# I

# NOȚIUNI INTRODUCTIVE

## I.1 O SCURTĂ DESCRIERE A EVOLUȚIEI INTERNETULUI

În era ,,tehnologiei informației", industria calculatoarelor şi rețelele de telecomunicații cunosc o dezvoltare spectaculoasă, susținută de cererea mare de comunicații rapide şi sigure, pentru transmisia informațiilor fără granițe, la nivel mondial.

Colectarea, stocarea, prelucrarea şi distribuția informației reprezintă principalele preocupări ale cercetătorilor din domeniu dar şi a celor implicați în proiectarea, instalarea, întreținerea şi dezvoltarea rețelelor de calculatoare.

Ansamblul tuturor calculatoarelor interconectate între ele în cea mai largă rețea de calculatoare din lume reprezintă aşa-numitul INTERNET (INTERnational NETwork).

Prin **rețea** de calculatoare (*internet*) se înțelege un ansamblu de calculatoare şi alte echipamente de comunicații sau terminale care pot comunica între ele, fiind interconectate atât fizic, cât şi logic.

Scopul realizării unei rețele de calculatoare este acela de a partaja (*sharing*) resursele fizice (*hardware*) şi logice (*software*) existente.

Rețeaua internațională Internet, care cuprinde în prezent peste 600 de milioane de calculatoare şi mai mult de 100.000 de rețele de comunicații, îşi are originile în rețeaua

ARPAnet, apărută în 1969 ca proiect al agenției ARPA (*Advanced Research Project Agency*) din Statele Unite ale Americii.

În 1973, rețeaua ARPAnet devine o rețea internațională prin conexiunile realizate între SUA, Anglia şi Norvegia.

Din 1975, ARPAnet intră sub controlul Departamentului de Apărare al SUA (DoD – *Department of Defense*).

În 1977, Universitatea din Wisconsin SUA adaugă acestei rețele serviciul de poştă electronică (*e-mail – Electronic Mail*), iar în 1979 apare serviciul de transmisie a ştirilor în rețeaua virtuală USENET.

Adevărata naştere a Internet-ului se produce în 1983, când se trece de la protocolul NCP (*Network Control Protocol*), la suita de protocoale TCP/IP (*Transmission Control Protocol/Internet Protocol*), cu adresare ierarhizată pe baza protocolului Internet, pe 4 octeți, în format zecimal cu puncte, şi transmisia datelor în pachete IP.

În general, prin **protocol** se înțelege o suită de reguli de comunicare şi formate impuse pentru reprezentarea şi transferul datelor între două sau mai multe calculatoare sau echipamente de comunicație.

Tot în 1983, din ARPAnet se separă rețeaua militară MILNET, ARPAnet rămânând o rețea experimentală dedicată cercetării şi învățământului.

Rețelele de calculatoare s-au extins în tot mai multe țări, din toate continentele, iar nevoile de informare la distanță au creat premisele extinderii Internet-ului în peste 150 de țări.

Internetul a crescut cu mult peste scopul inițial, evoluând de la o simplă rețea tip „coloană vertebrală" (*backbone*), spre o structură cu o ierarhie pe trei nivele (*three-tired hierarchical structure*).

Pe lângă serviciul electronic clasic de transfer al fişierelor, se dezvoltă noi servicii Internet precum cele de informare Gopher (1991) şi accesare a paginilor web WWW (*World Wide Web*) sau W3 (1992), de comerț electronic (*e-commerce*), de tranzacții bancare electronice (*e-banking*), de învățământ la distanță (*e-learning*), de transmisie a vocii prin Internet (VoIP – *Voice over Internet Protocol*), de conversații în timp real (IRC - *Internet Relay Chat*), de transmisii multimedia în timp real şi nu numai.

Toate aceste servicii se bazează pe diverse aplicații Internet dezvoltate în ultimii ani, precum pagini şi site-uri web editate cu diverse limbaje (HTML – *HyperText Markup*

*Language*, XML – *Extendable Markup Language*, PHP – *Personal Home Page* sau *Hypertext PreProcessor)*, baze de date care pot fi accesate numai pentru preluare de informații şi/sau pentru înscriere de date prin intermediul formularelor electronice etc.

Numărul furnizorilor de servicii Internet (ISP – *Internet Service Provider*) este în creştere. De asemenea, vitezele oferite pentru trafic sunt mai mari, întârzierile de transmisie şi pierderile de pachete mai mici datorită dezvoltării echipamentelor de comunicație pentru rețelele de calculatoare (modem – *Modulator DEModulator,* hub, switch, bridge, router), a diversificării mediilor fizice de transmisie (cablu torsadat, cablu coaxial, fibră optică, în eter "fără fir" sau "*wireless"*), dar şi a tehnologiilor Internet: *(Ethernet, FastEthernet, GigaEthernet*, *FDDI – Fiber Distributed Data Interface, WLAN – Wireless LAN, FR – Frame Relay, ATM – Asynchronous Transfer Mode, ISDN – Integrated Services Digital Network, ADSL – Asymmetric Digital Subscriber Line* etc.).

De asemenea, accesul la Internet poate fi asigurat şi din afara unei rețele propriu-zise de calculatoare, din alte rețele de comunicații cum sunt cele de telefonie mobilă. Transportul pachetelor Internet poate fi realizat nu numai de rețelele de calculatoare dedicate acestui scop ci şi de rețele de comunicații cu alt profil, precum cele de televiziune prin cablu.

În 1999, a apărut conceptul de INTERNET 2, administrat de UCAID (*University Corporation for Advanced Internet Development*), ca parteneriat între universități, corporații şi agenții guvernamentale din întreaga lume, având ca scop dezvoltarea de noi aplicații Internet şi a infrastructurii în care se vor utiliza acestea.

Pentru dezvoltarea Internet-ului, se au în vedere noi standarde şi protocoale pentru rețelele de comunicații, asigurarea securității comunicațiilor prin operații de autentificare a mesajelor, criptare a datelor şi folosirea semnăturilor digitale, implementarea de noi servicii la cererea clienților în special pentru dezvoltarea aplicațiilor de tip „realitate virtuală" cum sunt jocurile interactive, magazinele „virtuale" pentru cumpărături on-line sau spitalele „virtuale" cu accesare de la distanță, în care pot colabora doctori din diferite țări. Companiile multinaționale îşi creează rețele de calculatoare private, securizate (*intranet*) pentru comunicații între diverse locații de pe glob, securizate față de utilizatorii din afara rețelei (din *extranet*).

Costurile din ce în ce mai reduse şi diversitatea serviciilor oferite permit creşterea continuă a numărului de utilizatori Internet din întreaga lume şi a volumului traficului Internet.

Se pune problema lărgirii spațiului de adrese IP prin introducerea protocolului IPng (*IP next generation*), cu adresare pe 128 de biți şi capacități sporite de transmisie în timp real a vocii, imaginilor şi, în general, a pachetelor multimedia.

## I.2 ASPECTE GENERALE

Într-o rețea locală sunt interconectate mai multe calculatoare-gazdă (*host*) şi unul sau mai multe servere. De asemenea, în rețea pot fi incluse şi alte echipamente terminale (imprimante, scannere, maşini de tip xerox etc.) pe care utilizatorii le folosesc în mod partajat.

Un criteriu de clasificare a rețelelor de calculatoare este mărimea lor (Tabelul I.1):

1. rețele locale (LAN – *Local Area Network*);
2. rețele metropolitane (MAN – *Metropolitan Area Network*);
3. rețele de arie largă (WAN – *Wide Area Network*).

Tabelul I.1 Clasificarea rețelelor de calculatoare după aria de acoperire

| Ordin de mărime | Arie de acoperire | **Tipul rețelei** |
|---|---|---|
| 10 m | Camera | **LAN** |
| 100 m | Clădire | **LAN** |
| 1Km | Campus | **LAN** |
| 10 Km | Oraş | **MAN** |
| 100 Km | Țara | **WAN** |
| 1000 Km | Continent | **WAN** |
| 10.000 Km | Planetă | **Internet** |

Un alt criteriu de clasificare a rețelelor este cel al modului de transmisie. Există rețele cu difuzare către toate nodurile terminale, utilizate în general pentru arii mici de acoperire, şi rețele punct-la-punct cu conexiuni fizice între oricare două noduri, fără risc de coliziune a pachetelor.

Modelarea unei rețele de calculatoare se poate face pe baza teoriei grafurilor. Echipamentele terminale sau cele de comunicație sunt reprezentate ca noduri iar fiecare conexiune fizică existență între două noduri apare ca arc în graf.

Accesul la Internet extinde aria avantajelor oferite de o rețea de calculatoare prin serviciile oferite.

Termenul de *World Wide Web,* abreviat **WWW** sau W3 semnifică un sistem informațional distribuit, bazat pe o arhitectură de tipul client-server. Sugestiv este faptul că, printre altele, cuvântul *web* înseamnă, în limba engleză, şi "pânză de păianjen".

O aplicație de tip client Web adresează o cerere unui server Web care, la rândul său, răspunde fie prin transferul unor fişiere (de tip text, imagine, audio, video etc.) de la server la client, fie prin realizarea unor legături (*hyperlink*) spre alte surse de informații.

Navigarea pe Internet se poate face prin intermediul unui program de navigare (*browser*) cum sunt *Internet Explorer, Netscape Navigator* sau *Mozilla*, în funcție de sistemul de operare instalat (*Windows, Linux* etc.).

Accesul la paginile *web* ale diferitelor persoane, firme şi instituții ori la bazele de date, publice sau private, reprezintă un mod comod şi rapid de informare.

Un utilizator conectat la Internet de oriunde în lume are acces la informație, ignorând distanțele şi economisind timp şi bani, doar dacă ştie ,,adresa" respectivei pagini sau site web. WWW tinde să devină o bază de date universală.

Prin **URL** (*URL - Uniform Resource Locator*) înțelegem formatul standard în care se specifică locația documentelor sau surselor de informație dintr-o rețea, incluzând tipul protocolului, numele serverului care găzduieşte respectivul site web şi calea spre un anumit fişier. Scopul URL constă în încapsularea informațiilor necesare unui program de rețea pentru localizarea unui obiect în Internet. El acționează ca o adresă de rețea şi identifică inclusiv metoda de acces spre obiectul respectiv.

Sintaxa generică URL este:

*tip://gazda.domeniu/port/cale/nume.*

Prin *tip* se specifică protocolul utilizat pentru comunicație. De exemplu, pe un server web WWW se foloseşte tipul *http* (HTTP - *HyperText Transfer Protocol*), pe un server de fişiere se specifică *ftp* (FTP - *File Transfer Protocol*) iar în cazul unei cereri Telnet se specifică tipul *telnet*.

*Exemplu*: http://zeta.etc.tuiasi.ro.

Caracteristicile de bază ale URL sunt prezentate în documentul RFC 1738 (*Request for Comments*) disponibil pe Internet în format electronic.

Identificarea resurselor informaționale din Internet se face standardizat prin intermediul identificatorului URI (*Universal Resource Identifier*), iar specificarea denumirii unei resurse se realizează în formatul standard URN (*Universal Resource Name*).

Domeniul este declarat în Internet prin **DNS** (*Domain Name System*), un mecanism de asociere a numelor diferitelor locații (*site*-uri) cu adresele IP numerice de 32 de biți (4 octeți exprimați în format zecimal cu puncte) ale calculatoarelor-gazdă din rețelele bazate pe suita de protocoale TCP/IP. Mai exact, adresa IP respectivă este atribuită plăcii de rețea (NIC - *Network Interface Card*) cunoscându-se adresa MAC (*Media Access Control*) a acesteia, exprimată pe 6 octeți în format hexazecimal şi alocată în mod unic de către producător astfel: primii trei octeți identifică firma producătoare (OUI - *Organizational Unique Identifier*) iar ultimii trei, cei mai puțin semnificativi, sunt alocați de către producător, echipamentului.

*Exemple*: adresă IP 193.226.26.14; adresă MAC: AF-01-EC-42-0B-D9.

DNS împarte fiecare domeniu din Internet în subdomenii, structurate ierarhic pe baza unei diagrame de tip 'arbore'. Fiecare domeniu este denumit de calea în arbore până la nodul-rădăcină, componentele fiind separate prin puncte. O componentă are cel mult 64 de caractere, iar lungimea întregii căi nu depăşeşte 255 de caractere.

Domeniile pot fi inserate în 'arbore' fie pe criteriul **geografic** (de exemplu, *ro* - este indicativul de țară pentru România; pentru alte țări se folosesc indicativele geografice ale acestora, cum sunt: *us, ca, uk, fr, jp*), fie pe criteriul **generic** (*com* - comercial, *edu* - educațional, *gov* - guvernamental, *int* - internațional, *mil* - militar, *org* - organizații nonprofit, *net* - rețele de comunicații). Căutarea adresei IP a unei destinații se face prin interogarea iterativă, recursivă sau nerecursivă, a serverelor de nume (*name server*), responsabile de anumite zone din Internet.

Indiferent care sunt firmele producătoare de calculatoare şi de echipamente de comunicații, rețeaua de comunicații trebuie să asigure legătura între toți utilizatorii. Astfel a apărut conceptul de **sistem deschis** (*Open System*) care poate interconecta echipamentele produse în diferite tehnologii, de diverşi producători, pe baza **modelului de rețea OSI** (*Open Systems Interconnection*) cu suita de protocoale specificată prin standarde ISO (*International Organization for Standardization*).

Transmisia informației în rețea se realizează prin diferite medii fizice de transmisie (conductor metalic în cablu torsadat sau coaxial, fibră optică, eter).

Pentru transmisii de date la mare distanță, pe linie telefonică sau prin undă radio pentru comunicații 'fără fir' (*wireless*), se impune utilizarea unor **modem-**uri (DCE - *Data Communication Equipment*) care să convertească şirul de biți generat de calculator în semnal analogic modulat, adaptat benzii de transmisie a canalului de comunicații.

Controlul comunicației dintre terminalele sau calculatoarele dintr-o rețea (DTE - *Data Terminal Equipment*) se realizează prin intermediul echipamentelor de comunicație (interfață*, hub, switch, bridge, firewall, gateway* sau *router*) şi al serverelor, care dispun de puternice resurse hardware şi software (Fig.I.1).

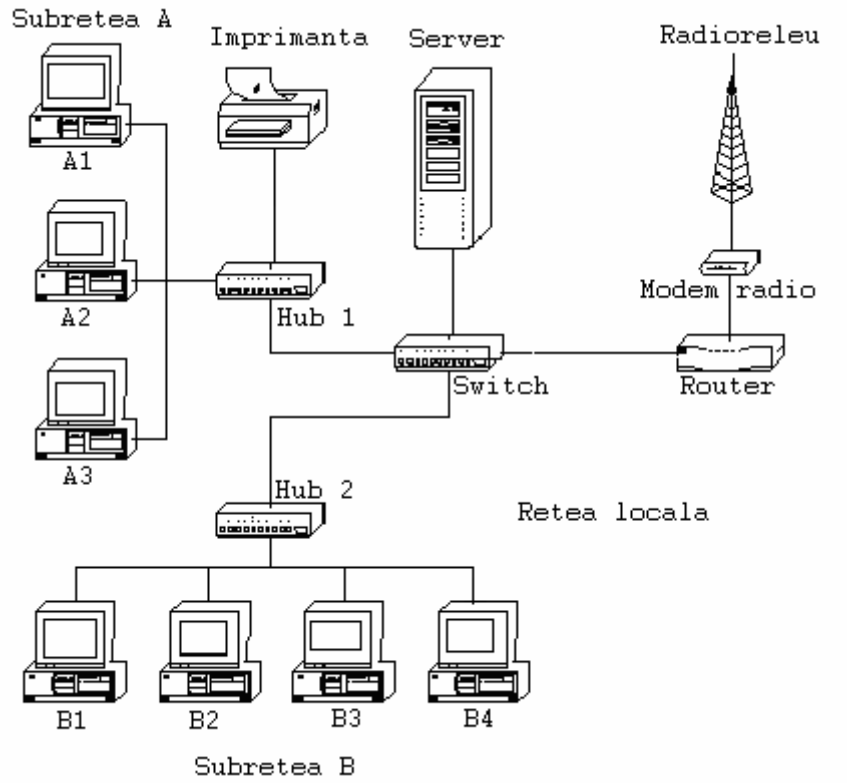


Fig.I.1. Exemplu de rețea locală cu legătură „radio" la distanță

În figură, este reprezentată o rețea locală de calculatoare cu două subrețele A şi B care deservesc două departamente. Fiecare hub asigură accesul multiplu al utilizatorilor dintr-o subrețea la un canal de transmisie reprezentat de cablul de legătură dintre switch şi hub. Evident se poate extinde rețeaua în funcție de numărul de porturi disponibile în switch.

Calculatorul server este conectat direct în switch astfel că viteza de transmisie a datelor înspre şi dinspre server este maximă.

Imprimanta de rețea poate fi activată de la distanță de către oricare utilizator din rețea.

Integrarea acestei rețele locale într-una de arie extinsă se face prin intermediul router-ului, care în particular poate funcționa ca "zid de protecție" (*firewall*).

Legătura la distanță cu alte rețele locale se poate implementa fie pe cablu, fie în eter prin undă radio. În particular, s-a considerat o legătură la distanță 'fără fir'. Modem-ul extern este necesar doar dacă nu se foloseşte un router radio.

Un radioreleu de mică capacitate amplasat corespunzător (la înălțime, pe o clădire sau pe un pilon), va asigura conexiunea cu un alt nod al rețelei WAN.

***Observații:***

1. Se preferă adoptarea şi utilizarea directă a termenilor din limba engleză întrucât achiziționarea echipamentelor se face de obicei cu documentația tehnică oferită de firma producătoare, redactată într-una din limbile de largă circulație, dintre care nu lipseşte cea engleză.

2. Includerea unui LAN într-un WAN se face prin intermediul routerului, acesta nefiind considerat o componentă a LAN-ului.

3. În graful asociat unei rețele de calculatoare, nodurile terminale corespund DTE-urilor, iar cele intermediare DCE-urilor. Arcurile, orientate sau neorientate, dintre noduri reprezintă legăturile fizice dintre echipamente. Graful rețelei este folosit pentru aplicarea eficientă a algoritmilor de rutare, bazați pe, algoritmul drumului minim" dintr-un graf (STA - *Spanning Tree Algorithm*).

O problemă acută a rețelelor o constituie asigurarea fluenței traficului informațional şi evitarea **congestiilor** (blocaje de trafic). Prin controlul traficului informațional (ca drept de acces, viteză de transmisie, lățime de bandă alocată etc.) se pot evita şi soluționa eventualele congestii din rețea.

Securitatea rețelelor de comunicație privind integritatea datelor stocate în rețea şi restricționarea accesului persoanelor neautorizate este o problemă stringentă în condițiile în care tot mai multe atacuri apar pe Internet, dar şi în rețelele locale şi regionale.

În principal, această problemă se soluționează prin configurarea adecvată a echipamentelor de comunicație (*server, bridge, router*) din rețea. La nivelul aşa-numitului *firewall* sau "zid de foc (de protecție)", echipament care aplică politica de securitate

referitoare la comunicația dintre două sau mai multe rețele, este posibil controlul accesului unităților de date prin filtrarea **pachetelor** (*packets filtering*), al utilizatorilor prin autentificare (*authentication*) pe baza unor parole (*password; passphrase*), verificarea drepturilor de accesare a anumitor aplicații prin includerea unor porți de rețea (*gateways*).

Se pot utiliza metode combinate de compresie şi criptare (ENCO - *ENcryption & COmpression*) ori cartele de acces cu suport magnetic sau optic (MAC - *MiniAccelerator Card*), pentru criptarea şi decriptarea datelor, limitând hardware accesul la informație al diferiților utilizatori. Pentru confidențialitatea mesajelor transmise prin poşta electronică se utilizează pentru criptare schema PGP (*Pretty Good Privacy*) sau algoritmii de tip MD (*Message Digest*).

## I.3 MODELUL DE REȚEA ISO/OSI

Proiectarea, întreținerea şi administrarea rețelelor de comunicații se poate face mai eficient prin folosirea unui model de rețea stratificat. De asemenea, pe baza unui model stratificat se pot realiza modulele software necesare funcționării rețelei care implementează diferite funcții (codare, criptare, împachetare, fragmentare etc.).

Organizația Internațională de Standardizare ISO a propus pentru rețelele de calculatoare **modelul OSI** (*Open Systems Interconnection*) stratificat, cu şapte nivele (*Layers*) numerotate de jos în sus (Fig.I.2):

1. nivelul fizic (*Physical Layer*)
2. nivelul legăturii de date (*Data Link Layer*)
3. nivelul de rețea (*Network Layer*)
4. nivelul de transport (*Transport Layer*)
5. nivelul sesiune (*Session Layer*)
6. nivelul de prezentare (*Presentation Layer*)
7. nivelul de aplicație (*Application Layer*).

Acestor nivele li se asociază seturi de protocoale, denumite **protocoale OSI**.

Fiecare nivel are rolul de a ascunde nivelului superior detaliile de transmisie către nivelul inferior şi invers. Nivelele superioare beneficiază de serviciile oferite de cele

inferioare în **mod transparent.** De exemplu, între nivelele-aplicație informația circulă fără erori (*error-free*), deşi apar erori de transmisie pe canalul de comunicație, la nivel fizic.

În figura I.2, calculatoarele A şi B sunt reprezentate pe baza modelului OSI. Transferul datelor de la A la B, respectiv de la B la A, se face pe traseele marcate cu linie continuă. Datele sunt transmise între echipamente prin legătura fizică.

Între nivelele similare ale terminalelor, comunicația se realizează pe baza unui protocol specific, denumit după numele nivelului. Cu excepția protocolului de la nivelul fizic, toate celelalte sunt asociate unor **comunicații virtuale** prin **legăturile virtuale** (*virtual path*) deoarece nu există o legătură reală între nivelele respective, datele transferându-se doar la nivel fizic, acolo unde are loc **comunicația reală (fizică)** dintre calculatoare, printr-un **circuit fizic**.

Dacă cele două calculatoare nu aparțin aceleiaşi rețele, atunci protocoalele de pe nivelele inferioare (1, 2 şi 3) se aplică prin intermediul echipamentelor de comunicație (*switch, bridge, router* sau *gateway*), în **subrețeaua de comunicație** sau **de transport.**

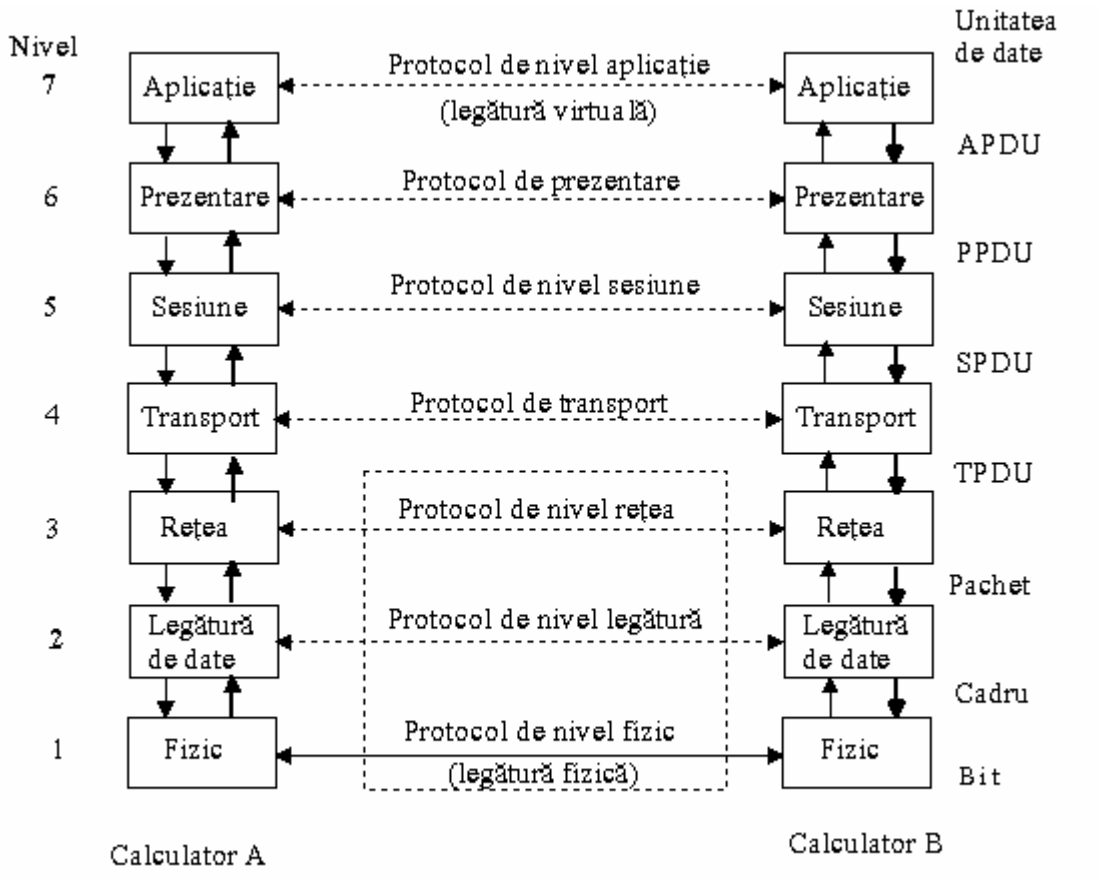


Fig. I.2 Modelul de rețea OSI și suita de protocoale OSI

Se observă că pe fiecare nivel se denumeşte altfel unitatea de date (DU - *Data Unit*).

Denumirea unității de date pe fiecare nivel al modelului OSI depinde de protocolul aplicat. În figura I.2, s-au folosit pentru nivelele superioare, termeni generici cum ar fi APDU (*Application Protocol Data Unit*), PPDU (*Presentation Protocol DU*), SPDU (*Session Protocol DU*), TPDU (*Transport Protocol DU*) care vor căpăta denumiri specifice în funcție de suita de protocoale folosită într-o anumită rețea. De exemplu, în rețelele TCP/IP se folosesc termenii de **datagramă** sau **segment** pe nivelul de transport (*L4*)**.** Pe nivelul de rețea (*L3*) se foloseşte termenul consacrat de **pachet** (*packet*). Pe nivelul legăturii de date (*L2*) se transferă **cadre de date** (*frame*). La nivel fizic (*L1*) datele sunt transmise sub formă de **biți**.

La **nivel fizic**, se transmit datele în format binar (biți 0 şi 1) pe canalul de comunicație din rețea. În standardele echipamentelor care lucrează la nivel fizic, precum şi în cele ale interfețelor fizice aferente acestora, sunt specificate caracteristicile lor electrice, mecanice, funcționale şi procedurale. Natura sursei de informație (date, voce, audio, video) nu se mai cunoaşte la acest nivel ceea ce face ca procesul de comunicație să fie considerat transparent.

La **nivelul legăturii de date** circulă **cadre** de biți, adică pachete încapsulate cu antet (H - *header*) şi marcaj final (T - *trail*), care includ adresele sursei (SA - *Source Address*) şi destinației (DA - *Destination Address*) pentru a se putea expedia datele între calculatoare. Suplimentar, în cadrul de date sunt incluse: un câmp de control al erorilor, unul responsabil de sincronizarea transmisiei, un câmp de protocol etc.

În principal, nivelul legăturii de date este responsabil de detecția erorilor de transmisie a datelor prin rețea.

Pe nivelul OSI 2, se folosesc **coduri ciclice** (CRC - *Cyclic Redundancy Checking*) care au o capacitate mai mare de detecție a erorilor decât sumele de control. Pentru aplicații speciale se codifică datele în baza unei tehnici de codare pentru corecția erorilor de transmisie (Hamming, Reed-Solomon etc.), ceea ce permite eliminarea retransmisiilor de cadre şi creşterea eficienței canalului de comunicație.

Nivelul legăturii de date este împărțit în două subnivele: LLC (*Logical Link Control*) şi MAC (*Media Access Control*) (Fig. I.3). Aceste subnivele stabilesc modalitățile de acces la mediu în cazul canalelor de comunicație cu acces multiplu şi realizează controlul traficului pentru a se evita efectele neadaptării ratelor de transmisie ale echipamentelor şi posibilitatea saturării lor (*flooding*).

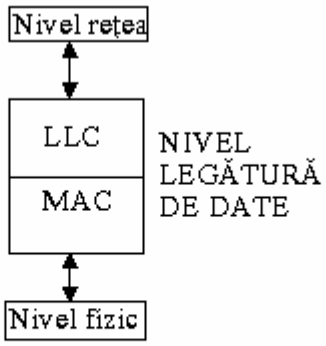


Fig. I.3 Subnivelele de nivel 2
și interconectarea cu nivelele adiacente din modelul OSI

Pe **nivelul de rețea**, se alege calea de expediere a pachetului, se realizează controlul traficului informațional din rețea şi dintre rețele, se rezolvă congestiile, eventual se converteşte formatul pachetului dintr-un protocol în altul. În unele LAN-uri, funcția nivelului de rețea se reduce la cea de stocare (*buffering*) şi retransmisie a pachetelor. În WAN-uri, la acest nivel se realizează operația de **rutare** a pachetelor, adică stabilirea căilor optime de transmisie între noduri. În Internet, se utilizează **sume de control** (*check sum*), calculate la emisie şi la recepție, prin sumarea pe verticală, modulo-2 bit cu bit în GF (*Galois Field*), a tuturor blocurilor de 16 biți din câmpul datelor (RFC 1071). Aceste sume permit detecția erorilor simple, eventual a unor erori multiple, urmată de cererea de retransmisie a pachetului.

**Nivelul de transport** deplasează datele între aplicații. Acest nivel răspunde de siguranța transferului datelor de la sursă la destinație, controlul traficului, multiplexarea şi demultiplexarea fluxurilor, stabilirea şi anularea conexiunilor din rețea. De asemenea, la acest nivel mesajele de mari dimensiuni pot fi **fragmentate** în unități mai mici, cu lungime impusă, procesate şi transmise independent unul de altul. La destinație, acelaşi nivel răspunde de refacerea corectă a mesajului prin ordonarea fragmentelor indiferent de căile pe care au fost transmise şi de ordinea sosirii acestora.

**Nivelul de sesiune** furnizează diverse servicii între procesele-pereche din diferite noduri: transfer de fişiere, legături la distanță în sisteme cu acces multiplu, gestiunea jetonului (*token*) de acordare a permisiunii de a transmite date, sincronizarea sistemului etc. O sesiune începe doar dacă legătura între noduri este stabilită, deci este orientată pe conexiune. Nivelul sesiune este considerat ca fiind interfața dintre utilizator şi rețea.

**Nivelul de prezentare** se ocupă de respectarea sintaxei şi semanticei impuse de sistem, de codificarea datelor (compresie, criptare) şi reprezentarea lor în formatul standard acceptat, de exemplu, prin codarea ASCII (*American Standard Code for Information Interchange*) a caracterelor. În plus, acest nivel supervizează comunicațiile în rețea cu imprimantele, monitoarele, precum şi formatele în care se transferă fişierele.

La **nivelul aplicație** se implementează algoritmii software care convertesc mesajele în formatul acceptat de un anumit terminal de date real. Transmisia se realizează în formatul standard specific rețelei. Față de aceste standarde de comunicație, DTE-ul real devine un **terminal virtual** care acceptă standarde de rețea specifice (de exemplu, VT100/ANSI).

Un program de aplicație pentru comunicații în rețea poate să ofere unul sau mai multe servicii de rețea, pe baza anumitor protocoale de transmisie.

Nivelele modelului OSI pot fi implementate fizic (*hardware*) sau logic (*software*). Evident nivelul fizic este implementat fizic (interfețe fizice, conectori de legătură). Nivelul legăturii de date poate fi implementat logic dar se preferă varianta fizică, aceasta asigurând viteze mari de procesare. Nivelele superioare sunt de obicei implementate logic, ca procese software, în cadrul sistemului de operare în rețea (NOS – *Network Operating System*), de cele mai multe ori inclus în sistemul de operare propriu-zis (OS – *Operating System*).

Echipamentele de comunicație din rețea se clasifică de asemenea pe baza modelului OSI.

Conectarea terminalului de date la mediul fizic de transmisie se realizează prin intermediul **interfeței fizice** cu caracteristicile specificate de nivelul fizic.

*Exemple:* ETHERNET, RS - 232 C(D), RS - 485, X.21, V.35.

Între nivelele superioare se intercalează interfețe implementate doar prin soft, denumite **interfețe logice**. De exemplu, în sistemele cu multiplexare în timp, cum ar fi sistemele de transmisie sincrone (SDH - *Synchronous Digital Hierarchy)*, un canal E1 cu 32 de canale primare trebuie partajat pentru asigurarea accesului multiplu. Utilizatorilor li se alocă anumite intervale de transmisie (*time slot*), pe baza protocolului de legătură punct-la-punct (PPP - *Point-to-Point Protocol*) prin interfețe logice *ppp.*

Echipamentele de comunicație din rețea de tip hub lucrează pe nivelul fizic.

Comutatoarele de rețea (*switch*) şi punțile de comunicație (*bridge*) sunt proiectate pe nivelul OSI 2, în timp ce routerele, configurate ca "gateway" sau "firewall", lucrează pe nivelul de rețea.

Modelul OSI este foarte general, pur teoretic, şi asigură o mare flexibilitate în cazul dezvoltării rețelelor prin separarea diverselor funcții ale sistemului pe nivele specifice. Numărul relativ mare de nivele din acest model face necesară utilizarea unui mare număr de interfețe şi a unui volum crescut de secvențe de control. De aceea, în numeroase cazuri se va folosi un număr redus de nivele. Modelul OSI nu constituie un standard, ci doar o referință pentru proiectanții şi utilizatorii de rețele de calculatoare.

# I.4 MODELUL CLIENT-SERVER

Deosebit de util pentru înțelegerea proceselor de comunicații şi realizarea programelor de aplicații pentru rețea este **modelul client-server.**

**Clientul** este partea hardware sau software care adresează o cerere (de acces, de informare, de transfer de fişiere etc).

**Serverul** este partea hardware sau software care răspunde cererii clientului (Fig. I.4).

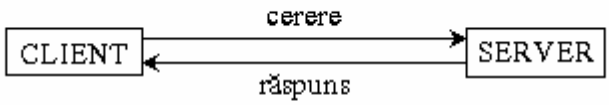


Fig. I.4 Modelul client-server

Pe aceste considerente, anumite calculatoare din rețea pe care sunt instalate programe software de tip server sunt denumite simplu servere (de nume, de fişiere, de web, de poştă electronică, de bază de date etc).

Numeroase procese de comunicație din rețea, dintre echipamente sau dintre module software, au loc pe baza modelului client-server. De multe ori, rolurile de client şi de server se inversează pe durata comunicației.

Aplicația server se autoinițializează după care rămâne într-o stare de aşteptare până la primirea unei cereri de serviciu de la un proces client. Aplicația client este cea care solicită a conexiune iar aplicația server primeşte cererea şi o rezolvă. Între cele două aplicații apare o conversație virtuală ca şi cum între ele ar exista o conexiune punct-la-punct.

# I.5 MODELUL TCP/IP

Familia de protocoale în baza căreia se realizează comunicația în rețelele eterogene de calculatoare conectate la Internet este denumită **suita de protocoale Internet** sau, mai simplu, TCP/IP (*Transmission Control Protocol/Internet Protocol*). De asemenea, termenul de **tehnologie Internet** semnifică suita de protocoale TCP/IP şi aplicațiile care folosesc aceste protocoale (RFC 1180).

Suita de protocoale TCP/IP gestionează toate datele care circulă prin Internet.

Modelul TCP/IP are patru nivele şi este diferit de modelul OSI (*Open System Interconnection*), dar se pot face echivalări între acestea (Fig.I.5).

Primul nivel TCP/IP de **acces la rețea** (*Network Access*) înglobează funcțiile nivelelor OSI 1 şi 2.

Al doilea nivel TCP/IP corespunde nivelului OSI 3 şi este denumit **nivel Internet** după numele principalului protocol care rulează pe acesta.

Al treilea nivel TCP/IP este cel **de transport,** echivalent ca nume şi funcționalitate cu nivelul OSI 4.

**Nivelul aplicație** din modelul TCP/IP include funcțiile nivelelor OSI superioare 5, 6 şi 7.

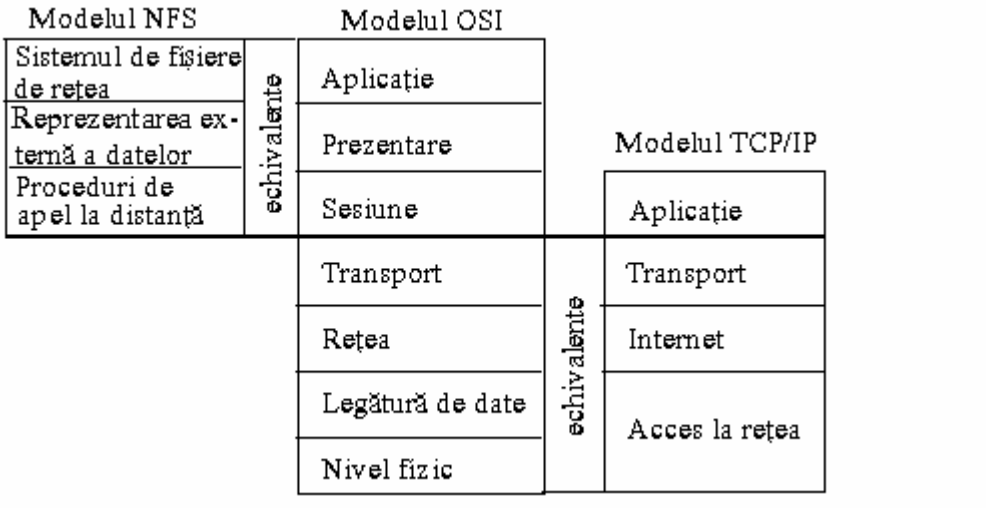


Fig.I.5 Echivalențele între modelele de rețea OSI, TCP/IP şi NFS

Modelul TCP/IP şi modelul NFS (*Network File System*) alcătuiesc împreună aşa-numitul context de operare a rețelelor deschise (ONC - *Open Network Computing*).

# I.6 SUITA DE PROTOCOALE TCP/IP

Suita de protocoale TCP/IP gestionează toate transferurile de date din Internet, care se realizează fie ca **flux de octeți** (*byte stream*), fie prin unități de date independente denumite **datagrame** (*datagram*).

Numele acestei suite de protocoale este dat de protocolul de rețea (IP) şi de cel de transport (TCP). Stiva de protocoale TCP/IP include mai multe protocoale deosebit de utile pentru furnizarea serviciilor Internet. Protocoalele de aplicație colaborează cu protocoalele de pe nivelele inferioare ale stivei TCP/IP pentru a transmite date prin Internet, mai precis pentru a oferi servicii utilizatorului (poştă electronică, transfer de fişiere, acces în rețea de la distanță, informații despre utilizatori etc).

Protocoalele din această familie sunt ierarhizate pe cele patru nivele ale modelului TCP/IP (Fig. I.6):

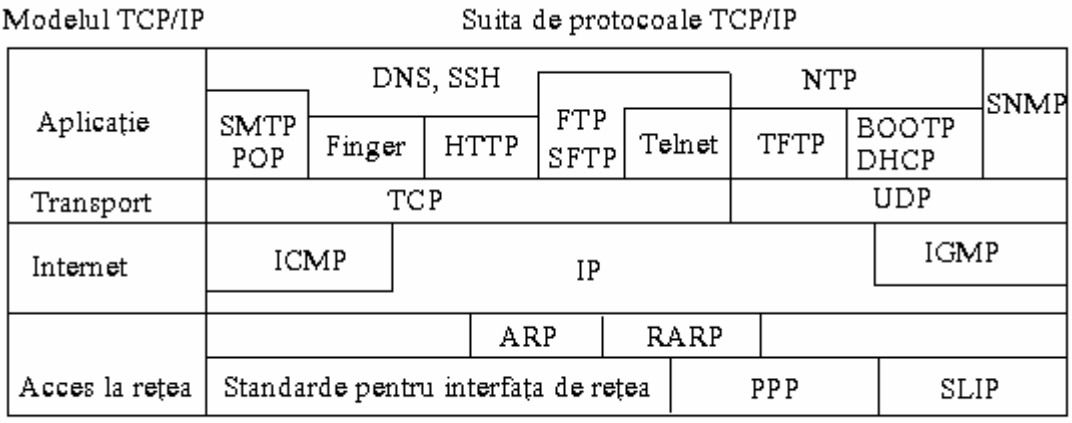


Fig. I.6 Stiva de protocoale TCP/IP

Pe nivelul de acces la rețea se definesc standardele de rețele (*Ethernet, Fast Ethernet, GigaEthernet, Token-Bus, Token-Ring, Wireless LAN* etc) şi protocoalele pentru comunicații seriale PPP (*Point -to-Point Protocol*) şi SLIP (*Serial Line Internet Protocol*).

Legătura cu nivelul Internet este făcut de cele două protocoale de adresare ARP (*Address Resolution Protocol*) şi RARP (*Reverse Address Resolution Protocol*).

ARP comunică la cerere, pe baza adresei IP a unui echipament, adresa fizică (MAC) de 6 octeți a acestuia (RFC 826). Tabelele ARP sunt stocate în memoria RAM a

echipamentului (calculator, router etc). Se pot face echivalări sugestive între numele unei persoane şi adresa MAC a echipamentului, respectiv între adresa poştală şi adresa IP, care permit localizarea destinației unui mesaj.

RARP furnizează la cerere adresa IP dată unui echipament cu adresa MAC, pe baza unor tabele de adrese (RFC 903).

ARP şi RARP se utilizează numai în interiorul unui LAN. Aceste protocoale nu folosesc IP pentru încapsularea datelor.

Pe nivelul Internet, se folosesc protocoalele IP (*Internet Protocol*), ICMP (*Internet Control Message Protocol*) şi IGMP (*Internet Group Management Protocol*).

Protocolul Internet este un protocol de nivel rețea prin intermediul căruia se transferă toate datele şi care stabileşte modul de adresare ierarhizat folosind adrese IP de 4 octeți, exprimați în format zecimal cu separare prin puncte (*dotted-decimal notation*), pentru localizarea sistematică a sursei şi destinației, într-o anumită rețea sau subrețea de calculatoare (RFC 791). Întrucât IP încapsulează datele provenite de pe nivelul de transport sau de la celelalte protocoale de pe nivelul Internet (ICMP, IGMP), nivelul de rețea mai este denumit şi **nivel IP**.

ICMP este un protocol de nivel rețea care transportă mesaje de control, de informare sau de eroare, referitoare la capacitatea sistemului de a transmite pachetele de date la destinație fără erori, informații utile despre rețea etc (RFC 792). Protocolul ICMP comunică direct cu aplicațiile, fără a accesa TCP sau UDP.

IGMP gestionează transferul datelor spre destinații de grup, care includ mai mulți utilizatori, prin transmisii *multicast* (RFC 1112).

Pe nivelul de transport se folosesc două protocoale:

TCP (*Transmission Control Protocol*) - protocol orientat pe conexiune, asemenea sistemelor telefonice. Permite controlul traficului, confirmarea sau infirmarea recepției corecte a mesajelor, retransmisia pachetelor şi ordonarea corectă a fragmentelor unui mesaj.

UDP (*User Datagram Protocol*) - protocol de transport fără conexiune, asemănător sistemului poştal clasic, mai puțin sigur decât TCP dar mai puțin pretențios.

O reprezentare echivalentă a suitei TCP/IP este dată în figura I.7. Protocoalele de pe nivelele superioare ale stivei beneficiază de serviciile furnizate de nivelele inferioare.

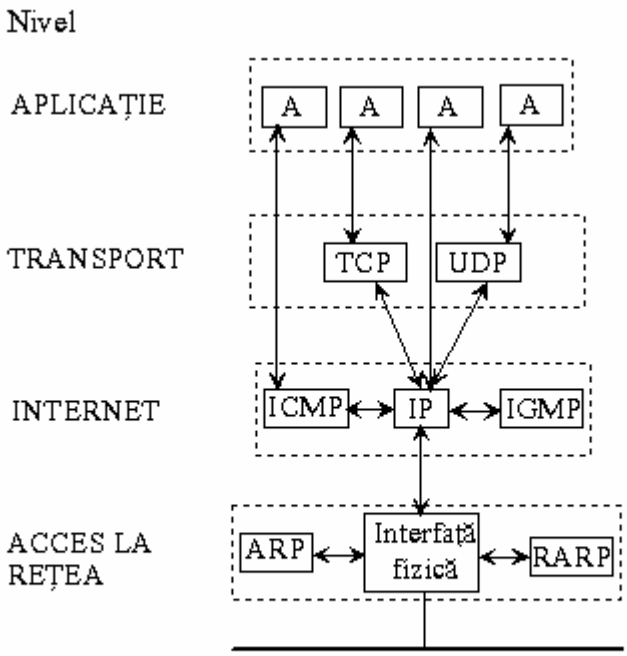


Fig.I.7 Comunicații între protocoalele din stiva TCP/IP (A= aplicatie)

Din figura I.7, se observă că un protocol de aplicație (A) poate comunica direct cu IP, dar în acest caz este nevoie să includă funcțiile de transport în propriul program de aplicație.

Toate protocoalele care folosesc încapsularea IP şi implicit adresele de rețea sunt **rutabile**.

Utilizatorul foloseşte serviciile de rețea prin intermediul unor programe de aplicații care implementează protocoalele de comunicație pentru serviciile respective, eventual folosind interfețe grafice pentru utilizatori (GUI - *Graphic Unit Interface*).

Ca **protocoale de aplicații**, care oferă direct servicii utilizatorului, se folosesc:

SMTP (*Simple Mail Transfer Protocol*) permite diferitelor calculatoare care folosesc TCP/IP să comunice prin poşta electronică (*electronic-mail*). Acest protocol stabileşte conexiunea punct-la-punct între clientul SMTP şi serverul SMTP, asigură transferul mesajului prin TCP, înştiințează utilizatorul despre noul mesaj primit, după care se desface legătura dintre client şi server (RFC 821).

POP (*Post-Office Protocol)* este protocolul prin care utilizatorul îşi preia mesajele din căsuța poştală proprie. Spre deosebire de versiunea POP 2, POP3 permite accesul de la distanță al utilizatorului la căsuța sa poştală.

FTP (*File Transfer Protocol*) este un protocol de transfer al fişierelor între calculatoare, mai precis un limbaj comun care permite comunicarea între oricare două sisteme de operare (WINDOWS, LINUX/UNIX etc) folosind programe FTP pentru client şi server. FTP foloseşte două conexiuni TCP pentru transferul sigur al datelor simultan cu controlul comunicației (RFC 959).

SFTP (*Simple File Transfer Protocol*) este o versiune simplificată a FTP, bazată pe o singură conexiune TCP, care nu s-a impus însă ca performanțe.

TFTP (*Trivial File Transport Protocol*), mai puțin sofisticat decât FTP, acesta este folosit pentru transferul unor mesaje scurte prin UDP. Se impun tehnici de corecție a erorilor întrucât UDP nu generează confirmarea de recepție corectă a mesajelor (ACK) ca TCP (RFC 783, RFC 906).

TELNET (*Virtual Terminal Connection Protocol*) este un protocol de terminal virtual care permite conectarea unui utilizator de la distanță la anumite calculatoare-gazdă, rulând programul *telnetd* al serverului. Se utilizează algoritmi de negociere cu terminalul respectiv, pentru a-i cunoaşte caracteristicile. Acesta este văzut ca un terminal virtual cu care se poate comunica de la distanță, indiferent de caracteristicile lui fizice (RFC 854, RFC 856).

FINGER (*Finger User-information Protocol*) este un protocol care permite obținerea de informații publice despre utilizatorii unei rețele.

SSH (*Secure Shell Protocol*) oferă mai multe servicii de rețea (poştă electronică, transfer de fişiere, conexiuni la distanță ş.a.) în mod securizat, folosind algoritmi de criptare.

BOOTP (*BOOTstrap Protocol*) este apelat de un utilizator pentru a-şi afla adresa IP. Acest protocol foloseşte UDP pentru transportul mesajelor. Un calculator care foloseşte BOOTP, expediază un mesaj în rețea prin broadcast (pe o adresă IP cu toți biții '1'). Serverul de BOOTP retransmite mesajul în toată rețeaua (*broadcast*) iar destinația îşi recunoaşte adresa MAC şi preia mesajul. Acest protocol nu poate lucra într-un sistem de alocare dinamică a adreselor IP, dar spre deosebire de RARP, acesta furnizează sursei atât adresa sa IP, cât şi adresele IP ale serverului şi routerului (*default gateway*) folosit de LAN (RFC 951).

DHCP (*Dynamic Host Configuration Protocol*), succesor al protocolului BOOTP, permite utilizarea unui număr limitat de adrese IP de către mai mulți utilizatori. Clientul solicită serverului DHCP o adresă IP. Acesta îi alocă o adresă dintr-un domeniu de adrese cunoscut, eventual îi furnizează şi masca de rețea. Alocarea este rapidă şi dinamică. Deşi routerele nu suportă transmisiile broadcast solicitate de ARP şi RARP, ele permit aceste

transmisii în cazul BOOTP şi DHCP ceea ce facilitează comunicațiile dintre diverse LAN-uri.

HTTP (*HyperText Transfer Protocol*), protocolul generic al serviciului de web, este folosit de utilizatorii *web* şi de serverele WWW pentru transferul unor fişiere de tip text, imagine, multimedia, în format special (*hypertext*), prin intermediul unui limbaj de editare HTML (*HyperText Markup Language*).

NTP (*Network Time Protocol*) este cel mai precis protocol de timp din Internet. Acesta sincronizează ceasurile interne din două sau mai multe calculatoare, cu o precizie de 1 - 50 ms față de timpul standard oficial (RFC 1305).

SNMP (*Simple Network Management Protocol*) este folosit pentru supravegherea funcționării rețelelor bazate pe TCP/IP (controlul statistic al traficului, performanțelor, modului de configurare şi securizare) utilizând bazele de informații de management (MIB), structurate pe baza unor reguli definite de SMI (*Structure of Management Information*) conform RFC 1155. Versiunea SNMP2 prevede posibilitatea aplicării unor strategii centralizate sau distribuite de management de rețea.

Există şi alte protocoale pe nivelul de aplicații al suitei TCP/IP care oferă diverse servicii utilizatorilor din Internet. În general, lista serviciilor Internet disponibile pe un PC din rețea, conținând informații despre protocoalele utilizate şi porturile de aplicații asociate se găseşte într-un fişier special (SERVICES), conceput ca o bază de date.

## I.6.1 PROCESUL DE ÎNCAPSULARE A DATELOR

**Încapsularea** datelor constă în adăugarea unor informații suplimentare la începutul (*header*), eventual şi la sfârşitul (*trailer*) blocului de date, în funcție de protocol.

Datele circulă în stiva de protocoale de sus în jos, în cazul transmisiei, şi de jos în sus, spre aplicații, la recepție. Datele sunt încapsulate la fiecare nivel de modulul software asociat protocolului după care sunt transmise nivelului inferior. La recepție, se preiau şi se interpretează informațiile conținute în fiecare antet pe nivelul corespunzător.

De exemplu, în cazul folosirii TCP ca protocol de transport pentru o aplicație rulată într-o rețea de calculatoare, încapsularea datelor se realizează în mai multe etape, la trecerea de pe un nivel pe altul, conform figurii I.8.

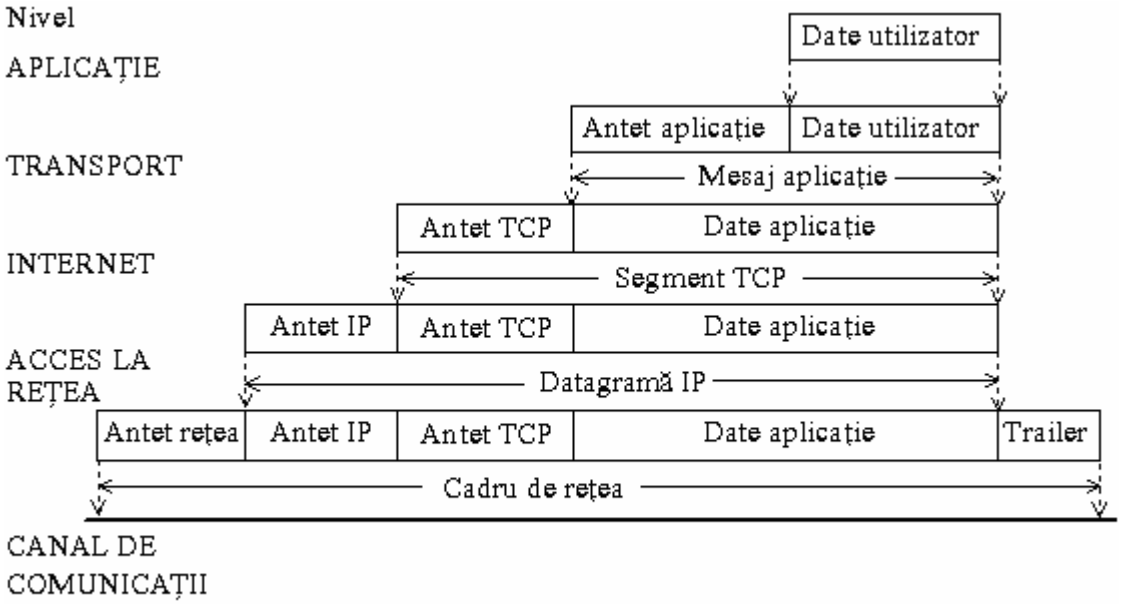


Fig.I. 8 Încapsularea datelor în stiva TCP/IP folosind TCP

Pe nivelul de aplicații, datele utilizatorului sunt încapsulate cu un antet de aplicație într-un **mesaj de aplicație.**

TCP încapsulează mesajul-aplicație cu antetul TCP generând un **segment TCP.**

Dacă se utilizează UDP ca protocol de transport, atunci mesajul-aplicație precedat de antetul UDP alcătuieşte o **datagramă UDP**.

Unitatea generată de nivelul de transport este încapsulată cu un antet IP într-o **datagramă IP**, denumită uneori şi **pachet IP** (RFC 1122).

Ca terminologie, termenul de 'datagramă' reprezintă un serviciu de livrare, specificând formatul şi conținutul unității de date, în timp ce se preferă utilizarea termenului de 'pachet' pentru unitățile de date neidentificate. Conform RFC 1122, 'pachetul' desemnează unitatea de date transferată între nivelul IP şi cel de acces la rețea.

Driverul interfeței fizice de acces la rețea va încapsula datagrama IP într-un **cadru** pe care îl transmite pe canalul fizic de comunicații.

Pe canalele sincrone, transmisia se poate face **serial**, ca şir de biți, sau **paralel,** sub formă de flux de octeți, în baza unui protocol de nivel fizic (HDLC - *High-level Data Link Control*, SLIP, PPP etc). Transmisiile în varianta "paralel" sunt admise numai pe distanțe relativ mici (de maximum 16 m).

În cazul comunicațiilor asincrone, se transmit unități de date individuale (5 - 8 biți), încapsulate cu un bit de **start** de nivel '0' logic (*low*) şi biți de **stop** (1; 1.5 sau 2 biți), de nivel '1' logic (*high*). În intervalele de **pauză de transmisie**, se menține nivelul logic '1'. Este

posibilă introducerea în cadrul datelor a unui bit de paritate (impară, pară etc) pentru detecția unui număr impar de erori de transmisie (Fig.I.9).


Fig.I.9 Formatul cadrului de transmisie asincronă

## I.6.2 IP

Protocolul Internet (IP) stabileşte modulul de distribuție a datelor pentru rețelele de comunicații bazate pe TCP/IP. Toate protocoalele folosesc IP pentru transmisie, cu excepția celor de conversie a adreselor.

Adresarea ierarhică sistematică a utilizatorilor din Internet simplifică modul de administrare a acestuia. Adresele MAC nu sunt ierarhizate şi localizarea destinației într-o rețea de arie largă este posibilă numai pe baza adreselor IP de 4 octeți, care specifică rețeaua, eventual subrețeaua în care se găseşte un anumit calculator.

Protocolul Internet este considerat nesigur întrucât nu este orientat pe conexiunea dintre sursă şi destinație dar permite identificarea corectă şi în mod unic a oricărui echipament din rețea. Realizarea transferului datelor către aplicația-destinație devine sarcina nivelului de transport şi a protocoalelor aferente acestuia.

Încapsularea datelor în formatul IP se face în **datagrame IP** sau **pachete IP** (RFC 1122), de minimum 576 octeți (B - Bytes) şi cel mult 65535 octeți (64 kB). Ca terminologie, termenul de 'datagramă' reprezintă un serviciu de livrare, specificând formatul şi conținutul unității de date, în timp ce se preferă utilizarea termenului de 'pachet' pentru unitățile de date neidentificate. Conform RFC 1122, 'pachetul' desemnează unitatea de date transferată între nivelul IP şi cel de acces la rețea.

În funcție de arhitectura de rețea adoptată (Ethernet, Token-Bus, Token-Ring etc), datagramele IP trebuie fragmentate în mai multe cadre cu lungimea maximă admisă în rețeaua respectivă, aşa-numita **unitate maximă de transfer** (MTU - *Maximum Transfer Unit*).

Formatul datagramei IP este prezentat în fig. I.10.

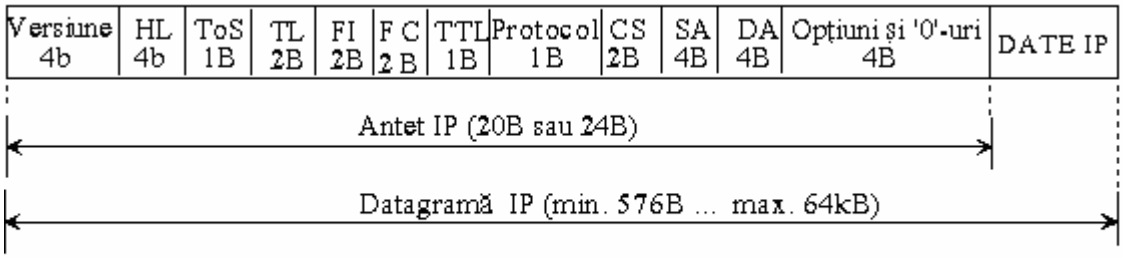


Fig. I.10 Formatul pachetului IP

Datele sunt precedate de un antet (*header*) de 20 sau 24 octeți, care include anumite câmpuri în care se specifică tipul de serviciu efectuat, gradul de securitate a transmisiei, detalii privind fragmentarea respectiv reasamblarea mesajelor de mari dimensiuni.

Semnificațiile câmpurilor din antetul IP sunt următoarele:

**Versiunea IP -** este importantă pentru evitarea incompatibilității sistemelor.

**HL** - *Header Length* - precizează, în format binar, lungimea antetului în cuvinte de 32 de biți, adică 5 sau 6 cuvinte pentru includerea unor opțiuni. În general, acest câmp are valoarea 0101. Dacă se includ opțiuni atunci valoarea câmpului devine 0110.

**ToS** - *Type of Service* - poate preciza opt nivele de precedență sau diferite condiții: prioritate, întârziere minimă, debit maxim, siguranță maximă, cost minim (RFC 1349). Majoritatea routerelor nu citesc acest câmp. De exemplu, o aplicație Telnet solicită întârzieri minime, pentru FTP se impune debit maxim, Usenet urmăreşte costuri minime iar SNMP este critic din punctul de vedere al siguranței transmisiei.

**TL** - *Total Length* - specifică pe 16 biți lungimea totală a pachetului exprimată în octeți (maximum 64 kB), inclusiv antetul IP.

**FI** - *Fragment Identification* - reprezintă un identificator (ID) al fragmentului de pachet util pentru reordonarea corectă a fragmentelor la destinație.

**FC** - *Fragment Control* - conține un indicator (*flag*) de 3 biți care precizează dacă datagrama este sau nu este fragmentată sau că acesta este ultimul fragment al ei. Ceilalți 13 biți indică poziția relativă a fragmentului în pachetul IP.

**TTL** - *Time-To-Live* - este un parametru care elimină riscul de propagare la infinit a unui pachet în rețea atunci când destinația nu este găsită. Poate fi inițializat cu valoarea maximă 255 dar se preferă valorile de 32 sau 16 pentru a evita supraîncărcarea rețelei. La fiecare router (*hop*), valoarea din câmp este decrementată cu 1. Când se ajunge la zero, pachetul este automat distrus.

**Protocol** - este un câmp care indică protocolul de nivel superior folosit pentru formatarea datelor din câmpul de date IP. Câteva valori tipice care pot fi înscrise în acest câmp sunt:

1 ICMP

2 IGMP

6 TCP

8 EGP (*External Gateway Protocol*)

17 UDP

89 OSPF (*Open Shortest Path First*).

**CS** - *Checksum* - este un câmp de control a erorilor de transmisie la nivelul header-ului, care garantează corectitudinea antetului IP, nu şi a datelor transferate.

**SA** - *Source Address* - adresa IP a sursei.

**DA** - *Destination Address* - adresa IP a destinației.

**"Opțiuni" şi '0'-uri** - reprezintă un câmp opțional folosit pentru diagnosticare (de exemplu, folosind PING - *Packet InterNetwork Groper*), securizare sau setare a rutelor. Acest câmp este completat eventual cu zerouri astfel că lungimea header-ului creşte cu 4 octeți atunci când se introduc diverse opțiuni (vezi Anexa A).

## I.6.3 DNS

Deoarece este mai comod să se rețină nume sugestive pentru utilizatorii Internet decât adrese IP, a devenit necesară conversia acestor nume în adrese IP şi invers folosind protocoale specifice de adresare precum şi crearea unei baze de date care să stocheze aceste nume. Sistemul numelor de domenii Internet (DNS - *Domain Name System*) reprezintă o bază de date distribuită prin care se alocă adrese numerice celor de tip alfanumeric, folosind diagrame-arbore, MIB-uri şi servere de nume, fiecare cu un anumit domeniu în care este autorizat să ruleze algoritmii de căutare (*authority zone*).

Asemenea claselor de adrese IP, şi aceste nume de domenii sunt structurate ierarhic, astfel încât să fie posibilă gestionarea lor în bune condiții (pe criterii de timp, unicitate, accesibilitate în baza de date etc).

Numele nodurilor din Internet sunt compuse din mai multe **etichete** separate prin puncte (de exemplu, etc.tuiasi.ro), fiecare etichetă reprezentând numele unui **domeniu Internet** în care este inclus calculatorul respectiv. Un domeniu Internet este definit pe baza unor caracteristici de activitate sau de localizare, folosind o diagramă de tip 'arbore', cu un nod 'rădăcină' şi mai multe nivele de ierarhizare (Fig. I.11).

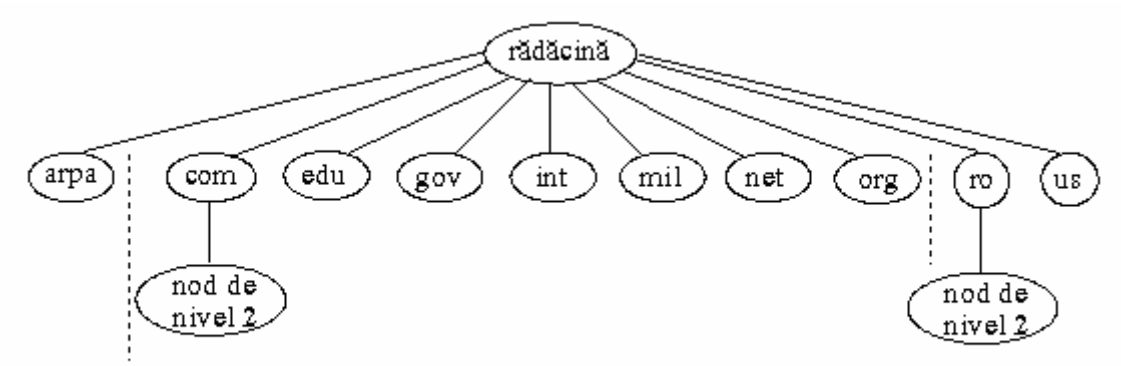


Figura I.11 Structura de bază a DNS

Pe primul nivel, DNS este împărțit în trei domenii:

1. **ARPA** (*Advanced Research Projects Agency*) - domeniul responsabil de transformarea numelor de domenii Internet în adrese numerice (IP)ş

2. **grupul generic** al organizațiilor, cuprinzând şapte categorii de bază, fiecare asociată unei etichete compusă din trei caractere (*com* - comercial, *edu* - educațional, *gov* - guvernamental, *int* - internațional, *mil* - militar, *org* - organizații nonprofit, *net* - rețele de comunicații).

3. **grupul geografic** al țărilor, specificate prin etichete cu două caractere stabilite de ISO (ISO 3166). De exemplu, ro - România, us - Statele Unite ale Americii, uk - Marea Britanie.

Fiecărui nod de pe primul nivel al diagramei îi corespund mai multe noduri de nivel 2, care la rândul lor au legături cu noduri de nivel 3 ş.a.m.d., rezultând o diagramă mult ramificată, dar structurată ierarhic pe principiul prefixului. Astfel se realizează identificarea în mod unic a fiecărui domeniu şi subdomeniu Internet.

InterNIC gestionează numai domeniile de pe primul nivel, subdomeniile fiind în responsabilitatea unor organizații regionale, respectiv a administratorilor fiecărei rețele locale.

Deoarece numărul subdomeniilor Internet este foarte mare, nu este indicată crearea unei baze de date unice pentru memorarea tuturor numelor din Internet, ci s-a preferat realizarea unei **baze de date distribuite** care memorează datele pe mai multe calculatoare dedicate programelor server de nume, numite simplu **servere de nume** sau **servere DNS**. Fiecare server gestionează calculatoarele dintr-un subdomeniu sau **zonă**, adică o anumită clasă de adrese IP.

Programul-client pentru translarea numelor de domenii Internet apelează o funcție de translare a adreselor, care deschide un canal de comunicație cu programul-server DNS, transmite cererea şi după ce primeşte de la server informația despre adresa respectivă, închide canalul şi transmite informația programului-client.

În funcție de modul în care serverul DNS răspunde cererii unui program-client DNS de translare a numelor (*name resolver*) şi furnizare a adresei IP asociate unui domeniu Internet, neinclus în baza de date proprie, aceste servere sunt de două tipuri:

1. **iterative** - răspunde negativ clientului, indicându-i acestuia să continue căutarea pe alt server de nume.

2. **concurențiale (recursive)** - rezolvă cererea prin contactarea altor servere DNS.

Pentru evitarea blocării unei rețele prin defectarea serverului DNS, este recomandată utilizarea a cel puțin un server de nume secundar sau de rezervă (*backup*), care deține o copie a bazei de date de pe serverul primar, periodic reactualizată. Prin utilizarea bazei de date distribuite pentru DNS şi a serverelor de nume secundare creşte siguranța funcționării sistemului numelor de domenii Internet.

Un server de nume primar nu dispune de adresele tuturor celorlalte servere similare din DNS, ci cunoaşte numai adresa serverului de nume 'rădăcină', de pe primul nivel al diagramei DNS, memorată în fişierul său de configurare. Fiecare server de nume 'rădăcină' are memorate numele şi adresele tuturor serverelor de nume de pe nivelul 2. În general, fiecare server deține o bază de date în care sunt incluse numele şi adresele altor servere de pe nivelele învecinate în vederea redirecționării cererilor pe care nu le poate soluționa.

Lista completă a serverelor de nume 'rădăcină' se găseşte pe Internet, în fişierul netinfo/root_server.txt.

## I.6.4 ARP, RARP

**Protocolul ARP** (*Address Resolution Protocol*) realizează conversia adreselor IP în adrese MAC, pe baza unor tabele ARP (RFC 826).

Unele sisteme de operare (Windows 9x, Windows NT) folosesc ARP pentru a se asigura că nu există adrese IP duplicate. Cererea ARP (exprimând "Care este adresa ta MAC?") se transmite în rețeaua locală în modul broadcast. Dacă adresa IP respectivă este alocată altui nod din rețea, atunci sistemul de operare nu inițializează suita TCP/IP şi generează un mesaj de eroare.

Transmisiile broadcast încarcă rețeaua. De aceea, se preferă păstrarea în memoria *cache* (de
tip RAM) a tabelelor ARP, în care se stabilesc corespondențele dintre adresele fizice şi adresele IP uzuale (*bindings*). În cazul alocării dinamice a adreselor, anumite informații din aceste tabele pot fi rejectate dacă nu sunt accesate în mod curent.

Cererea ARP (*ARP Request*) este transmisă în rețea numai dacă adresa solicitată nu există în tabelul ARP. Pachetul cu cererea ARP conține adresa MAC de broadcast, adresa MAC a sursei, adresele IP ale sursei şi destinației, precum şi un cod de cerere ARP (Fig.I.12). Stația de destinație din rețeaua locală răspunde printr-un alt pachet (*ARP Reply*) adresat stației care a inițiat cererea, pachet care include adresa sa MAC.

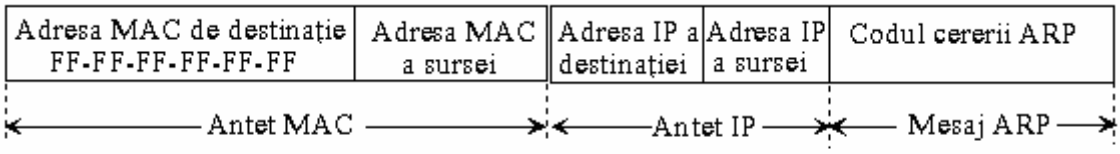


Fig.I.12 Formatul cadrului conținând cererea ARP

Când recepționează pachetul de răspuns, sursa îşi completează tabelul ARP cu noile adrese (MAC şi IP).

Dacă sursa nu primeşte nici un răspuns, atunci cererea este retransmisă. Dacă nici la retransmisie nu se răspunde, sursa recepționează un mesaj de eroare generat de protocolul ICMP.

În cazul în care destinația nu se află în rețeaua locală, routerul de legătură cu WAN-ul răspunde cu propria sa adresă, prin tehnica numită **Proxy ARP** (RFC 1027)**,** dacă prin configurarea conexiunii gazdei cu rețeaua nu este dezactivată opțiunea *proxy***.**

**Protocolul RARP** (*Reverse Address Resolution Protocol*) face conversia inversă, a adreselor fizice în adrese de rețea.

Dacă o stație de lucru nu-şi cunoaşte adresa IP, atunci trimite serverului RARP un pachet cu o cerere RARP (cu semnificația "Care este adresa mea IP?"), în modul broadcast (pentru Ethernet, se foloseşte adresa IP de destinație cu toți biții din câmpul gazdei egali cu '1').

Pachetul RARP include adresele MAC ale sursei şi destinației, adresa IP de broadcast, un câmp de adresă IP necompletat pentru adresa IP proprie şi codul cererii RARP, conținut în memoria sa ROM (Fig.I.13). Serverul RARP răspunde cererii cu un pachet conținând adresa IP solicitată.

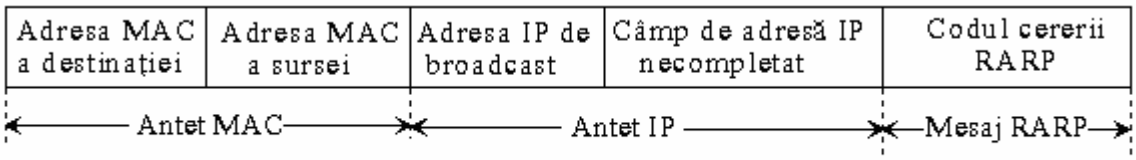


Fig.I.13 Formatul pachetului conținând cererea RARP

***Observație:***

Routerele nu retransmit în afara LAN cererile ARP/RARP în modul broadcast, evitând propagarea infinită a lor în WAN.

## I.6.5 BOOTP, DHCP

Adresa de rețea poate fi alocată unei interfețe în mod static sau în mod dinamic. **Static**, se stabileşte de către administratorul de rețea şi este setată în fişierul de configurare al echipamentului (stație terminală, router etc). Există riscul să se aloce aceeaşi adresă mai multor utilizatori, ceea ce creează erori de trafic sau face imposibilă conectarea stațiilor în rețea. Administratorii de rețea trebuie să aibă o evidență clară a adreselor alocate pentru a evita duplicarea lor. De aceea, în rețelele de mari dimensiuni, se preferă **metoda dinamică** de

alocare a adreselor de rețea, care face ca un anumit spațiu de adrese să fie folosit de mai mulți utilizatori. În acest caz, un utilizator nu va avea aceeaşi adresă la fiecare conectare. Metoda are dezavantajul că filtrarea traficului pe baza adreselor de rețea devine ineficientă.

**Protocolul BOOTP** (*BOOTstrap Protocol*) este apelat de un utilizator pentru a-şi afla adresa IP (RFC 951). Acest protocol foloseşte UDP pentru transportul mesajelor şi IP pentru încapsulare, fiind un protocol de nivel aplicație din suita TCP/IP.

BOOTP a fost inițial proiectat pentru stațiile de lucru fără disc, pe care nu erau memorate informațiile de configurare IP. Pe serverul BOOTP există o bază de date în care se stochează adresele MAC ale stațiilor din LAN şi adresele IP asociate fiecăreia, în mod static. Un calculator care foloseşte BOOTP, expediază cererea de aflare a adresei IP proprii (*BOOTP Request*) în rețea, prin broadcast (pe o adresă IP cu toți biții '1'). Serverul BOOTP transmite automat răspunsul (*BOOTP Reply*) în toată rețeaua prin broadcast, iar destinația îşi recunoaşte adresa MAC şi preia mesajul.

Acest protocol nu poate lucra într-un sistem de alocare dinamică a adreselor IP, dar spre deosebire de RARP, el furnizează sursei atât adresa sa IP, cât şi adresele IP ale serverului şi ruterului (*default gateway*) folosit de LAN.

Protocolul BOOTP este rutabil şi cererile clienților BOOTP sunt retransmise de router în afara LAN, prin **agentul de retransmisie BOOTP** (*BOOTP Relay Agent*) definit în RFC 1542. Acesta permite retransmisia prin router a răspunsurilor BOOTP către clienții conectați direct la router, dar şi pentru clienții din alte rețele, întrucât mesajul BOOTP este tratat sub formă de pachete IP şi retransmis unicast, multicast sau broadcast (*forwarding*) între rețelele locale din WAN, cu limitarea numărului maxim de noduri (*hops*) prin care trece pentru a nu încărca inutil rețeaua.

**Protocolul DHCP** (*Dynamic Host Configuration Protocol*) este succesorul protocolului BOOTP. DHCP permite utilizarea unui număr limitat de adrese IP de către mai mulți utilizatori prin metoda alocării dinamice (RFC 1541).

Clientul transmite cererea DHCP prin broadcast, cu adresa MAC proprie, pentru a i se aloca o adresă IP. Serverul DHCP îi răspunde clientului, identificat pe baza adresei MAC, oferindu-i o adresă IP şi o mască de rețea, cu o perioadă de valabilitate prestabilită. Clientul transmite serverului un mesaj de acceptare după care acesta îi confirmă primirea acceptului (ACK - *Acknowledge*) şi îi furnizează informații suplimentare despre serverul DNS şi gateway-urile disponibile.

Alocarea este rapidă şi dinamică, protocolul fiind deosebit de util pentru terminale mobile şi pentru serviciul de roaming în WAN.

***Observații:***

1. Întrucât DHCP alocă dinamic adresele IP şi identificarea stațiilor se face pe baza numelor, apar probleme de actualizare a bazelor de date de pe serverele DNS. De aceea, se preferă utilizarea DHCP cu servere WINS (*Windows Internet Name Service*)

2. Deşi routerele nu suportă retransmisiile broadcast solicitate de ARP şi RARP, ele permit aceste retransmisii în cazul BOOTP şi DHCP, ceea ce facilitează comunicațiile dintre diverse LAN-uri.

3. Suplimentar față de metoda alocării dinamice, DHCP suportă şi modul automat, şi modul manual de alocare a adreselor într-o rețea TCP/IP. Modul automat presupune alocarea de adrese IP permanente nodurilor din LAN. În modul automat, DHCP este utilizat doar pentru intermedierea procesului de negociere a adresei, dintre administratorul de rețea şi stația-gazdă.

În multe rețele, doar un număr mic de utilizatori dintr-un subdomeniu privat (*stub domain*) comunică în afara rețelei, celelalte comunicații realizându-se local. În general, acestor domenii li se alocă doar câteva adrese IP reale (în particular, o singură adresă). Se pot utiliza local, în mai multe subdomenii, aceleaşi adrese IP private, fiind necesară translarea lor în adrese IP publice doar pentru comunicațiile cu exteriorul. Pentru aceasta, echipamentele prin care un subdomeniu este interconectat în LAN sau WAN sunt configurate să aplice **procedeul de translare a adreselor** (NAT - *Network Address Translation*), pe baza unor tabele de translare (RFC 1631). În fiecare punct de ieşire din subdomeniu, adresa IP a sursei din fiecare pachet care urmează a fi transmis în Internet este translată, în mod static sau dinamic, într-o adresă IP globală, rezervată pentru NAT (RFC 1597).

Procedeul **NAT extins** (ENAT - *Enhanced Network Address Translation*) este utilizat pe scară largă în rețelele TCP/IP private (*stub domain*), care solicită o singură adresă IP globală din partea furnizorului de servicii Internet. Routerele de acces în WAN translează adresa IP a sursei în adresa IP globală şi numărul portului de protocol în cel prestabilit. Procedeul ENAT asigură o bună securitate la nivelul firewall-ului, o mare flexibilitate în alegerea ISP, dar are ca dezavantaj reducerea vitezei de transfer prin procesul de modificare a antetelor şi a sumelor de control din pachetele transmise. Există mai multe moduri de aplicare a procedeului ENAT: static, dinamic sau bazat pe tipul interfeței de acces în Internet.

Translarea statică a adreselor IP permite accesarea rețelei de oriunde din Internet, eventual numai pe un anumit port de protocol. Metodele dinamice de translare asigură o mai bună securitate a rețelei, prin limitarea accesului din afara acesteia.

## I.6.6 TCP, UDP

În suita de protocoale TCP/IP, pe nivelul de transport se pot folosi două protocoale, **TCP** (*Transport Control Protocol*) şi **UDP** (*User Datagram Protocol*), care oferă servicii de transport protocoalelor de aplicație.

**Protocolul TCP** este orientat pe conexiunea punct-la-punct dintre sursă şi destinație, realizând transferul sigur al informațiilor, fără erori. TCP foloseşte mesaje de confirmare a recepției corecte a fiecărui pachet şi cere retransmisia celor eronate.

Mesajul de pe nivelul aplicație este fragmentat în mai multe secvențe, pentru a nu depăşi lungimea maximă admisă a unității de date transmise pe nivelul fizic (MTU - *Maximum Transfer Unit*). Datele sunt este încapsulate cu antetul TCP (Fig. I.14) şi generate ca **segment TCP.** Acesta devine câmpul de date în datagrama IP. La recepție, TCP este responsabil de refacerea mesajului prin asamblarea corectă a tuturor secvențelor sale.

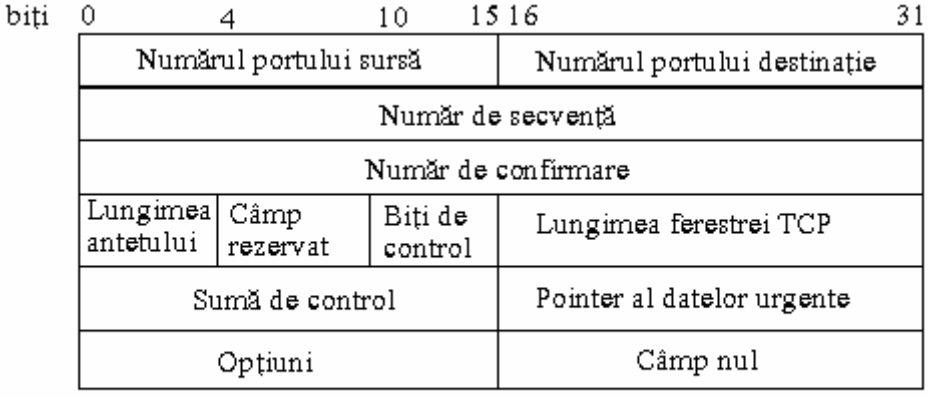


Fig.I.14 Formatul antetului TCP

În antetul TCP sunt specificate, pe 16 biți, **numerele porturilor logice** asociate aplicațiilor sursă şi destinație, între care se stabileşte comunicația virtuală. Fiecare capăt al conexiunii TCP se numeşte *socket.*

Fiecare secvență dintr-un mesaj de aplicație este indexată printr-un **număr de secvență** (*SN - Sequence Number*) care permite asamblarea lor în ordine corectă, la recepție.

**Numărul de confirmare** (ACK n) specifică recepția corectă a secvențelor transmise şi precizează numărul următoarei secvențe aşteptate.

**Lungimea antetului** (HLEN - *Header Length*) este exprimată în cuvinte de 32 de biți şi poate avea valorile 5 sau 6, în funcție de existența unor opțiuni în antet.

**Biții de control** (*flag*) specifică anumite funcții de control:

URG (*Urgent*) - indică receptorului existența unor date urgente

ACK (*Acknowledge*) - arată receptorului existența unui număr corect de confirmare

PSH (*Push*) - forțează receptorul să transmită imediat alte date

RST (*Reset*) - cere receptorului să reinițializeze conexiunea

SYN (*Synchronize*) - solicită receptorului să sincronizeze secvențele din mesaj

FIN (*Final*) - specifică sfârşitul transmisiei.

Stabilirea unei conexiuni TCP se face în trei paşi (*Three-Way Handshake Open Connection*), în care se folosesc aceşti biți pentru controlul fluxului şi inițierea numerelor de secvență (SN) în ambele sensuri (Fig. I.15).

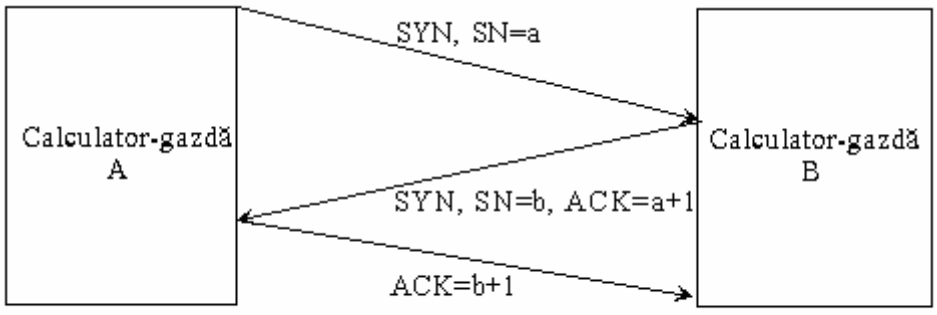


Fig. I.15 Algoritmul în trei paşi de deschidere a conexiunii TCP

Segmentele TCP se pot transmite mai multe într-o sesiune, înainte de primirea unei confirmări de recepție corectă, într-un grup denumit **fereastră** (*window*).

În antetul TCP se specifică lungimea ferestrei ca număr de octeți. Utilizarea ferestrei glisante (*sliding window*) permite controlul fluxului şi creşterea vitezei de transmisie, respectiv a lățimii de bandă a rețelei.

**Suma de control** se calculează pentru tot segmentul TCP, fiind aplicată antetului împreună cu câmpul datelor.

Dacă există date transmise în **modul urgent** (de exemplu, caracterele *escape* sau *întrerupere* într-o aplicație Telnet), atunci în antet se specifică poziția ultimului octet al secvenței de date urgente.

În câmpul facultativ **opțiuni**, se poate specifica lungimea maximă a segmentului TCP (valoarea sa implicită este de 536 octeți).

Comunicația prin TCP se realizează în mod duplex, astfel că închiderea conexiunii impune oprirea fluxurilor de date din ambele sensuri, în două etape (*Two-Way Close Connection*), prin activarea flagului FIN spre ambele părți.

TCP foloseşte porturi de aplicație sau de protocol pentru a realiza comunicații simultane cu mai multe programe. Numerotarea porturilor de protocol se face global, în mod unic, pe întregul Internet şi este descrisă în RFC 1700 (Tabel I.2). Aceste numere de protocol sunt utilizate atât de TCP, cât şi de UDP.

Aplicațiilor publice li se rezervă numere de port mai mici decât 255.

Numerele mai mari ca 256 şi mai mici decât 1023 sunt alocate aplicațiilor dezvoltate de anumite companii.

Valorile mai mari ca 1024 sunt alocate în mod dinamic pentru portul sursă.

Anumite numere de porturi de aplicații sunt utilizate numai de TCP, nu şi de UDP.

**Protocolul UDP** (*User Datagram Protocol*) este considerat nesigur deoarece nu este orientat pe conexiune, nu utilizează mesaje de confirmare a recepției corecte, nu face retransmisia pachetelor eronate, nu permite controlul fluxului informațional şi nu asamblează secvențele în cazul mesajelor fragmentate. Avantajul acestui protocol este dat de viteza mare de procesare a datelor comparativ cu TCP.

Mesajul generat de nivelul aplicație formează împreună cu antetul UDP de 8 octeți o **datagramă UDP** (Fig. I.16).

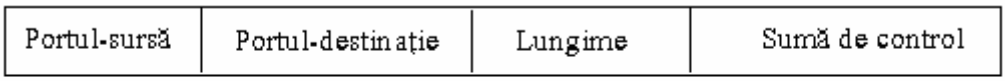


Fig. I.16 Formatul antetului UDP

În antet se specifică, pe câte doi octeți, numerele porturilor de aplicație corespondente, lungimea datagramei şi suma de control a antetului, pentru asigurarea corectitudinii adreselor.

***Observație:*** IP este un protocol fără conexiune, asemenea UDP. Ambele protocoale de transport din suita TCP/IP folosesc protocolul Internet pe nivelul rețea.

Tabel I.2

Numerotarea porturilor logice de protocol

| Protocol de aplicație | Numărul portului alocat |
|---|---|
| FTP | 21 |
| SSH | 22 |
| TELNET | 23 |
| SMTP | 25 |
| DNS | 53 |
| BOOTP SERVER | 67 |
| BOOTP CLIENT | 68 |
| TFTP | 69 |
| FINGER | 79 |
| HTTP* | 80 |
| POP2 | 109 |
| POP3 | 110 |
| NTP | 123 |
| SNMP | 161 |

* valabil numai pentru TCP

## I.6.7 Telnet

Protocolul TELNET *(Terminal Connection*) permite accesarea de la distanță a anumitor sisteme sau programe, prin operația de specificare a unui nume de utilizator şi a unei parole (*remote login*).

Acest protocol rezolvă incompatibilitățile dintre două sisteme implicate într-o conversație în rețea, prin folosirea conceptului de **terminal virtual de rețea** (NVT - *Network Virtual Terminal*), prin care se specifică anumite caracteristici de bază ale unui terminal simplu (*dumb*). De exemplu, VT100 este un NVT. Programele care comunică în rețea prin Telnet convertesc datele în formatul impus de NVT. TTY (*TeleTYpe*) reprezintă denumirea echivalentă a terminalului virtual, fiind împrumutată din sistemul de operare UNIX.

Specificațiile Telnet (RFC 854) impun pentru NVT codul ASCII de codare a datelor în rețea, cu şapte biți pe caracter, prin care se pot reprezenta în binar 95 de caractere printabile şi 33 de coduri de control.

NVT ASCII utilizează numai o parte din secvențele de control definite de ASCII (NUL, BEL, BS, HT, LF, VT, FF, CR)

De exemplu, combinația CR-LF reprezintă terminația standard pentru o linie conform formatului NVT ASCII.

Suplimentar, se introduce bitul al 8-lea, cel mai semnificativ din octet, pentru definirea şi a altor secvențe de control.

Formatul NVT ASCII, definit de specificațiile Telnet, este utilizat şi de alte protocoale de aplicație din suita TCP/IP.

Telnet este inclus în gama de servicii Internet oferite de rețeaua TCP/IP, specificate în baza de date cu servicii de rețea, în care sunt stocate numele protocolului, numărul portului asociat şi, eventual, numele echivalent (*nickname*). Pe un PC, această bază de date se găseşte în fişierul SERVICES, în format ASCII.

***Observație:***

Protocolul Telnet poate fi utilizat pentru încărcarea sau accesarea de la distanță a fişierelor de configurare a unor echipamente de comunicație din rețea (*bridge, router, firewall*) de către personalul autorizat.

## I.6.8 SMTP, POP

Poşta electronică (*e-mail / electronic mail*), unul dintre cele mai utilizate servicii de comunicații din Internet, este reglementat prin protocoalele SMTP şi POP.

Sistemul de poştă electronică are următoarele componente (Fig.I.17):

1. memorie de stocare a mesajelor ce urmează a fi transmise ("coadă de ieşire");
2. procesul client de mail;
3. procesul server de mail;
4. cutiile poştale (*mailbox*) ale utilizatorilor pentru stocarea mesajelor primite.

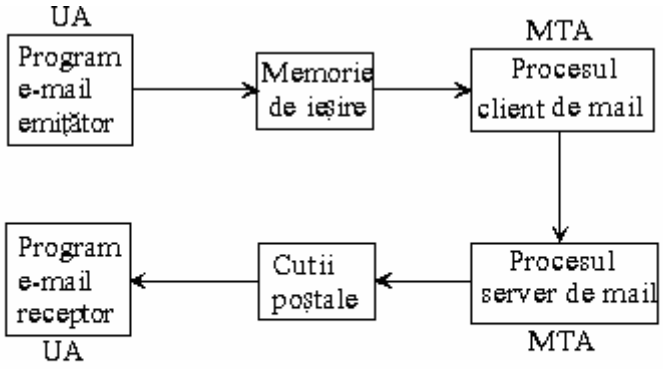


Fig. I.17 Structura sistemului de poștă electronică dintr-o rețea de calculatoare

Programul de poştă electronică de pe un calculator, denumit **agent utilizator** (UA - *User Agent*) oferă utilizatorului o interfață spre sistemul de poştă electronică din Internet, care, în general, nu este considerată parte componentă a acestuia. Scopul UA este de a facilita accesul utilizatorului la serviciul de e-mail din rețea.

Procesele (client sau server) care realizează serviciul de poştă electronică, prin transferul mesajelor în sau din Internet se numesc **agenți de transfer a mesajelor** (MTA - *Message Transfer Agent*). Între doi agenți de transfer a mesajelor se stabileşte o conexiune TCP, iar comunicarea se face pe baza protocoalelor de poştă electronică (de exemplu, SMTP - *Simple Message Transfer Protocol*, POP - *Post-Office Protocol*).

Majoritatea MTA folosesc SMTP pentru transferul mesajelor în format NVT ASCII, prin conexiuni TCP la portul 25 (RFC 821).

SMTP permite comunicații duplex între client şi server, pentru transmisia secvențelor de comandă în format NVT ASCII.

***Observații:***

1. Se poate utiliza SMTP pentru transmisia mesajelor de tip text, dar şi de altă natură (imagine, audio, video) prin definirea unor extensii ale protocolului.

2. SMTP este implicat în transmisia poştei electronice spre serverul de mail şi spre Internet. Preluarea mesajelor de poştă de la cutiile poştale sau din Internet se face conform protocolului POP.

Orice mesaj de e-mail este compus din **antet** şi **corp** (RFC 822). În antetul introdus de UA şi transmis către MTA, în funcție de programul de e-mail folosit, pot să apară mai multe câmpuri (*Date, From, Subject, Reply-To, cc-Carbon Copy, Atachement, Comment, Message-ID, X-Special-Action* etc ). La nivelul MTA se împachetează mesajul cu informații

suplimentare (eventual se specifică o cale cu agenți de comutare) în așa-numita **anvelopă** și se transmite altui MTA sau agentului de comutare local.

Se pot defini extensii ale protocolului SMTP pentru transmisia prin sistemul de e – mail a unor documente de tip multimedia (RFC 1425, RFC 1427, RFC1521).

Protocolul MIME (*Multipurpose Internet Mail Extension*) reprezintă o extensie a SMTP. Acest protocol adaugă cinci noi câmpuri în antet, care permit transmisia prin atașare la mesajele de e-mail a textelor formatate (de exemplu, RTF - *Rich Text Format*), a imaginilor cu diverse formate (GIF - *Graphic Interchange Format,* JPEG - *Joint Photographic Experts Group*), a datelor în format binar sau PS (*Postscript*), a documentelor audio în format ISDN (*Integrated Services Digital Network*) cu lege de compandare și codare pe 8 biți precum și a fișierelor video în format MPEG (*Movie Photographic Experts Group*).

SMTP este responsabil de livrarea poștei electronice în Internet. Pentru preluarea mesajelor de e-mail din Internet se utilizează **protocolul POP,** orientat pe conexiunea dintre client și server.(Figura I.18).

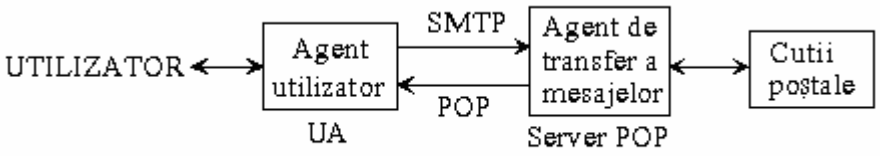


Fig.I.18 Configurația client-server POP

Deși oferă servicii relativ similare, versiunile POP2 (RFC 937) și POP3 (RFC 1225) sunt incompatibile și au asociate porturi de protocol diferite (109, 110).

POP2, corespondent fidel al SMTP, având comenzi asemănătoare, se aplică numai local.

Din motive de securitate, unii administratori de rețea dezactivează serviciul de acces de la distanță (*remote login*) în LAN.

Versiunea POP3 permite accesul de la distanță la serviciul de poștă electronică, mai precis la căsuța poștală rezervată utilizatorului.

O sesiune POP3 are trei stări: autorizare, tranzacție și actualizare (încheiere).

Pentru autorizarea accesului de la distanță la căsuța poştală a utilizatorului, aflată pe serverul POP3, protocolul identificarea utilizatorului, cu nume de utilizator (USER) şi parolă (PASS). După autorizare, se poate efectua tranzacția dorită.

## I.6.9 FTP, TFTP, SFTP

Serviciul de transfer a fişierelor în rețelele locale de calculatoare şi în Internet se realizează pe baza unui protocol de transfer al fişierelor, FTP (*File Transfer Protocol*), TFTP (*Trivial File Transfer Protocol*) sau SFTP (*Simple File Transfer Protocol*).

Protocoalele FTP (RFC 959) şi SFTP (RFC 913) folosesc TCP pentru transport, ceea ce permite transferul sigur al datelor la destinație.

Protocolul TFTP (RFC 783) este implementat cu datagrame, pe baza UDP, astfel încât transferul devine nesigur, dar este simplu şi rapid. TFTP este utilizat pentru transferul unor fişiere de mici dimensiuni.

Pentru transferul fişierelor în rețea, se poate utiliza şi protocolul SSH (*Secure Shell Protocol*), cu cheie de criptare pentru securizarea transmisiei.

**Protocolul FTP** foloseşte coduri de comandă şi de răspuns în formatul NVT ASCII, definit de Telnet, şi două conexiuni TCP: **conexiunea de date** pentru transferul datelor şi **conexiunea de control** pentru transmisia unor comenzi specifice.

Implementarea FTP se realizează pe baza modelului client-server în sisteme de operare diverse (Windows, Linux etc), prin programe simple, de tip 'linie de comandă', sau complexe, cu interfață grafică de utilizator şi structură de meniuri, comode din punctul de vedere al utilizatorilor.

Serverul FTP deschide o conexiune pasivă la portul de protocol 21, după care aşteaptă cererile clienților. O sesiune FTP se activează prin cererea clientului de stabilire a unei conexiuni TCP, la portul de protocol 21 al serverului, reprezentând **conexiunea de control**, activă pe toată durata comunicării.

Dacă serverul răspunde afirmativ, se inițiază **faza de autentificare**, prin operația de *login*, cu validarea numelui de utilizator şi a parolei.

După eventuala schimbare a directorului de lucru curent, pentru transferul datelor se deschid **conexiuni de date** separate pentru fiecare operație de transfer de fişiere, spre server

(*upload*) sau dinspre server (*download*). Clientul comunică serverului numărul de port la care să se conecteze, prin comanda FTP PORT, şi deschide o conexiune pasivă. Serverul activează conexiunea pe portul specificat de client. În această fază, clientul joacă rolul de server pe conexiunea de date. Spre deosebire de serverul FTP, care pe o conexiune pasivă acceptă accesul oricărui client, clientul FTP nu va accepta pe conexiunea pasivă inițiată de el decât accesul de la adresa serverului FTP cu care a comunicat. După transferul fişierelor, se închide sesiunea FTP. Procesul de transfer al unui fişier poate fi întrerupt în orice moment la solicitarea clientului, în modul de date urgente.

O configurație tipică FTP este reprezentată schematic în figura I.19.

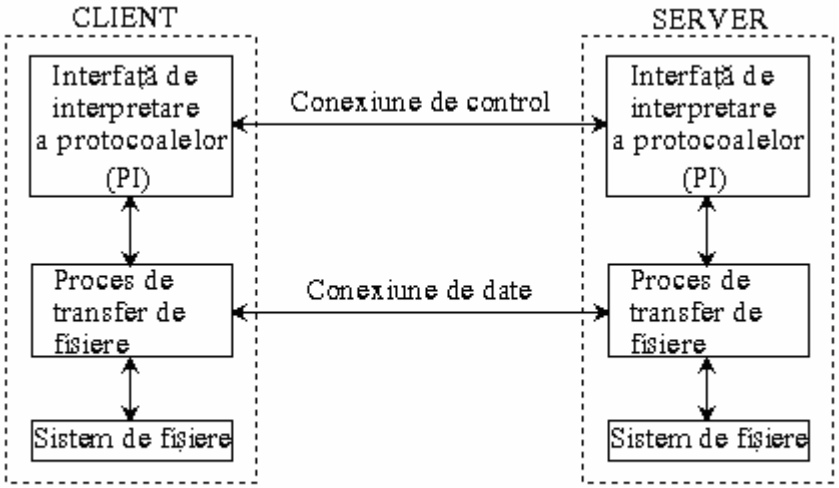


Fig.I.19 Schema de conexiuni FTP

Clientul şi serverul utilizează fiecare câte o interfață de interpretare a protocoalelor (PI - *Protocol Interpreter*), între acestea fiind stabilită conexiunea de control pe toată durata transferului.

Transferul fişierului se realizează prin conexiunea de date care se stabileşte între procesele FTP-client şi FTP-server.

FTP foloseşte Telnet pe conexiunea de control.

Asemenea protocoalelor de poştă electronică (SMTP, POP), FTP este un protocol de tip 'pas-cu-pas' (*lock step*), ceea ce înseamnă că după fiecare comandă lansată se aşteaptă un răspuns şi abia după primirea acestuia se transmite următoarea comandă.

Dacă un client nu dispune de un cont de utilizator pe un anumit server de fişiere, atunci se poate folosi FTP în varianta anonimă (*Anonymous FTP*), cu numele de utilizator *anonymous* şi parola *guest*.

**Protocolul SFTP** foloseşte o singură conexiune TCP şi permite:

1. validarea utilizatorilor pe baza listelor de control al accesului (ACL - *Access Control List*);

2. transferul sigur al fişierelor;

3. operații de listare, redenumire, ştergere de fişiere etc.

**Protocolul TFTP** utilizează un set restrâns de comenzi doar pentru scrierea sau citirea unui fişier, este mult mai simplu decât FTP şi poate fi folosit pentru transferul unor fişiere de dimensiuni mici, între echipamente interconectate direct (de exemplu, între două calculatoare sau între un calculator şi un router).

Fişierele sunt transferate fragmentat, în datagrame cu lungime de 512 octeți, cu excepția ultimei care prin dimensiunea sa redusă marchează sfârşitul transmisiei.

Deoarece pe nivelul de transport, TFTP utilizează UDP şi transferul este nesigur, se impune aplicarea unor coduri de corecție a erorilor la nivelul antetului datagramei pentru a se găsi destinația corectă.

TFTP este utilizat şi pentru transferul fişierelor de configurare (*boot*) din sistemul de operare, pe calculatoarele dintr-o rețea, la pornirea acestora (RFC 906). TFTP a devenit protocolul standard Internet pentru copierea programelor de boot pe stațiile de lucru fără disc, de pe un server de fişiere TFTP.

**Protocolul SSH** (*Secure Shell Protocol*) este un protocol utilizat pentru servicii de poştă electronică, transfer de fişiere şi acces de la distanță, pe portul de aplicații 22, în baza modelului client-server, cu autentificarea utilizatorului şi criptarea mesajelor. Acest protocol foloseşte ca algoritmi de criptare pentru clienți şi server, algoritmii DES (*Data Encryption System*) şi 3DES (*Triple DES*), cu chei publice de 512 - 2048 biți. Este utilizat cu succes pentru transferul mesajelor între procesele de management din rețea.

## I.6.10 ICMP

Protocolul ICMP (*Internet Control Message Protocol*) corespunde nivelului Internet din modelul TCP/IP, fiind responsabil de transmisia mesajelor de eroare sau de interogare, utile pentru procesele de comunicație din rețea, dar şi pentru testarea şi depanarea acesteia.

Aplicațiile comunică direct cu ICMP şi nu prin intermediul protocoalelor de transport.

Pentru încapsularea mesajelor şi transmisia lor în rețea sub formă de pachete, ICMP foloseşte protocolul Internet.

Protocolul ICMP are unele limitări:

1. Raportează eroarea de transmisie a unui pachet numai sursei.

2. Nu transmite mesaje de eroare asociate altor mesaje ICMP.

3. Nu generează mesaje pe adrese de destinație de tip 'broadcast' sau 'multicast', pentru a evita încărcarea rețelei prin apariția fenomenelor de "furtună-în-rețea" (*broadcast storm*).

4. Nu furnizează mesaje de eroare pentru toate fragmentele unei datagrame eronate, ci numai pentru primul.

ICMP foloseşte 15 tipuri de mesaje. În general, modulele software care implementează ICMP nu includ decât anumite mesaje (cerere de ecou, răspuns la ecou, informații de routare şi altele).

Împachetarea mesajelor ICMP se face cu un antet de 4 octeți, în care se specifică tipul mesajului, codul de răspuns şi suma de control Internet (Fig. I.20).

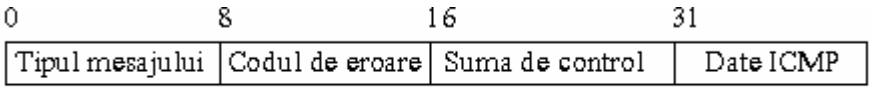


Fig. I. 20 Formatul mesajului ICMP

Lungimea şi conținutul câmpului de date ICMP depind de tipul mesajului.

Pentru mesaje de eroare, în acest câmp se transmit primii 64 de octeți din pachetul IP care a provocat eroarea.

Pentru mesaje de interogare de tip 'ecou' (0), folosite pentru testarea conexiunilor de către aplicația PING (*Packet INternet Groper*), câmpul de date ICMP include un octet de identificare, un octet 'număr de secvență' şi alți doi octeți reprezentând o secvență opțională de date.

Câmpul de date din mesajele ICMP de tip 3, "destinație inaccesibilă", conține 68 de octeți, dintre care primii patru corespund unui cuvânt de 32 de biți complet nul iar următorii 64 de octeți provin din pachetul original transmis.

Similar, pentru mesajele de redirecționare, se includ în câmpul datelor adresa IP a routerului (*next hop*) şi primii 64 de octeți din pachet.

Stațiile de lucru fără disc folosesc ICMP pentru aflarea propriei măşti de rețea. Mesajele ICMP de cerere şi răspuns referitoare la aceasta, includ în câmpul datelor ICMP de 8 octeți, un identificator şi un număr de secvență, urmate de masca de rețea propriu-zisă.

***Observații:***

1. Suma de control Internet calculată pe 16 biți (RFC 1071) se aplică atât antetului ICMP, cât şi câmpului de date.

2. La acelaşi tip de mesaj, se pot asocia coduri de răspuns diferite în funcție de cauza problemei. De exemplu, pentru destinație inaccesibilă sunt posibile 16 coduri de răspuns (rețea inaccesibilă, protocol inaccesibil, rețea de destinație necunoscută etc).

3. Mesajul ICMP este încapsulat în vederea transmisiei cu antetul IP.

4. Operația PING se realizează în două faze: prima de transmisie a cererii de ecou ICMP, a doua de recepționare a răspunsului la ecou prin intermediul ICMP. Un răspuns afirmativ, de găsire a destinației, include durata de transfer dus-întors a pachetului între sursă şi destinație, exprimată în milisecunde, rata de pierderi etc.

5. Mesajele ICMP de interogare a routerelor sunt utilizate pentru actualizarea dinamică a tabelelor de rutare.

## I.6.11 SNMP

Gestionarea rețelelor de calculatoare se realizează pe baza protocoalelor de management de rețea.

Suita TCP/IP include protocolul de management SNMP (*Simple Network Management Protocol*) definit în RFC 1155 - 1157, care implementează un mecanism de gestionare a resurselor rețelei, folosind baze de date MIB (*Management Information Base*), cu informații referitoare la toate componentele rețelei (RFC 1514 - *Host Resources MIB;* RFC 1398 - *Ethernet-like Interface Types MIB;* RFC 1493 - *Bridge MIB* şi altele). RFC 1213 definește MIB-II care include obiectele gestionate pentru rețelele bazate pe suita TCP/IP.

SNMP poate folosi oricare din protocoalele de transport din suita TCP/IP dar în cele mai multe cazuri utilizează UDP, pe porturile de aplicații 161 şi 162.

Un sistem de management a rețelelor de calculatoare include trei categorii de componente (Fig. I.21):

1. **componente gestionate** (*managed device*);

2. **stații de gestionare** sau **de management** (*network management station*);

3. **protocolul de management** (*management protocol*) utilizat pentru comunicația dintre celelalte componente ale sistemului de management.

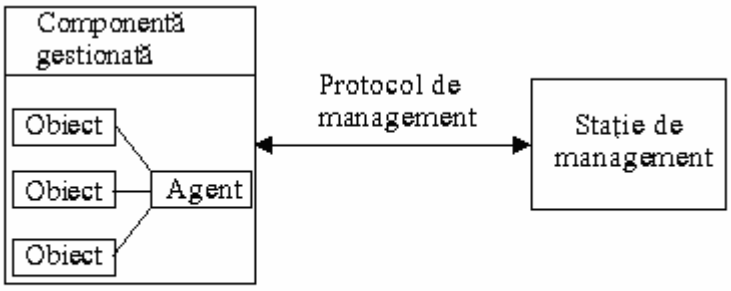


Fig.I.21 Structura de bază a sistemului de management al rețelei

RFC 1155 descrie un mecanism de identificare şi descriere a obiectelor din MIB, denumit SMI (*Structure of Management Information*), care defineşte schema de organizare a colecției de obiecte gestionate din MIB, pe baza unei diagrame 'arbore', cu mai multe nivele.

Obiectele din MIB sunt manipulate pe baza unor valori memorate la diverse momente (*instances*), ca date de tipuri diferite în funcție de natura obiectului.

Stațiile de management a rețelelor (NMS - *Network Management Station*) lucrează cu aceste valori instantanee ale obiectelor care sunt identificate prin aşa-numitul **identificator de valoare** (*instance-identifier*), ataşat identificatorului de obiect.

**Accesul** la un obiect din MIB poate fi restricționat (*not-accessible; read-only; write-only*) sau liber (*read-write*).

Prin **starea** unui obiect se exprimă condițiile de implementare ale acestuia:

1. **mandatar**: componenta gestionată de NMS implementează în mod obligatoriu acel obiect;

2. **opțional**: componenta gestionată de NMS implementează opțional acel obiect;

3. **depăşit:** componenta gestionată de NMS nu mai implementează acel obiect;

4. **depreciat**: componenta gestionată de NMS poate implementa acel obiect, dar există un nou obiect în MIB superior acestuia.

Protocolul SNMP este utilizat de stația de management (NMS) pentru a transmite mesaje componentei gestionate, mai precis agentului de management din cadrul acesteia.

În general, SNMP acționează în mod recursiv, prin interogarea periodică (*polling*) a agenților de management ai componentelor gestionate de NMS.

Numai în situații critice, un agent poate iniția schimbul de informații cu NMS, pentru a o înștiința de modificările apărute, transmițând mesaje-capcană (*trap*) care întrerup procesul de *polling*. Un agent nu poate transmite oricât de multe mesaje-capcană spre NMS, pentru a evita pierderea controlului asupra întregii rețele.

Unitatea de date sau mesajul SNMP (PDU - *Protocol Data Unit*) poate fi denumită în cinci moduri distincte, în funcție de natura informației transmise:

1. **cerere simplă** (*get-request*) - NMS cere unui agent de management informații despre un obiect;

2. **cerere recursivă** (*get-next-request*) - NMS cere unui agent de management informații despre obiectul următor din MIB;

3. **cerere de impunere** (*set-request*) - NMS impune o anumită valoare pentru un obiect din MIB-ul agentului;

4. **răspuns** (*get-response*) - un agent trimite informații spre NMS, despre un obiect, ca răspuns la cererea acesteia;

5. "**capcană"** (*trap*) - un agent transmite spre MIB informații referitoare la un eveniment extraordinar care a afectat componenta gestionată prin intermediul său (reinițializarea agentului de management, schimbarea stării unei interfețe, nerespectarea unor condiții de autentificare etc). Există şapte tipuri de mesaje-capcană SNMP.

Primele patru tipuri de mesaje SNMP se transmit prin UDP, pe portul 161. Numai mesajele-capcană se transmit pe portul de aplicație 162.

SNMP este considerat a fi un protocol simplu deoarece nu are decât cinci operații, corespunzătoare celor cinci tipuri de mesaje SNMP (*get, get-next, set, get-response* şi *trap*).

În funcție de modul de acces, se poate folosi un număr mai mic de mesaje SNMP.

Obiectele din MIB pot fi grupate în subseturi (SNMP MIB *View*), în funcție de accesibilitatea acestora: parțială (*read-only*) sau totală (*read-write*).

Pentru agenții de management, se definesc **profile** prin care se stabilesc drepturile de acces la diferitele subseturi de obiecte din MIB, total sau parțial accesibile:

1. cu drept de citire (*read-only*);

2. cu drept de scriere (*write-only*);

3. cu drepturi de citire şi de scriere (*read-write*);

4. fără drepturi de acces la MIB (*not-accessible*).

***Observații:***

1. Se impun măsuri stricte de securitate referitor la mesajele SNMP, întrucât prin definirea unui profil de agenți cu drept de scriere pe un grup de obiecte cu accesibilitate totală se pot produce daune majore rețelei de către persoane neautorizate care cunosc numele profilului.

2. În rețelele de mari dimensiuni unde volumul informațiilor de management este foarte mare şi necesită capacități extinse de memorie, se folosesc baze de date (MIB) distribuite pe mai multe servere de management din rețea.

3. SNMP este un protocol rutabil întrucât foloseşte protocolul IP pentru încapsularea datelor şi, implicit, adresarea IP.

4. Există şi protocoale de management al rețelelor locale de calculatoare, nerutabile. Un astfel de protocol este NetBeui (*Network BIOS extended user interface*), dezvoltat de firma Microsoft pentru rețele Netware (de PC-uri), cu sistem de operare NT, pe baza modelului client-server. Pe lângă operațiile de management de rețea, NetBeui include şi funcțiile de transport, de corecție a erorilor de transmisie, de confirmare a recepției corecte a datelor (ACK), fiind echivalent unei stive de protocoale cu funcții distincte.

## I.6.12 IPsec

Securitatea comunicațiilor în rețelele locale de calculatoare se referă la mai multe aspecte:

1. mesajele transmise provin din surse autorizate şi sunt autentice;

2. datele sunt corecte şi complete;

3. accesul la anumite mesaje cu caracter confidențial este restricționat în mod corespunzător.

Există diferite metode de asigurare a securității transmisiei într-o rețea prin operații de autentificare a utilizatorilor, criptare a mesajelor, filtrare a traficului etc.

Metodele de securitate din Internet se pot aplica pe diferite nivele ale modelului OSI.

La nivel fizic, se pot folosi module hardware de criptare şi decriptare (ENCO).

La nivelul legăturii de date şi la nivel de rețea se pot defini filtre de includere sau de excludere pe diverse interfețe ale echipamentelor.

Se pot utiliza programe de aplicație specializate pentru asigurarea securității transmisiei datelor în rețea.

Primele măsuri de securitate a rețelelor defineau **asociații de securitate** (SA - *Security Association*), adică grupuri de utilizatori autorizați să folosească o anumită rețea, denumită **rețea virtuală privată** (VPN - *Virtual Private Network*).

În prezent, în rețelele TCP/IP se utilizează suita de protocoale de securitate **IPsec** (*Internet Protocol Security Facility*), care realizează criptarea şi autentificarea pachetelor IP cu performanțe superioare sistemului inițial SA. VPN pot fi configurate în mod adecvat să aplice protocoalele de securitate din suita IPsec.

Gradul de protecție a pachetelor IP şi cheile de criptare utilizate de IPsec se stabilesc prin mecanismul IKE (*Internet Key Exchange*), care se aplică folosind protocolul ISAKMP (*Internet Security Association and Key Management Protocol*). Astfel IPsec beneficiază de serviciile ISAKMP/IKE.

IPsec oferă următoarele servicii de securitate pe nivelul IP al rețelelor TCP/IP:

1. **integritatea conexiunii** - asigură faptul că în procesul de comunicație nu intervin entități neautorizate care să modifice datele sau să genereze mesaje false în rețea;

2. **autentificarea sursei de date** - permite identificarea sursei şi asigurarea autenticității mesajelor;

3. **criptarea datelor** - asigură confidențialitatea mesajelor transmise şi imposibilitatea preluării neautorizate a informațiilor;

4. **protecția la atacuri în rețea** - detectează pachetele repetitive, replici ale aceluiaşi pachet, care se transmit la infinit în rețea şi pot produce blocaje sau saturarea rețelei (*flooding*).

Autentificarea sursei se face pe baza protocolului AH (*IP Authentication Header*) din suita IPsec (RFC 2401, RFC 2402). Acest protocol asigură integritatea conexiunii şi a datelor transmise, precum şi autenticitatea mesajelor. AH asigură securitatea integrală a pachetelor IP, inclusiv antetelor de securitate ataşate ulterior acestora.

Serviciile de securitate sunt asigurate şi de protocolul ESP de încapsulare a pachetelor IP (*IP Encapsulating Security Payload*), care stabileşte operații de criptare a datelor şi de autentificare a sursei de informații (RFC 2406).

ESP oferă servicii de securitate numai protocoalelor de pe nivelele superioare celui de rețea, excluzând antetele de securitate ulterior adăugate pachetelor.

Protocoalele AH şi ESP pot fi implementate prin diverşi algoritmi software şi se pot aplica fie individual, fie ambele simultan, în funcție de gradul de securitate impus pachetelor IP (RFC 2403, RFC 2404).

IPsec asigură securitatea comunicației dintre două calculatoare-gazdă, dintre două echipamente de comunicații (de exemplu, routere) sau dintre un DTE şi un DCE.

Un router sau un server pe care sunt activate protocoalele de securitate IPsec se numeşte **poartă de securitate** (*security gateway*) sau **"zid" de protecție** (*firewall*).

În general, asigurarea securității unei transmisii se realizează la ambele capete ale căii de comunicație, cu două echipamente care folosesc IPsec lucrând în pereche (*IPsec peers*).

Cele două protocoale de securitate în Internet (AH sau ESP) pot acționa în două moduri:

1. **modul de transport** - protocolul de securitate intervine în pachetul IP şi adaugă un antet de securitate imediat după antetul IP (cu sau fără opțiuni exprimate). ESP oferă protecție numai protocoalelor de nivel superior, în timp ce AH securizează total pachetul, inclusiv antetul IP.

2. **modul de tunelare** (*IP tunneling*) - se introduc două antete de securitate în fiecare pachet, înainte (*outer header*) şi după (*inner header*) antetul IP. Antetul extern specifică perechea de entități între care se creează tunelul IP şi se aplică măsurile de securitate pe baza IPsec. Antetul intern precizează destinația finală a pachetului. ESP protejează numai pachetul transmis prin tunelul IP, în timp ce AH asigură şi securitatea antetului exterior ataşat.

Configurarea echipamentelor dintr-o rețea în vederea aplicării IPsec se realizează de către o persoană cu drepturi depline de stabilire a securității rețelei (*security officer*), în trei etape:

1. crearea grupurilor de securitate (SA) şi stabilirea drepturilor şi atribuțiilor acestora;

2. configurarea legăturilor dintre SA-uri şi stabilirea ierarhiilor de priorități, folosind ISAKMP/IKE (RFC 2408, RFC 2409);

3. stabilirea modalităților de clasificare a pachetelor IP şi de acțiune asupra lor (permite sau interzice accesul în rețea, aplică procedurile de securitate conform IPsec).

Aceste configurații referitoare la IPsec sunt stocate în bazele de date pentru securitatea rețelei (SPD - *Security Policy Database*), la care are acces doar administratorul de rețea.

Prin SA înțelegem o conexiune simplex definită pe o pereche IPsec, pentru securitatea traficului doar într-un sens, folosind un singur protocol de securitate (AH sau ESP).

Pentru transmisiile duplex se defineşte câte un SA pentru fiecare sens de comunicație cu rețeaua (*inbound/outbound traffic*).

Dacă la unul din capetele canalului de comunicație definit de SA, se găseşte un echipament de securitate (*security gateway; firewall*), atunci este obligatoriu ca acel SA să lucreze în modul de tunelare pentru a evita problemele create prin fragmentarea pachetelor şi de existența căilor multiple de rutare.

Un SA este identificat prin trei parametri:

1. un număr aleator denumit **identificator de securitate** (SPI - *Security Parameter Index*);

2. **adresa IP de destinație;**

**3. protocolul de securitate** (AH sau ESP).

Dacă este necesară utilizarea ambelor protocoale de securitate în Internet (AH şi ESP), atunci se creează şi se configurează legăturile dintre două sau mai multe SA.

Regulile de securitate aplicate într-o rețea folosind IPsec sunt memorate în SPD. Acestea stabilesc trei moduri posibile de acțiune asupra pachetelor IP:

1. se aplică pachetului, serviciile de securitate conform IPsec;

2. se interzice accesul pachetului în rețea (*deny*);

3. se acordă permisiunea de acces în rețea, fără aplicarea măsurilor de securitate IP (*bypass IPsec*).

Modul de acțiune asupra unui pachet IP se stabileşte pe baza antetelor conținute de acesta, prin operația de clasificare a pachetelor, în funcție de diverşi **factori de selecție**:

- adresa IP a sursei;
- adresa IP a destinației;
- portul-sursă;
- portul-destinație;
- protocolul de transport;
- numele utilizatorului sau al sistemului;
- gradul de prioritate al informațiilor conținute în pachet.

Filtrarea pachetelor se poate face pe baza unui factor dintre cei menționați anterior în vederea reducerii încărcării rețelei şi evitarea anumitor atacuri efectuate asupra rețelei.

Aplicarea măsurilor de securitate IPsec asupra unui pachet (autentificare, criptare, compresie), se realizează pe baza mecanismului ISAKMP/IKE prin care se generează şi se transmit între părți cheile de criptare utilizate de SA în diferite sesiuni, memorate într-o bază de date proprie ISAKMP ca atribute ale SA.

În rețelele TCP/IP, se utilizează diverşi algoritmi de criptare, uzuali fiind cei cu cheie publică (RSA – *Rivest-Shamir-Adleman*, DES, 3-DES etc) (Anexa B).

De exemplu, protocolul SSH, utilizat pentru transferul securizat al fişierelor şi al mesajelor prin sistemul de poştă electronică din Internet, foloseşte diverşi algoritmi de criptare cu cheie publică, precum MD4, MD5 ş.a. Operația de autentificare se bazează de asemenea pe secvențe de tip 'cheie de transmisie'.

***Observație:***

O altă posibilitate de securizare a rețelelor locale de calculatoare, în vederea evitării pătrunderii neautorizate a unor utilizatori, constă în definirea unor LAN-uri virtuale (VLAN – *Virtual LAN*), separate logic.

# I.7 ADRESAREA IP

Adresele MAC nu sunt ierarhizate şi localizarea destinației într-o rețea de arie largă este posibilă numai pe baza adreselor IP, care specifică rețeaua, eventual subrețeaua în care se găseşte un anumit calculator.

O adresă IP are 32 de biți şi este exprimată compact pe 4 octeți, în format zecimal cu puncte. Aceasta conține identificatorul rețelei (NID – *Network IDentifier)*, eventual al subrețelei (SID – *Subnetwork IDentifier*) care include echipamentul-gazdă şi identificatorul plăcii de rețea a acestuia (HID – *Host IDentifier*). Identificatorul de rețea precede identificatorul plăcii de rețea. Adresa IP astfel formată este alocată în mod unic în Internet de InterNIC (*Internet Network Information Center*).

Administrarea în mod unic a întregului spațiu de adrese din Internet este practic imposibilă, fiind vorba de circa 4 miliarde de adrese. De aceea s-a procedat la divizarea acestuia în rețele mai mici, cu un număr mai mic de adrese, ierarhizate pe baza unei diagrame-arbore, care sunt administrate local de ISP (*Internet Service Provider*). Acest fapt a determinat reducerea numărului de adrese din Internet la circa 3,7 miliarde dar nu constituie

un dezavantaj major deoarece alocarea adreselor se poate face dinamic, nu static (adresare fixă a gazdelor), numai pentru utilizatorii activi la un moment dat din rețea.

Adresarea ierarhică sistematică a utilizatorilor din Internet simplifică modul de administrare a acestuia.

Schema de adresare IP este structurată pe cinci clase de adrese, diferențiate în funcție de lungimea câmpului alocat rețelei, dar şi prin prefixul binar utilizat (Tabel I.3) stabilit pe baza unui cod-prefix.

Adresele cu toți biții identici sunt rezervate ('1' - pentru *broadcast*; '0' - pentru rețea) şi nu se alocă subrețelelor sau gazdelor.

Tabel I.3 Clasele de adrese IP

| Clasa de adrese | Mărime NID (octeți) | Prefix binar fix | Domeniul de valori ale primului octet | Mărime NID (biți) | Mărime HID (biți) | Număr de calculatoare gazdă adresabile | Număr de rețele adresabile |
|---|---|---|---|---|---|---|---|
| A | 1 | 0 | 0 - 127 | 7 | 24 | 16 777 214 | 126 |
| B | 2 | 10 | 128 - 191 | 14 | 16 | 65 534 | 16382 |
| C | 3 | 110 | 192 - 223 | 21 | 8 | 254 | 2 097 150 |
| D | multicast | 1110 | 224 - 239 | - | - | - | - |
| E | rezervată | 11110 | 240 - 247 | - | - | - | - |

În aceeaşi rețea se foloseşte un singur identificator de rețea (*network ID*) dar identificatori de gazdă (*host ID*) diferiți.

Se spune că adresele de clasă A, B sau C sunt de tip *unicast* deoarece identifică în mod unic gazda.

Simbolic adresele IP pot fi scrise astfel (N – *network,* H – *host*):

1. adresele de clasă A:

0NNN NNNN. HHHH HHHH. HHHH HHHH. HHHH HHHH

2. adresele de clasă B:

10NN NNNN.NNNN NNNN. HHHH HHHH. HHHH HHHH

3. adresele de clasă C:

110N NNNN. NNNN NNNN. NNNN NNNN. HHHH HHHH

De exemplu, rețeaua cu 4 calculatoare având adresele IP: 192.168.20.1; 192.168.20.2; 192.168.20.3; 192.168.20.4 are identificatorul de rețea 192.168.20.0.

Conform RFC 1597, anumite spații de adrese IP din clasele A, B şi C sunt rezervate şi sunt numite **adrese private** (*private*):

10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255.

Adresarea în interiorul LAN-ului poate fi făcută cu adrese locale private, alocate de administratorul de rețea, adrese care nu au legătură cu adresele IP publice alocate rețelei respective.

Pentru pachetele care se transmit în afara LAN este necesară aplicarea procedeului NAT (*Network Address Translation*), de translare a adreselor private în adrese publice, utilizabile în Internet, la nivelul routerelor.

***Observații:***

1. Unui echipament de comunicație, de exemplu, unui router, i se pot aloca mai multe adrese IP în funcție de câte interfețe de comunicație are.

2. Pentru aplicații care necesită adresarea multicast se utilizează adrese de clasă D, în baza protocolului IGMP. Există adrese de grup prestabilite de către IANA (*Internet Assigned Numbers Authority*), organizație subordonată societății ISOC (*Internet SOCiety*) care coordonează funcționarea întregului Internet.

*Exemple de adrese multicast permanente* (conform RFC 1112):

224.0.0.1 transmisie multicast către toate sistemele dintr-un LAN.

224.0.0.2 transmisie multicast către toate routerele dintr-un LAN.

224.0.0.5 transmisie multicast către toate routerele OSPF dintr-un LAN.

224.0.0.9 transmisie multicast pentru toate routerele RIP-2 dintr-un LAN.

224.0.1.1 transmisie multicast pentru protocolul NTP.

3. Adresa 127.0.0.1 este rezervată şi semnifică adresa generică a propriei plăci de rețea a unui calculator, fiind posibilă testarea funcționalității acesteia prin efectuarea locală a comenzii PING pe această adresă.

4. În multe cazuri chiar şi 254 de adrese reprezintă un număr prea mare pentru o rețea de calculatoare locală. Se impune împărțirea spațiului de adrese de clasă A, B sau C în mai multe subclase alocate **subrețelelor** (*subnetwork*) cu un anumit număr de utilizatori. Pentru identificarea subrețelei se împrumută biți din câmpul identificatorului gazdei, dintre cei mai semnificativi. Numărul biților utilizați pentru identificatorul de subrețea, respectiv pentru ID-ul gazdelor, este restricționat la **minimum doi,** întrucât combinațiile de biți identici '1' sau '0' sunt rezervate.

Se observă faptul că pentru rețelele de clasă C se pot folosi minimum 2 şi maximum 6 biți pentru ID-ul subrețelelor. În rețelele de clasă B, se pot defini subrețele folosind minimum 2, maximum 14 biți pentru ID-ul de subrețea.

De exemplu, pentru o subclasă de adrese de tip C cu subrețele de cel mult 6 utilizatori, se aplică formatul:

110N NNNN. NNNN NNNN. NNNN NNNN. SSSS SHHH

Se folosesc 5 biți de subrețea şi se pot forma $2^5$-2 = 30 subrețele, fiecare cu maximum $2^3$-2 = 6 utilizatori.

Interconectarea subrețelelor în LAN se poate realiza prin intermediul routerelor interne. Interconectarea LAN-urilor în WAN se face prin routere externe.

Rutarea pachetelor prin Internet presupune că la nivelul routerelor externe se citeşte adresa rețelei (fără ID-ul gazdei), iar la nivelul routerelor interne se extrage adresa subrețelei. Pentru aceasta se folosesc **măşti de rețea** (NM - N*etwork Mask*) pe care le aplicăm adresei IP a destinației pentru a selecta ID-ul rețelei, respectiv **măşti de subrețea** (SM- *Subnetwork Mask*) pentru determinarea adresei subrețelei. În acest scop, se efectuează operația 'ŞI' logic (AND), bit cu bit, între adresa IP a destinației şi mască. Masca de rețea sau de subrețea se obține prin impunerea valorii '1' tuturor biților din câmpul rețelei, respectiv a subrețelei, şi '0' pe toate pozițiile din câmpul gazdei.

Masca de rețea este definită pentru fiecare clasă de adrese IP:

1. masca de rețea în clasa A: 255.0.0.0
2. masca de rețea în clasa B: 255.255.0.0
3. masca de rețea în clasa C: 255.255.255.0.

Măştile de subrețea se particularizează în funcție de numărul de biți alocați acesteia.

Pentru aflarea numărului de identificare a gazdei în rețea sau subrețea, se aplică o combinație binară echivalentă măştii de rețea sau subrețea negate pe care o vom denumi

simplu **masca negată** (*wild card*), având toți biții '0' în câmpul rețelei şi subrețelei, respectiv '1' în câmpul gazdei.

*Exemplul 1*

Pentru citirea adresei rețelei în care se află calculatorul cu adresa 192.110.12.1 se aplică masca de rețea de clasă C: 255.255.255.0.

În binar se obține:

| | |
|---|---|
| Adresa IP a destinației: | 1100 0000. 0110 1110. 0000 1100. 0000 0001 |
| | AND |
| Masca de rețea: | 1111 1111. 1111 1111. 1111 1111. 0000 0000 |
| Rezultă ID-ul rețelei: | 1100 0000. 0110 1110. 0000 1100. 0000 0000 |

Adresa acestei rețele este 192.110.12.0.

Adresa de broadcast pentru această rețea se obține impunând ca toți biții din câmpul HID să fie "1", deci valoarea zecimală a ultimului octet din adresa de broadcast are valoarea 255. Primii trei octeți din adresa de broadcast sunt cei care identifică rețeaua (192.110.12.HID). Rezultă că adresa de broadcast a rețelei este: 192.110.12.255.

*Exemplul 2*

Pentru adresa IP 170.202.112.23, de clasă B, se aplică masca de rețea 255.255.0.0 care păstrează primii doi octeți nemodificați dar ascunde valoarea octeților din câmpul *host,* rezultând adresa rețelei: 170.202.0.0.

*Exemplul 3*

Pentru rețeaua 192.110.12.0 cu masca de rețea este 255.255.255.0, se pot forma 30 de subrețele cu câte 6 utilizatori, folosind 5 biți din câmpul gazdei pentru subrețea (SID) şi trei biți pentru HID.

Se folosesc deci 29 de biți pentru rețea şi subrețea (*network bits*).

Masca de subrețea exprimată în binar este:

11111111.11111111.11111111.11111000

Valoarea în zecimal a măştii de subrețea este 255.255.255.248.

*Exemplul 4*

Pentru rețeaua din exemplul 3, masca negată, în binar, este:

00000000.00000000.00000000.00000111

iar în format zecimal cu puncte rezultă 0.0.0.7.

Prima subrețea formată are adresa 192.110.12.8 şi spațiul de adrese pentru calculatoarele-gazdă de la 192.110.12.9 până la 192.110.12.14. Adresa de broadcast a subrețelei este 192.110.12.15.

A doua subrețea are adresa 192.110.12.16, spațiul de adrese 192.110.12.17 ... 192.110.12.22 şi adresa de broadcast 192.110.12.23.

Similar se analizează toate subrețelele formate.

***Observații***

1. Pentru garantarea unicității adreselor IP utilizate în Internet, organizații naționale şi internaționale alocă fiecărei rețele un număr unic de identificare ASN (*Autonomous System Number*), asemenea adresei fizice (MAC) a unui echipament.

2. Adresele IP ale interfețelor echipamentelor de comunicație (gateway, firewall, router) prin care se transportă pachetele între LAN şi WAN, mai sunt denumite şi **adrese de transport** şi este indicat ca acestea să fie definite într-o subrețea separată. Rutarea pachetelor se va face pe baza tabelelor de rutare în care sunt stabilite rutele între adresele de transport.

3. Pentru lărgirea spațiului de adrese din Internet s-a propus folosirea **IPng** (*IP next generation*) sau IPv6 care, spre deosebire de IPv4, foloseşte adrese de 128 de biți, ordonate ierarhic; elimină broadcast-ul în favoarea multicast-ului; include în cadrul IP un antet (*header*) cu lungime fixă conținând informații strict necesare rutării pachetelor, altele fiind incluse în subantete; suportă modul automat de alocare a adreselor IP; permite autentificarea şi criptarea datelor; prevede un sistem de priorități privind transmisia care să faciliteze transmisiile multimedia (voce, audio, video).

IPv6 poate procesa adresele date prin IPv4 dar DNS necesită un MIB (*Management Information Base*) suplimentar pentru stocarea numelor şi adreselor de utilizator de 128 de biți.

# I.8 ARHITECTURA REȚELELOR DE COMUNICAȚII

Pentru descrierea arhitecturii unei rețele de calculatoare trebuie precizate modalitatea de acces la mediu, topologia logică şi topologia fizică a acesteia.

Alegerea mediului de transmisie şi a unei arhitecturi specifice reprezintă operația de **configurare** a rețelei.

Rețelele de calculatoare se pot implementa fizic fie ca **rețele cu difuzare** (PMP - *Point - to - Multipoint*), fie ca **rețele punct-la-punct** (PP - *Point-to-Point*).

În cadrul unei **rețele cu difuzare**, toate calculatoarele sunt conectate la un singur canal de transmisie cu acces multiplu (*Multiple Access Channel*), multiplexarea făcându-se static sau dinamic:

1. în frecvență (FDMA - *Frequency Division Multiple Access*);
2. în timp (TDMA - *Time Division Multiple Access*);
3. în cod (CDMA - *Code Division Multiple Access*);
4. în lungime de undă (WDMA - *Wavelength Division Multiple Access*).

Într-o astfel de rețea, un mesaj sau pachet de date poate fi transmis unui singur terminal (*unicast*), către un grup predefinit de utilizatori (*multicast*) sau către toate calculatoarele din rețea (*broadcast*).

Într-o rețea de tip **"punct-la-punct"**, există conexiuni multiple între terminale (**noduri**) astfel că un pachet poate fi transmis la destinație pe mai multe căi, fiind necesară implementarea unor algoritmi de dirijare sau rutare a pachetelor.

## I.8.1 Metode de acces la mediul fizic de transmisie

Într-o rețea cu difuzare este posibil ca mai mulți utilizatori să transmită date în acelaşi timp. Dacă aceştia sunt conectați la un singur canal de comunicație (*media-sharing*), atunci este nevoie de o modalitate de arbitraj pentru a stabili care dintre utilizatori poate transmite la un moment dat.

Metoda **CSMA/CD** (*Carrier Sense Multiple Access with Collision Detection*) permite accesul permanent la mediu al tuturor utilizatorilor, fără cereri prealabile pentru acordarea permisiunii de transmisie.

În principiu, aplicarea acestei metode presupune testarea sau "ascultarea" canalului de comunicații (*listening*) pentru detecția unei purtătoare pe linie (*carrier sense*). Dacă linia este liberă, atunci utilizatorul transmite date. Când două calculatoare transmit date simultan, apare o coliziune şi unul dintre pachete este distrus. Calculatorul-sursă este înştiinţat de pierderea pachetului şi este necesară retransmisia lui. Procesul de retransmisie introduce întârzieri care afectează negativ performanţele rețelei.

Acest inconvenient se rezolvă prin metoda **Token Passing** (în traducere, "jeton de trecere"). Fiecare utilizator cere permisiunea de transmisie şi în momentul în care o are, transmite datele pe canal, în final primind confirmarea recepției corecte a lor la destinație.

Evident, metoda necesită capacitate suplimentară de procesare şi timpi de transmisie a mesajelor de control (ENQ - *ENQuire* - cerere de transmisie; ACK - *ACKnowledge* - confirmare de primire; NAK - *Not AcKnowledge* - pentru pachete neexpediate ş.a.) dar avantajul major este acela că nu apar coliziuni în rețea.

Uzual, în rețelele cu fir, de arie mică şi viteză redusă, se utilizează procedeul CSMA/CD iar în cele de arie largă, cu rate mari de transmisie, se aplică metoda Token Passing.

O altă metodă de acces la mediu este cea la cerere, pe bază pe priorități (DPMA - *Demand Priority Media Access*), prin protocolul DPP (*Demand Priority Protocol*).

Pentru sistemele de transmisie 'fără fir' (*wireless*) se aplică metoda **CSMA/CA** (*CSMA with Collision Avoidance*) care încearcă evitarea apariției coliziunilor, prin transmiterea în prealabil de către stația emițătoare a unei cereri de acordare a permisiunii de transmisie din partea stației de destinație.

## I.8.2 Topologia logică

Modul de expediere a mesajelor într-o rețea este descris prin topologia logică a acesteia.

Există **topologia logică de difuzare** (*broadcast logical topology*) în care mesajul este transmis tuturor terminalelor, fiind ignorat de cele cărora nu le este destinat.

A doua variantă de topologie logică este cea **secvențială** sau "**în inel**" (*ring logical topology*), care presupune transmiterea mesajului în rețea, treptat, de la un nod la altul. După citirea adresei-destinație, se decide la nivelul nodului dacă îi este adresat acestuia sau trebuie

transmis următorului nod din rețea. Topologia logică secvențială are avantajul că reduce încărcarea rețelei dar timpul de transfer al mesajului creşte comparativ cu topologia logică cu difuzare.

### I.8.3 Topologia fizică

Modalitatea de interconectare a calculatoarelor şi a celorlalte echipamente de comunicație defineşte topologia fizică a rețelei.

Frecvent, topologia rețelelor cu difuzare (PMP) este de tip "magistrală" (*bus*), "inel" (*ring*) sau "stea" (*star*) (Fig. I.22).

În rețeaua de tip "magistrală", la un anumit moment doar un singur calculator poate transmite date întrucât terminalele sunt conectate liniar la mediu, fie prin fir cu conectori, fie 'fără fir', folosind echipamente de transmisie-recepție (*transceiver*). Dezavantajul acestei rețele îl constituie posibilitatea de întrerupere totală a comunicației în cazul blocării canalului de transmisie.

Topologia de tip "inel" presupune trecerea mesajelor prin mai multe noduri ale rețelei. Dacă unul dintre terminale nu funcționează, rețeaua se blochează.

Rețeaua de tip "stea" este cea mai flexibilă şi mai fiabilă ca topologie, prin **centralizarea** controlului traficului cu o structură de tip *master-slave*. În centrul rețelei este plasat un DCE care poate fi un concentrator (*hub*), un comutator (*switch*), un repetor (*repeater*) sau o unitate centrală de acces (CU - *Central Unit* sau MAU - *Multistation Access Unit*). Ieşirea din uz a unui calculator nu afectează comunicația dintre celelalte noduri ale rețelei. Conectarea unui nou calculator la rețea se poate face fără întreruperea funcționării acesteia, în limita numărului de porturi disponibile la nivelul nodului central.

Existența echipamentului central de comunicație permite o mai bună monitorizare, securizare şi administrare a rețelei.

Rețelele cu arie largă de răspândire (WAN) sunt de tip punct-la-punct (PP) având ca topologii fizice cele de tip "stea", "inel", "arbore" (*tree*), "plasă" (*mesh*) sau combinate (inel-stea, inel-inel etc) (Fig.I.22). Topologia “arbore” mai este denumită şi “stea extinsă” (*extended star*).

În rețelele WAN de tip "mesh", utilizate în cele mai multe cazuri, routerele aleg căile optime de transmisie a pachetelor, pe baza grafului care modelează matematic rețeaua.

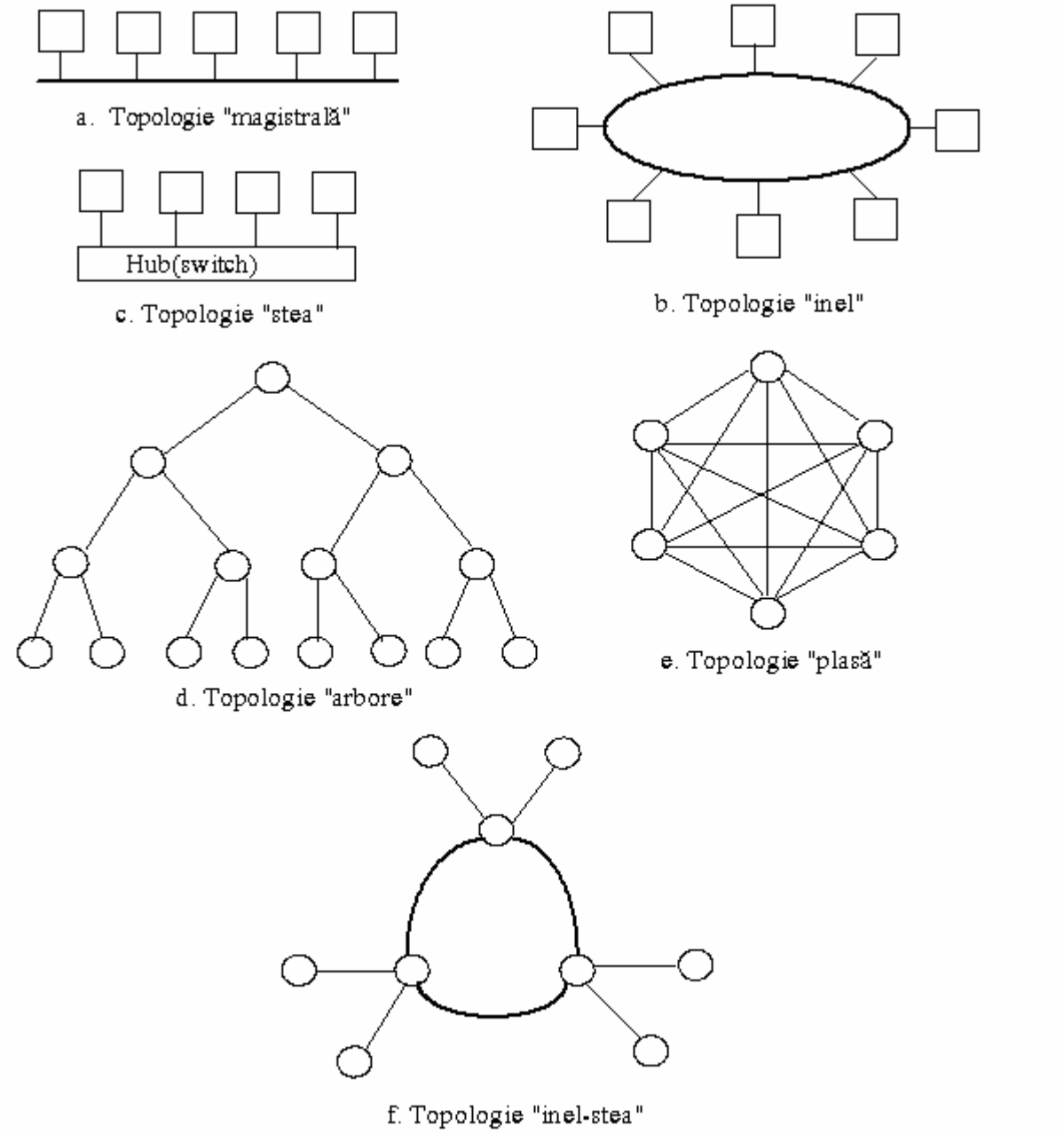


Fig.I.22 Topologii fizice de rețele

Algoritmii de rutare sunt aplicați în vederea alegerii rutei optime, în baza unui criteriu de optim care diferă de la un protocol la altul: timp minim de transmisie, cea mai scurtă cale, risc minim de coliziune a pachetelor etc.

Routerele şi mediul fizic prin intermediul cărora se interconectează mai multe LAN-uri alcătuiesc o **subrețea de comunicație** (*subnetwork*) care funcționează conform celor trei nivele inferioare ale modelului OSI: fizic, legătură de date şi rețea. Uneori protocoalele de rutare fac apel şi la nivelul de transport pentru transmisia pachetelor numai spre anumite

aplicații, în vederea reducerii încărcării rețelei sau pentru restricționarea accesului pe motive de securitate.

Avantajul topologiei *mesh* este acela că nu apar coliziuni între pachete, dar costurile necesare pentru achiziționarea materialelor şi cele de instalare sunt relativ mari în comparație cu alte topologii fizice de rețea.

Pentru realizarea fizică a unei rețele cu transmisie pe cablu, **cablarea** (*wiring*) se poate face respectând diverse topologii (Fig.I.23):

1. **liniară -** un singur cablu este trecut prin toate punctele dorite iar calculatoarele se conectează la acesta în punctul cel mai apropiat; eventual între stațiile aflate la distanțe mai mari decât lungimea maximă admisă a segmentului de cablu, se pot intercala repetoare obținându-se astfel o rețea **segmentată;**

2. de tip **"coloană vertebrală"** (*backbone*) - există cabluri orizontale şi repetoare pe fiecare nivel, toate fiind conectate la cablul central care reprezintă "coloana vertebrală" a rețelei;

3. de tip **"arbore" -** este cea mai generală topologie şi are avantajul că reduce riscul de coliziune în rețea. În plus, se pot conecta noi utilizatori în rețea fără modificarea structurii de cablare aferente celor existenți.

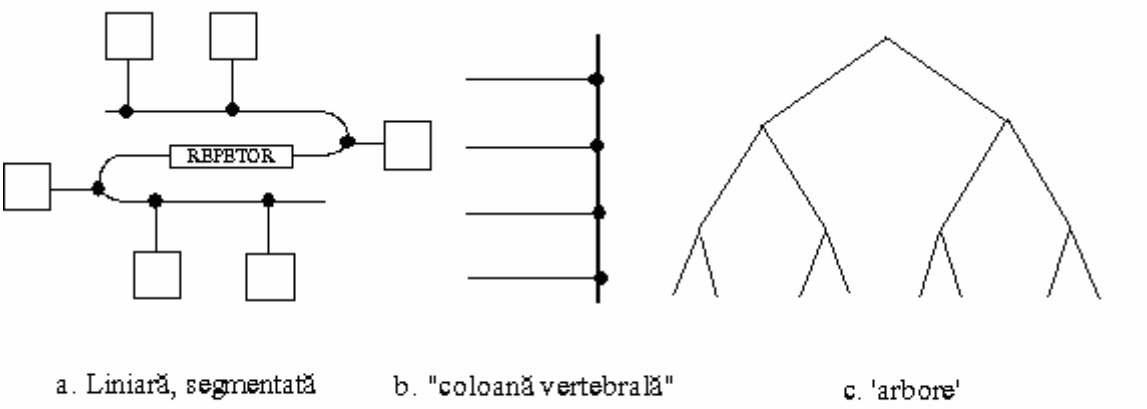


Fig. I. 23 Topologii de cablu

Numeroase probleme de transmisie sunt cauzate de defectele apărute în nodurile centrale ale unei rețele sau la nivelul mediului fizic de transmisie (cablu sau legătură prin undă radio). De aceea, este indicat ca în rețelele cu risc mare de întrerupere a întregului proces de transmisie, să existe rezerve de transmisie (*backup*), atât pentru calculatoarele de tip server (de exemplu, servere de nume, de e-mail etc), cât şi pentru structurile de transmisie (cabluri sau linii de radioreleu). În cazul rețelelor cu topologie fizică de tip "inel", se poate

folosi ca rezervă fie un al doilea inel de transmisie cu caracter redundant, fie o structură de cablare de tip "stea" cu un nod central denumit **centru de cablare** (*wiring center*), astfel încât defectarea unui nod al rețelei să nu afecteze toate comunicațiile din rețea. Sistemele de *backup* impun costuri suplimentare pentru realizarea rețelei dar asigură performanțe mai bune în funcționare.

## I.9 TEST-GRILĂ 1

I.1 O suită de reguli de comunicare şi formate impuse pentru reprezentarea şi transferul datelor între două sau mai multe calculatoare sau echipamente de comunicație se numeşte:

- ❑ rețea de calculatoare
- ❑ bază de date
- ❑ protocol
- ❑ serviciu de rețea

I.2 Furnizorul de servicii Internet se notează abreviat:

- ❑ IPng
- ❑ IRC
- ❑ ISDN
- ❑ ISP

I.3 Producătorii alocă în mod unic fiecărei plăci de rețea o adresă de tip:

- ❑ IP
- ❑ MAC
- ❑ URL
- ❑ URI

I.4 Câte subdomenii sunt incluse în DNS pe criteriul generic:

- ❑ 4
- ❑ 5
- ❑ 6
- ❑ 7

I.5 Algoritmii MD sunt aplicați datelor pentru:

- ❑ compresie
- ❑ criptare
- ❑ fragmentare
- ❑ modulare-demodulare

I.6 Unitatea de date se numeşte „pachet” pe nivelul OSI:

- ❑ 1
- ❑ 2
- ❑ 3
- ❑ 4

I.7 Codurile ciclice CRC se aplică pe nivelul OSI:

- ❑ legătură de date
- ❑ rețea
- ❑ transport
- ❑ aplicație

I.8 Funcțiile nivelelor OSI 1 şi 2 sunt cumulate în nivelul TCP/IP:

- ❑ rețea
- ❑ transport
- ❑ acces la rețea
- ❑ aplicație

I.9 Ca protocol de transport din suita TCP/IP se poate folosi:

- ❑ FTP
- ❑ HTTP
- ❑ TCP
- ❑ TFTP

I.10 Dacă adresa de destinație a unui pachet este 172.17.9.201, pentru aflarea adresei rețelei de destinație routerul aplică masca:

- ❑ 255.0.0.0
- ❑ 255.255.0.0
- ❑ 255.255.255.0
- ❑ 172.17.9.255

I.11 Nu apar coliziuni într-o rețea de calculatoare cu topologie fizică de tip:

- ❑ magistrală
- ❑ stea
- ❑ inel
- ❑ plasă

I.12 În rețeaua cu adresa IP 193.220.30.0 se aplică masca de subrețea 255.255.255.224. Câte subrețele se pot realiza?

- ❑6
- ❑8
- ❑14
- ❑16

I.13 Adresa 109.70.210.14 este de clasă:

- ❑ A
- ❑ B
- ❑ C
- ❑ D

I.14 Pentru exprimarea opțiunilor se introduc în antetul IP:

- ❑ 2 octeți
- ❑ 4 octeți
- ❑ 6 octeți
- ❑ un număr nelimitat de octeți

I.15 În rețeaua 160.119.0.0 se foloseşte adresa de broadcast:

- ❑ 160.119.0.255
- ❑ 160.119.255.255
- ❑ 160.255.255.255
- ❑ 255.255.0.0

I.16 Pentru translarea adreselor IP private în adrese IP reale se aplică:

- ❑ ARP
- ❑ BOOTP
- ❑ DHCP
- ❑ NAT

I.17 În antetul TCP, numărul portului de aplicație se exprimă pe:

- ❑ 1 octet
- ❑ 2 octeți
- ❑ 4 octeți
- ❑ 8 octeți

I.18 Accesarea de la distanță a unui router se face pe baza protocolului:

- ❑ POP
- ❑ SMTP
- ❑ Finger
- ❑ Telnet

I.19 Care dintre următoarele afirmații referitoare la ICMP este **falsă**?

- ❑ nu transmite mesaje de eroare asociate altor mesaje ICMP
- ❑ raportează eroarea de transmisie a unui pachet numai destinației
- ❑ nu generează mesaje de eroare pe adrese de broadcast
- ❑ transmite mesaj de eroare numai pentru primul fragment al unei datagrame eronate

I.20 Procesul de transfer al unei chei de criptare prin Internet este supervizat de:

- ❑ AH
- ❑ DES
- ❑ ESP
- ❑ ISAKMP