transport comunică prin segmente, nivelurile Rețea comunică prin pachete, iar cele Legătură de Date creează prin frame-uri (cadre). În figura 3.2 este prezentat modul de comunicare dintre straturile analoage corespunzătoare pentru două stații (sursă, respectiv destinație).

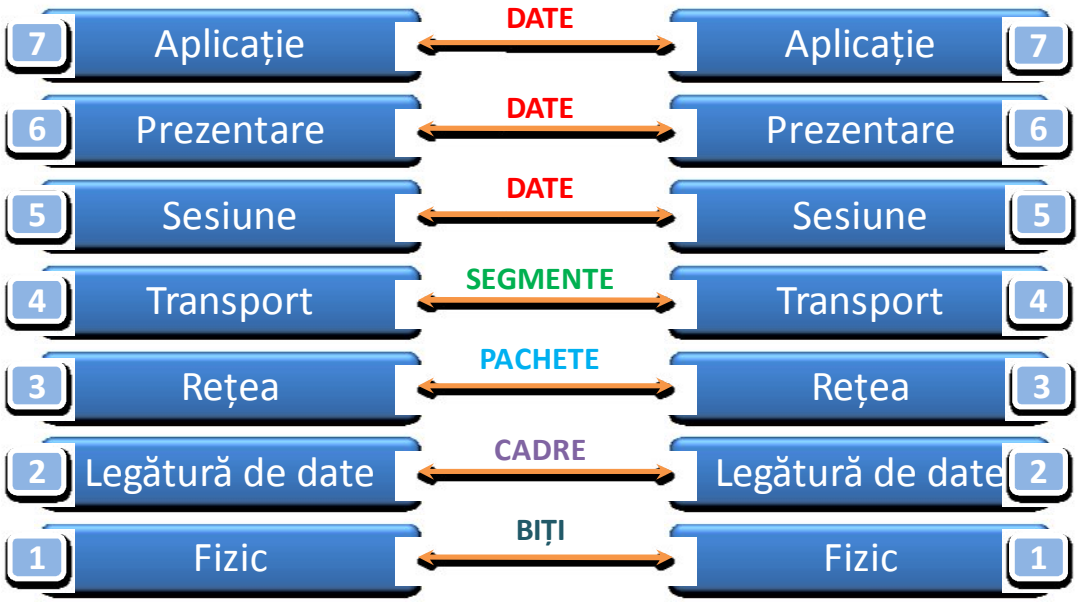

Fig.3.2. Comunicarea între straturile analoage corespunzătoare pentru două stații (sursă, respectiv destinație)

Datele sosesc prin intermediul mediului de comunicație ca un flux de biți. La nivelul legăturii de date, biții sunt transformați în cadre, la nivelul Rețea în pachete, iar la nivelul Transport în segmente. În cele din urmă, datele ajung la nivelul Aplicație unde sunt preluate de browser şi sunt prezentate. Fiecare nivel adaugă sau şterge o parte din informațiile de control ataşate datelor de celelalte nivele.

După cum se observă în figura 3.2 straturile de la sursă comunică cu echivalentul lor de la destinație. De exemplu nivelul 4 al sursei transmite informații nivelului 4 al destinației (receptorului). Comunicarea se realizează pe baza protocoalelor fiecărui nivel. Acest tip de comunicare se numeste *comunicare peer-to peer*. Pentru a putea fi adresată informația către un anumit nivel corespunzător şi pentru ca acesta să o poată recunoaşte ca fiind adresată lui, datele sunt supuse unor modificări pe parcursul comunicării.

Acest proces este numit **încapsulare,** în cazul în care informația este prelucrată în stația sursă şi **decapsulare** în cazul în care informația este prelucrată în stația de destinație**.**

În cazul încapsulării sunt incluse informațiile de la emițător, precum şi alte elemente care sunt necesare pentru a face posibilă şi sigură comunicarea cu receptorul.

Prin procesul de încapsulare fiecare nivel adaugă un anumit identificator la informația primită (antete/headers, secvențe terminale/trailers şi alte informații) şi o trimite mai departe.

Astfel, de la emițător datele pornesc de la nivelul 7 Aplicație şi ajung să fie împachetate până la nivelul 1 Fizic iar la receptor se va derula procesul invers, despachetând de la nivelul 1 spre nivelul 7.

Acest proces (încapsulare) poate fi prezentat conform următorului algoritm:

- **Construirea datelor** - utilizatorul lansează o aplicație - de exemplu scrie un e-mail al cărui text şi eventual imagine vor fi procesate în straturile superioare (Aplicație, Prezentare, Sesiune) pentru a avea un format care să poată fi trimis în rețea.
- **Segmentare datelor** - se face la nivelul 4 (Transport), în felul acesta garantându-se că datele vor ajunge în siguranță la destinație. Tot la acest nivel are loc **primul proces de încapsulare**. Datele se transformă în segmente prin adăugarea unui antet (header) ce conține în principal informații legate de tipul aplicației generate.
- **Adăugarea adreselor logice** - se face la nivelul nivelul 3 (Rețea) şi se efectuează prin adaugarea unui antet (header) la segmentul stratului 4 rezultând ceea ce se numeşte pachet. În acest header se menționează adresa logică a destinației şi adresa logică a sursei (IP-ul). Tot la acest nivel se decide care va fi următorul dispozitiv (device) căreia i se va livra pachetul (next hop).
- **Adaugarea adreselor fizice** - şi se efectuează prin adaugarea unui antet (header) şi secvență terminală (trailer) la segmentul stratului 3 rezultând ceea ce se numeşte cadru (frame). În acest header se menționează adresa fizică a următorului dispozitiv (next hop) şi adresa fizică a sursei (MAC-ul). Trebuie diferențiată aceasta adresare de cea de la nivel 3. De exemplu dacă informația va fi trimisă în aceeaşi rețea, IP-ul şi MAC-ul destinației vor fi ale maşinii către care se trimite informația. În cazul în care informația este trimisă spre o altă rețea, IP-ul va fi al destinatiei iar MAC-ul va fi al default gateway-ul (poarta de ieşire) din rețeaua sursei.
- **Plasare informației în mediul de propagare -** cadrul trebuie convertit într-un format binar pentru transmiterea printr-un mediu de propagare. O funcție de tip clocking permite echipamentelor să distingă aceşti biți, pe măsură ce aceştia călătoresc prin mediul de transmitere. Mediul fizic de transmitere poate varia de-a lungul căii folosite.

4. MODELUL ARHITECTURAL TCP/IP

Desi modelul OSI este universal recunoscut, standardul aplicat comunicării într-o rețea (sau între rețele) este TCP/IP, adică Transmission Control Protocol/Internet Protocol.

TCP/IP (Transmission Control Protocol/Internet Protocol) este cel mai utilizat protocol folosit în rețelele locale cât şi pe Internet datorită disponibilității şi flexibilităţi lui având cel mai mare grad de corecţie al erorilor. TCP/IP permite comunicarea între calculatoarele din întreaga lume indiferent de sistemul de operare instalat.

În anii 1960, guvernul SUA finanțează proiectarea şi dezvoltarea procotolului TCP/IP. Ministerul Apărării Naționale al SUA dorea un protocol de rețea care să funcționeze indiferent de condițiile de pe rețea.

Atât timp cât conexiunea fizică între calculatoare este funcțională, trebuia să fie funcțională şi conexiunea logică, chiar dacă alte calculatoare din rețea se opresc brusc. Era nevoie de o arhitectură flexibilă, mergând de la transferul de fişiere până la transmiterea vorbirii în timp real.

Datorita fiabilitatii sale a fost mai tarziu preluat de dezvoltatorii de UNIX si adus la un nivel care sa permita comunicarea in Internet.

Crearea acestui protocol a rezolvat multe probleme dificile din acea vreme, astfel devenind modelul standard pe care Internetul se bazează. La început el a fost folosit pentru rețelele militare, apoi a fost furnizat şi agenţiilor guvernamentale, universităţilor ca la urmă să poată fi folosit de publicul larg.

3.1 Structura modelului TCP/IP

Spre deosebire de OSI, modelul TCP/IP are doar patru niveluri (straturi, stive). În figura 4.1 este prezentată structura modelului TCP/IP.

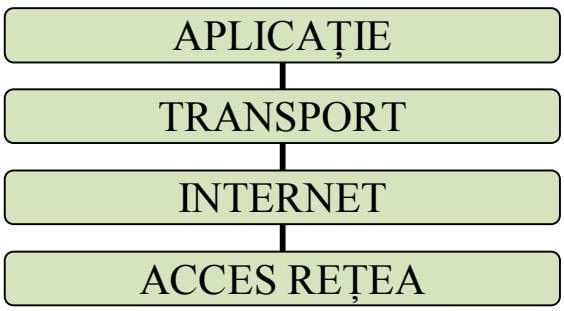

Fig.4.1. Structura modelului TCP/IP

Deşi două dintre straturi au acelaşi nume ca la modelul OSI, nu trebuie confundate între ele pentru că fiecare nivel are funcţii total diferite pentru fiecare model în parte.

Cele patru niveluri realizează funcţiile necesare pentru a pregăti datele înainte de a fi transmise pe rețea. Un mesaj porneşte de la nivelul superior (nivelul Aplicaţie) şi traversează de sus în jos cele patru niveluri până la nivelul inferior (nivelul Acces rețea).

Informaţiile din header sunt adăugate la mesaj în timp de acesta parcurge fiecare nivel, apoi mesajul este transmis.

După ce ajunge la destinaţie, mesajul traversează din nou, de data aceasta de jos în sus fiecare nivel al modelului TCP/IP. Informaţiile din header care au fost adăugate mesajului sunt înlăturate în timp ce acesta traversează nivelurile destinaţie.

4.2. Funcţiile straturilor asociate modelului TCP/IP

Funcţiile principale ale fiecărui strat (nivel) asociat modelului TCP/IP sunt prezentate în tabelul 4.1.

Tabelul 4.1

Modelul TCP/IP	Descriere
Aplicaţie	La acest nivel funcţionează protocoalele la nivel înalt
Transport	La acest nivel are loc controlul de debit/flux şi funcţionează protocoalele de conexiune
Internet	La acest nivel are loc adresarea IP
Acces Reţea	La acest nivel are loc adresarea după MAC şi componentele fizice ale reţelei

- **Stratul Aplicaţie**

Acest nivel comasează straturile Aplicaţie, Prezentare şi Sesiune din modelul OSI. Proiectanţii TCP/IP au considerat că protocoalele de nivel superior trebuie să includă detaliile nivelurilor Prezentare şi Sesiune ale modelului OSI. Pur şi simplu au creat un nivel Aplicaţie care manevrează protocoalele de nivel superior, problemele de reprezentare, codificările şi controlul dialogurilor.

TCP/IP combină toate aceste deziderate într-un singur nivel, care asigură împachetarea corectă a datelor pentru nivelul următor.

Nivelul Aplicaţie oferă servicii de reţea aplicaţiilor utilizator cum ar fi browserele web, programele de e-mail, terminalul virtual (TELNET), transfer de fişiere (FTP).

- **Stratul Transport**

Nivelul Transport al modelului TCP/IP administrează transmisia de date de la un computer la altul, asigurând calitatea serviciului de comunicare, siguranţa liniei de transport, controlul fluxului, detecţia şi corecţia erorilor.

Una dintre funcţiile acestui nivel este de a împărţi datele în segmente mai mici pentru a fi transportate uşor prin reţea. El este proiectat astfel încât să permită conversaţii între entităţile pereche din gazdele sursă, respectiv, destinaţie.

Nivelul transport include protocoale TCP şi UDP.

- TCP (Trasmission Control Protocol) este un protocol orientat pe conexiune care permite ca un flux de octeţi trimişi de la un calculator să ajungă fără erori pe orice alt calculator din Internet. Dacă pe calculatorul destinaţie un pachet ajunge cu erori, TCP cere retrimiterea acelui pachet.

Orientarea pe conexiune nu semnifica faptul că există un circuit între computerele care comunică, ci faptul că segmentele nivelului Aplicaţie călătoresc bidirecţional între două gazde care sunt conectate logic pentru o anumită perioadă.

Acest proces este cunoscut sub denumirea de packet switching.

TCP/IP fragmentează fluxul de octeţi în mesaje discrete şi transferă fiecare mesaj nivelului Internet. TCP tratează totodată controlul fluxului pentru a se asigura că un emiţător rapid nu inundă un receptor lent cu mai multe mesaje decât poate acesta să prelucreze.

- Al doilea protocol din acest nivel, UDP (User Datagram Protocol), este un protocol nesigur, fără conexiuni, destinat aplicaţiilor care doresc să utilizeze propria lor secvenţiere şi control al fluxului.

Protocolul UDP este de asemenea mult folosit pentru interogări rapide întrebare-răspuns, client-server şi pentru aplicaţii în care comunicarea promptă este mai importatntă decât comunicarea cu acurateţe, aşa cum sunt aplicaţiile de transmisie a vorbirii şi a imaginilor video.

- **Stratul Internet**

Nivelul Internet este cel care face adresarea logică în stiva TCP/IP. Pe scurt, el poate face doua lucruri:

- identifică cea mai buna cale pe care trebuie sa o urmeze un pachet pentru a ajunge la destinație;
- realizează comutația acelui pachet, aceasta fiind posibilitatea de a trimite pachetul printr-o altă interfață decât aceea de primire.

Inițial nivelul Internet trebuia să asigure rutarea pachetelor în interiorul unei singure rețele. Cu timpul a apărut posibilitatea interconexiunii între rețele, astfel încât acestui nivel i-au fost adăugate funcționalități de comunicare între o rețea sursă şi o rețea destinație.

Pe lângă rolul nivelului Internet de a trimite pachete de la sursă spre rețeaua internetwork (dintre rețele) este şi cel de a controla sosirea lor la destinație indiferent de traseul sau rețelele traversate până la destinație.

Protocolul specific care guvernează acest nivel se numeşte protocol Internet (IP). În acest nivel se realizează alegerea căii optime şi distribuirea pachetelor. Acesta este locul unde acționeaza routerul în internet.

În stiva TCP/IP, protocolul IP asigură rutarea pachetelor de la o adresă sursă la o adresă destinație, folosind şi unele protocoale adiționale, precum ICMP sau IGMP.

Comunicarea la nivelul IP este nesigură, sarcina de corecție a erorilor fiind plasată la nivelurile superioare (de exemplu prin protocolul TCP).

- **Stratul Acces Rețea**

Nivelul Acces la Rețea se ocupă cu toate problemele legate de transmiterea efectivă a unui pachet IP pe o legătură fizică, incluzând şi aspectele legate de tehnologii şi de medii de transmisie, adică nivelurile OSI 1 şi 2 (Legătură de Date şi Fizic).

Driverele, modemurile, plăcile de rețea, şi alte componente se găsesc în nivelul Acces la Rețea.

Nivelul de Acces la Rețea defineşte procedurile folosite pentru interogarea cu echipamentele de rețea şi de acces la mediu de transmisie.

4.3. Comparație între modelele OSI şi TCP/IP

O comparație între nivelurile modelului OSI şi ale modelului TCP/IP, este prezentată în figura 4.2. Se observă că modelul TCP/IP este o arhitectură stratificată de comunicație pe 4 niveluri, spre deosebire de modelul OSI compus din 7 niveluri.

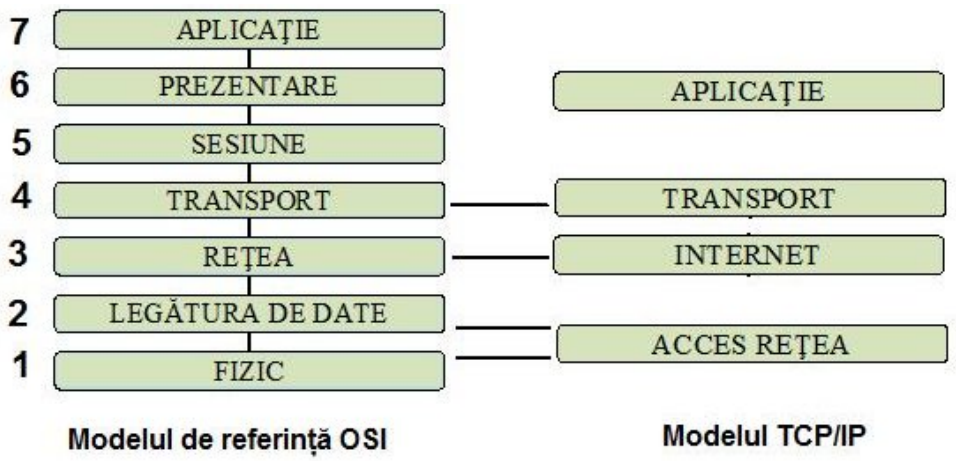

Fig.4.2. Comparație între structurile modelelor OSI şi TCP/IP

Modelul OSI şi modelul TCP/IP sunt ambele modele de referinţă folosite pentru a descrie procesul de transmitere a datelor.

Dar de ce trebuie să le studiem pe amândouă când unul poate ar fi suficient?

Modelul OSI este folosit pentru dezvoltarea standardelor de comunicaţie pentru echipamente şi aplicaţii ale diferiţilor producători. Specialiştii îl preferă pentru analize mai atente şi ca fundament în orice discuţie legată de reţele.

Pe de altă parte este adevărat că TCP/IP este folosit pentru suita de protocoale TCP/IP şi este mai folositor pentru că este implementat în lumea reală.

Ca utilizatori finali avem de-a face numai cu nivelul Aplicaţie, dar cunoaşterea detaliată a nivelurilor este vitală pentru realizarea unei reţele. Este adevărat că majoritatea utilizatorilor nu ştiu mai nimic despre protocoale de rutare sau alte detalii, dar este de asemenea adevărat că aceşti utilizatori nu trebuie să realizeze reţele scalabile şi sigure aşa cum trebuie să realizeze un specialist.

Dacă am compara din punct de vedere structural modelul OSI cu modelul TCP/IP, am observa că între ele există o serie de asemănări dar şi deosebiri.

- Asemănări:
  - Ambele modele de date descriu procesul de comunicaţie a datelor în reţea pe straturi;
  - Ambele conţin straturile Aplicaţie şi Transport, cu funcţii asemănătoare;
  - Ambele folosesc tehnologia de tip packet switching;
  - Administratorii de reţea trebuie să le cunoască pe amândouă.
- Deosebiri:
  - Spre deosebire de modelul OSI care foloseşte şapte niveluri, modelul TCP/IP foloseşte patru;
  - Nivelurile OSI Sesiune şi Prezentare sunt tratate de nivelul TCP/IP Aplicaţie;
  - Nivelurile OSI Legătură de Date şi Fizic sunt tratate de nivelul TCP/IP Acces Reţea.
  - Modelul TCP/IP pare simplu pentru că are mai puţine niveluri.

Diferenţe rezultă şi din modul în care sunt alese soluţiile privind asigurarea fiabilităţii şi amplasarea conducerii proceselor de comunicaţie în sistem. Acestea sunt:

- Cele două arhitecturi de reţea tratează diferit problema fiabilităţii.
  - La modelul OSI, protocoalele detectează şi soluţionează erorile la nivelul Legăturii de Date. Deci, în reţelele realizate folosind protocoalele specificate de modelul OSI, fiabilitatea este asigurată la nivelul Legăturii de Date.

Protocoalele pentru a asigura transferul corect al cadrelor între calculatorul transmiţător şi comutatorul de pachete la care este conectat, sunt complexe, deoarece suma de control CRC însoţeste fiecare cadru transferat, iar receptorul confirmă fiecare cadru recepţionat corect folosind algoritmi cu pauză de aşteptare şi de retransmisie, care să prevină pierderea datelor şi să permită recuperarea acestora dacă se produce o întrerupere a funcţionării echipamentelor hardware.

Şi la nivelul Reţea se efectuează detecţia erorilor şi recuperarea pachetelor transferate în reţea, utilizând o sumă de control şi tehnici de pauză de aşteptare şi de retransmisie.

În fine, nivelul Transport oferă fiabilitate între utilizatorii finali prin faptul că obligă sursa să comunice cu destinaţia finală pentru a verifica livrarea corectă a pachetelor.

- Modelul arhitectural al TCP/IP a fost proiectat astfel încât fiabilitatea să fie realizată doar la calculatorul receptor.

Altfel spus, reţelele WAN se construiesc pornind de la premisa că echipamentele de comutaţie, adică routerul, pot să piardă sau să altereze datele fără să încerce să le recupereze.

Această implementare a modului de realizare a fiabilității transmisiei de date prin rețeaua de comunicație, simplifică mult programele de comunicație de la nivelul Legăturii de Date. Programele software de la nivelul Legăturii de Date, asigură doar o fiabilitate redusă.

- În modelul TCP/IP, fiabilitatea este realizată la nivelul Transport al stivei de protocoale, unde se realizează detectarea şi corectarea erorilor de transmisie.

Eliberarea interfeței nivelului Rețea de sarcina verificării corectitudinii transmiterii datelor, conduce la o implementare mult mai usoară a softului TCP/IP.

Routerele intermediare pot elimina pachele care au fost afectate de erorile de transmisie, cele pe care nu le pot livra sau cele care sosesc cu o frecvență mai mare decât capacitatea lor de prelucrare. De asemenea, ele pot redirecționa pachetele pe trasee cu întârzieri mai mari sau mai mici, fără a fi obligate să informeze sursa sau destinația.

- Alegerea locului în care se realizează conducerea proceselor de comunicație.
  - Rețelele implementate după modelul OSI sunt realizate după principiul că o rețea de calculatoare este un mijloc care oferă servicii de transport de informații.

Furnizorul de servicii controlează accesul în rețea şi monitorizează traficul, îl înregistrează, în vederea contorizării şi taxării utilizatorilor. Producătorii de echipamente pentru comunicație sunt cei care rezolvă probleme precum: dirijarea traficului, controlul fluxului şi confirmarea primirii corecte a datelor.

Acest punct de vedere preia multe din responsabilitățile calculatoarelor. În concluzie, o rețea de calculatoare poate folosi calculatoare simple, întrucât calculatoarele participă în foarte mică măsură la funcționarea rețelei.

- Rețelele implementate după modelul TCP/IP sunt concepute după principiul că oricare calculator trebuie să participe la realizarea tuturor funcțiilor de comunicație în rețea, deci trebuie să conțină toate protocoalele de rețea.

Toate calculatoarele din rețea au implementată funcția de detectare şi corectare a erorilor. Comparativ cu modelul OSI, o rețea realizată după modelul TCP/IP este un sistem de comunicație realizat cu echipamente de comunicație simple, ruterul, dar care au calculatoare mai performante pentru comunicație care sunt denumite şi host (gazdă), pentru că au implementată toată stiva de protocoale.

Ruterele au implementate doar protocoalele de la nivelul Internet şi nivelul de Acces în Rețea.

Un specialist va folosi modelul OSI, dar şi protocoalele TCP/IP. Va privi protocolul TCP ca pe un protocol al nivelului Transport (4) din modelul OSI, IP ca pe un protocol al nivelului Rețea (3) din modelul OSI, şi Ethernet ca o tehnologie a nivelelor Legătură de date şi Fizic (2 şi 1) din modelul OSI.

4.4. Concluzii

Avantajele oferite de împărțirea rețelelor în niveluri sunt:

- Standardizarea componentelor rețelelor, permițând astfel crearea acestora de către diversi producători;
- Permiterea comunicării între tipuri diferite de componente software şi hardware;
- Previne ca schimbările apărute într-un nivel să nu afecteze celelalte niveluri, permițând astfel dezvoltarea rapidă a acestora;
- Fenomenul de comunicare în rețea este descompus în părți mai mici şi implicit mai simple;
- Comunicarea prin rețea devine mai puțin complexă, înțelegerea şi învățarea modului în care informația este trimisă şi primită devenind mai uşor de făcut;
- Studierea acestor niveluri permite înțelegerea modului de circulație a pachetelor de

date de la o rețea la alta şi ce echipamente operează în fiecare nivel în momentul când informația circulă prin el. Astfel troubleshooting-ul problemelor care pot apărea în cursul fluxului pachetului de date se poate face mai uşor.

5. NIVELUL APLICAȚIE

Nivelul Aplicație – vezi figura 5.1 are rolul de a face legătura dintre o aplicație şi serviciile oferite de rețea pentru acea aplicație. Are ca scop traducerea informațiilor în formate pe care maşinile care comunică între ele le pot înțelege.

Fig.5.1. Poziția nivelului Aplicație în structura modelului OSI

Nivelul Aplicație identifică şi stabileşte disponibilitatea partenerului de comunicație, sincronizează aplicațiile între ele şi stabileşte procedurile pentru controlul integrității datelor şi erorilor. De asemenea identifică dacă există suficiente resurse pentru a sprijini comunicația între parteneri.

El se ocupă cu protocoalele de nivel înalt, codificarea şi controlul dialogului, împachetarea datelor şi trimiterea lor la următoarele niveluri.

Un protocol reprezintă un set de reguli şi convenții ce se stabilesc între participanții la o comunicație în rețea în vederea asigurării bunei desfăşurări a comunicației respective. Este de fapt o înțelegere între părțile care comunică, asupra modului de realizare a comunicării.

Câteva din protocoale de la acest nivel care fac posibilă comunicarea sunt:

- HTTP (Hyper Text Transfer Protocol) - aplicații web (prezentare, baze de date etc);
- Telnet - terminale virtuale;
- FTP (File Transfer Protocol) - transfer de fişiere;
- SMTP (Simple Mail Transfer Protocol)- standard pentru transmiterea e-mail-urilor;
- IMAP (Internet Message Access Protocol) şi POP (Post Office Protocol) – protocoale folosite de clienții locali de email de preluare a e-mail-urilor de pe servere de email;
- DNS (Domain Name System) – translatarea numelor în adrese IP;
- DHCP (Dynamic Host Configuration Protocol) - atribuirea dinamica de adrese IP echipamentelor de rețea;
- SNMP (Simple Network Management Protocol) -administrare şi monitorizare;
- SSH (Secure Shell) – transmitere securizată a datelor;

5.1 Protocolul HTTP

Este un protocol utilizat pentru a transmite informații între un program de navigare Web (browser) şi un server Web, fiind un protocol de tip text (hypertext).

Prin hypertext se înțelege o colecție de documente unite între ele prin legături (link) ce permit parcurgerea acestora bidirectional.

HTTP permite aducerea pe calculatorul local a unor documente HTML (Hyper Text Markup Language), fişiere grafice, audio, animație sau video, programe executabile pe server sau un editor de text.

Este softul utilizat de browsere (Internet Explorer , Safari, FireFox …) pentru aducerea paginilor web pe calculatorul propriu, fiind protocolul implicit al www.

Există HTTP server (furnizează pagini web) şi HTTP client (cere pagini web).

Protocoalele nu sunt identice din punctul de vedere al eficienței, vitezei de lucru, resurselor utilizate, uşurinței în instalare, uşurinței în administrare, etc. Diferențele sunt date de tipul rețelei, tipul infrastructurii acesteia, dacă protocolul este routabil sau nu, de tipul clienților din rețea, de tipul de echipamente existent în rețea şi modul cum este utilizat protocolul.

Protocolul HTTP se caracterizează prin faptul că nu memorează o succesiune a stărilor prin care trece legătura client-server. Astfel fiecare tranzacție este independentă: clientul trimite o cerere, serverul răspunde cu resursa cerută. Pentru fiecare resursă, există o tranzacție corespunzătoare.

Mod de funcționare:

- Serverul HTTP aşteaptă, pe portul 80, cereri de la clienți (navigator / browser), care sunt de fapt adrese ale documentelor dorite;
- Clientul primeşte un document în mod text şi dacă găseşte în el legături către imagini şi le vrea şi pe acestea le cere. Astfel transferul unei pagini hipertext constă de fapt în una sau mai multe sesiuni de transfer informație de la şi către serverul HTTP.
- După primirea informațiilor, browser-ului hotărăşte în ce format acestea vor fi afişate.

Aplicațiile care folosesc acest protocol trebuie să poată formula cereri şi/sau recepționa răspunsuri (modelul client-server). Clientul cere accesul la o resursă, iar serverul răspunde printr-o linie de stare (care conține, printre altele, un cod de succes sau eroare şi, în primul caz, datele cerute).

Resursa trebuie să poată fi referită corect şi fără echivoc.

- Pentru denumirea unei resurse în Internet, se foloseşte termenul generic URI – Uniform Resource Identifier.
- Pentru denumirea unei adrese, se foloseşte termenul generic URL - Universal Resource Locator.
- Dacă se face referire la un nume se foloseşte termenul generic URN- Universal Resource Name

Adresarea unei resurse în Internet se face prin construcții de forma protocol://[servciu].nume_dns[.nume_local/cale/subcale/nume_document

Cererile sunt transmise de software-ul client HTTP, care este şi o altă denumire pentru un browser web.

Altfel spus, protocolul HTTP este specializat în transferul unei pagini web între browserul clientului şi serverul web care găzduieşte pagina respectivă.

HTTP defineşte exact formatul cererii pe care browserul o trimite, precum şi formatul răspunsului pe care serverul i-l returnează.

Conținutul paginii este organizat cu ajutorul codului HTML (Hyper Text Markup Language), dar regulile de transport al acesteia sunt stabilite de protocolul http.

HTML (HyperText Markup Language) este o modalitate de descriere a documentelor pentru ca ele să fie afişate în cel mai favorabil format pe ecranul

terminalului. Este format dintr-un set de comenzi ce descriu modul cum este structurat un document. Comenzile sunt etichete sau tag-uri pereche, una de deschidere <eticheta> şi alta de închidere </eticheta>. Browserul interpretează aceste etichete şi afişează rezultatul pe ecran.

Spre deosebire de procesoarele de texte care formatează diferitele componente ale documentului (titlu, antet, note etc.), codul HTML marchează doar aceste elemente, fără a le formata, această sarcină revenind programului client (browser).

5.2. Protocolul TELNET

Telnetul este o aplicaţie destinată accesului, controlului şi depanării de la distanţă a calculatoarelor şi a dispozitivelor de reţea.

Acest protocol permite utilizatorului să se conecteze la un sistem de la distanţă şi să comunice cu acesta printr-o interfaţă. Folosind telnetul, comenzile pot fi date de pe un terminal amplasat la distanţe foarte mari faţă de computerul controlat, ca şi când utilizatorul ar fi conectat direct la acesta. Se asigură o conexiune logică între cele două echipamente: cel controlat şi cel folosit ca terminal numită sesiune telnet.

Astfel se pot conecta calculatoare slabe la super-servere şi rula pe ele programe complexe, fără a fi nevoie de staţii puternice la fiecare post de lucru.

Telnet permite introducerea de comenzi utilizate pentru a accesa programe şi servicii care se află pe un computer la distanţă, ca şi cum clientul s-ar afla chiar în faţa lui.

Monitorul local devine al doilea monitor al calculatorului de la distanţă şi tastatura locală a doua tastatură a calculatorului de la distanţă. Protocolul Telnet poate fi utilizat pentru mai multe lucruri, inclusiv pentru accesarea poştei electronice, a bazelor de date sau a fişierelor.

Este utilizat de administratori pentru configurarea de la distanţă a dispozitivelor de reţea.

Pentru a se realiza accesul este necesar să existe:

- Telnet server - instalat de administratorul de reţea pe un calculator care astfel devine server Telnet. Prin Telnet server administratorul de sistem creează conturi Telnet (username şi parolă) şi stabileşte în ce zonă se poate conecta clientul şi ce poate face în acea zonă;
- Telnet client - instalat pe un alt calculator care astfel devine client Telnet. Softul Telnet client deschide canalul de comunicaţii cu serverul şi realizează conectarea la calculatorul server.

5.3. Protocolul FTP

File Transfer Protocol (FTP) este protocolul care oferă facilităţi pentru transferul fişierelor pe sau de pe un calculator din reţea. FTP este cea mai folosită metodă pentru transferul fişierelor de la un calculator la altul, prin intermediul Internetului, indiferent de tipul şi dimensiunea acestora.

Transferul poate fi de două tipuri:

- Upload - fişierele sunt transferate de pe calculatorul local pe cel de la distanţă;
- Downlod- fişierele sunt transferate de pe calculatorul aflat la distanţă pe cel local;

FTP nu necesită codarea fişierelor înainte de a fi încărcate, aşa cum se întâmplă în cazul fişierelor din e-mail sau de la grupuri de discuţii.

Pentru a se realiza transferul fişierelor este necesar să existe:

- FTP server – care este instalat de administratorul de reţea pe un calculator care astfel devine server FTP. Prin FTP server administratorul de sistem creează conturi FTP şi stabileşte în ce zonă se poate conecta clientul şi ce poate face în acea zonă;
- FTP client - care este instalat pe un alt calculator care astfel devine client FTP.

Clientul deschide canalul de comunicaţii cu serverul şi realizează upload sau download în şi din zona permisă.

Secvenţa prin care ere loc transferul are următoarea succesiune de paşi:

- Solicitarea de a se preciza calculatorul cu care se doreşte să se schimbe fişiere;
- Pornirea aplicaţiei (programului) FTP şi realizarea conectării la calculatorul de la distanţă;
- Introducerea de către utilizator (după realizarea conectării) a username (numele de login) şi parolă;
- După acceptarea de către sistemul de la distanţă a numelui de conectare şi a parolei, utilizatorul poate să înceapă transferul fişierelor;

Cu ajutorul FTP se pot transfera fişiere în ambele direcţii.

FTP se foloseşte atunci când:

- se transferă (upload) pentru prima dată fişierele unui site la o gazdă web;
- se înlocuieşte un fişier sau o imagine;
- se încarcă (download) fişiere de pe un alt calculator pe calculatorul propriu;
- se permite accesul unei alte persoane pentru a încărca un fişier dintr-un anumit site;

În general, când se iniţiază un transfer prin FTP trebuie precizate următoarele aspecte:

- Tipul fişierului - se specifică maniera în care datele conţinute de un fişier vor fi aduse într-un format transportabil prin reţea:
  - fişiere ASCII – calculatorul care transmite fişierul îl converteşte din formatul local text în format ASCII;
  - fişiere EBCDIC – similar cu ASCII;
  - fişiere binare (binary) – fişierul este transmis exact cum este memorat pe calculatorul sursă şi memorat la fel pe calculatorul destinaţie;
  - fişiere locale – folosite în mediile în care cel care transmite precizează numărul de biti/byte;
- Controlul formatului – se referă la fişierele text care sunt transferate direct către o imprimantă.
- Structura
- Modul de transmitere - care poate fi:
  - Stream – fişierul este transferat într-o serie de bytes;
  - Bloc – fişierul este transferat bloc cu bloc, fiecare cu un header;
  - Comprimat – se foloseşte o schemă de comprimare a secvenţelor de bytes identici.

5.4. Protocolul SMTP

Poşta electronică funcţionează pe baza unor protocoale de comunicaţie. În continuare se prezintă succint câteva din aceste protocoale punându-se accent pe SMTP.

SMTP(Simple Mail transport Protocol) – Protocolul de transport simplu de e-mail – oferă servicii de transmitere de mesaje peste TCP/IP şi suportă majoritatea programelor de e-mail de pe Internet.

SMTP este un protocol folosit pentru a transmite un mesaj electronic de la un client la un server de poştă electronică. După stabilirea conexiunii TCP la portul 25 (utilizat de SMTP), calculatorul-sursă (client) aşteaptă un semnal de la calculatorul-receptor (server).

Serverul începe să emită semnale declarându-şi identitatea şi anunţând dacă este pregătit sau nu să primească mesajul.

Dacă nu este pregătit, clientul părăseşte conexiunea şi încearcă din nou, mai târziu.

Dacă serverul este pregătit să accepte mesajul, clientul anunţă care este expeditorul mesajului şi care este destinatarul. Dacă adresa destinatarului este validă, serverul dă

permisiunea de transmitere a mesajului. Imediat clientul îl trimite, iar serverul îl primeşte. După ce mesajul a fost transmis, conexiunea se închide.

Pentru ca un client al serviciului de poştă electronică să primească un mesaj de la serverul specializat în aceste tipuri de servicii, apelează fie la Post Office Protocol (POP) sau POP3, fie la Internet Message Access Protocol (IMAP).

Spre deosebire de POP (mai vechi) care presupune că utilizatorul îşi va goli cutia poştală pe calculatorul personal la fiecare conectare şi va lucra deconcectat de la rețea (off-line) după aceea, IMAP păstrează pe serverul de e-mail un depozit central de mesaje care poate fi accesat on-line de utilizator de pe orice calculator.

În figura 5.2 se prezintă modul de transmitere a unui e-mail între două calculatoare.

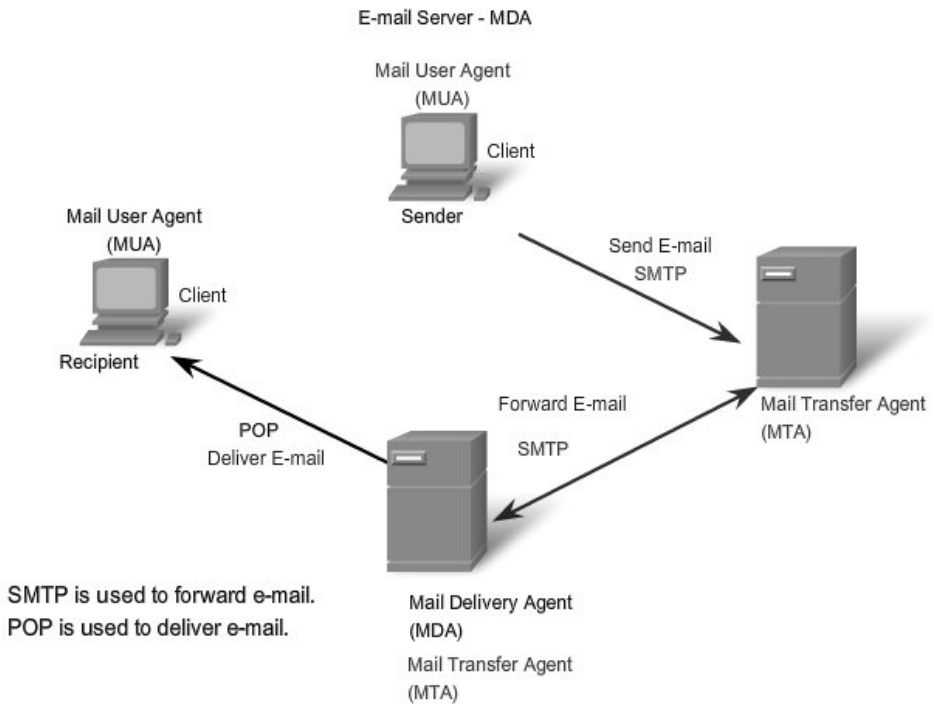

Fig.5.2. Protocoale utilizate la poşta electronică [ ]

Se observă că:

- Protocolul SMTP este utilizat pentru trimiterea unui e-mail de la expeditor la servere, precum şi la transmiterea acestora între serverele intermediare (Send and Forward e-mail);
- Protocolul POP este utilizat la livrare (recepție) de la ultimil server la calculatorul client (Deliver e-mail);

Revenind la protocolul SMTP se subliniază că acesta specifică modul în care mesajele de poştă electronică sunt transferate între procese SMTP aflate pe sisteme diferite. Procesul SMTP care transmite un mesaj este numit client SMTP, iar procesul SMTP care primeşte mesajul este numit server SMTP.

Protocolul nu se referă la modul în care mesajul ce urmează a fi transmis este trecut de la utilizator către clientul SMTP, sau cum mesajul ce urmează a fi recepționat de serverul SMTP este livrat destinatarului, nici la modul în care este memorat mesajul şi nici de câte ori clientul SMTP încearcă să transmită mesajul.

Obiectivul protocolului SMTP este de a trimite mail-uri într-un mod eficient. El este independent de sistemele care participă la comunicație, dacă se asigură un canal prin care datele să fie transmise într-un mod ordonat.

SMTP foloseşte următorul model de comunicație: transmițătorul, ca urmare a unei cereri de transmisie a mail-ului, stabileşte o legătură bidirecțională cu receptorul, care poate fi destinatarul final al mail-ului sau doar un intermediar. De aceea este necesar să se precizeze numele de host al destinației finale precum şi utilizatorul căruia îi este destinat mesajul.

Mod de funcționare al acestui protocol este următorul:

- Comunicarea între client / transmițător şi server / receptor se realizează prin texte ASCII. Inițial clientul stabileşte conexiunea către server şi aşteaptă ca serverul să-i răspundă cu mesajul "220 Service Ready". Dacă serverul e supraîncărcat, poate să întârzie cu trimiterea unui răspuns;
- După primirea mesajului cu codul 220 , clientul trimite comanda HELO prin care îşi indică identitatea;
- Odată ce comunicarea a fost stabilită, clientul poate trimite unul sau mai multe mesaje (prin comanda MAIL), poate încheia conexiunea sau poate folosi unele servicii precum verificarea adreselor de e-mail;
- Serverul trebuie să răspundă după fiecare comandă indicând dacă aceasta a fost acceptată, dacă se mai aşteaptă comenzi sau dacă există erori în scrierea acestor comenzi;
- Atunci când un mesaj este trimis către mai mulți destinatari, protocolul SMTP urmăreşte trimiterea datelor din mesaj o singură dată pentru toți destinatarii care aparțin aceluiaşi sistem destinație.

Comenzile specifice protocolului SMTP sunt următoarele:

- HELO - identificare computer expeditor;
- EHLO - identificare computer expeditor cu cerere de mod extins;
- MAIL FROM - specificare expeditorului;
- RCPT TO - specificarea destinatarului;
- DATA - conținutul mesajului;
- RSET – Reset;
- QUIT - termină sesiunea;
- HELP - ajutor pentru comenzi;
- VRFY – verificare o adresa;

5.4. Protocolul DNS

DNS (Domain Name Service) este un protocol care traduce adresele Internet literale în adrese Internet numerice, adrese utilizate de un calculator pentru a găsi un calculator receptor.

Adresa literală conține succesiuni de nume asociate cu domenii, subdomenii sau tipuri de servicii. Acest mod de adresare este utilizat exclusiv de nivelul aplicație şi este util deoarece permite operatorului uman să utilizeze o manieră prietenoasă şi comodă de localizare a informațiilor.

Forma generala a unei astfel de adrese este [tip_serviciu].[nume_gazda].[subdomeniu2].[subdomeniu1].[domeniu].[tip_domeniu]

Sistemul de nume DNS are o organizare ierarhică, sub formă de arbore. Acesta are o rădăcină unică (root) care are subdomenii. Fiecare nod al arborelui reprezintă un nume de domeniu sau subdomeniu.

Caracteristicile sistemului de nume (DNS) sunt:

- foloseşte o structură ierarhizată;

Referitor la structura ierarhizată, Internetul este divizat în peste 100 de domenii de nivel superior, fiecare domeniu superior este divizat la rândul său în subdomenii, acestea la rândul lor în alte subdomenii, etc.

- deleagă autoritatea pentru nume;

Domeniile de pe primul nivel se împart în două categorii:

  - generice (com, edu, gov, int, mil, net, org);
  - țări (cuprind câte o intrare pentru fiecare țară, de ex.pentru Român - ro).

- baza de date cu numele şi adresele IP este distribuită.

Baza de date DNS se numeşte distribuită deoarece nu există un singur server care să aibă toată informația necesară traducerii oricărui domeniu într-o adresă IP.

Fiecare server are o bază de date cu propriile domenii, la care au acces toate sistemele de pe Internet. Fiecare server DNS are un server DNS superior cu care face periodic schimb de informație.

Fiecărui domeniu, fie că este un calculator-gazdă, fie un domeniu superior, îi poate fi asociată o mulțime de înregistrări de resurse (resource records). Deşi înregistrările de resurse sunt codificate binar, în majoritatea cazurilor ele sunt prezentate ca text, câte o înregistrare de resursă pe linie, astfel:

- Nume_domeniu - precizează domeniul căruia i se aplică înregistrarea. În mod normal există mai multe înregistrări pentru fiecare domeniu;
- Timp_de_viață - exprimă, în secunde, cât de stabilă este înregistrarea. De exemplu, un timp de 100 de secunde este considerat a fi scurt, iar informația instabilă, pe când o valoare de ordinul a 100000 de secunde este o valoare mare, informația fiind considerată stabilă;
- Tip - precizează tipurile înregistrării. Cele mai importante tipuri sunt prezentate în tabelul 5.1.

Tabelul 5.1

Tip	**Semnificație**
A	Adresa IP a unui sistem gazdă
MX	Schimb de poştă
NS	Server de nume
CNAME	Nume canonic
PTR	Pointer

  - Înregistrarea A păstrează adresa IP a calculatorului gazdă;
  - MX precizează numele calculatorului gazdă pregătit să accepte poşta electronică pentru domeniul specificat. Dacă cineva doreşte de exemplu să trimită un mail la adresa *student@afahc.ro,* calculatorul care trimite trebuie să găsească un server la *afahc.ro* ce acceptă acest mail. Această informație poate fi furnizată de înregistrarea MX;
  - NS specifică serverele de nume. De exemplu fiecare bază de date DNS are în mod normal o înregistrare NS pentru fiecare domeniu de pe primul nivel;
  - Înregistrările CNAME permit crearea pseudonimelor.
  - Tipul PTR se referă, la fel ca şi CNAME la alt nume. Spre deosebire de CNAME care este în realitate o macro-definiție, PTR este un tip de date, utilizat în practică pentru asocierea unui nume cu o adresă IP, pentru a permite căutarea adresei IP şi obținerea numelui sistemului de calcul corespunzător. Acest tip de căutări se numesc căutări inverse (reverse lookups).

tabilă;

- Valoare - poate fi un număr, un nume de domeniu sau un cod ASCII

Componente DNS sunt următoarele:

- Servere DNS - Un server DNS este o stație pe care rulează un program de server DNS.

Serverele DNS stochează informații despre o porțiune din structura ierarhică a spațiului de nume şi rezolvă interogări de rezoluție de nume pentru clienții DNS. Când sunt interogate, serverele DNS răspund cu informația cerută dacă aceasta este disponibilă sau generează o referință către un alt server DNS care poate rezolva interogarea.

Un client poate cere o transformare a numelor în două moduri:

- cu rezolvare recursivă – serveru-l contactează la rândul lui un alt server de nume, de obicei de pe un nivel superior din arborele serverelor de nume. Acesta la rândul lui, va examina cererea şi, dacă nu poate face transformarea contactează un alt server. Procesul continuă până se contactează un server care poate face transformarea;
- cu rezolvare iterativă – serverul comunică clientului ce server să contacteze mai departe. Clientul adresează o cerere acestui server şi tot aşa mai departe până când cererea ajunge la un server care face transformarea. Când un server recepționează o cerere cu rezolvare iterativă şi nu poate traduce numele de domeniu, acesta transmite clientului ce server să contacteze mai departe.

- Zone DNS-O zonă DNS este o secțiune continuă din cadrul spațiului de nume.

Înregistrările pentru o astfel de zonă sunt memorate şi gestionate la un loc, chiar dacă domeniul este împărțit în subdomenii.

Zona poate fi de două feluri:

- primară – secțiunea în care se pot face actualizări;
- secundară – copia zonei primare.

Înregistrările unei zone oferă DNS-ului informațiile de care are nevoie pentru a rezolva cererile lansate de clienți sau alte servere DNS. Cea mai importantă astfel de înregistrare este adresa resursei folosită pentru a translata numele domeniului într-o adresă IP.

Pentru a stabili corespondența dintre un nume şi o adresă IP, programul de aplicație apelează un resolver, transferându-l numele ca parametru, resolverul trimite un pachet UDP (printr-un protocol de transport fără conexiune) la serverul DNS local, care caută numele şi returnează adresa IP către resolver, care o trimite mai departe apelantului. Înarmat cu adresa IP, programul poate stabili o conexiune TCP cu destinația sau îi poate trimite pachete UDP.

În concluzie, serviciul DNS transformă adresa IP într-o adresă literală, şi invers. Privit în amănunt, DNS este un soft care gestionează şi controlează o bază de date distribuită, constituită dintr-o sumă de fişiere memorate pe calculatoare diferite-localizate în spații geografice diferite, ca pe o singură bază de date.

5.5. Protocolul DHCP

Protocolul DHCP (Dynamic Host Configuration Protocol) are scopul de a permite calculatoarelor dintr-o rețea să obțină automat o adresă IP, printr-o cerere către serverul DHCP. Serverul poate să furnizeze stației respective toate informațiile de configurare necesare, inclusiv adresa IP, masca de subrețea, default gateway, adresa serverului DNS, etc.

Astfel, când serverul primeşte o cerere de la o stație, selectează adresa IP şi un set de informații asociate dintr-o mulțime de adrese predefinite care sunt păstrate într-o bază de date. Odată ce adresa IP este selectată, serverul DHCP oferă aceste valori stației care a efectuat cererea. Dacă stația acceptă oferta, serverul DHCP îi împrumută adresa IP pentru o perioadă, după care o regenerează.

Generarea adreselor IP prin serverul DHCP este o metodă utilizată pe scară largă în administrarea rețelelor de mari dimensiuni.
Folosirea unui server DHCP simplifică administrarea unei rețele pentru că software-ul ține evidența adreselor IP. În plus, este exclusă posibilitatea de a atribui adrese IP invalide sau duplicate.

5.6. Protocolul SNMP

Protocolul SNMP(Simple Network Manage Protocol) – permite administratorilor de rețea gestionarea performanțelor unei rețele, identificarea şi rezolvarea problemelor care apar, precum si planificarea dezvoltărilor ulterioare ale rețelei.

SNMP are trei componente de bază:

- Stațiile de administrare (Network Management Station) - pot fi oricare din calculatoarele rețelei pe care se execută programele de administrare;
- Agenții - dispozitivele administrate;
- Informațiile de administrare (Management Information Base) – colecție de date organizate ierarhic care asigură dialogul dintre stația de administrare şi agenți

Protocolul SNMP permite unei stații de administrare să interogheze un agent cu privire la starea obiectelor locale şi să le modifice, dacă este necesar. În plus, dacă un agent sesizează că s-a produs un eveniment, trimite un raport către toate stațiile de administrare care îl interoghează ulterior pentru a afla detalii despre evenimentul care a avut loc.

6. NIVELUL TRANSPORT

Nivelul Transport este miezul întregii întregii ierarhii de protocoale, având ca sarcină transportul datelor de la sursă la destinație într-un mod sigur, eficace din punctul de vedere al costurilor şi independent de rețeaua fizică utilizată. Fără nivelul Transport şi-ar pierde sensul întregul concept de ierarhie de protocoale.

Nivelul Transport este conținut atât în modelul TCP/IP, care este fundamentul Internetului, cât şi în modelul OSI – vezi figura 6.1.

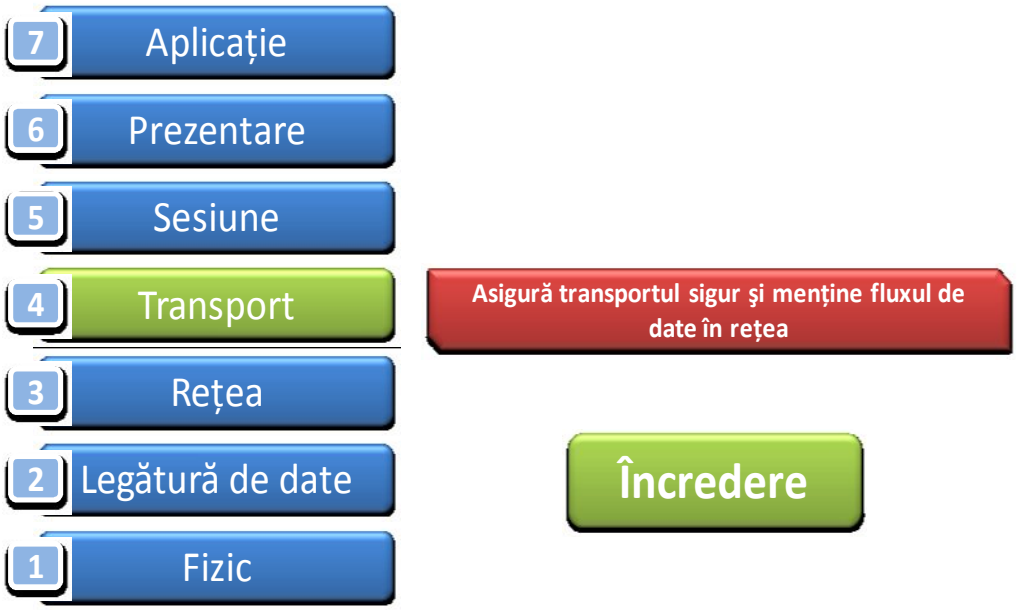

Fig.6.1. Poziția nivelului Transport în structura modelului OSI

Nivelul Transport separă nivelurile orientate pe aplicații (5, 6 şi 7 - menite să asigure livrarea corectă a datelor între calculatoarele interlocutoare), de cele destinate operării subrețelei (nivelurile 1, 2 şi 3 - responsabile de deplasarea mesajelor prin rețea, stive ce pot suferi modificări de implementare fără a influența nivelurile superioare).

Nivelul Transport administrează transmisia de date de la un computer la altul, putând asigura unele servicii, ca de exemplu: calitatea în comunicare, siguranța liniei de transport, controlul fluxului sau detecția şi corecția erorilor.

Una dintre funcțiile acestui nivel este de a împărți datele în segmente mai mici pentru a fi transportate uşor prin rețea. El este proiectat astfel încât să permită conversații între entitățile pereche din gazdele sursă, respectiv, destinație.

În cadrul acetui nivel sunt implementate diferite protocoale, două din cele mai cunoscute şi utilizate fiind:

- TCP (Trasmission Control Protocol) este un protocol sigur orientat pe conexiune

care permite ca un flux de octeți trimişi de pe un calculator să ajungă fără erori pe orice altă maşină din rețea. Orientarea pe conexiune nu semnifica faptul că există un circuit între computerele care comunică, ci faptul că segmentele nivelului Aplicație călătoresc bidirecțional între două gazde care sunt conectate logic pentru o anumită perioadă. Acest proces este cunoscut sub denumirea de packet switching.

TCP fragmentează fluxul de octeți în mesaje discrete şi transmite aceste segmente nivelului Rețea. TCP tratează totodată controlul fluxului pentru a se asigura că un emițător nu aglomerează (congestionează) un receptor mai lent cu mai multe mesaje decât poate acesta să prelucreze.

- UDP (User Datagram Protocol), este un protocol nesigur, fără conexiuni, destinat aplicațiilor care doresc să utilizeze propria lor secvențiere şi control al fluxului. Protocolul UDP este de asemenea mult folosit pentru interogări rapide întrebare-răspuns, client-server şi pentru aplicații în care comunicarea promptă este mai importatntă decât acuratețea acesteia, aşa cum sunt aplicațiile de transmisie a vorbirii sau a imaginilor video.

Principala diferență între cele două protocoale ale nivelului transport (TCP şi UDP), este fiabilitatea.

6.1 Funcțiile nivelului Transport

Principalele funcții sau responsabilități pentru nivelul transport, pentru a realiza conexiunea sursă – destinație, sunt următoarele:

- Identificarea diferitelor aplicații;

Un calculator are in general o singură legatură fizică la rețea. Orice informație destinată unei anumite maşini (de exemplu alt calculator) trebuie să specifice obligatoriu adresa de IP a acelei maşini. Dar pe un calculator pot exista în acelaşi timp mai multe procese care au stabilite conexiuni în rețea. Prin urmare datele trimise către o destinație trebuie să specifice pe langă adresa logică (IP-ul) a calculatorului şi procesul căreia îi aparține informația respectivă. Identificarea proceselor se realizează prin intermediul porturilor.

Un port este un număr pe 16 biți care identifică în mod unic procesele care rulează pe o anumita maşină. Orice aplicație care realizează o conexiune în rețea va trebui să ataşeze un număr de port acelei conexiuni.

Valorile pe care le poate lua un număr de port sunt cuprinse intre 0 si 65535 (deoarece sunt numere reprezentate pe 16 biți).

Există trei tipuri diferite de număr de porturi - vezi tabelul 6.1.

Tabelul 6.1

Tipul portului	Număr de port
Rezervate (Well Known Ports)	0 - 1023
Înregistrate (Registered Ports)	1024 - 49151
Private (Dynamic or Private Ports)	49152 - 65535

- Rezervate (0 - 1023) Aceste numere de port sunt rezervate unor aplicații Binecunoscute sau standard;
- Înregistrate (Registered Ports) (1024 - 49151) - Aceste numere de port pot fi alocate unor aplicații;
- Private (Dynamic or Private Ports) (49152 - 65535) - Aceste numere de port sunt, în mod curent, alocate dinamic clienților unor aplicații.

Exista numere de porturi care pot fi alocate dinamic.

- Multiplexarea şi demultiplexarea datelor;

Adresarea aplicațiilor este un exemplu de funcționare a multiplexării, putând exista mai multe conexiuni transport pentru o singura conexiune de rețea. Folosind adresele de port, protocoalele de la nivelul Transport, multiplexează la transmisie datele venite de la mai multe aplicații, combinându-le într-un singur flux de date care va fi transmis.

Aceleaşi protocoale, primesc datele la recepție şi demultiplexează fluxul de date, direcționând fiecare segment către aplicația sau procesul destinatar.

- Trasarea comunicației individuale între aplicațiile sursei şi respectiv destinației;

Identificarea diferitelor aplicații are ca efect posibilitatea de a se realiza o comunicare individuală între diverse aplicații. Atunci cînd un proces aplicație doreşte să

stabilească o conexiune cu o aplicație aflată la distanță, el trebuie să specifice cu care proces doreşte să se conecteze. Metoda folosită în mod normal este de a defini adrese de transport la care procesele pot să aştepte cereri de conexiune. Aceste adrese sunt porturile.

- Segmentarea datelor în segmente şi administrarea fiecărui segment în parte;

Pentru a realiza comunicația între procese, nivelul Transport trebuie să realizeze mai multe sarcini diferite dar dependente între ele. Pentru transmisie, nivelul Transport trebuie să țină evidența datelor venite de la fiecare aplicație şi apoi să combine aceste date într-un singur flux de date pe care să-l trimită la nivelele inferioare.

De la nivelele superioare, nivelul Transport primeşte cantități mari de data pe care nu poate să execute operația de multiplexare. Pentru a rezolva această problemă, se sparge fluxul de date în segmente de dimensiuni mici care sunt mai uşor de manipulat la transmisie de către rețea.

Pentru a exemplifica segmentarea, să presupunem că un computer încearca să trimită prin rețea un fişier de dimensiuni foarte mari. Transferul acestui fişier ar dura foarte mult.

Dacă acest fişier (flux de date) nu ar fi segmentat, nu există nicio posibilitate ca alte terminale să folosească rețeaua pe durata de transfer al acestor date. Alte terminale ar trebui să aştepte ca fişierul să fie transmis complet înainte ca ele să înceapă să transmită. Deoarece rețeaua trebuie să poată fi folosită de multe terminale în acelaşi timp trebuie facută segmentarea (şi apoi binențeles multipexarea sau întrețeserea segmentelor).

Datele de la fiecare proces (terminal) se împart în bucați mici care ocupă puțin legatura pe rețea şi astfel şi celelalte terminale pot trimite aparent simultan date pe rețea (acest procedeu poartă deumirea de multiplexare în timp).

- Reasamablarea segmentelor în fluxuri de date de aplicații

Terminalul care primeşte informatia trebuie să realizeze operațiile inverse, adică să reasambleze datele din segmentele primite şi să refacă fluxul inițial de date.

5.2. Protocolul TCP

TCP este protocolul principal care permite transportul sigur al datelor de la un capăt la altul al unei conexiuni într-o rețea nesigură. A fost proiectat special pentru Internet şi este larg folosit în acest scop.

TCP este un protocol orientat pe conexiuni, care permite ca un flux de octeți trimişi de un calculator să ajungă fără erori pe orice alt calculator din rețeaua Internet.

Fiabilitatea comunicării prin intermediul protocolului TCP este dată de sesiunile orientate pe conexiune. Înainte ca o gazdă să trimită date către o altă gazdă folosind protocolul TCP, nivelul Transport inițiază un proces pentru a crea o legătură cu destinația.

Această conexiune permite urmărirea sesiunii, sau fluxului de comunicare între gazde. Acest proces se asigură că fiecare gazdă are cunoştință despre comunicare şi este pregătită pentru aceasta. O conversație TCP completă cere stabilirea unei sesiuni între gazde, în ambele direcții.

După ce sesiunea a fost stabilită, destinația trimite confirmări la sursă pentru fiecare segment pe care îl primeşte. Aceste confirmări formează baza de fiabilitate în cadrul sesiunii TCP.

Când sursa primeşte o confirmare, se ştie că datele, pentru care s-a primit respectiva confirmare, au fost livrate cu succes şi astfel se poate încheia urmărirea acelor datele. În cazul în care sursa nu primeşte o confirmare în cadrul unei sume prestabilite de timp, se retransmit datele către destinație.

Cîteva dintre cele mai cunoscute aplicații care sunt transmise cu ajutorul protocolului TCP sunt prezentate (prin intermediul numerelor de port) în tabelul 6.2.

Tabelul 6.2

Număr de port	Protocol
21	FTP
23	Telnet
25	SMTP
80	HTTP
110	POP-3

5.2.1. Caracteristicile protocolului TCP

Principalele caracteristici ale TCP sunt:

- Transfer de date în flux continuu - datele circulă în acelaşi timp, în ambele sensuri ale conexiunii;
- Siguranța transmisiei - recuperează pachetele transmise cu erori, pierdute sau cu număr de secvență eronat;
- Controlul fluxului de date – în transferul de date dintre două procese, când aplicația destinație trimite o confirmare către emitent, se indică şi numărul permis de octeți ce se pot recepționa, pentru a se asigura că transmiterea rapidă de mesaje de către un emițător, nu face ca un receptor lent să primească mai multe mesaje decât poate prelucra. În urma unui astfel de mesaj, emițătorul îşi va dimensiona pachetele transmise la lungimea indicată de receptor;
- Multiplexarea - permite mai multor procese, care rulează pe acelaşi calculatorhost, să utilizeze facilitățile protocolului TCP simultan;
- Controlul conexiunii (fiabilitatea conexiunii) - presupune stabilirea numărului de secvență şi a dimensiunii ferestrei, pentru fiecare segment TCP;
- Stabilirea conexiunii.

5.2.2. Stabilirea conexiunii

Când două gazde comunică folosind TCP, o conexiune este stabilită înainte ca datele să poată fi transmise. După ce comunicarea este completă, sesiunile sunt închise, iar conexiunea se încheie. Mecanismele de conectare şi de sesiune activează funcția de fiabilitate a protocolului TCP.

Gazda urmăreşte fiecare segment de date în cadrul unei sesiuni şi face schimb de informații cu privire la ce date sunt primite de fiecare gazdă, utilizând informațiile din antetul TCP.

Pentru a stabili o conexiune, gazdele efectuează o metodă numită three-way handshake. Biții de control din antetul TCP indică evoluția şi starea conexiunii. Acest algoritm conține următorii paşi prezentat în figura 6.2:

- Clientul inițiator trimite un segment care conține:
  - o valoare de secvență inițială ($SEQ_{client} = 100$), ce serveşte ca o cerere

către server pentru a începe o sesiune de comunicații;

- Serverul răspunde cu un segment care conține:
  - o valoare de confirmare ($ACK_{server} = SEQ_{client} + 1 = 101$), egală cu

valoarea secvenței primite plus 1.Valoarea de confirmare este una mai mare decât valoarea secvenței, deoarece ACK este întotdeauna următorul octet aşteptat. Această valoare de confirmare permite clientului de a fi sigur că cererii lui de realizare a conexiunii i se răspunde;

  - valoarea ei proprie de secvență de sincronizare ($SEQ_{server} = 300$).

- Clientul inițiator răspunde cu un segment care conține;
  - o valoare de confirmare ($ACK_{client} = SEQ_{server} + 1 = 301$), egală cu valoarea secvenței primite plus 1;
  - valoarea ei proprie de secvență de sincronizare plus 1 ($SEQ_{client} + 1 = 101$).

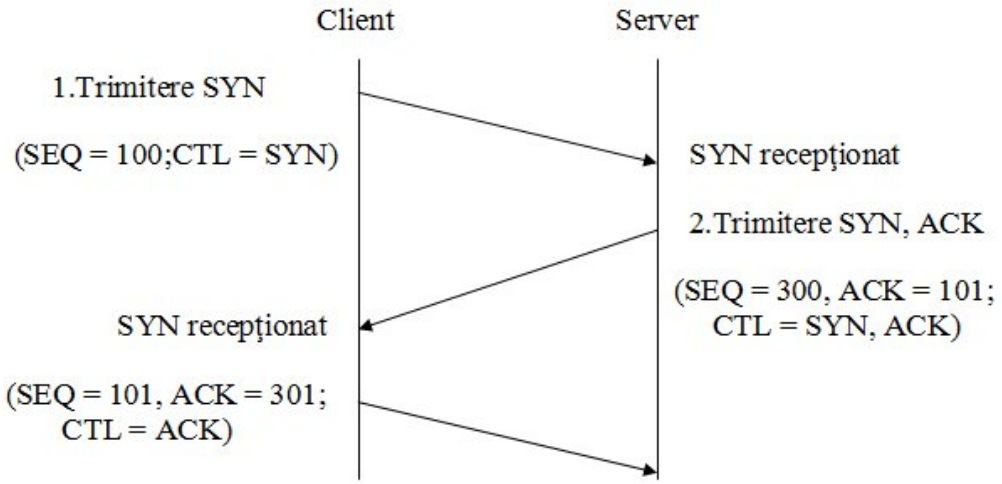

Fig.6.2. Secvențele necesare stabilirii conexiunii TCP

SYN - Sincronizează valorile de secvență;
SEQ - Valoarea secvenței;
ACK - Valoarea de confirmare;
CTL - Specifică biții de control din antetul segmentului TCP ce sunt setați pe 1.

5.2.3. Antetul segmentului TCP

În cadrul nivelului Transport după procesul de segmentare are loc împachetarea datelor. Această împachetare constă în lipirea unui antet, noile entități de transmisie şi de recepție purtând numele de segmente.

Un segment TCP constă dintr-un antet de 20 de octeți (plus o parte opțională) urmat de zero sau mai mulți octeți de date - vezi figura 6.3.

Bit 0			Bit 15	Bit 16	Bit 31
Număr port sursă				Număr port destinație	
Număr secvență					
Număr confirmare					
Lungime antet	Rezervat	Steaguri		Lungime fereastră	
Control TCP – Sumă de control				Idicator de urgență	
Opțiuni					
DATA (de aplicații)					

Fig.6.3. Antetul TCP (primele 5 rânduri ale segmentului)

Programul TCP este cel care decide cît de mari trebuie să fie aceste segmente. Dimensiunea segmentului este limitată de unitatea maximă de transfer sau MTU (Maximum Transfer Unit).

Deoarece MTU este în general de 1500 octeți (dimensiunea informației utile din Ethernet) se defineşte o limită superioară a dimensiunii unui segment.

Semnificația informațiilor introduse în antet este următoarea:

- Număr port sursă - 16 biți (2 octeți) - numărul de port al celui ce face apelul;
- Număr port destinație - 16 biți (2 octeți) - numărul de port de destinație al celui ce este apelat;

Câmpurile Număr port sursă şi Port destinație identifică punctele finale ale conexiunii şi constituie totodată un identificator al conexiunii.

- Numărul de secvență – 32 biți (4 octeți) - numărul primului octet de date din cadrul segmentului curent de date;
- Numărul de confirmare – 32 biți (4 octeți) - valoarea următorului octet pe care sursa se aşteaptă să-l primească (şi nu a ultimului octet recepționat în mod corect);
- Lungime antetului – 4 biți - indică numărul de cuvinte de 32 de biți care sunt conținute în antetul TCP. Această informație este utilă, deoarece cîmpul Opțiuni este de lungime variabilă, proprietate pe care o transmite astfel şi antetului;
- Rezervat – 6 biți - câmp neutilizat, rezervat pentru viitor;
- Steaguri (indicatori) – 6 biți – ce au următoarea semnifibație:
  - Bitul URG poziționat pe 1 arată că Indicatorul urgent este valid;
  - Bitul ACK pe 1 indică faptul că Numărul de confirmare este valid. Dacă este poziționat pe 0, segmentul în discuție nu conține o confirmare si câmpul Număr de confirmare este ignorat;
  - Bitul PSH indică faptul că informația trebuie livrată aplicației îndată ce a fost recepționată, fără a mai fi memorată în buffere din rațiuni de eficiență;
  - Bitul RST este folosit pentru a desființa o conexiune care a devenit inutilizabilă din cauza unur defecțiuni ale maşinilor gazdă sau din alte motive;
  - Bitul SYN este folosit pentru stabilirea unei conexiuni. Cererea de conexiune conține $SYN = 1$ si $ACK = 0$, iar răspunsul la o astfel de cerere este confirmată prin combinația $SYN = 1$ si $ACK = 1$;
  - Bitul FIN este folosit pentru a încheia o conexiune.
- Lungime fereastră – 16 biți (2 octeți) - indică numărul de octeți, începând cu cel indicat prin numărul de confirmare, pe care cel ce trimite mesajul îi poate recepționa;

În TCP, fluxul de control este tratat prin ferestre glisante de dimensiune variabilă.

- Suma de control – 16 biți (2 octeți) - indică suma câmpurilor de antet şi date, calculată pentru verificare;
- Indicator de urgență – 16 biți (2 octeți) - permite identificarea poziției unor date de urgență, în cadrul protocolului TCP;
- Optiuni – 32 biți (4 octeți) - a fost proiectat pentru a permite adăugarea unor facilități suplimentare neacoperite de antetul obişnuit. Cea mai importantă opțiune este aceea care permite fiecărei maşini să specifice încărcarea maximă de informație utilă TCP pe care este dispusă să o accepte;
- Date - Datele protocolului nivelului superior;

5.2.4. Reasamblarea în ordine a segmentelor

În procesul de transmitere a informației există posibilitatea ca segmentele să ajungă la destinație în cu totul altă ordine față de cea în care au fost trimise. Pentru ca mesajul original să fie înțeles de receptor, segmentele sunt reasamblate în ordinea inițială. Sunt alocate numere de secvență în antetul fiecărui segment.

În timpul instalării sesiunii, un număr de secvență inițial (ISN) este setat. Acest număr de secvență inițial reprezintă valoarea de pornire a octeților pentru această sesiune, care vor fi transmişi la receptoar. În timp ce datele sunt transmise în timpul sesiunii, numărul de ordine este incrementat cu numărul de octeți ce au fost transmişi. Această

urmărire a octeților de date permite fiecărui segment să fie unic identificat şi recunoscut. Segmentele ce lipsesc pot fi identificate foarte uşor.

Numerele de ordine ale segmentelor ajută la creşterea fiabilității prin indicarea modului de reasamblare şi reordonare a segmentele primite, aşa cum se prezintă în figura 6.4.

Procesul de primire cu protocolul TCP aşează datele dintr-un segment într-un buffer de primire. Segmentele sunt plasate în ordinea corectă a numărului de ordine şi se transmit mai departe la nivelul aplicație atunci când acestea sunt reasamblate. Orice segment care soseşte cu un număr de secvență diferit de cel aşteptat este reținut pentru prelucrare ulterioară. Apoi, atunci când ajung segmentele cu octeții lipsă, aceste segmente reținute sunt prelucrate.

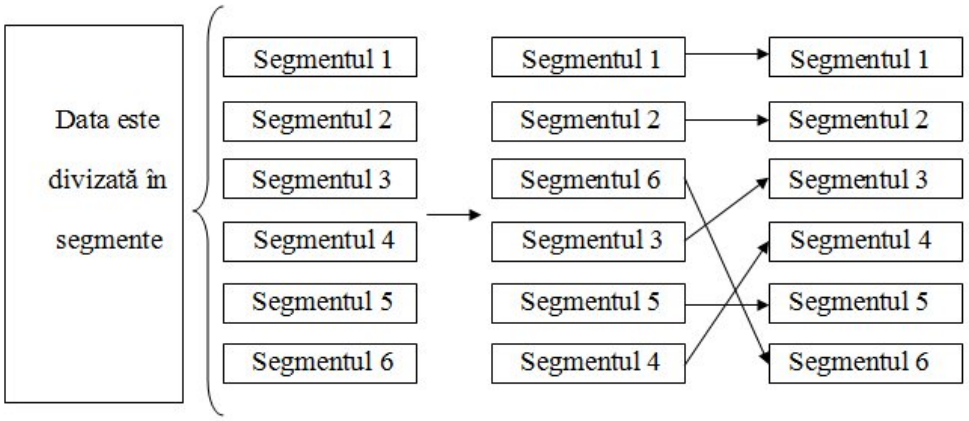

Fig.6.4. Reasamblarea segmentelor

5.2.5. Controlul congestiei în TCP

Una dintre funcțiile protocolului TCP este să se asigure că fiecare segment ajunge la destinație. Serviciile TCP de la destinație confirmă datele pe care le-a primit de la aplicația sursă. Valoarea de secvență a antetului de segment şi numărul de confirmare sunt folosite împreună pentru a confirma primirea de octeți de date conținute de segmente.

Numărul de ordine este numărul relativ de octeți care au fost transmişi în această sesiune, plus 1 (care este numărul primului octet de date din segmentul curent). TCP foloseşte numărul de confirmare în segmentele trimise înapoi la sursă pentru a indica octetul următor în această sesiune, pe care receptorul se aşteaptă să-l primească. Aceasta se numeşte confirmare (acknowledgement).

Sursa este astfel informată că destinația a primit toți octeții în acest flux de date de până la, dar nu inclusiv, octetul indicat de numărul de confirmare. Este de aşteptat ca dispozitivul ce trimite, să trimită un segment care utilizează un număr de ordine egal cu numărul de confirmare. Pe scurt, fiecare conexiune este de fapt un ansamblu de două sesiuni, fiecare pe o singură direcție. Numerele de secvență şi numerele de confirmare sunt transmise în ambele direcții.

Cantitatea de date pe care o sursă o poate transmite înainte de a trebui să primească o confirmare, se numeşte dimensiunea (lungimea) ferestrei. Lungimea ferestrei este un câmp din antetul TCP care permite gestionarea de date pierdute şi controlul fluxului.

Protocolul TCP oferă, de asemenea, mecanismele de control al fluxului de date. Controlul fluxului asistă fiabilitatea transmisiei prin TCP prin ajustarea ratei efective a fluxului de date între cele două servicii din sesiune. Atunci când sursa este informată că valoarea de date specificată în segmente este primită, se poate continua transmisia mai multor date pentru această sesiune.

Lungimea ferestrei în antetul TCP precizează cantitatea de date care pot fi transmise înainte ca o confirmare să fie primită. Dimensiunea ferestrei inițiale se determină în cursul pornirii sesiunii. Mecanismul de feedback TCP ajustează rata efectivă de transmitere a datelor la debitul maxim pe care rețeaua şi dispozitivul destinație îl pot suporta fără pierderi. Protocolul TCP încearcă să administreze rata de transmitere astfel încât toate datele să fie primite şi retransmisiile să fie minimizate.

În figura 6.5 apare o reprezentare simplificată a dimensiunii ferestrei şi confirmarea corespunzătoare.

În acest exemplu, dimensiunea (lungimea) ferestrei inițiale pentru o sesiune TCP reprezentată este setată la 3000 bytes (octeți). În cazul în care expeditorul a transmis 3000 bytes, se aşteaptă o confirmare a acestor octeți înainte de a transmite mai multe segmente în această sesiune. Odată ce expeditorul a primit această confirmare de la receptor, expeditorul poate transmite o suplimentare de 3000 bytes.

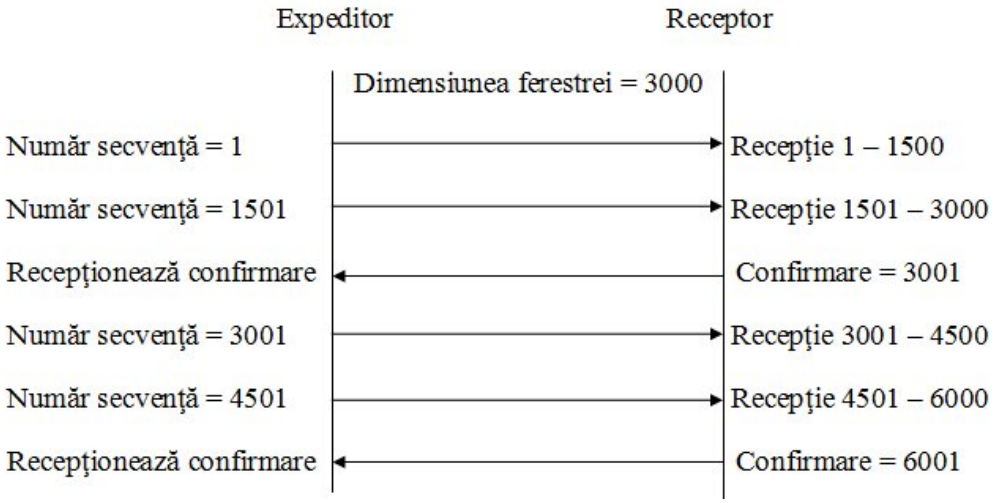

Fig.6.5. Confirmarea primirii segmentelor şi dimensiunea (lungimea) ferestrei

În timpul întârzierii, până se primeşte confirmarea, expeditorul nu va mai trimite segmente suplimentare pentru această sesiune. În perioadele când rețeaua este saturată sau resursele receptorului sunt limitate, întârzierea poate creşte. Cu cât această întârziere creşte mai mult, rata de transmitere eficientă a datelor pentru această sesiune scade.

5.3. Protocolul UDP

UDP este un protocol simplu care oferă funcțiile de bază ale nivelului transport.

Protocolul UDP nu stabileşte o conexiune între sursă şi destinație înainte de a transmite date şi furnizează o încărcătură scăzută transportului de date, datorită faptului că antetul datagramei este mic şi pentru că nu administrează traficul rețelei.

Deoarece UDP nu este orientat pe conexiune, sesiunile nu sunt stabilite înainte ca comunicarea să aibă loc, cum se întâmplă cu TCP. UDP este declarat a fi bazat pe tranzacții. Cu alte cuvinte, atunci când o aplicație are de transmis date, acesta trimite pur şi simplu acele date.

O parte din protocoalele nivelului Aplicație ce utilizează UDP sunt următoarele:

- DNS (Domain Name System);
- SNMP (Simple Network Management Protocol);
- DHCP (Dynamic Host Configuration Protocol);
- RIP (Routing Information Protocol);
- TFTP (Trivial File Transfer Protocol);

Unele aplicații, cum ar fi jocurile on-line sau VoIP (Voice over IP), pot tolera pierderea unor date. În cazul în care aceste aplicații utilizau TCP, mai mult ca sigur, ele prezentau mari întârzieri de timp, deoarece TCP-ul detectează pierderea de date şi retransmite acele date pierdute. Aceste întârzieri ar fi mult mai dăunătoare aplicațiilor decât micile pierderi de date. Unele aplicații, cum ar fi DNS, va reîncerca pur şi simplu cererea, în cazul în care nu primesc un răspuns, şi prin urmare nu au nevoie de TCP pentru a garanta livrarea mesajului.

5.3.1. Caracteristicile protocolului UDP

UDP este un protocol simplu, cu puține facilități.

Nu realizează controlul fluxului, a erorilor, nu retransmite datagrame pierdute etc. El pur şi simplu oferă IP-ului un mijloc de multiplexare a proceselor (aplicațiilor) folosind porturile de nivel transport. Este utilizat în transferurile scurte de date, gen întrebare – răspuns în aplicațiile client - server. Un client trimite o cerere scurtă spre server şi aşteaptă un răspuns scurt. Dacă aceste nu vine într-un timp aşteptat, atunci repetă cererea.

Un exemplu tipic de utilizare este între un client şi serverul DNS (Domain Name System) pentru aflarea adresei IP corespunzătoare unui nume de gazdă. Nu este nevoie de deschiderea unei conexiuni, nici de închidere, pentru un transfer pentru două mesaje scurte care traversează rețeaua.

Atunci când mai multe datagrame sunt trimise la destinație, ele pot lua diferite căi şi pot ajunge în ordine greşită. UDP nu ține cont de numerele de secvență cum le utilizează protocolul TCP.

UDP nu are nici o modalitate de a reordona datagramele în ordinea în care au fost transmise. În figura 6.6 se observă acest lucru şi mai ales faptul că datagramele pierdute nu se mai retransmit.

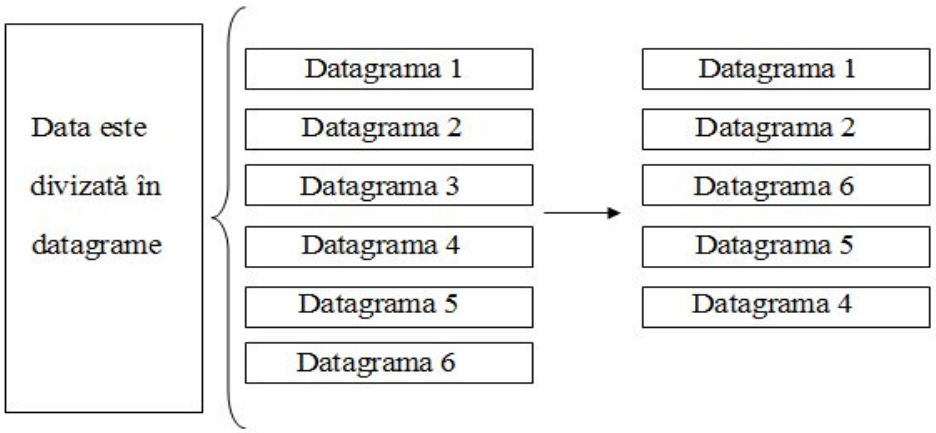

Fig. 6.6. Transmiterea datagramelor

Prin urmare, UDP reasamblează pur şi simplu datele, în ordinea în care acestea au fost primite şi le transmite mai departe aplicației. În cazul în care secvența de date este importantă pentru aplicație, aplicația va trebui să identifice secvența corectă a datelor şi să stabilească modul în care datele ar trebui să fie prelucrate.

5.3.2. Antetul datagramei UDP

La fel ca în cazul utilizării protocolului TCP, după procesul de segmentare are loc împachetarea datelor. Această împachetare constă în lipirea unui antet, noile entități de transmisie şi de recepție purtând numele de datagrame.

PDU-ul (Protocol Data Unit) protocolului UDP este numit datagramă, deşi uneori termenii segment şi datagramă sunt folosiți alternativ pentru a descrie un PDU de nivel transport.

O datagramă UDP constă dintr-un antet de 8 de octeți urmată de zero sau mai mulți octeți de date - vezi figura 6.7.

Bit 0 Bit 15	Bit 16 Bit 31
Număr port sursă	Număr port destinație
Lungime UDP	Sumă de control
DATA (de aplicații)	

Fig.6.7. Antetul UDP (primele 2 rânduri ale datagramei)

Semnificația informațiilor introduse în antet este următoarea:

- Număr port sursă - 16 biți (2 octeți) - numărul de port al celui ce face apelul;
- Număr port destinație - 16 biți (2 octeți) - numărul de port de destinație al celui ce este apelat;

Câmpurile Număr port sursă şi Port destinație identifică punctele finale ale conexiunii şi constituie totodată un identificator al conexiunii.

- Lungime antetului – 16 biți (2 octeți) – include antetul şi datele;
- Suma de control – 16 biți (2 octeți) - indică suma câmpurilor de antet şi date, calculată pentru verificare;

5.4. Comparație între protocoalele de nivel transport

O comparație între caracteristicile celor două protocoale este oferită în tabelul 6.3

Tabelul 6.3

Caracteristică	**TCP**	**UDP**
Mărimea headerului pachetului	20-60 Bytes	8 Byte
Entitatea pachetului de nivel rețea	Segment	Datagramă
Orientare pe conexiuni	Da	Nu
Transport de încredere	Da	Nu
Livrarea în ordinie	Da	Nu
Livrarea neordonată	Nu	Da
Suma de verificare a datelor	Da	Opțional
Mărimea sumei de verificare (biți)	16	16
Controlul fluxului	Da	Nu
Controlul congestiei	Da	Nu

7. NIVELUL REȚEA

Nivelul rețea este un nivel complex care oferă conectivitate şi selectează drumul de urmat între două sisteme gazdă care pot fi localizate în rețele separate geografic.

Acesta este nivelul cel mai important în cadrul Internetului, asigurând posibilitatea interconectării diferitelor rețele. Tot la acest nivel se realizează adresarea logică a tuturor nodurilor din Internet. La nivelul rețea operează ruterele, dispozitivele cele mai importante în orice rețea de foarte mari dimensiuni.

Nivelul Rețea este stratul cu numărul 3 corespunzător modelului OSI – vezi figura 7.1.

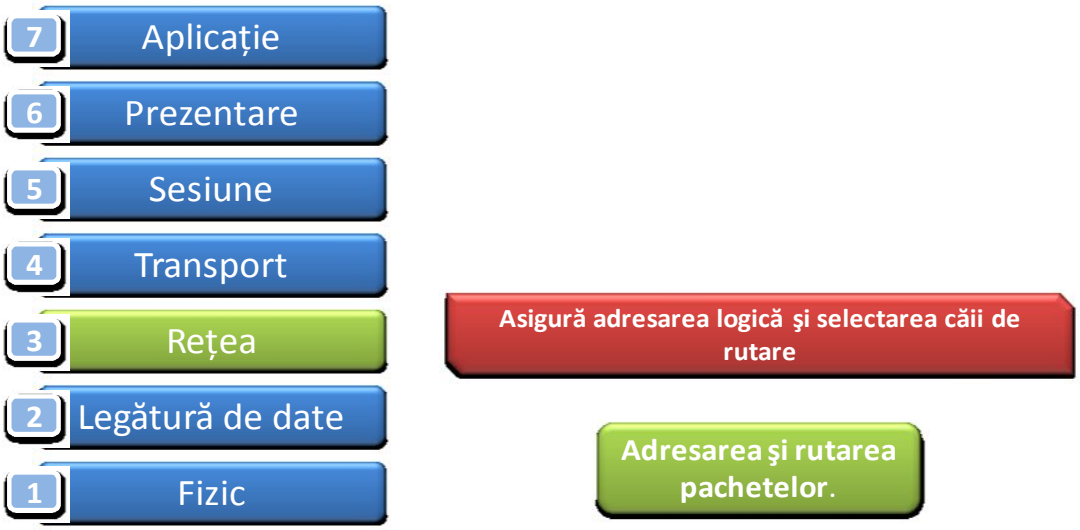

Fig.7.1. Poziția nivelului Rețea în structura modelului OSI

În cadrul nivelului Rețea are loc un nou proces de încapsulare prin adaugare antetul propriu ce transformă segmentele de la nivelul Transport în pachete. Cele mai importante informații conținute de acest antet sunt adresele logice ale sursei, respectiv destinației.

Nivelul rețea are ca sarcină principală transferul datelor de la sursă la destinație prin trecere din nod în nod de-a lungul rețelei.

Transferul datelor la nivel rețea se poate face în modul orientat pe conexiune sau neorientat pe conexiune. Şi într-un caz şi în altul, rețeaua trebuie să poată face dirijarea pachetelor în noduri, adică să facă rutarea.

Nodurile de rețea care fac dirijare se numesc rutere. Ele trebuie să fie echipamente inteligente, capabile să ia decizii de rutare optime, să aleagă calea cea mai potrivită de urmat dintre multe variante posibile.

Pentru aceasta, ruterele trebuie să cunoască topologia rețelei, să aibă mereu informații despre starea rutelor, să poată folosi diferite criterii de performanță pentru a compara rutele, să poată utiliza algoritmi de rutare în timp real.

Prin deciziile de rutare trebuie să se asigure o încărcare cât mai uniformă posibilă a rețelei, fără a congestiona unele rute şi a lăsa neîncărcate altele.

Dacă pachetele sau fluxurile de date traversează rețele diferite, interconectarea dintre ele se face prin conversie de protocol de către echipamente speciale numite porți (gateways) care operează la nivel transport. În fiecare rețea omogenă operează protocoale specifice de nivel rețea care asigură ruterea în acea rețea. Principalul protocol implementat la acet nivel este Ipv4 (Internet Protocol version 4)

7.1 Funcțiile nivelului Rețea

Nivelul rețea, controlează operațiile din subrețea prin crearea, menținerea şi apoi întreruperea unei conexiuni virtuale a nivelurilor transport al calculatoarelor aflate în comunicație.

Nivelul rețea, în cazul comunicației dintre două calculatoare care aparțin unei rețele WAN, are rolul de a proteja nivelurile superioare de arhitectura fizică a rețelelor LAN, deoarece se interconectează rețele de calculatoare care au fost realizate de diferite firme care au dezvoltat propriile tipuri de rețele, bazate pe propriile standarde.

În consecință, este important ca nivelurile superioare să nu fie dependente de tehnologia utilizată în rețelele LAN.

Principalele funcții realizate la acest nivel sunt:

- Alegerea traseelor pentru mesajele dintre utilizatorii finali şi eventuala modificare a acestora, pentru a asigura transmiterea lor pe un traseu optim. Altfel spus se realizează alegerea traseului (path) sau căii (route), adică a succesiunii de tronsoane de canale fizice de la calculatorul ce emite la cel receptor, pe care este transportat fiecare pachet. Procesul se numeste rutare.;
- Alocarea adreselor logice ale calculatoarelor şi efectuarea conversiilor între aceste adrese şi adresele fizice ale respectivelor calculatoare;
- Rezolvarea strangulărilor (bottleneck) provocate de prezența simultană a prea multor pachete în subretea, fie prin realegerea traseelor, fie cerând nivelului transport să oprească temporar emisia mesajelor;
- Realizarea conversiei dintre diferite protocoale, în situatia în care mesajele parcurg rețele eterogene, adică realizate cu tehnologii diferite (Ethernet, FDDI, Token Ring, etc).

7.2. Protocolul IPv4

Principalalul protocol al nivelului retea este protocolul IP (în prezentarea de față se va face referire doar la caracteristicile protocolului IPv4). Acesta este un protocol fără conexiune, care asigură o transmisie nefiabilă a pachetelor de date. Un astfel de protocol este caracterizat prin faptul că fiecare pachet este considerat o entitate independentă, care nu are legătură cu celelalte pachete transmise.

Adresa unică, atribuită fiecărui echipament de comunicatie dintr-o retea, se numeste adresă IP având o lungime de 4 bytes sau 32 de biți. Procesul prin care se face alocarea adresei IP unui echipament din rețea se numeste adresare. Fiecare pachet de date, , contine atât adresa IP a calculatorului sursă, cât si adresa IP a calculatorului destinatie, astfel încât poate fi transmisă si rutată independent de celelalte pachete.

Protocolul IP este nefiabil, pentru că nu garantează că pachetele vor ajunge la destinație şi nici că transmisia lor pe canalul de comunicație va fi fără erori. Totuşi, pachetul IP conține o sumă de control a antetului.

Dacă antetul unui pachet IP nu este corespunzător, întreg pachetul este anulat şi nu mai este transmis nivelului superior, nivel care verifică toate datele conținute de pachet. Protocolul IP este responsabil cu rutarea pachetelor în Internet şi cu o posibilă fragmentare a datelor.

Fragmentarea unui pachet este făcută de un gateway atunci când pachetul este prea mare pentru a parcurge rețeaua prin care se va transmite, aceasta fiind o rețea de alt tip (Ethernet, Token Ring, FDDI, etc.). În acest caz, fragmentele rezultate sunt transmise în continuare ca pachete IP independente şi sunt reasamblate la destinație, reconstituind astfel pachetul initial. Dacă unul dintre fragmente este eronat sau pierdut, se anulează întregul pachet.

În cadrul nivelului Rețea are loc o nouă împachetare a datelor. Această împachetare constă în lipirea unui antet, noile entități de transmisie şi de recepție purtând numele de pachete.

Un pachet constă dintr-un antet de 20 de octeți (plus o parte opțională cu lungime variabilă) urmat de zero sau mai mulți octeți de date - vezi figura 7.2.

<table>
<tr><td colspan="3">Bit 0 Bit 15</td><td colspan="2">Bit 16 Bit 31</td></tr>
<tr><td>Versiune</td><td>Lungime antet</td><td>Tip serviciu</td><td colspan="2">Lungime totală</td></tr>
<tr><td colspan="3">Identificare</td><td>Semnalizări</td><td>Deplasarea fragmentului</td></tr>
<tr><td colspan="2">Timp de viață</td><td>Protocol</td><td colspan="2">Sumă de control a antetului</td></tr>
<tr><td colspan="5">Adresa IP a sursei</td></tr>
<tr><td colspan="5">Adresa IP a destinației</td></tr>
<tr><td colspan="5">Opțiuni</td></tr>
<tr><td colspan="5">DATA (de aplicații)</td></tr>
</table>

Fig.7.2. Antetul IPv4 (primele 5 rânduri ale pachetului)

Semnificația informațiilor introduse în antet este următoarea:

- Versiune - 4 biți - versiunea protocolului IP utilizat. Versiunea actuală este versiunea 4, notată cu IPv4;
- Lungime antet - 4 biți - Lungimea antetului ataşt segmentului (sau datagramei). Când a fost concepută structura unei pachet, s-a stabilit ca antetul să fie multiplu de 32 biti. Un antet are în mod normal 20 de octeti, adică 5 blocuri de cîte 4 octeti. Ca urmare, acest câmp va contine, de cele mai multe ori, valoarea 5. Mai exact, valoarea acestui câmp este numărul binar 0101. Datele încapsulate în pachet urmează imediat după antet. Examinând câmpul Lungime antet se poate determina pozitia la care încep datele;
- Tip serviciu – 8 biți (1 octet) – precizează informații referitoare la prioritatea pachetului de date. Acest câmp este împărtit la rândul său în 6 subcâmpuri care permit stabilirea priorităților pentru pachetul IP. Echipamentul de retea, citeşte valoarile din acest câmp, poatând lua decizii corecte pentru gestiunea datelor. Într-o rețea, sau în internet, circulă nu numai pachete de date, ci si pachete de control (informatii de routare, etc). Utilizând acest câmp se pot acorda priorități diferite pachetelor de control față de cele de date;
- Lungime totală – 16 biți (2 octeți) – este o valoare care specifică lungimea totală a pachetului (în octeti), incluzând şi antetul. Având 16 biti, rezultă că dimensiunea teoretică maximă este de 65.535 octeți. La stabilirea acestei valori s-a ținut cont de nivelul Legăturii de Date al rețelei, nivel care încapsulează diferit pachetele pentru tipuri diferite de rețele.

Fiecare tip de rețea defineşte o valoare pentru dimensiunea maximă a unui pachet. Aceasta valoare se numeste unitate maximă de transfer a rețelei (MTU – Maximum Transfer Unit). Astfel, rețelele Ethernet au un MTU de 1500 octeți, Token Ring au unitatea maximă de transfer a rețelei de 4464 octeți.

Alte tipuri de rețea pot avea valori mult mai mici ale unității maxime de transfer a rețelei, chiar până la 128 octeți. Dacă o aplicație încearcă să transporte un pachet IP mai mare decât MTU, se produce fragmentarea datelor, la destinație urmând să se producă reasamblareastora;

- Identificare – 16 biți (2 octeți) – permite (împreună cu câmpurile de adrese şi protocol), identificarea, pe parcursul reasamblării, a diferitelor fragmente ale pachetelor de către;
- Semnalizări – 3 biți - este un câmp de informație de control format din 3 biti (un bit nefolosit), care conține 2 indicatori:

- DF setat pe 1 interzice fragmentarea; DF setat pe 0 precizează că pachetul a fost fragmentat;
- MF setat 1 precizează că mai urmează fragmente; MF poziționat pe 0 indică ultimul fragment al pachetului;

- Deplasarea fragmentului – 13 biți – precizează poziția fragmentului curent în cadrul pachetului. Toate fragmentele dintr-un pachet, cu excepția ultimului, trebuie să fie un multiplu de 8 octeți - unitatea de fragmentare elementară.

Din moment ce sunt prevăzuți 13 biți, există un maxim de 8192 de fragmente pe pachet, obținîndu-se o lungime maximă de 65536 octeți, cu unul mai mult decît cîmpul lungime totală;

- Timp de viață – 8 biți (1 octet) - este un contor folosit pentru a limita durata de viață a pachetelor. A fost introdus pentru a împiedica pachetele să rătăcească prin Internet. La primirea pachetului, fiecare router dintre calculatorul sursă şi calculatorul destinație decrementează acest câmp cu o unitate.

Atunci când un pachet atinge valoarea $TTL = 0$ este distrus. În acest caz sursa este anuntată printr-un mesaj generat de protocolul ICMP (Internet Control Message Protocol). În concluzie este imposibil ca un pachet să circule la infint, deoarece după ce trece prin maximum 255 de device-uri (de exemplu routere) este distrus;

- Protocol – 8 biți (1 octet) - permite specificarea tipului de protocol de nivel superior (nivelul Transport) utilizat (TCP, UDP, etc);
- Suma de control a antetului – 16 biți (2 octeți) - verifică numai antetul. O astfel de sumă de control este utilă pentru detectarea erorilor generate de locații de memorie proaste din interiorul unui router. Suma de control pentru toate datele încapsulate este calculată de protocoalele de nivel superior care au creat datele respective. În cazul unui segment eronat, protocolul IP nu obligă calculatorul destinație să trimită calculatorului emițător (sursă) un mesaj de eroare;
- Adresa IP a sursei - 32 biți (4 octeți) – indică adresa logică a sursei;
- Adresa IP a destinației - 32 biți (4 octeți) – indică adresa logică a destinației;

7.3. Adresarea IP

Pentru orice comunicare în rețea trebuie să existe un mecanism de adresare, care să permită recunoaşterea unică a calculatoarelor conectate.

La conceperea protocolului IP s-a impus utilizarea unui mecanism de adresare care să identifice unic fiecare dispozitiv gazdă din rețea.

O adresă IP este un număr binar pe 32 de biti, reprezentat prin 4 numere zecimale separate prin puncte, fiecare număr fiind reprezentat prin 8 biți.

Un exemplu de adresă IP este: 192.0.128.64. Această notație este cunoscută sub numele "dotted decimal".

Adresa IP este reprezentată în calculator în forma binară:
11000000 00000000 10000000 01000000.

7.3.1. Clase de adrese IP; Adresarea IP pe baza claselor de adrese (Classful IP Addressing)

Orice adresă IP este formată din două părti, una care identifică rețeaua (Network ID) şi una care identifică nodulsau gazda (Host ID).

Deşi această exprimare facilitează semnificativ lucrul cu adresele IP, există unele limitări legate de uşurinta de a discerne între porțiunea de rețea şi cea de stație din cadrul adresei IP.

Încercarea de a păstra reprezentarea zecimală ca model de referință pentru adresa IP şi de a permite să se facă uşor distincția între cele două componente ale adresei IP, a condus la definirea claselor de adrese IP.

Au fost definite 5 clase diferite de adrese IP: A, B, C, D si E. Se poate determina clasa din care face parte adresa IP prin examinarea primilor 4 biți ai adresei IP:

- Adresele de clasă A sunt adresele care încep cu 0xxx, de la 1 la 126 în zecimal;

Adresele de clasă A sunt destinate rețelelor de dimensiuni mari.
La aceste adrese IP, pentru definirea rețelei (network) se foloseste primul octet, iar ceilalți trei octeți sunt utilizați pentru identificarea gazdei (host), vezi figura 7.3.

Rețea (Network) NNNNNNN	Gazdă (Host) hhhhhhhh. hhhhhhhh. hhhhhhhh		
Octetul 1	Octetul 2	Octetul 3	Octetul 4
0XXXXXXX	xxxxxxxx	xxxxxxxx	xxxxxxxx

Fig.7.3. Adrese IP ce clasă A

Domeniul de valori pentru adresele din clasa A este de la 1 la 126, adică adresele de la 0.0.0.1 până la 126.255.255.255.

Clasa de adrese 0.0.0.0 nu este folosită datorită posibilelor confuzii cu rutele implicite, iar clasa 127.0.0.0 este rezervată pentru adrese de loopback, în scopul monitorizării şi testării rețelei locale.

Adresa de loopback nu poate fi accesată decât local, orice pachet trimis va avea ca destinatie exact calculatorul de pe care sunt trimise pachetele.

În tabelul 7.1 este prezentată succint clasa A de adrese IP.

Tabelul 7.1. Clasa A de adrese IP

Clasa A primul bit este întotdeauna 0				
	Scriere în binar		Zecimal	Primul Octet
Interval teoretic de adrese	**0**0000000	00000000 00000000 00000000	0.0.0.0	0-127
	01111111	11111111 11111111 11111111	127.255.255.255	
Rute implicite	**0**0000000	00000000 00000000 00000000	0.0.0.0	0
Interval de adrese folosit la teste	**0**1111111	00000000 00000000 00000000	127.0.0.0	127
	01111111	11111111 11111111 11111111	127.255.255.255	
Interval teoretic de IP-uri ce pot fi alocate	**0**0000000	00000000 00000000 00000001	0.0.0.1	1-126
	01111110	11111111 11111111 11111111	126.255.255.255	
Interval teoretic de IP-uri private	**0**0001010	00000000 00000000 00000000	10.0.0.0.	10
	00001010	11111111 11111111 11111111	10. 255.255.255	
	Adrese Rețele (Network)	Adrese Gazdă (Host)		
	$128\left(2^7\right)$	$16.777.216\left(2^{24}\right)$		

Cei 24 de biți folositi pentru identificarea hostului, permit adresarea a 16.777.216 hosturi. Rezultă că rețelele de clasă A sunt rețele foarte mari, datorită numărului foarte mare hosturi ce pot fi adresate, folosite de companii mari şi de unele țări.

- Adresele de clasă B sunt adresele care încep cu 10xx, de la 128 la 191 în zecimal;

Adresele de clasă B sunt destinate rețelelor de dimensiuni mai mici decât cele de clasă A. La aceste adrese IP, pentru definirea rețelei (network) se folosesc primii doi octeți, iar următorii doi octeți sunt utilizati pentru identificarea gazdei (host), vezi figura 7.4.

Rețea (Network) NNNNNNN. NNNNNNN		Gazdă (Host) hhhhhhhh. hhhhhhhh	
Octetul 1	Octetul 2	Octetul 3	Octetul 4
10XXXXXX	XXXXXXXX	xxxxxxxx	xxxxxxxx

Fig.7.4. Adrese IP ce clasă B

Domeniul de valori pentru adresele de clasă B este de la 128 la 191, adică adresele de la 128.0.0.0 până la 191.255.255.255.

În tabelul 7.2 este prezentată succint clasa B de adrese IP.

Tabelul 7.2. Clasa B de adrese IP

Clasa B primii biți sunt întotdeauna 10				
	Scriere în binar		Zecimal	Primul Octet
Interval teoretic de adrese	**10**000000 00000000	00000000 00000000	128.0.0.0	128-191
	10111111 11111111	11111111 11111111	191.255.255.255	
Interval teoretic de IP-uri ce pot fi alocate	**10**000000 00000000	00000000 00000000	128.0.0.0	128-191
	10111111 11111111	11111111 11111111	191.255.255.255	
Interval teoretic de IP-uri private	**10**010000 00000000	00000000 00000000	172.16.0.0	172.16 172.31
	10011111 11111111	11111111 11111111	172.31.255.255	
	Adrese Rețele (Network)	Adrese Gazdă (Host)		
	$16.384\left(2^{14}\right)$	$65.536\left(2^{16}\right)$		

În acest interval se pot adresa 16.324 rețele. Cei 16 biți folosiți pentru identificarea hostului permit adresarea a 65.534 hosturi. Rezultă că rețelele de clasă B sunt rețele medii spre mari, datorită numărului de hosturi ce pot fi adresate, cum ar fi cele folosite în universități.

- Adresele de clasă C sunt adresele care încep cu 110x, de la 192 la 223 în zecimal;

Adresele de clasă C sunt destinate rețelelor de dimensiuni mici. La aceste adrese IP, pentru definirea rețelei (network) se folosesc primii trei octeți, ultimul fiind utilizat pentru identificarea gazdei (host), vezi figura 7.5.

Rețea (Network) NNNNNNN. NNNNNNN.NNNNNNNN			Gazdă (Host) hhhhhhhh
Octetul 1	Octetul 2	Octetul 3	Octetul 4
110XXXXX	XXXXXXXX	XXXXXXXX	xxxxxxxx

Fig.7.5. Adrese IP ce clasă C

Cei 8 biți folosiți pentru identificarea hostului permit adresarea a 256 hosturi. Rezultă că rețelele de clasă C sunt rețele mici, datorită numărului de hosturi ce pot fi adresate, cum ar fi cele folosite în departamentele universităților.

În tabelul 7.3 este prezentată succint clasa C de adrese IP.

Tabelul 7.3. Clasa C de adrese IP

Clasa C primii biți sunt întotdeauna 110				
	Scriere în binar		Zecimal	Primul Octet
Interval teoretic de adrese	**110**00000 00000000 00000000	00000000	192.0.0.0	192-223
	11011111 11111111 11111111	11111111	223.255.255.255	
Interval teoretic de IP-uri ce pot fi alocate	**110**00000 00000000 00000000	00000000	192.0.0.0	192-223
	11011111 11111111 11111111	11111111	223.255.255.255	
Interval teoretic de IP-uri private	**110**00000 10101000 00000000	00000000	192.168.0.0	192.168
	11000000 10101000 11111111	11111111	192.168.255.255	
	Adrese Rețele (Network)	Adrese Gazdă (Host)		
	2.097.152 (2^{21})	256 (2^{8})		

În afară de cele trei clase de IP-uri au mai fost definite încă două, cu observația că aceste adrese nu vor fi alocate unor rețele.

- Adresele de clasă D sunt adresele care încep cu 1110, de la 224 la 239 în zecimal;

Adresele de clasă D sunt destinate traficului multicast, toți cei patru octeți fiind alocați pentru identificarea rețelei, vezi figura 7.6.

Rețea (Network) NNNNNNN. NNNNNNN.NNNNNNNN.NNNNNNNN			
Octetul 1	Octetul 2	Octetul 3	Octetul 4
1110XXXX	XXXXXXXX	XXXXXXXX	XXXXXXXX

Fig.7.6. Adrese IP ce clasă D

Domeniul de valori pentru adresele de clasă D este de la 224 la 239, adică adresele de la 224.0.0.0 până la 239.255.255.255.

- Adresele de clasă E sunt adresele care încep cu 1111, de la 240 la 254 în zecimal;

Adresele de clasă E sunt destinate utilizărilor experimentale. Domeniul de valori pentru adresele de clasă se întinde de la 240.0.0.0 până la 254.255.255.255.

IANA (Internet Asigned Numbers Authority) a definit ca spațiu de adresare privată intervalele:

- 10.0.0.0 - 10.255.255.255 (clasa A);
- 172.16.0.0 - 172.31.255.255 (clasaB);
- 192.168.0.0 - 192.168.255.255 (clasa C)

Totodată intervalul 169.254.0.0 -169.254.255.255 este rezervat pentru adresarea IP automată privată (APIPA - Automatic Private IP Addressing) utilizată pentru alocarea

automată a unei adrese IP la instalarea inițială a protocolului TCP/IP peste anumite sisteme de operare.

Adresele private sunt ignorate de către echipamentele de rutare ele putând fi utilizate pentru conexiuni nerutate, în rețelele locale.

Restul adreselor au statutul de adrese IP publice beneficiind de vizibilitate potențială la nivelul rețelei mondiale Internet.

După cum s-a precizat anterior protocolul IPv4 defineşte adrese pe 32 de biți, rezultând un număr de maxim de 2^{32} (4.294.967.296) de adrese. Alocarea spațiilor de adrese nu a fost făcută în mod eficient, acest lucru constituind în prezent un motiv care determină iminenta epuizare a adreselor IPv4. A doua problemă este cauzată de creşterea dimensiunii tabelelor de rutare. Routerele care formează coloana vertebrală (backbone) a Internetului trebuie să memoreze informații complete de rutare. Problema rutării nu se rezolvă doar prin instalarea unor memorii suplimentare în routere cu scopul de putea stoca tabele de rutare mai mari, ci este nevoie şi de putere de calcul sporită, astfel încât să nu fie eliminată nici o rută din cauza creşterii volumului de trafic şi a intrărilor în tabele de rutare.

Soluția acestor probleme constă în implementarea noului protocol IPv6 (IP Next Generation – IPng), însă tranziția de la IPv4 la IPv6 nu este simplu de realizat, fiind necesar consensul marilor furnizori de servicii Internet la nivel mondial.

Adresarea IP este o adresare de tip ierarhic. Acesta este motivul pentru care cei 32 de biți ai adresei IP este împărțită în două categorii (biții de rețea-network- respectiv biții gazdei-host).

Atunci când protocolul IP a fost standardizat (1981), specificațiile prevedeau ca o gazdă (PC-uri, routere, imprimante, camere web, telefoane VoIp, etc) conectată la o rețea să aibă alocată o adresă unică pe 32 de biți.

Dacă o gazdă conținea mai multe interfețe (conexiuni la mai multe rețele), atunci fiecare interfață trebuia să aibă alocată propria adresă unică pe 32 de biți.

Modelul de adresare IP era format din două nivele, un nivel identifica rețeaua în care se afla gazda, iar celălalt nivel identifica gazda din rețeaua respectivă.

Toate stațiile dintr-o rețea au acelaşi prefix de rețea (adrese rețele, vezi figurile 7.3, 7.5), însă trebuie să aibă un număr de stație unic (adrese gazdă, vezi figurile 7.3, 7.5).

În mod similar, două gazde aflate în rețele diferite trebuie să aibă prefixe diferite de rețea, însă pot avea acelaşi număr de stație.

Specificațiile IP inițiale împărțeau spațiul de adrese IP în trei clase principale: A, B şi C **(classful addressing).** Fiecare clasă defineşte în mod diferit zona prefixului de rețea şi zona numărului de stație. Astfel, fiecare adresă conține o cheie care identifică în mod precis locul de demarcație dintre prefixul de rețea şi numărul de stație. Această abordare simplifica procesul de rutare în trecut, deoarece protocoalele de rutare inițiale nu furnizau o cheie de descifrare sau o mască de rețea asociată fiecărei rute pentru identificarea lungimii.

Pentru împărțirea adresei IP în numărul rețelei şi a gazdei este utilizată masca IP, ce conține 32 de biți.

În forma binară masca de rețea este formată dintr-o:

- succesiune de biți de valoare 1 ce corespund zonei de biți rețea (network) a IP-ului;
- succesiune de biți de valoare 0 ce corespund zonei de biți gazdă (host) a IP-ului;

Masca de rețea ce este asociată adreselor IP corespunzătoare claselor A, B sau C se numeşte mască implicită (default network mask).

În figura 7.7 este prezentată asocierea dintre IP şi mască în cazul adresării IP pe baza claselor de adrese (Classful IP Addressing)

	Octetul 1	Octetul 2	Octetul 3	Octetul 4
CLASĂ A				
	Adrese Rețele (Network)	Adrese Gazdă (Host)		
Adresă IP binar	**0XXXXXXX**	xxxxxxxx	xxxxxxxx	xxxxxxxx
Mască IP (Default subnet mask) binar	**11111111**	00000000	00000000	00000000
Mască IP (Default subnet mask) zecimal	**255**	0	0	0
CLASĂ B				
	Adrese Rețele (Network)		Adrese Gazdă (Host)	
Adresă IP binar	**10XXXXXX**	**XXXXXXXX**	xxxxxxxx	xxxxxxxx
Mască IP (Default subnet mask) binar	**11111111**	**11111111**	00000000	00000000
Mască IP (Default subnet mask) zecimal	**255**	**255**	0	0
CLASĂ C				
	Adrese Rețele (Network)			Adrese Gazdă (Host)
Adresă IP binar	**110XXXXX**	**XXXXXXXX**	**XXXXXXXX**	xxxxxxxx
Mască IP (Default subnet mask) binar	**11111111**	**11111111**	**11111111**	00000000
Mască IP (Default subnet mask) zecimal	**255**	**255**	**255**	0

Fig.7.7 Asocierea dintre IP şi mască (default subnet mask)

În concluzie orice IP este insoțit de mască. În exemplul următor se preyintă această asociere pentru trei IP-uri.

- **10**.28.34.87 **255**.0.0.0
- **172.17**.56.239 **255.255**.0.0
- **192.168.0**.4 **255.255.255**.0

Există să o altă variantă (mai simplă) de a nota asocierea dintre un IP şi mască lui aferentă:

- IP/nr biți ai rețelei

Acestă scriere poartă numele de “scriere cu prefix”, vezi figura 7.8.

Clase de adrese IP	Generic	Exemplu
CLASĂ A	**IP/8**	**10**.28.34.87/**8**
CLASĂ B	**IP/16**	**172.17**.56.239/**16**
CLASĂ C	**IP/24**	**192.168.0**.4/**24**

Fig.7.8 Asocierea dintre IP şi mască (default subnet mask) scrisă cu prefix

7.3.2. Adrese IP – CIDR - clasaless inter-domain routing

Deoarece, la ora actuală, se conectează la Internet câte o nouă rețea la fiecare câteva minute, Internetul se confruntă cu două probleme critice:

- Depăşirea numărului de adrese IP disponibile;

Există un număr maxim de rețele şi gazde cărora le pot fi alocate adrese IP unice de 32 biți. Inițial s-au utilizat clasele de adrese A, B ,C. Utilizând clasele, schema de adresare în Internet poate suporta:

- 126 rețele de clasă A (cu maximum 16,777,214 gazde/rețea fiecare);
- 65,000 rețele de clasă B (cu maximum 65,534 gazde/rețea fiecare);
- peste 2 milioane rețele clasă C (cu maximum 254 gazde/rețea fiecare);

Deoarece adresele de pe Internet au fost alocate conform schemei de adresare pe clase (Classful IP Addressing), au rezultat o mulțime de adrese neutilizate. De exemplu, dacă sunt necesare 120 de gazde, va fi alocat un domeniu de clasă C rămânând neutilizate 134 de adrese. CIDR a fost creat pentru a permite o alocare mult mai eficientă a adreselor IP.

- Depăşirea capacității tabelelor de rutare globale;

Odată cu creşterea numărului de rețele conectate la Internet a crescut şi numărul de rute. S-a estimat că, în câțiva ani, routerele de pe backbone-urile Internetului vor atinge limita numărului de rute pe care le pot suporta. Chiar utilizând cele mai noi tehnologii în domeniul routerelor, valoarea teoretică maximă a numărului de intrări intr-o tabelă de rutare este de approximativ 60.000. Dacă nu s-ar fi făcut nimic Internetul şi-ar fi oprit creşterea.

Pentru rezolvarea problemei s-au dezvoltat două soluții:

- Agregarea ierarhică a rutării în scopul minimizării numărului de intrări în tabelele de rutare;
- Restructurarea alocării adreselor IP în scopul creşterii eficienței;

CIDR (Clasaless Inter-Domain Routing) înlocuieşte sistemul clasic de alocare al adreselor IP pe baza claselor, prin utilizarea unui ”prefix” generalizat de rețea. În locul limitării ID-urilor de rețea (sau "prefixelor") la 8, 16 sau 24 biți, CIDR utilizează în mod curent prefixe cuprinse între 10 şi 30 de biți. Astfel, pot fi alocate blocuri de adrese de gazdă cuprinse între 2 şi peste 500.000 . Aceasta permite alocarea de domenii de adrese mult mai apropiate ca număr de necesitățile unei organizații.

În cadrul CIDR nu mai există o delimitare rigidă între ID-ul de rețea şi cel de gazdă (pe bază de octeți).

Separarea între ID-ul de rețea şi cel de gazdă se poate face oriunde în interiorul unui octet. Adresa CIDR arată ca o adresă IP standard de 32-biți, dar se termină cu prefixul IP de rețea (IP network prefix).

De exemplu, în adresa CIDR 192.168.0.4/**26,** "/26" indică faptul că primii 26 biți sunt utilizați pentru identificarea rețelei, iar restul biților – 6 - sunt pentru identificarea gazdei.

8. NIVELUL LEGĂTURII DE DATE

Nivelul Legăturii de date este nivelul care face trecerea datelor din calculator în mediul prin care este trimisă informația (cablu, fibra optică sau unde radio).

Acest nivel controlează fluxul de date în mediul de transport şi oferă adresarea fizică (adresele MAC). Aici se implementează tehnologiile care asigură diferite topologii logice ale rețelelor (Ethernet, IEEE 802.3, IEEE 802.11 etc).

Pe scurt, se poate afirma că nivelul Legătură de date este responsabil cu adresarea fizică şi cu accesul la mediu (canal de comunicare).

Nivelul Legăturii de date este stratul cu numărul 2 corespunzător modelului OSI – vezi figura 8.1.

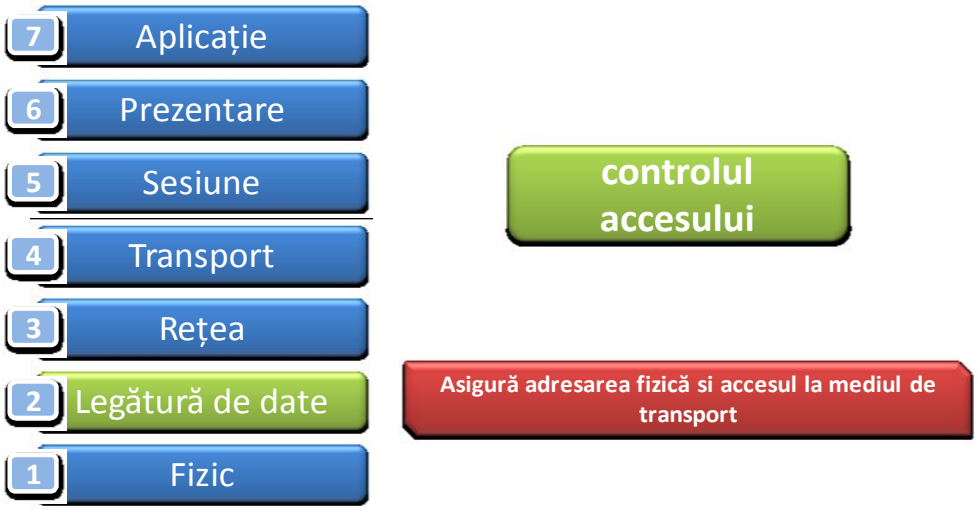

Fig.8.1. Poziția nivelului Legăturii de date în structura modelului OSI

În cadrul nivelului Legăturii de date are loc un nou proces de încapsulare prin adaugarea:

- unui antet, în care principala informație este adresa fizică (MAC address);
- unei cozi (trailer) ce conține informații pentru corectarea de erori.

În urma acestui proces PDU poartă numele de cadru (frame).

Nivelul legătură de date este deci responsabil cu transmiterea corectă a datelor printr-o legătură fizică existentă, între două puncte conectate direct prin această legătură fizică.

Nivelul fizic nu poate realiza acest lucru, deoarece la nivelul fizic nu putem vorbi despre nici un fel de date, ci numai despre biți şi, mai exact, despre reprezentarea fizică a acestora (niveluri de tensiune, intensitate a luminii etc.).

Nivelul legătură de date este împărțit în două subniveluri, cu roluri diferite:

- Subnivelul de control al legăturii logice, LLC (Logical Link Control);

Acest subnivel are scopul de a asigura comunicarea între nivelul Legăturii de date şi nivelul superior, nivelul Rețea. Acest subnivel este independent de tehnologie, adică el oferă nivelurilor superioare funcții ce sunt aceleaşi pentru orice variații ale nivelului fizic şi ale subnivelului MAC.

El se ocupă de formarea cadrelor, controlul erorilor, servicii de confirmare dacă este cazul, interfața cu nivelul superior etc. indiferent cum este partajat mediul de transmisie. El crează o interfață uniformă între nivelele superioare şi subnivelul MAC.

- Subnivelul de control al accesului la mediu, MAC (Media Acces Control)

Al doilea subnivel are două roluri majore:

- stabilirea şi respectarea regulilor de acces la mediu comun de transmisie a mai multor utilizatori;
- adaptarea la mediul fizic, astfel încât, să ascundă diferenţele legate de diferite medii de transmitere, forme de semnal, coduri de linie etc.

Acest subnivel asigură accesul ordonat şi controlat la mediu. Aceasta înseamnă, spre exemplu, că două staţii nu pot transmite în acelaşi timp, iar erorile cauzate de încercările de a transmite simultan sunt detectate.

Acest subnivel este dependent de tehnologia LAN care este implementată. De exemplu, în cazul Ethernet-ului, este necesar un mecanism de detecţie a coliziunilor, dar în cazul Token Ring acest lucru nu mai este necesar.

Formatul cadrelor diferă de la un protocol la altul, dar o formă generală este cea din figura 8.2.

Antet (Header)			Data	Coadă (Trailer)	
Start	Adresă	Control		Verificare	Stop

Fig.8.2. Formatul general al nui cadru

Semnificaţia câmpurilor din figura 8.2 este următoarea:

- Câmpurile Start şi Stop au structură fixă şi reprezintă delimitatori de cadru;
- Câmpul Adresă conţine adresele de nivel fizic (sau MAC) ale sursei şi ale destinaţiei;
- Câmpul Control are rolul de a permite controlul transmisiei în funcţie de timpul de recepţie, inclusiv prelucrare şi retransmisie în caz de erori;
- Câmpul Verificare este destinat monitorizării erorilor de transmisie;

Cea mai simplă metodă de control a erorilor este bitul de paritate.

O altă metodă mai elaborată este suma de control. Ea se efectuează la emisie, se înscrie în câmpul de control şi se verifică la recepţie. Dacă valorile sunt diferite, rezultă că în timpul transmisiei au apărut erori şi se iau decizii în consecinţă. Verificarea erorilor se poate face pentru tot blocul de date (tot cadrul) sau numai pentru antet.

La nivelurile 1 şi 2 ale modelului ISO-OSI s-au impus de-a lungul timpului standardele stabilite de IEEE (Institutul Inginerilor Electricieni şi Electronişti).

Conform acestora, cele două niveluri au fost împărţite în două părţi, una dependentă de tehnologie, care de obicei este materializată prin implementare hardware şi una independentă de tehnologie, ce este reprezentată de nivelul LLC.

Comparând modelul OSI cu standardele IEEE, vezi figura 8.3, ar putea părea, la prima vedere, că acestea din urmă nu respectă modelul OSI din două puncte de vedere.

- standardul IEEE creează propriul nivel în model, nivelul LLC;
- standardele IEEE pentru MAC traversează două niveluri din modelul OSI.

Pentru a explica această neconcordanţă, trebuie întâi să facem observaţia că modelul OSI constituie baza teoretică general acceptată în ceea ce priveşte reţelele de calculatoare. Standardele IEEE au apărut mai târziu pentru a rezolva unele probleme de natură pur practică apărute în timp.

Prin urmare, din considerente de natură exclusiv practică, a apărut acest model al standardelor IEEE, model ce separă partea ce depinde de implementarea fizică efectivă a reţelei şi a tehnologiilor folosite de interfaţa cu nivelurile superioare, ce sunt niveluri unde prelucrările se realizează prin software.

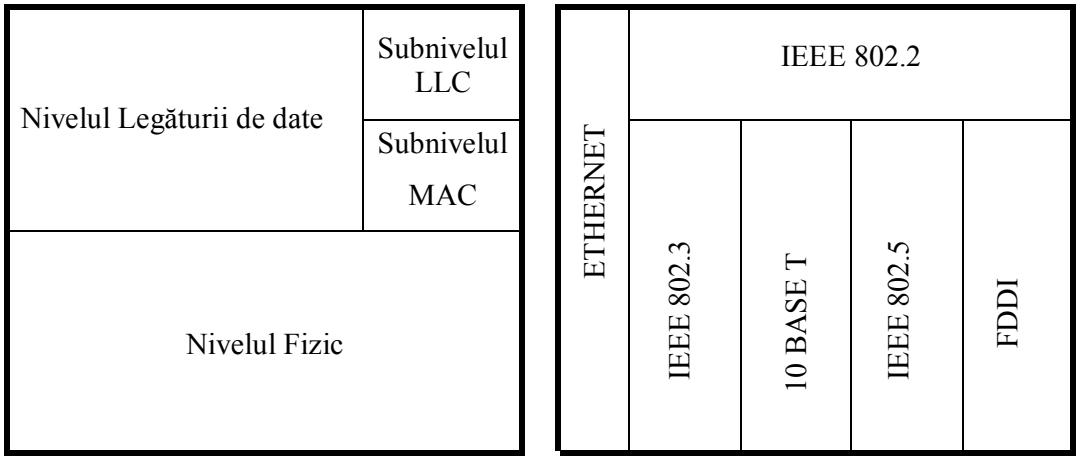

Fig.8.3. Formatul general al nui cadru

8.1 Funcțiile nivelului Legăturii de date

Nivelul Legăturii de date este situat deasupra nivelului fizic şi asigură servicii pentru nivelul Rețea. Rolul său de bază este transmiterea corectă a blocurilor de date între două noduri vecine din rețea.

Nivelul legătură de date oferă transportul sigur al informației printr-o legătură fizică directă. Pentru a realiza acest lucru, nivelul legătură de date se ocupă cu adresarea fizică, topologia rețelei, accesul la rețea, detecția şi anunțarea erorilor şi controlul fluxului fizic (flow control).

Problemele principale rezolvate de nivelul legatura de date se refera la:

- Oferirea unor funcții de comunicare generice către nivelurile superioare, ascunzând tehnologia pe care se bazează rețeaua.

Acestea sunt asigurate la subnivelul LLC şi au scopul de a uniformiza transmisia din punctul de vedere al nivelului Rețea şi de a face prezența diferitelor tehnologii de rețea transparentă pentru acesta;

- Oferirea unei modalități de indetificare fizică a nodurilor care comunică (identificarea sursei si destinatiei datelor).

Acest lucru se realizează printr-o schemă de adresare fizică bazată pe adrese MAC. Adresele MAC sunt unice pentru fiecare calculator şi nu pot fi modificate. Este important de reținut că adresele MAC sunt asignate unic pe fiecare placă de rețea şi nu pe fiecare calculator. Astfel, dacă unui calculator i se schimbă placa de rețea, adresa acestuia de MAC se va modifica. Adresele MAC nu pot fi modificate şi vor rămâne aceleaşi dacă calculatorul este mutat dintr-o rețea în alta;

- Gruparea şirurilor de biți transmise de nivelul fizic în cadre.

Aceasta este prima forma de interpretare a biților, care fără această grupare în cadre sunt lipsiți de semnificație;

- Asigurarea accesului ordonat şi controlat la mediu prin subnivelul MAC;
- Detecția erorilor de transmisie.

Acest lucru se realizează prin intermediul adaugării la cadre a unei informații de control, constituită dintr-o sumă ciclica CRC ce permite identificarea erorilor apărute în transmisia realizată de nivelul fizic.

8.2. Protocoale de acces la mediu

Nivelul Legaturii de date este responsabil cu asigurarea accesului sigur la mediu. Responsabilitatea sa este de a gestiona şi de a organiza accesul la mediul de transmisie astfel încât transmiterea efectivă să se realizeze corect.

Acest lucru presupune, spre exemplu, în cazul în care conexiunea este de tipul share-media (în care mediul de transmisie este accesibil tuturor simultan şi este împărţit între staţii), să se realizeze detecţia şi corecţia cazurilor în care doua staţii încearcă să transmită simultan (aşa-numitele coliziuni).

Subnivelul MAC conţine protocoalele care determină într-o reţea locală care staţie are dreptul să transmită la un moment dat. Aceste protocoale organizează comunicarea şi gestionează modul şi momentul în care fiecare staţie are acces la mediul de transmisie.

Exista doua mari categorii de acces la mediu de transmisie:

- Determinist (asigurarea unui interval exclusiv de emisie, pe rând, pentru fiecare staţie), care presupune faptul că fiecare staţie ştie exact când va transmite.

Se presupune că există o secvenţă garantată şi regulată (reproductibilă) de oportunitaţi de transmisie pentru fiecare staţie. În această metodă, fiecare staţie are dreptul să transmită pe rând. De obicei implementarea pentru accesul la mediu determinist este realizată prin pasarea unui jeton (token). O staţie care doreşte să transmită date captează jetonul şi astfel nici o altă staţie nu mai poate transmite. După ce a terminat transmisia, staţia care deţinea jetonul îl eliberează pentru a putea fi folosit de o altă staţie. În funcţie de topologia reţelei, există protocoale cu jeton pe magistrală (IEEE 802.4 - Token bus) sau pe inel (IEEE 802.5 - Token ring).

Asigurarea unui interval exclusiv de emisie permite garantarea, pentru fiecare staţie, a unui debit minim cu care poate emite şi a unui interval maxim de aşteptare din momentul în care are ceva de transmis şi până la intrarea în emisie;

- Nedeterminist (acceptarea posibilităţii coliziunilor şi retransmisia pachetelor distruse în coliziuni) care utilizeaza o abordare de tipul primul venit, primul servit.

Această alocare dinamică permite accesul abonaţilor la mediu după anumite reguli care pot asigura utilizarea eficientă a acestuia. Alocarea dinamică are la bază câteva ipoteze:

- Există N staţii (terminale) independente care generează cadre de transmis. Rata generării cadrelor este constantă iar probabilitatea de a genera un cadru într-un interval de timp este proporţională cu acest interval. Odată ce a fost generat un cadru, staţia nu mai generează altul până nu s-a transmis acesta.
- Canalul unic este accesibil tuturor staţiilor pentru a transmite sau recepţiona din linie.
- Când două sau mai multe cadre se suparpun chiar şi parţial în canal, apare o coliziune şi transmisia trebuie să înceteze deoarece semnalele electrice interferează.
- Timpul apariţiei cadrelor este o varibilă continuă. Nu există un ceas care să împartă timpul în momente discrete. Într-o altă variantă se poate lua în considerare şi ipoteza unui timp discret.
- Detecţia purtătoarei este metoda curentă prin care se poate afla dacă un canal este ocupat sau liber.

Prima procedură bine elaborată de control a accesului la mediu a fost ALOHA. La început se baza pe ipoteza timpului continuu (ALOHA pur) iar ulterior a apărut şi varianta cu timp cuantificat (slotted ALOHA). Ideea de bază la ALOHA pur este că utilizatorii sunt lăsaţi să transmită în voie cadrele după necesităţi. Când apar coliziuni pachetele vor fi distruse şi cadrele retransmise, deoarece transmiţătorul este anunţat despre acest lucru. Într-ul LAN retransmisia este imediată datorită distanţei de propagare mici. Pe o linie cu întârzieri mare (270 ms) reacţia este mult mai lentă şi eficienţa transmisiei scade foarte mult.

În scopul reducerii riscului coliziunilor, înainte de a transmite, o stației ascultă mediul de transmisie pentru a vedea dacă este libel şi apoi transmite. Şi în acest caz există mai multe reguli.

- CSMA (Carrier Sense Multiple Access) persistent. Când o stație are date de transmis, asultă mediul şi dacă este liber transmite imediat. Din cauza timpului de propagare prin canal, o altă stație (mai apropiată sau mai depărtată) ascultând canalul îl găseşte liber şi începe şi ea să transmită. În scurt timp apare coliziunea şi ambele stații încetează emisie revenind în ascultare. La prima sesizare de canal liber începe din nou să emită.
- CSMA nepersistent diferă de primul caz prin aceea că stațiile nu sunt aşa de lacome să emită imediat ce găsesc din nou liber pe canal, ci aşteaptă un timp aleator. În acest mod sacde probabilitatea unei noi coliziuni.
- CSMA cu detecția coliziunii (CSMA/CD). Când două stații găsesc canalul liber şi încep emisia simultan, vor detecta imediat şi coliziunea şi opresc imediat transmisia cadrelor care oricum se pierd. Astfel se gâştigă oarece timp în care canalul este ocupat. Protocolul CSMA/CD este larg folosit în LAN-urile Ethernet.
- CSMA cu evitarea coliziunii CSMA/CA) este folosit în LAN-urile wireless (standardul 802.11). Evitarea coliziunii se face în acest caz prin trimiterea unui cadru scurt care să oprească toate transmisiile care ar putea exista la un moment dat.

8.2.1. Protocolul CSMA/CD

Protocolul CSMA/CD este cel pe baza căruia funcționează Ethernetul. După cum se ştie, Ethernetul se bazează pe un mediu de tip share-media, deci numai o singura stație poate transmite la un moment dat.

Când o stație doreşte să transmită, ea urmează umătorul procedeu:

- Ascultă mediul până când nu mai transmite nimeni (exista mijloace hardware de detecție a faptului că o altă stație foloseşte mediul pentru a transmite);
- Când este sesizat faptul că nimeni altcineva nu mai transmite, se aşteaptă un timp aleator şi apoi se începe transmisia. Este posibil însă ca la acelaşi moment o altă stație să fi început să transmită în acelaşi timp, caz în care apare o coliziune;
- La detectarea unei coliziuni, este transmis un semnal de bruiaj (semnalul de jam) o perioada foarte scurtă de timp, pentru a avertiza toate stațiile din rețea asupra producerii unei coliziuni.
- După ce această coliziune a fost remarcată de toate stațiile din rețea (din domeniul de coliziune mai exact), este apelat un algoritm de backoff şi transmisia încetează. Toate stațiile se opresc din transmis pentru o perioadă aleatoare de timp, după care reîncearcă să transmită.

Procedurile anterioare ridică mai multe probleme de timp (temporizare), toate depinzind de Perioada Critică (Slot Time).

Slot Time are următoarele semnificații:

- este o limită superioară a timpului necesar pentru a detecta o coliziune, deci a pierderii de banda de transmisie;
- este o limită superioară a timpului de ocupare efectivă a mediului (acquisition time of the
- medium), adică perioada după care transmisia nu mai sufera coliziuni;
- este o limită superioară a lungimii fragmentului de cadru transmis la apariția unei coliziuni;
- este o cuantă de planificare pentru retransmisie.

Pentru a acoperi aceste functii, Slot Time este definită ca fiind mai mare decât suma dintre timpul de propagare a semnalului dus-întors pe mediul fizic (de doua ori timpul necesar ca un semnal sa parcurgă drumul de la un capat la celalalt al mediului fizic)

şi timpul de bruiaj (la nivelul MAC). Acest timp depinde de particularitatile mediului fizic.

8.2.2. Protocolul CSMA/CA

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) este un protocol de acces la mediu care ascultă mediul pentru a evita coliziunile, spre deosebire de CSMA/CD, care îşi reglează transmisia de date odată ce coliziunile s-au produs.

Staţiile care fac parte dintr-o reţea fără fir emit într-o bandă de frecvenţe alocată, limitată ca dimensiune. Din cauza limitării intervalului alocat, mediul partajat de staţii este deschis coliziunilor. Tehnica de acces la mediu folosită în prezent de reţelele locale este CSMA/CA, un protocol de acces care are câteva asemănări cu CSMA/CD pe Ethernet.

CSMA/CA este proiectat astfel încât să reducă probabilitatea de coliziune la accesarea multiplă a mediului, în punctele în care e cel mai probabil să apară coliziuni, adică imediat ce mediul de transmisie devine liber în urma unei transmisii, când mai multe staţii care îşi aşteptau rândul ar putea începe să transmită.

Protocolul foloseşte ascultarea mediului, ca şi CSMA/CD. În plus, pentru a acapara mediul se trimit rezervări, în forma unor mesaje de cerere de ocupare a mediului. Distribuirea informaţiilor de rezervare a mediului se face prin interschimbarea de către staţiile care vor să converseze a unor cadre de tip RTS (Request to Send) şi CTS (Clear to Send). Aceste două tipuri de cadre conţin un câmp de durată, care specifică perioada de timp pentru care se doreşte ocuparea mediului pentru transmisia datelor, a cadrului ACK de la terminarea conversaţiei, şi a tuturor intervalelor de timp dintre cadrele trimise. routerele.

8.2.3. Domeniul de coliziune şi de broadcast

Domeniul de coliziune este acea zona dintr-o retea care va fi afectată de apariţia unei coliziuni în interiorul ei. Dispozitivele din categoria hub-urilor şi repetoarelor propagă coliziunea. Creşterea numărului de coliziuni este cauzată de intensificarea transmisiilor mai ales datorită unui număr crescând de staţii din acelaşi domeniu de coliziune şi duce la degradarea abruptă a performanţelor reţelei.

Reteaua locala poate fi împarţită în domenii de coliziune separate prin intermediul switch-urilor.

Domeniul de broadcast este constituit din staţiile care vor auzi un mesaj de tip broadcast trimis de unul dintre ele. Creşterea numărului broadcast-urilor duce la scăderea performanţelor reţelei. Singurele dispozitive care pot separa domeniile de broadcast sunt routerele.

8.3. Standardul ETHERNET

Pentru orice comunicare în reţea trebuie să existe un mecanism de adresare, care să permită recunoaşterea unică a calculatoarelor conectate.

Primul standard Ethernet a fost publicat în 1980 de un consorţiu format din firmele DEC, Intel şi Xerox, consorţiu numit DIX. Ethernet-ul funcţiona atunci pe un suport de cablu coaxial gros, numit thicknet, şi atingea viteze de până la 10Mbps.

În 1985, IEEE (Institute of Electrical and Electronics Engineers) au publicat o serie de standarde pentru LAN, serie care începea cu 802.x. Standardul pentru Ethernet este 802.3 şi a adus ceva modificări faţă de standardul iniţial propus de DIX, însă modificările sunt atât de mici, încât în linii mari cele două standarde sunt aproape identice.

Datorită creşterii spectaculoase a performanţelor în domeniul calculatoarelor personale, a fost foarte clar simţită nevoia creşterii performanţelor în lumea reţelelor, care trebuiau să poată oferi viteze de acces din ce în ce mai mari.

Astfel, în 1995 IEEE a anunțat un standard pentru Ethernet la 100Mbps - Fast Ethernet (IEEE 802.3u), iar în 1999 alt standard pentru Gigabit Ethernet (1 Gbps) - Gigabit Ethernet (IEEE 802.3z).

Formatul de bază a cadrului (frame-ului) rămâne acelaşi. Atunci când apare o dezvoltare nouă în această familie de tehnologii (aşa cum a fost cazul FastEthernet-ului şi GigabitEthernet-ului) IEEE scoate un nou supliment la standardul 802.3.

Ethernet-ul foloseşte semnalizarea în banda de bază (baseband), de aici provine şi termenul de "Base" din denumirile tehnologiilor:10BaseT, 100BaseTX, etc.

- Standardul Ethernet 802.3.

Ethernet-ul este situat pe două niveluri ale stivei OSI şi anume partea de jos a nivelului legătură de date (subnivelul MAC) şi nivelul fizic.

Pentru codificarea semnalului la nivel fizic în Ethernet sunt utilizate: codificarea Manchester (Manchester encoding) şi codificarea Manchester diferențială (diferential Manchester encoding).

- Codul Manchester la care intervalul de un bit este împărțit în două intervale egale. În prima jumătate a bitului 1 se transmite un nivel ridicat de tensiune, iar în a doua jumătate un nivel scăzut de tensiune. Bitul 0 este şi el împărțit în două jumătăți, în prima jumătate se transmite nivelul scăzut de tensiune iar în a doua jumătate nivelul ridicat;
- Codul Manchester diferențial la care bitul 0 are tranziție la începutul intevalului iar bitul 1 nu are tranziție la începutul intervalului. În ambele cazuri la jumătatea intervalului de bit are loc o tranziție între cele două nivele semnificative ale semnalului electric.

Necesitatea folosirii unor coduri de linie speciale apare din nevoia de a evita succesiunile lungi de 1 sau 0 consecutivi.

Structura cadrului Ethernet este aproape identică, indiferent de varianta de Ethernet folosită, fiind prezentată în figura 8.4.

Preambul	Început cadru	Adresa sursei	Adresa destinației	Lungime	Data	Pad	Sumă control

Fig.8.4. Formatul general al cadrului Ethernet

Semnificația câmpurilor din figura 8.4 este următoarea:

- Preambul - 7 octeți pentru sincronizarea ceasului receptorului. Fiecare octet conține şablonul de biți 10101010. Acest preambul permite ceasului receptorului să se sincronizeze cu cel al emițătorului. Ceasurile trebuie să rămînă sincronizate pe durata cadrului, folosind codificarea Manchester pentru a detecta granițele biților;
- Început cadru - 1 octet delimitator de cadru inițial;
- Adresa destinație - 6 octeți. Bitul cel mai semnificativ al adresei destinație este 0 pentru adresele obişnuite şi 1 pentru adresele de grup. Adresele de grup permit mai multor stații să asculte de la o singură adresă. Cînd un cadru este trimis la o adresă de grup, toate stațiile din grup îl recepționează. Trimiterea către un grup de stații este numită multicast (trimitere multiplă). Adresa avînd toți biții 1 este rezervată pentru broadcast (difuzare). Un cadru conținînd numai biți de 1 în cîmpul destinație este distribuit tuturor stațiilor din rețea;
- Adresa sursă - 6 octeți;
- Lungime/Tip (Type field) - 2 octeți. Câmpul Lungime/Tip poate fi interpretat în două feluri: dacă valoarea acestuia este mai mică de 1536 (0x600 în hexazecimal) atunci el reprezintă lungimea. Dacă este mai mare de 1536, el reprezintă protocolul de nivel superior folosit;
- Date – până la 1500 octeți. Pentru a facilita distingerea cadrelor valide de reziduri, Ethernet cere ca toate cadrele valide să aibă cel puțin 64 de octeți, incluzînd adresa destinației şi suma de control. Dacă porțiunea de date dintr-un cadru este mai mică de 46 de octeți, se foloseste cîmpul de completare pentru a se ajunge la lungimea minimă

necesară. Câmpul de date nu are voie să depăşească valoarea de MTU - Maximum Transmission Unit - care pentru Ethernet este 1500 octeți, ceea ce înseamnă că un cadru Ethernet nu are voie să fie mai mic de 64 şi mai mare de 1518 octeți;

- Pad – până la 46 octeți. Câmpul de date trebuie să fie mai mare de 46 de octeți. Dacă cumva datele sunt de lungime mai mică, atunci i se adaugă o "umplutură" numită padding pentru a ajunge la dimensiunea de 46 octeți
- Sumă contol (FCS) - 4 octeți. Aceasta este un cod de dispersie pe 32 de biți (32-bit hash-code) a datelor. Algoritmul sumei de control este un control cu redundanță ciclică (CRC). El realizează doar detectarea erorilor şi nu are legătură cu corectarea lor.

- Fast Ethernet (Ethernet-ul rapid) IEEE 802.3u

Din punct de vedere tehnic schimbările nu sunt multe schimbări la Fast Ethernet. În loc de codificarea Mancester se utilizează codificarea 8B/6T şi 4B/5B.

- GigaBit Ethernet (Ethernetul Gigabit) IEEE 802.3z

Ethernetul Gigabit suportă două moduri diferite de operare: modul duplex integral şi modul semi-duplex. Schema codificării semnalului la nivel fizic - 8B/10B.

8.4. Standardul pentru rețele fără fir (WLAN)

Rețelele locale fără fir (**WLAN**) oferă utilizatorilor aceleaşi facilități ca şi rețelele locale bazate pe infrastructura de cablu, dar fără limitarea impusă de fire. În plus, conform standardului, este posibilă şi conectarea fără fir la distanță mare între rețele (până la 40Km).

Standardizarea impusă rețelelor fără fir de IEEE şi Wi-Fi Alliance a permis interoperabilitatea echipamentelor, ceea ce a dus în final la scăderea costurilor şi la un proces de dezvoltare mai rapid. În momentul de față costurile de instalare a rețelei fără fir sunt considerabil mai mici, ceea ce face ca instalarea unui LAN fără fir să fie o soluție viabilă, nu numai în cazul utilizatorilor mobili, ci şi ca un substitut al LAN-urilor clasice.

IEEE 802.11 este o familie de protocoale care defineşte nivelul fizic şi subnivelul MAC al nivelului legatură de date. Standardul stabileşte ca medii de transmisie benzi de unde din domeniul infraroşu şi radio (incluzând microundele). În domeniul radio sunt specificate trei tipuri de transmisie folosind unde radio din benzile nelicențiate de frecvențe ISM de 2.4GHz şi 5GHz:

- 802.11b este primul standard lansat în domeniul rețelelor LAN fără fir, şi cea mai populară tehnologie astăzi; lucrează în banda de 2.4GHz şi atinge viteze de 11Mbps; problemele de care s-a lovit acest standard au fost încărcarea benzii ISM de 2.4GHz (în care lucrează multe alte sisteme, cum sunt Bluetooth şi cuptoarele cu microunde) şi viteza de transfer relativ mică;
- 802.11a lucrează în banda de 5GHz şi atinge viteze de 54Mbps; din cauza benzii diferite de transmisie este incompatibil cu 802.11b, dar lucrează într-o bandă de frecvențe mult mai puțin aglomerată şi oferă viteze de transmisie comparabile cu cele oferite de rețelele de cupru;
- 802.11g este în fapt un amendament la 802.11b, care specifică o viteză de transfer de 54 Mbps (egală cu viteza 802.11a); este perfect compatibilă cu tehnologia 802.11b şi oferind viteze ri de transfer.

Echipamentele necesare implementării unei rețele fără fir 802.11 sunt:

- adaptoare de rețea, care înlocuiesc plăcile de rețea tradiționale pentru calculatoare fixe sau mobile;
- acces point (AP), care este punctul central al unei rețele fără fir, dar care poate funcționa şi ca un repetor sau poate asigura conectivitatea între o rețea fără fir şi una clasică;

9. NIVELUL FIZIC

Nivelul fizic defineşte specificaţii electrice, mecanice, procedurale şi funcţionale pentru activarea, menţinerea şi dezactivarea legăturilor fizice între sisteme. În această categorie de caracteristici se încadrează nivelurile de tensiune, durata schimbărilor acestor niveluri, ratele de transfer fizice, distanţele maxime la care se poate transmite şi alte atribute similare care sunt definite de specificaţiile fizice.

Nivelul Fizic transformă cadrele în biţi pentru a putea fi transmişi prin mediul de comunicare.

Scopul nivelului fizic este de a transporta o secvenţă de biţi de-a lungul unei reţele de calculatoare. Pentru aceasta pot fi utilizate diverse medii fizice. Fiecare dintre ele este definit de lărgimea sa de bandă, întârziere, cost şi uşurinţa de instalare şi de întreţinere.

Nivelul Fizic este stratul cu numărul 1 corespunzător modelului OSI – vezi figura 9.1.

Fig. 9.1. Poziţia nivelului Fizic în structura modelului OSI

Standardele asociate nivelului fizic conţin specificaţii electrice (parametrii de semnal, proprietăţi ale mediului de comunicaţie) şi mecanice (conectică, cabluri).

Nivelul fizic are deci, rolul de a transmite datele de la un calculator la altul prin intermediul unui mediu de comunicatie. Datele sunt văzute la acest nivel ca un şir de biţi. Problemele tipice sunt de natură electrică: nivelele de tensiune corespunzatoare unui bit 1 sau 0, durata impulsurilor de tensiune, cum se iniţiază şi cum se opreşte transmiterea semnalelor electrice, asigurarea păstrării formei semnalului propagat.

Astfel, la acest strat se defineşte la nivel electric, mecanic, procedural şi funcţional legatura fizică între calculatoarele care comunică.

9.1 Funcţiile nivelului Fizic

Ca atribuţii nivelul fizic se ocupă de codarea şi sincronizarea la nivel de bit, delimitând lungimea unui bit şi asociind acestuia impulsul electric sau optic corespunzător canalului de comunicaţie utilizat.

La acest nivel se definesc:

- Tipul de transmitere şi recepţionare a şirurilor de biţi pe un canal de comunicaţii;

- Topologiile de rețea;
- Tipurile de medii de transmisie: cablu coaxial, cablu UTP sau STP, fibră optică, linii închiriate de cupru, wirelles, etc.;
- Modul de transmisie: simplex, half-duplex, full-duplex;
- Standardele mecanice şi electrice ale interfețelor;
- Este realizată codificarea şi decodificarea şirurilor de biți;
- Este realizată modularea şi demodularea semnalelor purtătoare (modem-uri).

9.2. Tipuri de medii de transmisie

Principalele medii de transmisie sunt următoarele:

- Cablu torsadat;
- Cablu coaxial;
- Fibră optică;
- Wirelles.

9.2.1. Cabluri torsadate (Twisted Pair)

Cablul torsadat este un tip de cablu, care în compoziția sa conține cupru. Se foloseşte în rețelele telefonice şi în majoritatea rețelelor Ethernet. Constă din două fire de cupru izolate, răsucite unul împrejurul celuilalt. O pereche de fire formează un circuit.

Torsadarea oferă protecție împotriva interferențelor cauzate de celelalte perechi de fire din cablu. Perechile de fire de cupru sunt acoperite intr-o izolație de plastic codificată pe culori şi sunt torsadate împreună. O izolație exterioară protejează fasciculul de perechi torsadate.

La trecerea curentului printr-un fir de cupru, este creat un câmp magnetic în jurul firului. Fiecare circuit are două fire, iar intr-un circuit cele două fire au câmpuri magnetice de sens opus. Astfel se produce efectul de anulare a câmpurilor magnetice.

Cablurile torsadate pot fi de două tipuri:

- Cablu torsadat neecranat (Unshielded twisted-pair - UTP) vezi figura 9.2.

Cablu are patru perechi de fire. Acest tip de cablu se bazează numai pe efectul de anulare obținut prin torsadarea perechilor de fire care limitează degradarea semnalului cauzată de interferențe electromagnetice (EMI) şi interferențe în frecvența radio (RFI). UTP este cel mai folosit tip de cablu în rețele. Lungimea unui segment poate fi de maxim 100 m.

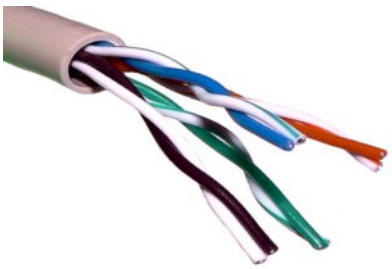

Fig. 9.2. Cablu torsadat neecranat UTP

- Cablu torsadat ecranat (Shielded twisted-pair - STP) vezi figura 9.3.

Cablu are tot patru perechi de fire. Fiecare pereche de fire este acoperită de o folie metalică pentru a ecrana şi mai bine zgomotul. Patru perechi de fire sunt ulterior învelite într-o altă folie metalică (Cablu torsadat în folie FTP – veyi figura 9.4.).

STP reduce zgomotele electrice din interiorul cablului. De asemenea reduce EMI şi RFI din exterior. Lungimea unui segment poate fi de maxim 100 m.

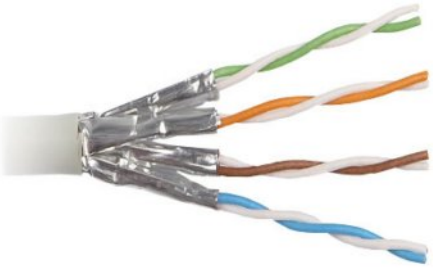

Fig. 9.3. Cablu torsadat ecranat STP

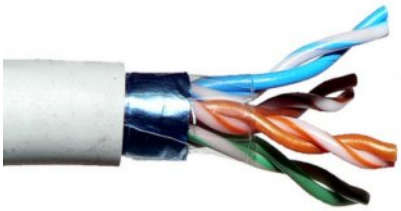

Fig. 9.4. Cablu torsadat în folie FTP

Standardul EIA/TIA (Electronic Industries Association / Telecommunications Industries Association) 568 cuprinde specificațiile cablului UTP referitor la cablarea clădirilor comerciale.

- Categoria 2 (CAT2) este certificat pentru transmisii de date de până la 4 Mbps. Conține patru perechi torsadate;
- Categoria 3 (CAT3) este certificat pentru transmisii de date de până la 10 Mbps. Conține patru perechi torsadate;
- Categoria 4 (CAT4) este certificat pentru transmisii de date de până la 16 Mbps. Conține patru perechi torsadate;
- Categoria 5 (CAT5) este certificat pentru transmisii de date de până la 100 Mbps. Conține patru perechi torsadate;
- Categoria 5e (CAT5e) este certificat pentru transmisii de date de până la 100 Mbps. Conține patru perechi torsadate. Are mai multe torsadări pe metru decât cel de categoria 5. Este descris de standardul EIA/TIA 568-B. Este cel mai folosit tip de cablu;
- Categoria 6 (CAT6) este certificat pentru transmisii de date de până la 1Gbps. Conține patru perechi răsucite. Impune specificații mai stricte pentru interferențe (crosstalk) şi zgomotul de fundal (system noise);
- Categoria 6A (CAT6A) este certificat pentru transmisii de date de până la 10 Gbps. Conține patru perechi răsucite care pot avea un despărțitor central pentru a separa perechile din interiorul cablului.

Tipul de conector şi priză folosit pentru cablul UTP şi STP/FTP se numeşte 8 Position 8 Contact (8P8C).

Denumirea mai răspândită este cea de de conector şi priză RJ-45. Pentru cablul torsadat UTP sefoloseşte conectorul RJ-45 neecranat, pentru STP şi FTP conectorul RJ-45 ecranat (vezi figura 9.5).

Conectorul şi priza RJ-45 are 8 pini care fac legătura între firele cablului torsadat şi priza UTP care se află îngropată în echipamente, de exemplu: în plăci de rețea (vezi figura 9.6).

Fig. 9.5. Conectori RJ-45 ecranat şi neecranat

Fig. 9.6. Priză RJ-45

Montarea conectorului RJ-45 se face conform standardelor TIA/EIA-568A şi TIA/EIA-568B (vezi figura 9.7).

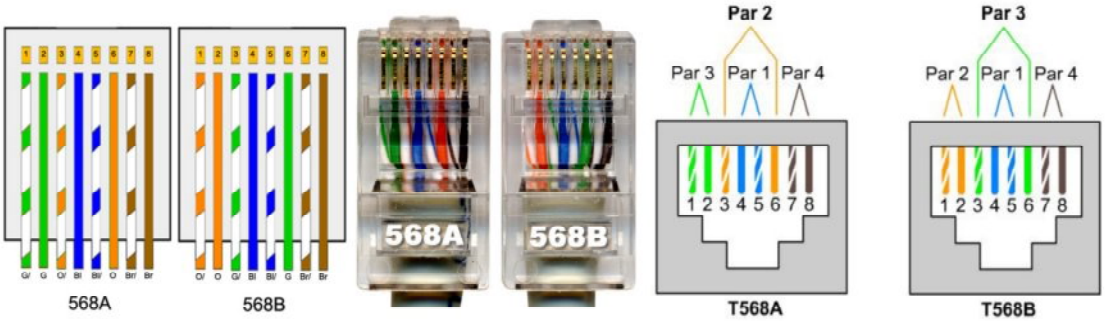

Fig. 9.7. Ordinea firelor în conectorul şi priza RJ-45 conform standardelor TIA/EIA 568A şi TIA/EIA 568B

Conectorii RJ-45 folosți pentru terminarea cablurilor UTP conțin 8 găuri în care trebuie introduse cele 8 fire, apoi cu ajutorul unui cleşte de sertizat UTP se sertizează conectorul RJ-45. În dreptul fiecărei găuri din conectorul RJ-45 se află o lamelă metalică care inițial este deasupra găurii, astfel încât firul intră uşor. În timpul acestui proces de sertizare lamela metalică din dreptul fiecărei găuri este apăsată şi străpunge firul, astfel se realizează contactul electric.

Trebuie acordată mare atenție la detorsadarea firelor. Atunci când este îndepărtat manşonul de plastic cu ajutorul unui tăietor de cabluri şi sunt detorsadate perechile pentru a putea introduce firele în conector, trebuie avută mare grijă ca bucata de cablu detorsadat să

fie cât mai mică. În caz contrar, va apărea o interferență între fire, generând crosstalk (diafonie).

Trebuie tăiați cam 3-4 cm din manşon, apoi sunt detorsadate firele, sunt aranjate în ordinea dorită conform standardului, iar apoi cu ajutorul unor lame pe care le are cleştele de sertizat, sunt tăiate firele, lăsând cam 3/4 din lungimea conectorului RJ-45. În acest fel firele vor ajunge până în capătul conectorului RJ-45, asigurând un contact electric perfect, iar bucata detorsadată va fi aproape inexistentă, minimizând riscul apariției crosstalk-ului.

Rețelele de calculatoare au ca scop primar interconectarea echipamentelor de rețea pentru asigurarea comunicării între ele. Pentru interconectare se folosesc în majoritate cabluri torsadate ecranate sau neecranate (STP, FTP sau UTP) şi conectori RJ-45.

S-au creat şi sunt aplicate anumite standarde atât în ceea ce priveşte culoarea celor 8 fire, dar şi ordinea de dispunere a acestora. Aceste standarde sunt consacrate în literatura de specialitate drept TIA/EIA 568A şi TIA/EIA 568B.

Pentru interconectarea echipamentelor de rețea se foloseşte unul dintre cele două standarde. Cele mai multe rețele sunt cablate în conformitate cu standardul TIA/EIA 568B (în Europa).

Cablurile UTP / STP / FTP folosesc doar patru fire din cele opt disponibile pentru transmiterea şi recepția datelor în rețea. Cele patru fire folosite pentru recepția şi transmisia datelor sunt:

- portocaliu;
- portocaliu-alb;
- verde;
- verde-alb.

Pinii folosiți la transmiterea datelor sunt pinii 1 şi 2, în timp ce pinii 3 şi 6 sunt utilizați pentru recepția informației. Deci se folosesc două fire pentru transmisie (Tx+ şi Tx-) şi două pentru recepție (Rx+ şi Rx-).

Firele de Tx şi firele de Rx trebuie să facă parte din aceeaşi pereche de fire. Prima pereche ajunge pe pinii 1 şi 2, iar a doua pereche pe pinii 3 şi 6.

Dacă nu este respectat standardul există marele risc ca cele două fire folosite pentru Rx sau Tx să nu facă parte din aceeaşi pereche, moment în care torsadarea nu mai este practic folosită şi nu se vor mai anula câmpurile electrice generând interferențe serioase.

Denumirea universală a cablurilor pentru interconectarea echipamentelor de rețea este Patchcord.

Un patchcord este de fapt un cablu torsadat ecranat sau neecranat cu conectori RJ-45. Un patchcord poate să fie de 3 feluri, în funcție de dispunerea firelor la cele două capete, cu fiecare dintre tipuri destinate conexiunilor între anumite echipamente.

- Straight-through cable (cablul direct) - este cel mai des utilizat tip de cablu în

rețele locale pentru interconectarea echipamentelor de rețea. Distribuția firelor, pe culori, la cele două capete ale unui asemenea cablu, este prezentată în figura 9.8.

Fig. 9.8. Ordinea firelor într-un cablu Straight-Through (cablu direct)

Cablurile straight-through sunt folosite (vezi figura 9.9) la interconectarea echipamentelor de categorii diferite, de exemplu:

- calculator cu hub/switch;
- switch cu router;

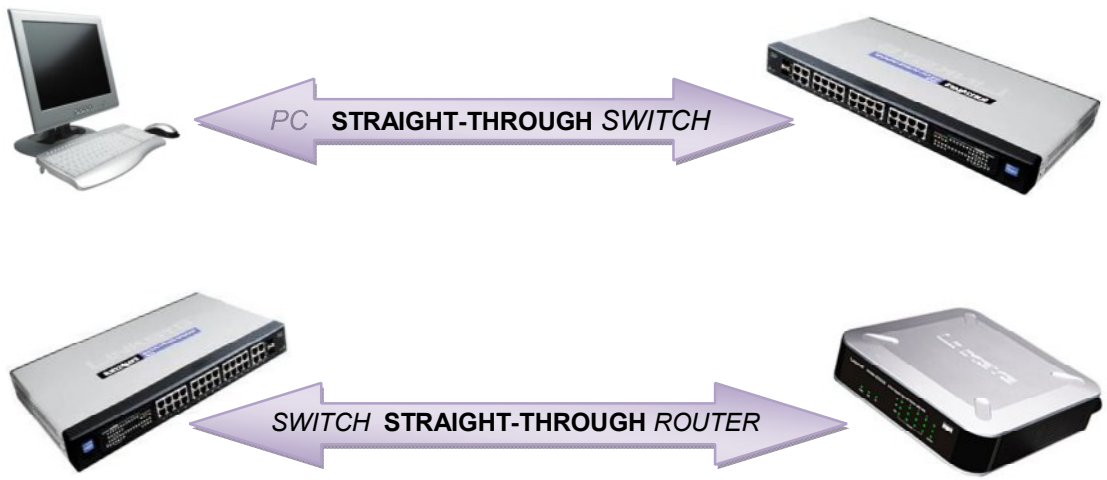

Fig. 9.9. Tipuri de echipamente ce se interconectează cu cablu Straight-Through (cablu direct)

- Cross-over cable (cablul inversor)- dacă se inversează la cele două capete ale unui patch-cord firele corespunzătoare pinilor folosiți pentru transmisie, respectiv recepție, se obține un cablu cross-over. Acest cablu inversează pinii 1 şi 2 cu pinii 3 şi 6. Pinul 1 ajunge în cealaltă parte la pinul 3 şi pinul 2 la pinul 6. Acest cablu se realizează făcând un conector pe standardul A şi una pe standardul B. Practic se inversează perechile portocaliu cu verde (vezi figura figura 9.10).

Fig. 9.10. Ordinea firelor într-un cablu Cross-Over (cablu inversor)

Cablurile crossover sunt folosite (vezi figura 9.11) la interconectarea echipamentelor similare, de exemplu:

- calculator cu calculator;
- switch cu hub;
- calculator cu router;

Un calculator foloseşte pinii 1 şi 2 ai conectorului pentru a transmite date, respectiv pinii 3 şi 6 pentru recepția informațiilor. Pentru a putea comunica între ele, două calculatoare interconectate doar printr-un cablu UTP necesită inversarea la cele două capete ale patchcord-ului a pinilor de transmisie cu cei destinați recepției. De aceea, în cazul unui asemenea aranjament, se folosesc cabluri crossover, care inversează pinul 1 cu pinul 3, respectiv pinul 2 cu pinul 6.

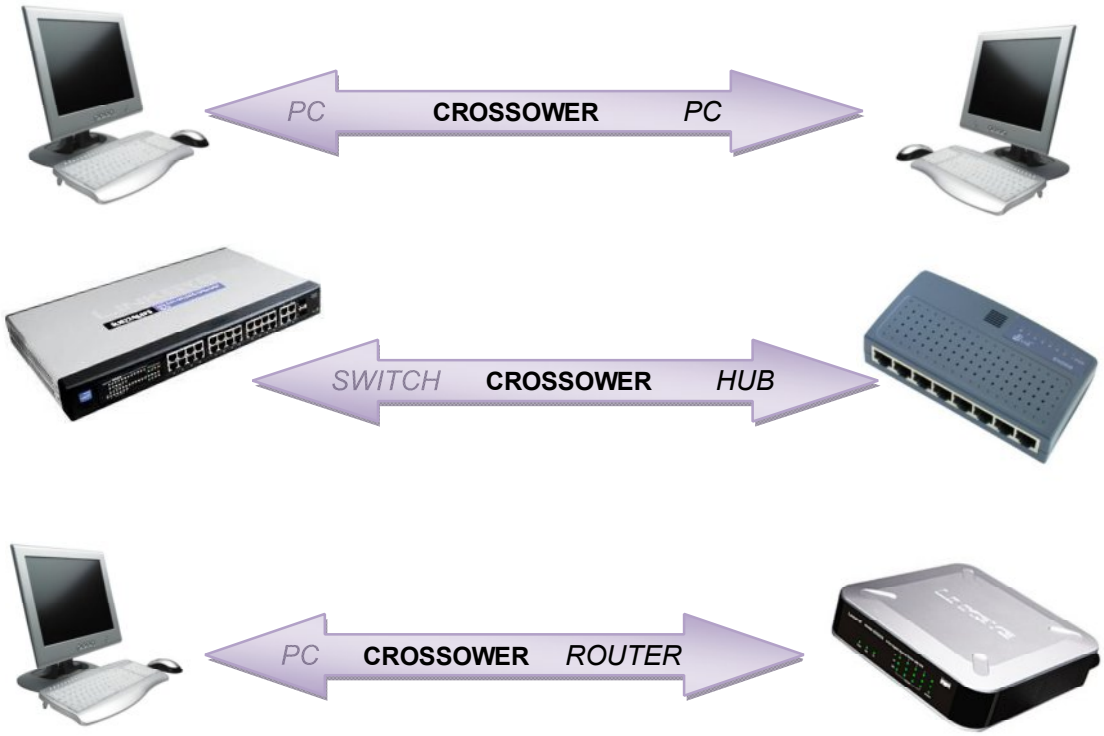

Fig. 9.11. Tipuri de echipamente ce se interconectează cu cablu Cross-Over (cablu inversor)

Switch - urile de ultimă generație acceptă ambele tipuri de cabluri (straight-through şi crossover), indiferent de echipamentul la care se conectează, autoconfigurându-se corespunzător. Tehnologia folosită care face posibilă autoconfigurarea se numeşte MDI / MDI-X.

- Rollover cable – (Cablu consolă) dacă se dispun firele la celălalt capăt în ordine inversă, se obține un cablu rollover. Este un tip de cablu null-modem care este des folosit pentru conectarea unui calculator cu portul consolă a unui router sau switch (vezi figura 9.12).

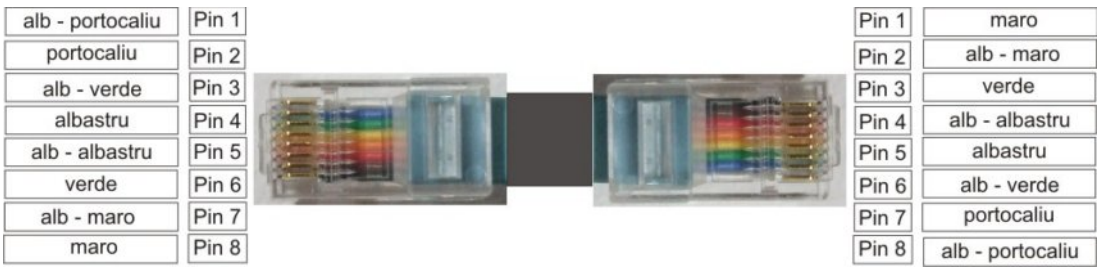

Fig. 9.12. Ordinea firelor într-un cablu Rollover (cablu consolă)

Aceste routere sau switchuri moderne sunt echipate cu un port "consolă", prin intermediul căruia se face posibilă configurarea echipamentului folosindu-se un laptop sau un desktop şi un program gen Hyperterminal

9.2.2. Cabluri coaxiale

Cablul coaxial constă dintr-un miez de cupru, înconjurat de un înveliş izolator, apoi de un strat de ecranare format dintr-o plasă metalică şi de o cămaşă exterioară de protecţie (Fig 7.1.1.1). Ecranele protejează datele transmise prin cablu, eliminând zgomotul, astfel datele nu vor fi distorsionate. Miezul unui cablu coaxial transportă semnale electrice.

Aceste semnale electrice reprezintă datele. Dacă miezul şi plasa de sârmă se ating, se produce un scurtcircuit. Acesta conduce la distrugerea datelor care circulă prin cablu.

Cablul coaxial este destul de rezistent la interferenţe. Acesta a fost motivul pentru care cablul coaxial a fost utilizat în cazul distanţelor mari.

Tipuri de cablu coaxial:

- Thicknet 10BASE5 (vezi figura 9.13) este un cablu coaxial gros (aprox. 12 mm) care a fost folosit în reţelistică şi funcţiona la viteze de 10 megabiţi pe secundă până la o distanţă maximă de 500 de metri;
- Thinet 10BASE2 (vezi figura 9.14) este un cablu coaxial subţire (aprox. 6 mm), care a fost folosit în reţelistică şi funcţiona la viteze de 10 megabiţi pe secundă până la o distanţă maximă de 185 de metri, după ce semnalul începea să se atenueze. Face parte din familia numită RG-58 şi are o impedanţă de 50 ohmi.

Fig. 9.13. Cablu coaxial de tipul Thicknet 10BASE5

Fig. 9.14. Cablu coaxial de tipul Thicknet 10BASE2

Pentru conectarea la calculator (vezi figura 9.15) se folosesc componente de conectare BNC (British Naval Connector), astfel:

- Conectorul de cablu este sertizat la cele două capete ale cablului;
- Conectorul BNC-T cuplează placa de reţea din calculator la cablul de reţea;
- Conector BNC bară conectează doua segmente de cablu coaxial subţire;
- Terminatorul BNC se foloseşte la fiecare capăt al magistralei pentru a absorbi semnalele parazite. Fără terminatoare o reţea de tip magistrală nu poate funcţiona.

Fig. 9.15. Conector de cablu; Conector BNC-T; Conector BNC bară; Terminator BNC

Cablul coaxial este destul de rezistent la interferențe. Acesta a fost motivul pentru care cablul coaxial a fost utilizat în cazul distanțelor mari.

Avantajele utilizării cablurilor coaxiale:

- Răspunsul foarte bun în frecvență (cablurile coaxiale permit transmisia unei benzi foarte largi de frecvențe, de la frecvențe joase la frecvențe foarte înalte ca în cazul semnalelor de cablu TV şi a semnalelor video analogice);
- Sunt mai robuste decât cablurile cu perechi rasucite;
- Pot fi folosite pentru distanțe mai mari decât în cazul cablurilor torsadate;
- Sunt mai ieftine decât fibra optică.

Dezavantajele folosirii cablurilor coaxiale:

- Dacă scutul din cupru nu este legat la împământare atunci vor apărea interferențe electromagnetice puternice (zgomotele electrice vor interfera cu semnalul transmis);
- Unele cabluri coaxiale au un diametru mare ceea ce determină o scădere a flexibilității şi utilizarea unor conductoare groase;
- Rata de transfer a informației este de până la 10 Mbps care este mult mai mică în comparație cu rata de transfer a cablurilor cu perechi răsucite care este cuprinsă în intervalul de la 100 Mbps la 1Gbps sau chiar 10Gbps.

Există şi alte tipuri de cabluri coaxiale :

- Cablul triaxial (triax) - vezi figura 9.16 - este un cablu coaxial care are un al treilea rând de dielectric şi material conductor. Scutul extern care este împământat protejează scutul intern de interferențe electromagnetice din afara sursei.

Fig. 9.16. Cablul triaxial

- Cablul coaxial semirigid - vezi figura 9.17 - utilizează o teacă dură din cupru.

Acest cablu oferă o ecranare superioară în comparație cu alte tipuri de cabluri chiar şi la frecvențe înalte, marele dezavantaj fiind acela, după cum spune şi numele, că nu este flexibil.

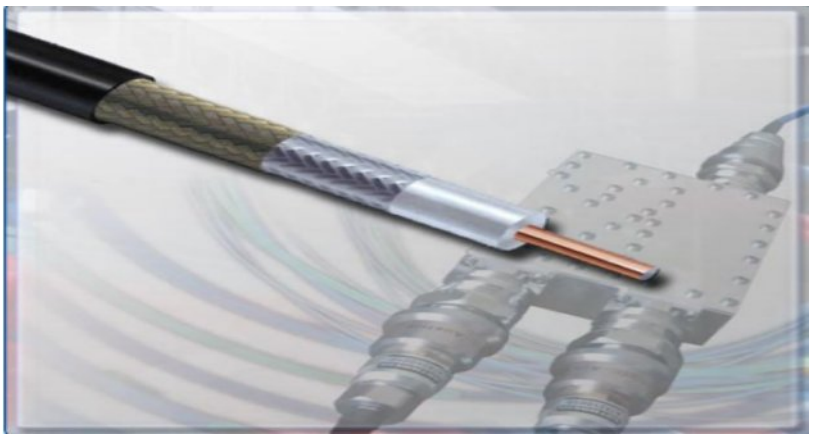

Fig. 9.17. Cablul coaxial semirigid

9.2.3. Cabluri şi conectori de fibră optică

În acest tip de cablu, fibrele optice transportă semnale de date digitale sub forma unui impulsuri luminoase modulate. Prin fibră optică nu circulă semnale electrice, ca urmare, este un mod sigur pentru transport de date, deoarece datele nu pot fi interceptate.

Un cablu cu fibră optică, este format dintr-una sau mai multe fibre optice învelite intr-o teacă sau cămaşă. Fibra optică este un conductor din sticlă sau plastic. Fibrele optice sunt alcătuite dintr-un cilindru de sticlă, numit armătură.

Fiecare fibră de sticlă transmite semnalele într-o singură direcție.

Tehnic vorbind, transmisia datelor prin fibra optică se bazează pe conversia impulsurilor electrice în lumină. Aceasta este apoi transmisă prin mănunchiuri de fibre optice până la destinație, unde este reconvertită în impulsuri electrice.

Câteva dinaAvantajele utilizării fibrelor optice sunt următoarele:

- rată de transfer foarte mare în raport cu celelalte tipuri de conexiune (practic nelimitată, şi încă imposibil de folosit la maximum de către aplicațiile existente);
- mai multă siguranță - fibra optică este insensibilă la perturbații electromagnetice şi este inaccesibilă scanărilor ilegale (interceptări ale transmisiunilor);
- posibilitatea de instalare rapidă şi simplă, în orice condiții, datorită greutății reduse a cablului optic şi existenței mai multor tipuri de cabluri;
- fibra optică reprezintă soluția pentru accesul de mare viteză la serviciile Internet, utilizând fibra optică pentru conexiuni dedicate permanente. Este recomandată firmelor cu un număr mare de posturi de lucru cuplate la rețeaua Internet şi cu un transfer informațional susținut pe tot timpul unei zile de lucru.

Proprietățile de bază ale fibrei optice sunt următoarele:

- Fibra optică are o structura cilindrică;
- Este construită din SiO_2;
- Este un ghid de undă;
- Are un coeficient de atenuare pe km foarte mic;
- Fabricată din sticlă printr-un proces de turnare la cald;
- Indicele de refracție al miezului este întotdeauna mai mare decât indicele de refracție al învelişului primar (cladding);
- Fenomenul de propagare a luminii este bazat pe reflexia internă totală în miezul fibrei.

Tipuri de cabluri cu fibră optică (vezi figura 9.18):

- Single Mode – cablul cu fibră optică unimodal permite doar unui singur mod (lungime de undă) de lumină să treacă prin fibră. Acest tip de cablu permite lățimi de bandă mari precum şi parcurgerea unor distanțe mult mai mari. Cablul are un miez foarte subțire. Este mai greu de fabricat, foloseşte rază laser ca metodă de generare a luminii şi poate transmite semnale la distanțe de zeci de kilometri cu uşurință. Lungimea maximă a cablului este de 10 km sau chiar mai mult. Miezul fibrei este de 9 microni în diametru şi transmite lumina de la laser în infraroşu (lungimea de undă este de la 1300 nm până la 1550 nm). Cablul unimodal este folosit de obicei pentru magistralele de comunicații dintre campusuri şi oraşe;
- Multimode – cablul de fibră optică multimodal permite propagarea a multiple moduri de lumină prin fibră. Cablul are un miez mai gros decât cablul single-mode. Este mai uşor de fabricat, poate folosi surse de lumină mai simple (LED-uri) şi funcționează bine pe distanțe de câtiva kilometri sau mai puțin. De obicei lungimea maximă a cablului este de 2 km. Miezul fibrei optice este de 62.5 microni în diametru şi transmite lumina în infraroşu de la LED-uri (lungimea de undă de la 850 nm la 1300 nm). Este utilizat adeseori pentru aplicațiile grup de lucru şi pentru aplicațiile intra-clădire;

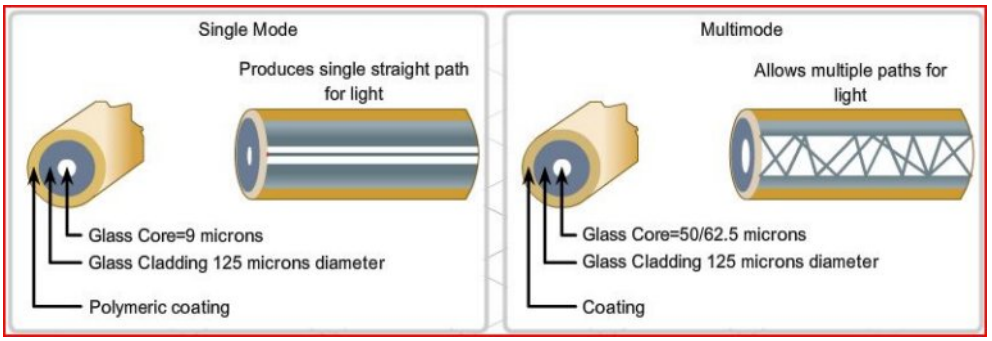

Fig. 9.18. Cabluri de fibră optică

Exista mai multe tipuri de conectori utilizați : SC, ST, LC, MT, MIC (FDDI) si FC (vezi figura 9.19) Aceste tipuri de conectori pentru fibra optică sunt half-duplex, ceea ce permite datelor să circule intr-o singură direcție. Astfel, pentru comunicație este nevoie de două fire.

Părți componente ale unei fibre optice sunt:

- miez (core) - centrul fibrei prin care circulă lumina;
- învelis optic (cladding) - material optic care înveleşte miezul şi care reflectă total lumina;
- învelis protector (coating) - înveliş de plastic care protejează fibra de zgârieturi şi umezeală

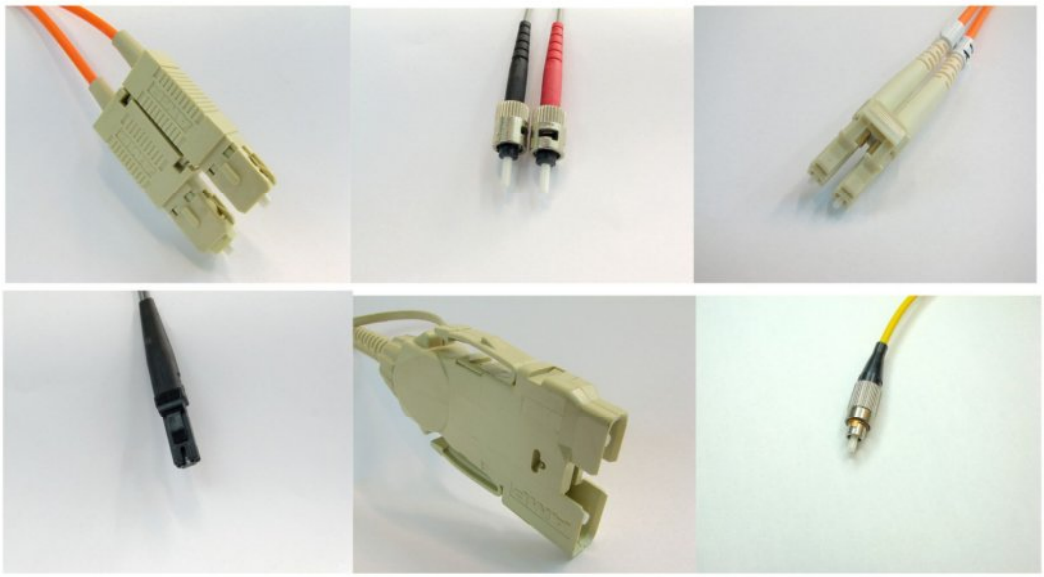

Fig. 9.19. Conectori pentru fibră optică

9.2.4. Wirelles

Wireless LAN, cunoscut şi sub denumirile de WLAN, 802.11 sau WiFi, deşi este cea mai recentă metodă de conectare, a cunoscut în ultimii ani o creştere fără precedent a popularității. Această popularitate se datorează chiar principalei sale caracteristici: lipsa cablurilor.

Reteaua wireless are drept componentă principală un echipament care se numeşte Punct de Acces. El este un releu care emite şi receptează unde radio către, respectiv de la dispozitivele din raza sa de acțiune.

Există şi dezavantaje în cazul rețelelor wireless. Pe langă cea mai uşoară utilizare şi cea mai mare flexibilitate, o reîea wireless este şi cea mai expusă din punct de vedere al vulnerabilității la interceptări neautorizate.

La nivelul fizic, oricine poate să acceseze o rețea wireless. Din fericire, nu este suficient să ai acces la nivelul fizic pentru a obține şi accesul efectiv la retea, deoarece producătorii echipamentelor de comunicații au conceput modalități de criptare a informațiilor, care să le facă inaccesibile intruşilor. Securitatea rețelelor wireless este un punct de discuție foarte aprins, deoarece din motive de necunoştinta a utilizatorilor sau de neprofesionalism al administratorilor, ori pentru a permite conectarea uşoară, aceste caracteristici de protecție nu sunt întotdeauna activate.

Figura 9.20 prezintă o imagine globală a standardelor wireless :

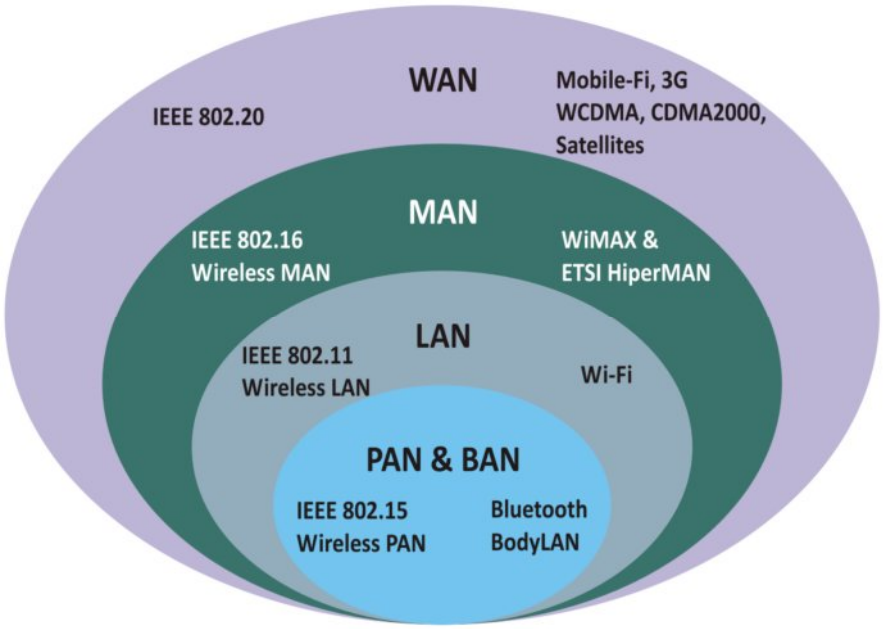

Fig. 9.20. Standarde wireless

Rețelele wireless se împart în două clase importante, factorul decisiv fiind frecvența de bandă. Tehnologiile mai vechi folosesc banda de 2.4 GHz, în timp ce variantele ulterioare folosesc banda mai lată, de 5 GHz.

În figura 9.21 se precizează principalele caracteristici ale celor mai utilizate tehnologii aplicate standardelor 802.11.

Standard	Viteză	Bandă	Distanță	Interoperabilitate
IEEE 802.11a	54 Mbps	5 Ghz	150 ft (45.7 m)	Necompatibil cu 802.11b, 802.11g, 802.11n
IEEE 802.11b	11 Mbps	2.4 Ghz	300 ft (91 m)	Compatibil cu 802.11g
IEEE 802.11g	54 Mbps	2.4 Ghz	300 ft (91 m)	Compatibil cu 802.11b

Fig. 9.21. Tehnologii 802.11

Standardul 802.11a a fost ratificat de IEEE în 16 septembrie 1999. Utilizează tipul de modulație OFDM. Are o viteză maximă de 54 Mbps cu implementări de pâna la 27 Mbps. Operează in banda ISM între 5,745 si 5,805 GHz şi în banda UNII (Unlicensed National Information Infrastructure) între 5,170 si 5,320 GHz. Aceasta îl face incompatibil cu 802.11b sau 802.11g. Frecvenței utilizate mai mari îi corespunde o bătaie mai mică la aceeaşi putere de ieşire şi, cu toate că în subgamele utilizate spectrul de frecvențe este mai

liber în comparație cu cel din jurul frecventei de 2,4 GHz, în unele zone din lume, folosirea acestor frecvențe nu este legala. Utilizarea unui echipament bazat pe acest protocol în exterior se poate face numai după consultarea autoritaților locale. De aceea, echipamentele cu protocolul 802.11a, cu toate ca sunt ieftine, nu sunt nici pe departe la fel de populare ca cele cu 802.11b/g.

Standardul 802.11b - a fost ratificat de IEEE în 16 septembrie 1999 şi este, probabil, cel mai popular protocol de rețea wireless utilizat în prezent. Utilizează tipul de modulație DSSS (Direct Sequence Spread Spectrum). Operează în banda de frecvențe ISM (Industrie, Stiinta, Medicina); nu sunt necesare licențe atât timp cât se utilizează aparatura standardizată. Limitările sunt: puterea la ieşire de pâna la 1 watt iar modulațiile numai de tipul celor care au dispersia spectrului cuprinsă între 2,412 şi 2,484 GHz. Are o viteză maximă de 11 Mbps.

Standardul 802.11g a fost ratificat în iunie 2003. În ciuda startului întârziat, acest protocol este, în prezent, de facto protocolul standard în rețelele wireless, deoarece este implementat practic pe toate laptopurile care au placa wireless şi pe majoritatea celorlalte dispozitive portabile. Foloseşte aceeaşi subbandă de frecvențe din banda ISM ca şi 802.11b, dar utilizează tipul de modulatie OFDM (Orthogonal Frecvency Division Multiplexing). Viteza maximă de transfer a datelor este de 54 Mbps, cu implementări practice la 25 Mbps. Viteza poate coborî până la 11 Mbps sau chiar la valori mai mici, trecând la tipul de modulatie DSSS, pentru a se realiza compatibilitatea cu mult mai popularul protocol 802.11b.

9.3. Codarea semnalelor codificarea şi decodificarea şirurilor de biți;

Într-o transmisiune de date, informația transmisă poate fi de origine analogică sau numerică. Un semnal este considerat numeric (digital) dacă el este discretizat în timp şi în amplitudine, ceea ce înseamnă că amplitudinea sa poate lua doar anumite valori, care rămân constante pe intervale bine precizate de timp (respectiv pe intervalul corespunzător duratei unui simbol). Pentru semnalele analogice, amplitudinea acestora variază de o manieră continuă în timp.

O informație analogică poate fi convertită în numeric, de exemplu semnalele video sau audio. De asemenea şi procesul invers este posibil, respectiv conversia din numeric în analogic.

În general, semnalul binar propriu zis nu este transmis pe linia de comunicație sub forma sa brută, ci se utilizează diverse tehnici de codare a acestuia în prealabil. Motivele care stau la baza acestei codări sunt diverse:

- Recuperarea tactului necesar unei transmisii sincrone este facilitată de către secvențele binare care prezintă tranziții cât mai numeroase între două stări care corespund unor simboluri. Este astfel de dorit evitarea transmiterii unor secvețe de date care să corespundă unor şiruri lungi de 1, respectiv 0;
- Formarea spectrală („spectrum shaping”) a semnalului ce se transmite fără a utiliza tehnici de modulare sau filtrare. Acest lucru poate fi important de exemplu în aplicațiile pe liniile telefonice, care introduc atenuări puternice ale semnalului la frecvențe mai mari de 300kHz;
- Eliminarea componentei continue din semnal;
- Utilizarea eficientă a benzii de frecvență. Se pot transmite date cu un debit mai mare utilizând aceeaşi bandă de frecvență.

9.3.1. Codarea NRZ (Not Return to Zero)

Acest tip de codare foloseşte două nivele de tensiune diferite. Astfel un „1” logic este reprezentat printr-un nivel pozitiv de tensiune (+V), în timp ce unui „0” logic îi corespunde fie o tensiune nulă (0V)- în varianta unipolară NRZ, fie o tensiune negativă (-V) dacă ne referim la NRZ bipolar.

Sunt uzuale trei tipuri de coduri NRZ (Non Return to Zero):

- NRZ-L (NRZ- Level): 1 - nivel ridicat, 0 – nivel coborât;
- NRZ-M (NRZ- Mark): 1- apare o tranziție, 0 – nu apare nici o tranziție;
- NRZ-S (NRZ- Space) 1 – nu apare nici o tranziție, 0 – apare o tranziție.

Codul NRZ-L – vezi figura 9.22 - păstrează nivelul de semnal constant în timpul intervalului de bit, fiind alocat câte un nivel fiecărei stări logice. În cazul NRZ-M sau NRZ-S are loc o schimbare (tranziție) a nivelului la începutul intervalului de bit pentru una din stările logice şi nici o tranziție pentru starea complementara.

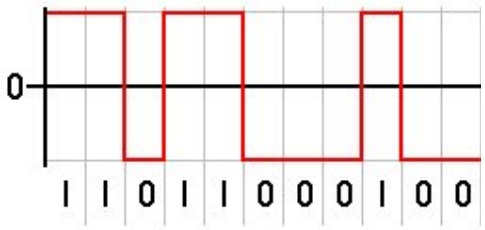

Fig. 9.22. Codare NRZ - L

În codarea NRZ_M (Non Return to Zero - Mark) bitul 1 este reprezentat alternativ prin nivelele logice H şi L iar bitul 0 este reprezentat prin nivelul logic utilizat pentru reprezentarea ultimului bit 1 - vezi figura 9.23. Această codare diferențială sau prin tranziții rezolvă problema ambiguității de fază care poate apare prin inversarea firelor unei linii de transmisie, ceea ce conduce la obținerea informației negate, în cazul utilizării codului NRZ-L.

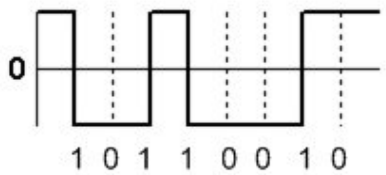

Fig. 9.23. Codare NRZ - M

În codarea NRZ_S (Non Return to Zero - Space), accepția este inversă, biții 1 şi 0 schimbându-şi rolurile.

Principalul dezavantaj al codării de tip NRZ îl constituie lipsa tranzițiilor în cazul unor secvențe lungi de biți identici, ceea ce poate duce la pierderea sincronizării la receptor.

9.3.2. Codarea Bifazică

Se utilizează trei variante ale acestui tip de codare: BIΦ-L, BIΦ-M, BIΦ-S.

Prima dintre ele (BIΦ-L) este cunoscută şi sub denumirea de codare Manchester, şi va fi prezentată ulterior.

În ceea ce priveşte codarea BIΦ-M, ea presupune apariția unei tranziții la începutul oricărui interval de bit. Dacă bitul este de „1”, atunci o a doua tranziție va apare la mijlocul intervalului de bit. Pentru transmisia unui „0” nu se va mai produce nici un fel de tranziție.

Codarea BIΦ-S este exact inversa codării BIΦ-M (tranziție la începutul intervalului

de bit, urmată de o altă tranziție la jumătatea acestui interval dacă se transmite „0”, sau fără tranziție dacă se transmite „1”).

- Codarea Manchester

Ideea care stă la baza codării Manchester este aceea de a determina o tranziție pentru semnalul emis, tranziție care să apară la mijlocul perioadei de bit. Astfel, un „1” este reprezentat printr-o tranziție de la nivelul +V la nivelul –V, în timp ce unei tranziții de la nivelul –V la nivelul +V îi corespunde un „0” - vezi figura 9.24. Este evident că în acest fel se asigură sincronizarea între emițător şi receptor, chiar şi în cazul transmisiei unor secvențe lungi de „0” sau „1”. Mai mult decât atât, întrucât simbolurile binare sunt reprezentate prin tranziții şi nu prin nivele constante (stări) ca la codarea de tip NRZ, scade drastic probabilitatea apariției unor erori. Un zgomot care afectează semnalul poate modifica nivelele transmise, dar este puțin probabil că el va duce la inversarea tranziției sau la lipsa ei, conducând astfel la erori la recepție.

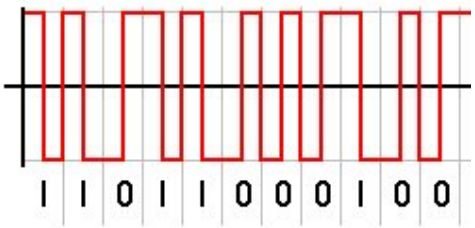

Fig. 9.24. Codare Manchester

Dezavantajul codării Manchester constă în faptul că, pentru a transmite cu un anumit debit binar, este nevoie de o bandă de frecvențe disponibilă dublă față de cea pe care am utiliza-o în cazul altor tipuri de codare.

- Codarea Manchester diferențială

La baza codării Manchester diferențiale stă prezența sau absența unei tranziții la începutul intervalului de tact. Astfel, un bit de „1” este reprezentat prin lipsa unei tranziții, în timp ce fiecare bit de „0” este semnificat prin prezența unei tranziții - vezi figura 9.25. Avantajele, respectiv dezavantajele acestui tip de codare sunt în general aceleaşi ca la codarea Manchester nediferențială.

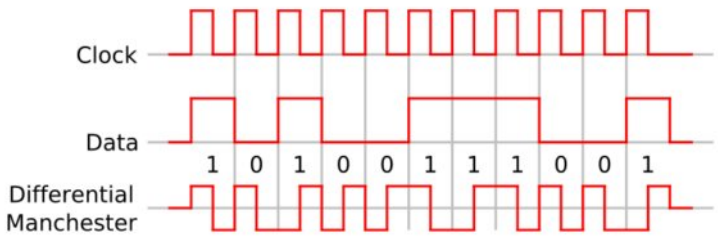

Fig. 9.24. Codare Manchester diferențială

Avantajele codurilor Manchester.

- Sunt eliminate ambele neajunsuri ale codurilor NRZ.
- Codul se autosincronizează prin existența obligatorie a unei tranzitii de nivel la mijlocul fiecărui bit.
- Nivelul mediu al semnalului în canal este 0, valabil pentru fiecare bit.

Dezavantajele codurilor Manchester

- Pentru a asigura aceeaşi viteză de transmisie de date ca la NRZ este necesară o viteză de modulare a impulsului de două ori mai mare, de aici şi o lățime de bandă a mediului de transmisie de două ori mai mare.