Rețele de calculatoare

C. Rețele de calculatoare

Noțiuni prezentate în acest capitol:
- rețele de calculatoare, topologie, arhitectură
- echipamente de rețea: *hub*, *switch*, cabluri
- desfăşurarea fluxului de date, protocolul TCP-IP
- administrarea rețelelor, politici de lucru în rețea

Scopul acestui capitol:
- introducere în terminologia specifică domeniului
- introducere în alcătuirea şi funcționarea rețelelor

1. Rețele locale

O rețea este un grup de calculatoare şi alte echipamente, conectate între ele prin cabluri, astfel încât fiecare echipament poate interacționa cu oricare altul.

Calculatoarele se conectează între ele în rețele pentru a putea folosi în comun resurse din cele mai diferite (fişiere, periferice etc.). *Server*-ul este calculatorul central, ale cărui resurse sunt folosite în comun de utilizatorii rețelei. Clientul este calculatorul care se conectează la *server* şi foloseşte resursele acestuia.

După dimensiuni şi aşezare, rețelele se împart în:
- rețele locale (*Local Area Network*, LAN), sunt rețele ale căror componente se găsesc aproape unele față de altele, de exemplu în aceeaşi sală, în săli vecine sau clădiri alăturate
- rețele mari (*Wide Area Network*, WAN), sunt rețele ale căror componente se află la distanță mare unele față de altele, de exemplu în localități diferite.

Caracteristicile rețelelor:
- topologia, descrie modul de organizare şi interconectare a componentelor şi echipamentelor de comunicație din cadrul rețelei,
- arhitectura, descrie categoriile de echipamente şi protocoale de comunicații utilizate în cadrul rețelei.

1.1 Topologia rețelelor

În funcție de tipul componentelor şi cablurilor utilizate şi de dispunerea calculatoarelor, rețelele pot fi:
- de tip magistrală sau *bus* (Figura C.1),
- de tip stea (Figura C.2),
- plasă, inel (*ring*), mixte.

Topologia LAN de tip stea are următoarele caracteristici:
- fiecare echipament de rețea dispune de un mediu de acces propriu, realizat prin intermediul unui traseu de cablu UTP,
- pentru gestionarea accesului este prevăzut un concentrator LAN (*hub* sau *switch*) care să centralizeze toate conexiunile UTP ale echipamentelor din rețea.

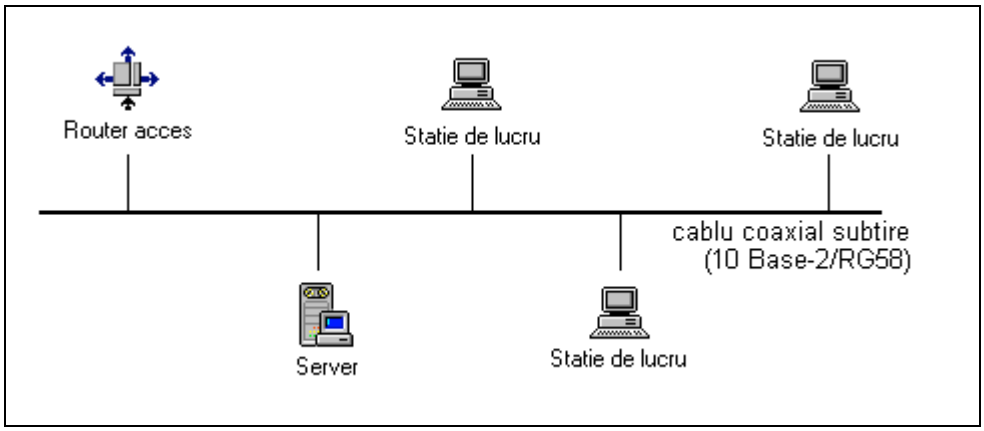

Figura C.1.

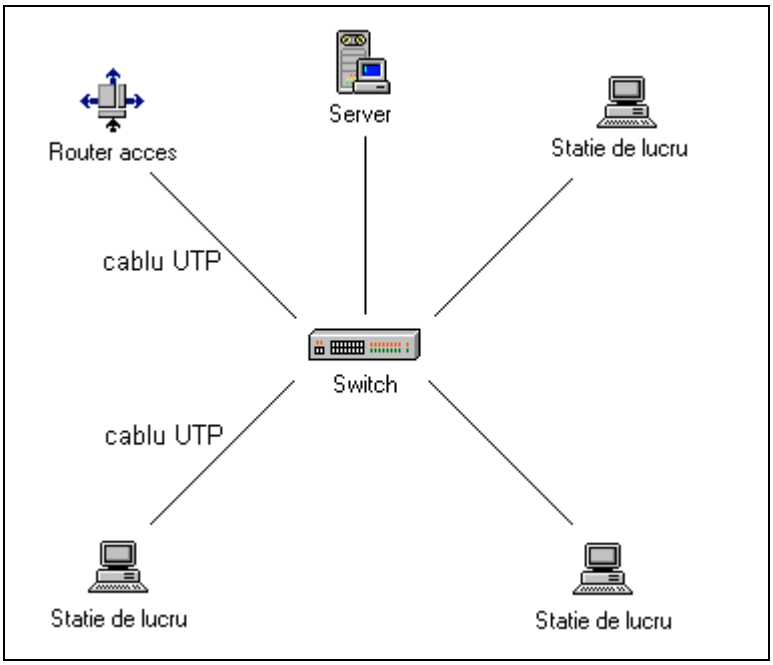

Figura C.2.

1.2 Arhitectura rețelelor

Indiferent de topologia utilizată, arhitectura standard a unei rețele *Ethernet* este următoarea:

- Server-e,
- stații de lucru (clienți),
- echipamente de comunicație LAN (*hub*/*switch*) sau WAN (*router*)

Server-ul este un calculator din rețea care gestionează resursele rețelei (de exemplu, stochează date pentru orice utilizator din rețea, gestionează imprimantele din rețea, gestionează traficul etc.), respectiv are instalate aplicații pe care membrii rețelei le pot utiliza.

Clientul este un calculator care este legat la un *server* în scopul efectuării unor operații şi depinde de acesta cu utilizarea de fişiere şi programe, pentru acces la *Internet*, pentru lansare de aplicații de calcul mari consumatoare de resurse etc.

Ethernet este o arhitectură de rețea locală dezvoltată de firma Xerox în 1976, în colaborare cu DEC şi Intel. Utilizează o topologie de tip magistrală sau stea şi suportă rate de transfer de până la 10Mbps. O versiune mai nouă de *Ethernet*, *100Base-T* sau *Fast Ethernet* (*Ethernet* rapid) transferă date cu până la 100Mbps. Acest tip de rețele utilizează cabluri cu perechi răsucite. Fiecare placă de rețea se conectează printr-un cablu (*patch cord*) la echipamentul central (*hub*, *switch*), rezultând astfel o topologie tip stea. Lungimea cablului care conectează plăcile de rețea la *hub* sau *switch* nu trebuie să fie mai mare de 100m. În rețelele tip stea, dacă se defectează cablul care conectează un calculator sau se opreşte un calculator, este afectat numai calculatorul respectiv, nu şi restul rețelei.

Când se doreşte conectarea sau deconectarea fizică a unui calculator din rețea, se închid toate programele active ale utilizatorului, se închide sistemul de operare, se scoate calculatorul din priza de alimentare electrică, se scoate sau se introduce cablul de rețea, se conectează calculatorul din nou la priza de alimentare şi se porneşte prin apăsarea butonului *Power*.

1.3 Echipamente de comunicație

1.3.1 Hub-ul

Hub-ul este un dispozitiv de rețea cu mai multe porturi (intrări) necesar pentru interconectarea prin cabluri UTP a calculatoarelor dintr-o rețea (*host*-uri). *Hub*-ul amplifică semnalul primit de la un *host* şi îl distribuie către toate celelalte calculatoare. Într-o rețea existentă pot fi adăugate

noi *host*-uri prin conectarea fizică a acestora cu cabluri UTP la *hub*-ul existent. Există *hub*-uri cu 4, 8, 16 sau 24 de intrări. *Hub*-urile pot fi montate în cascadă pentru a obține extinderea unei rețele existente.

1.3.2 Switch-ul

Switch-ul este un dispozitiv de rețea cu mai multe porturi care filtrează şi expediază pachete de date între segmentele rețelei. Operează pe nivelele 2 şi uneori 3 ale modelului de referință OSI, care va fi tratat într-un subcapitol următor, şi suportă orice protocol de transfer de date (protocol de comunicare, codul de adresare şi împachetare de date care constituie „limbajul comun" al calculatoarelor din rețea).

Principiul de funcționare a *switch*-ului are la bază mecanismul *store-and-forward*. Pentru aceasta, fiecare *switch* întreține o tabelă de redirecționare compusă din adrese MAC şi numere de porturi (căi de acces). Pentru un anumit port, care defineşte un domeniu de coliziune distinct, *switch*-ul memorează adresele MAC ale stațiilor din domeniul respectiv (conectate la acel port). Termenul de valabilitate al intrărilor din această tabelă este dat de un parametru numit *age* (vârsta), care stabileşte cât timp sunt reținute în *buffer*-e (zone tampon de stocare intermediară de date) adresele MAC ale stațiilor care nu generează şi nu primesc trafic. Prin urmare, valoarea acestui parametru poate influența performanțele unei rețele: dacă are valori prea mici, stațiile care generează puțin trafic vor fi mai greu de găsit în rețea de către alte echipamente, iar dacă valoarea parametrului este prea mare, există riscul ocupării *buffer*-elor şi al blocării echipamentului. După recepția de date este analizată adresa MAC de destinație şi este căutată în tabela de redirecționare. Prin acest mecanism *switch*-ul identifică interfața prin care este disponibilă stația de destinație şi direcționează datele printr-un canal de comunicație virtual, complet separat de traficul generat de celelalte interfețe. Astfel se reduce numărul coliziunilor, ceea ce conduce la creşterea benzii de transfer si la optimizarea modului de utilizare a canalului de comunicație

1.3.3 Router-ul

În Internet, *router*-ul este un dispozitiv, sau în unele cazuri un software instalat pe un calculator, care determină care este următorul punct din rețea către care se expediază un pachet de date în drum spre destinația sa finală. *Router*-ul este conectat la cel puțin două rețele (în punctul în care o rețea comunica cu cealaltă, adică în *gateway*). Decizia asupra direcției în care se trimite fiecare pachet de date se bazează pe determinarea stării rețelelor la care este conectat. *Router*-ul poate fi şi o parte a *switch*-ului.

Router-ul creează şi/sau stochează un tabel al rutelor disponibile, cu informații despre starea lor, şi îl utilizează împreună cu algoritmii de determinare a distanței şi costurilor pentru a selecta cea mai bună cale de urmat pentru pachetul dat. De obicei, un pachet parcurge un număr de puncte de rețea cu *router*-e înainte de a ajunge la destinație. Rutarea este o operație asociată cu nivelul 3 din standardul OSI (*Open Systems Interconnection*), nivelul rețea.

Pentru a determina calea optimă între două rețele, *router*-ul foloseşte două metode:

- Rutarea statică, constând dintr-o tabelă de adrese pentru a determina locația în care să direcționeze datele
- Rutarea dinamică, constând dintr-un protocol specializat (RIP, OSPF, IGRP, BGP)

Router-ul nu identifică tipul şi conținutul datelor transmise.

IP specifică formatul pachetelor de date şi schemele de adresare. Majoritatea rețelelor combină IP cu un protocol de nivel mai înalt, TCP (*Transmission Control Protocol*), care stabileşte conexiunea virtuală între sursă şi destinație. IP-ul singur funcționează ca sistemul poştal. Permite adresarea unui pachet de date şi lansarea sa în Internet fără o legătură directă cu destinația. TCP/IP stabileşte conexiunea între sursă şi destinație, astfel încât pe linia respectivă de poate face schimb de mesaje continuu pe perioade de timp determinate.

1.4 Cabluri şi conectori

Pentru rețele locale se realizează cablarea structurată de tip UTP/STP. Conceptul de cablare structurată a fost dezvoltat ca urmare a necesității uniformizării celor două tipuri de cablaje

existente: cablajul de voce (telefonie) şi cel de date. Până la elaborarea standardelor de cablare structurată, partea de telefonie a unei clădiri era realizată pe cabluri răsucite (topologie stea), în timp ce pentru rețeaua de date s-a utilizat cablul coaxial (topologie de tip magistrală).

Cablurile torsadate (*Twisted Pair, TP*) pot fi de mai multe tipuri (Figura C.3):

- UTP (*Unshielded Twisted Pair*), ieftine, subțiri, flexibile, ne-ecranate (fără înveliş izolator), cu patru perechi de fire răsucite din cupru. Dintre aceste perechi, două (verde şi portocaliu) sunt folosite pentru transmisa de date, o pereche (albastră) pentru transmisia de voce (telefonie), cealaltă pereche (maro) putând fi utilizată pentru alte aplicații (alarme, monitorizare clădire etc.). Transmisia date/voce nu se poate realiza simultan pe acelaşi tronson de cablu UTP. Pentru rețele mici (cu distanțe scurte între componente) acest tip de cablu este suficient. Structura ne-ecranată a UTP creşte riscul de interferență cu radiațiile electromagnetice parazite. Pentru creşterea imunității la zgomote se mai utilizează o variantă de cablu denumită ScTP (*Screened Twisted-Pair*), identică cu UTP dar la care toate cele patru perechi de fire de cupru sunt ecranate cu o folie metalică.
- STP (*Shielded Twisted Pair*), cablu torsadat ecranat, prevăzut cu patru sau două (varianta STP-A) perechi de fire de cupru, fiecare pereche fiind ecranată cu o folie metalică în vederea reducerii zgomotelor parazite care pot afecta semnalul util (perturbații electrice, diafonie).

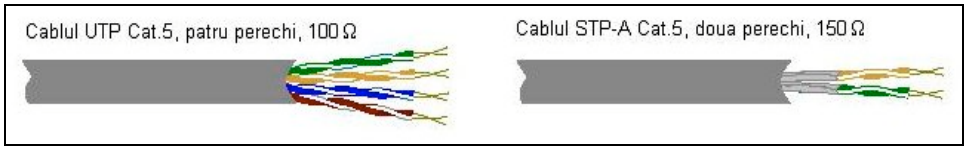

Figura C.3.

Conectorul RJ45 (*Registered Jack 45*) este un conector cu 8 fire, folosit în rețele locale, în special de tip *Ethernet*. Arată la fel ca RJ11 folosit în telefonie, doar că este puțin mai lat. În Figura C.4 sunt prezentate priza şi mufa conectorului RJ45.

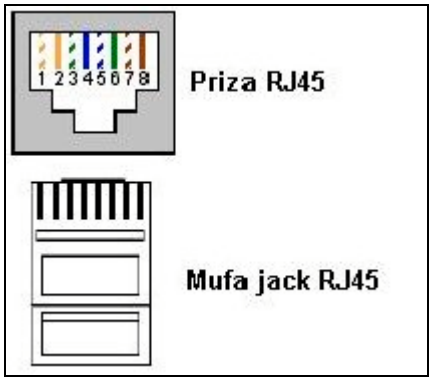

Figura C.4.

1.5 Conectarea la Internet

Pentru conectarea rețelei locale la *Internet* se utilizează un *router* şi un *modem* (descris în secțiunea A, capitolul 2.9). *Router*-ul face legătura între rețele, iar *modem*-ul transformă semnalul digital în semnal analogic (la transmisie) şi invers (la recepție) (Figura C.5).

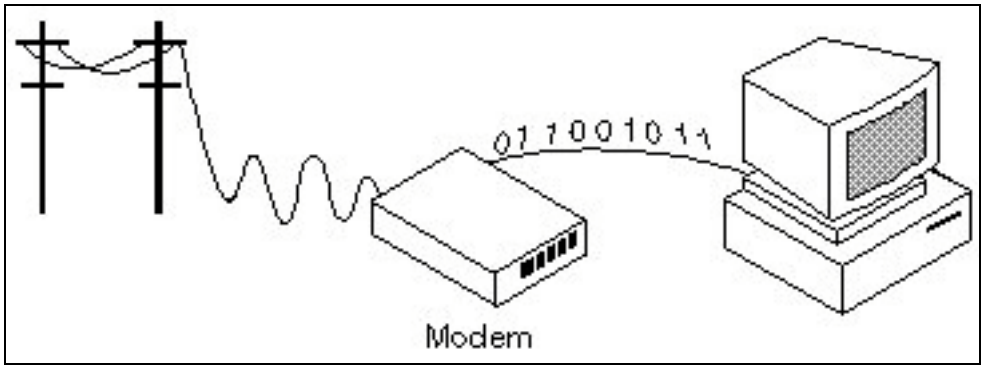

Figura C.5.

Funcția de *router* poate fi îndeplinită de echipamente *hardware* specializate sau de calculatoare pe care rulează un *software* specializat. Modemul se conectează cu un cablu serial la *router* şi cu un cablu telefonic la o linie telefonică obişnuită. *Modem*-ul folosit este unul pentru *dial-up*. Accesul *dial-up* funcționează ca o legătură telefonică obişnuită, doar că în loc să facă legătura între persoane, leagă calculatoare. Calitatea conexiunii nu este întotdeauna bună, iar viteza de transfer a datelor este limitată de performanțele legăturii telefonice. Rata normală de transfer este de 56KBps. Tehnologii mai noi (gen *Integrated Services Digital Network, ISDN*, care transmite date pe linii telefonice cu legături dedicate) asigură rate de transfer mai mari (64/128 KBps).

Legătura la *Internet* se face prin intermediul unui furnizor de servicii de *Internet* (*Internet Service Provider, ISP*). Acest furnizor va comunica modalitatea prin care se va face conectarea rețelei locale la *Internet*, va furniza adresele IP, măştile, adresele DNS (*Domain Name System*), adresele de *server* proxy etc.

DNS este prescurtarea de la *Domain Name System* sau *Domain Name Service*, un serviciu *Internet* care transformă numele de domenii în adrese IP. Numele de domenii sunt şiruri de litere şi cifre care sunt mai uşor de memorat decât adresele IP. De exemplu, domeniul *microsoft.com* are adresa IP 207.46.249.27, care se poate afla introducând comanda *ping www.microsoft.com* într-o fereastră DOS, care se deschide în *Windows* selectând *Start/All_Programs/Accessories/Command Prompt*.

Domeniul de *Internet* este un grup de calculatoare dintr-o rețea care sunt administrate printr-un set de reguli şi proceduri comune. În *Internet*, domeniile sunt definite prin nume, care au asociate adrese IP.

1.6 Adrese IP

Protocolul este un format prestabilit de transmitere a datelor între două componente de rețea. Prin protocol se definesc următoarele: tipul de detectare de erori, metoda de comprimare a datelor (dacă este cazul), felul în care expeditorul semnalează sfârşitul transmisiei, felul în care destinatarul semnalează primirea unui mesaj, modul de transmitere (sincron, asincron), rata de transfer de date etc.

TCP/IP (*Transmission Control Protocol/Internet Protocol*) este o suită de protocoale de comunicare utilizată pentru conectarea sistemelor locale (*host*-uri).

Interfața de conectare la o rețea este reprezentată fizic (*hardware*) de placa de rețea, iar din punct de vedere *software*, de „entitatea” care va primi o adresă IP. Această adresă este atribuită unei interfețe de rețea şi nu unui calculator. Un calculator cu două plăci de rețea va avea două interfețe, fiecare cu adresă IP proprie, distinctă.

În rețeaua locală adresele IP trebuie să fie unice. Pentru a minimiza posibilitatea existenței de adrese duplicate în rețea se poate instala un *server* DHCP (*Dynamic Host Configuration Protocol*) care va asigna automat o adresă oricărei stații care se va conecta în rețea.

Forma unei adrese IP: din punct de vedere al utilizatorului adresa IP este o secvență formată din patru octeți separați de caracterul „.” (punct), fiecare octet putând lua valori între 0 şi 255. Pentru echipamentul de rețea, adresa respectivă apare ca o succesiune continuă de 32 de biți, fiecare grup de opt fiind reprezentarea binară a unui octet din formatul vizibil pentru utilizator.

Exemplu:

10010110	11010111	00010001	00001001
150	215	017	009

Adresa IP este alcătuită din două componente cu format variabil:

- componenta de rețea. În funcție de numărul de biți rezervați acestei componente, spațiul de adrese se împarte în următoarele clase:
    - clasa A: primii 8 biți reprezintă adresa de rețea 10.0.0.0 până la 127.255.255.255.

- clasa B: primii 16 biți reprezintă adresa de rețea 128.0.0.0 până la 191.255.255.255.
- clasa C : primii 24 de biți reprezintă adresa de rețea 192.0.0.0 până la 233.255.255.255. În cadrul clasei C există două subclase cu destinații speciale: D (adrese *multicast*, pentru rețele multimedia (voce, video), 224.0.0.0 până la 239.255.255.255), E (clasă pentru dezvoltări ulterioare, 240.0.0.0 până la 247.255.255.255.

- componenta de *host*: biții rămaşi după ocuparea adresei cu componenta de rețea identifică echipamentele din cadrul unei rețele. Numărul de biți ai componentei de *host* determină numărul maxim de echipamente din rețeaua definită prin prima componentă:
  - în clasa A: 256 de rețele, 16.777.216 echipamente adresabil în fiecare rețea,
  - în clasa B: 65.536 de rețele, 65.536 echipamente adresabile în fiecare rețea,
  - în clasa C: 16.777.216 de rețele, 256 echipamente adresabile în fiecare rețea.

De exemplu, pentru adresa IP 150.215.017.009, dacă se presupune că este o adresă de clasă B, 150.215 reprezintă adresa de rețea de clasă B, iar 017.009 identifică un *host* în acea rețea.

Adresele utilizate pot fi publice sau private. Pentru rețelele de instituții se recomandă utilizarea adreselor private (ne-rutate). Se pot utiliza şi adrese reale publice dintr-o clasă oarecare, cu condiția ca rețeaua sa nu fie conectată la *Internet*. Gama pentru adrese private este:

- adrese de rețea de la 10.0.0.0 până la 10.255.255.255, mască 255.0.0.0
- adrese de rețea de la 172.16.0.0 până la 172.31.255.255, mască 255.255.0.0
- adrese de rețea de la 192.168.0.0 până la 192.168.255.255, mască 255.255.255.0

Observații:

- primul bloc este un singur număr de rețea de clasă A,
- al doilea bloc este un set de 16 numere de rețea de clasă B (adrese contigue),
- al treilea bloc este un set de 255 de numere de rețea de clasă C (adrese contigue).

Masca este un filtru care determină cărei subrețele (*subnet*) îi aparține o adresă IP. Sistemul de subrețele îi permite administratorului de rețea să gestioneze mai uşor adresele alocate. De exemplu, pentru adresa IP „10010110.11010111.00010001.00001001” (scrisă în sistem binar), componenta de rețea de clasă B este „10010110.11010111” şi adresa de *host* este „00010001.00001001” Primii patru biți ai adresei de *host* vor identifica eventualele subrețele.

Masca este formată din adresa de rețea plus biții de identificare a subrețelei. Prin convenție, biții de rețea sunt de valoare 1. În exemplul de mai sus, masca va fi de forma „11111111.11111111.11110000.00000000”. Subrețeaua din exemplu este astfel uşor de identificat. Adresa ei este „10010110.11010111.00010000.00000000”.

Pentru o identificare mai uşoară, exemplul de mai sus poate fi prezentat în format tabelar:

Masca de subrețea	255.255.240.000	11111111.11111111.11110000.00000000
Adresa IP	150.215.017.009	10010110.11010111.00010001.00001001
Adresa subrețelei	150.215.016.000	10010110.11010111.00010000.00000000

2. Modelul de rețea OSI

Modelul de referință OSI-RM (*Open Systems Interconnection-Reference Model*) este un standard ISO (*International Standards Organization*) care defineşte un set de reguli universal valabile pentru proiectarea protocoalelor de comunicațiilor, în scopul înlesnirii interconectării dispozitivelor *hardware* si *software* indiferent de producător.

Prin intermediul acestui model (Figura C.6), suita de operații necesare pentru desfăşurarea unui flux de date între clienții din rețea este organizată ierarhic pe şapte niveluri:

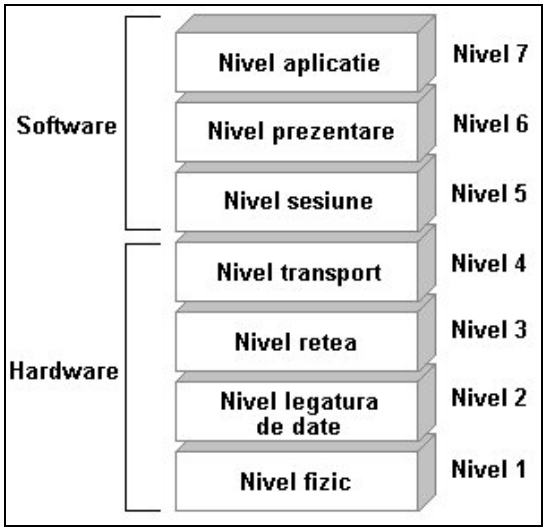

Figura C.6.

- nivelul fizic: stabileşte proprietățile cablurilor şi conectorilor, defineşte protocoalele necesare pentru transmisia datelor pe o linie de comunicație,
- nivelul legăturii de date: defineşte modalitățile de acces la mediul de transmisiune partajat de mai multe echipamente, stabileşte modul de transfer al datelor între nivelurile superioare şi conectorii fizici,
- nivelul rețea: permite identificarea nodurilor de destinație prin prelucrarea informațiilor rezultate din adresele de rețea şi tabelele de direcționare ale *router*-elor,
- nivel de transport: defineşte metodele prin care se asigură integritatea datelor către nodul de destinație,
- nivelul sesiune: sincronizează comunicația între două calculatoare, controlează când un utilizator poate transmite sau recepționa date,
- nivelul prezentare: efectuează translația datelor între formatul utilizat de aplicație şi formatul informației transferate prin rețea,
- nivelul aplicație: asigură interfața *software* pentru utilizatori.

Primele patru niveluri sunt caracteristice echipamentelor de comunicații cu funcții specializate implementate pe o platformă *hardware*. Următoarele trei niveluri sunt oferite de orice aplicație (*software*) de rețea existentă pe *server*-e, calculatoare sau echipamente de comunicație specializate. Modul de reprezentare a stivei OSI în cadrul unei rețele cu un *server*, un client si un echipament de comunicație este ilustrat în Figura C.7.

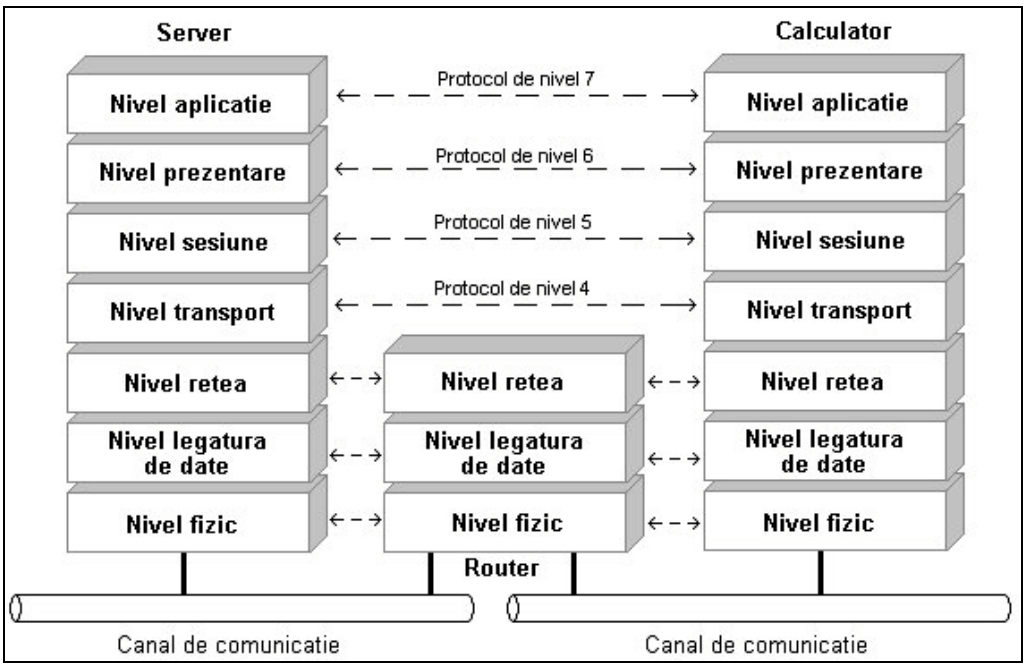

Figura C.7.

2.1 Nivelul fizic

În cadrul nivelului fizic se definesc următoarele funcții:

- tipul de transmitere şi recepționare a şirurilor de biți pe un canal de comunicații:
    - transmisia asincronă: semnalul de ceas al receptorului se sincronizează pe semnalul de start transmis de emițător. Din această cauză, canalul de comunicație nu este utilizat eficient şi nu se pot obține rate de transfer mari, de maxim 115 KBps. Este frecvent utilizată pentru conectarea a două echipamente de rețea prin intermediul cablurilor seriale sau a *modem*-urilor analogice.
    - transmisia sincronă: şirurile de biți se succed fără întrerupere, fiecare echipament având nevoie de un semnal de sincronizare propriu. De aceea, receptorul este mai complicat, însă se asigură o utilizare eficientă a canalului de comunicație şi se pot obține viteze mari de transfer (2 MBps).
- se definesc topologiile de rețea.
- în funcție de topologie, se stabileşte tipul rețelei:
    - rețea *broadcast* (topologii magistrală, stea, inel): la acelaşi mediu de transmisiune sunt ataşate mai multe echipamente de rețea, iar un pachet de date transmis de o stație este recepționat de toate celelalte (de exemplu, *Ethernet/Fast Ethernet*, *Token Ring*)
    - rețele punct-la-punct (topologii stea, plasă): la o conexiune fizică sunt ataşate numai două echipamente. Într-o rețea cu mai mult de două noduri, un pachet de date trebuie să tranziteze mai multe noduri intermediare pentru a ajunge la destinație.
- se definesc tipurile de medii de transmisiune : cablu coaxial, cablu UTP, fibră optică, linii închiriate de cupru etc.
- se stabileşte modul de transmisie: simplex (un singur echipament poate transmite, iar corespondentul doar recepționează), half-duplex (ambele echipamente pot să transmită şi să recepționeze semnale, dar nu în acelaşi timp), full-duplex (ambele echipamente pot să transmită şi să recepționeze semnale în acelaşi timp).
- se definesc standardele mecanice şi electrice ale interfețelor, seriale (RS-232, V.35, G.703) şi LAN (BNC, AUI, RJ45).
- este realizată codificarea şi decodificarea şirurilor de biți (repetoare, media-convertoare etc.).
- este realizată modularea şi demodularea semnalelor purtătoare (modem-uri).
- unitatea de date utilizată la nivel fizic este bitul.

2.2 Nivelul legăturii de date

Realizează transferul datelor între sisteme adiacente (care partajează acelaşi mediu de acces). Este alcătuit din două sub-niveluri:

- controlul accesului la mediu (MAC - *Medium Access Control*): defineşte echipamentul care poate avea acces la rețea atunci când mai multe stații încearcă să transmită simultan:
    - asigură controlul fluxului de date (*flow-control*) prin stabilirea momentelor de transmisie sau aşteptare,
    - efectuează controlul accesului la mediul fizic,
    - în cadrul rețelelor de tip *broadcast*, prin intermediul legăturii de date se realizează identificarea unui nod destinație, prin utilizarea adreselor MAC.
- controlul legăturii logice (LLC - *Logical Link Control*): defineşte modul de transfer al datelor către nivelul fizic şi furnizează serviciul de transport către nivelul rețea:
    - introduce în fluxul de biți furnizat nivelului fizic delimitatorii necesari pentru separarea cadrelor. La recepție, nivelul legăturii de date recunoaşte aceşti delimitatori şi reconstituie cadrele. Scopul acestei încadrări este determinat de necesitatea gestionării fluxului continuu de biți preluați de la nivelul fizic.
    - controlul erorilor, realizat în două moduri: FEC (*Forward Error Correction*, foloseşte biții de control pentru detectarea şi corectarea erorilor), ARQ (*Automatic Retransmition Query*, utilizat numai pentru detectare, nu şi pentru corectarea erorilor, ca mijloc de alertare a sursei că informația nu a fost recepționată corect).

Unitatea de date este *cadrul*, format din şiruri de *bytes* (1 byte = 8 biți).

La nivelul legăturii de date sunt definite protocoalele de interconectare a rețelelor LAN, în funcție de tipul transmisiei utilizate la nivel fizic:

- protocoale orientate pe biți, utilizate pe transmisii seriale: PPP (*Point-to-Point Protocol*, destinat legăturilor sincrone şi asincrone), HDLC (*High Data Link Control*, destinat numai legăturilor sincrone punct-la-punct sau legăturilor multipunct şi permite lucrul *full-duplex*).
- protocoale orientate pe comutație de pachete. Mesajul utilizatorului este împărțit în pachete, fiecare pachet fiind transmis separat şi pe trasee fizice diferite.

2.3 Nivelul rețea

Permite transferul de date între sistemele neadiacente (care nu partajează acelaşi mediu de acces). Unitatea de date utilizată este *pachetul*.

Funcția principală a acestui nivel constă în dirijarea pachetelor între oricare două noduri de rețea. Cu alte cuvinte, nivelul rețea realizează rutarea (direcționarea) pachetelor de date prin infrastructura de comunicații, această operație fiind efectuată la nivelul fiecărui nod de comunicație intermediar. Nivelul rețea asigură interfața între furnizorul de servicii şi utilizator, serviciile oferite fiind independente de tehnologia subrețelei de comunicație.

Acest nivel oferă două categorii de servicii de transport:

- orientate pe conexiuni (ATM): înainte de transferul datelor între două echipamente trebuie stabilită o conexiune (circuit virtual), care se închide la terminarea transferului. La stabilirea conexiunii se pot negocia anumiți parametri legați de calitatea serviciului (viteză, întârziere, cost). Ruta (secvența de noduri intermediare) pe care vor fi trimise pachetele se stabileşte în momentul stabilirii circuitului virtual. În acest sens, circuitul virtual va primi un identificator (adresă), fiecare pachet fiind rutat pe baza acestui identificator. Prin utilizarea serviciilor orientate pe conexiuni se realizează un control foarte eficient al fluxului de date, putând fi definite categorii de servicii (CoS - *Class of Services*) şi criterii de calitate a serviciilor (Qos - *Quality of Services*). Aceste avantaje implică o complexitate ridicată la nivelul arhitecturii de rețea. În cazul defectării unui nod intermediar, toate circuitele virtuale care îl tranzitează se închid. Latența inițială necesară pentru stabilirea conexiunii este mare.
- fără conexiuni (IP): nu este necesară stabilirea unei conexiuni prin subrețeaua de comunicație în vederea transferului datelor. Ruta este determinată pentru fiecare pachet în parte, iar direcționarea (rutarea) se realizează pe baza adreselor (sursă şi destinație) conținute în fiecare pachet. Deoarece nu este necesară memorarea informațiilor de stare cu privire la

conexiuni, complexitatea este redusă, fiind posibilă implementarea unor rețele mai rapide. În cazul defectării unui nod intermediar, comunicația poate continua pe căi alternative. Dezavantajul principal al acestor servicii constă în faptul că nu se mai poate efectua un control al congestiei traficului.

Cel mai cunoscut si utilizat protocol la acest nivel este IP (*Internet Protocol*), utilizat pentru interconectarea rețelelor din *Internet*. Este un protocol fără conexiune care permite transmiterea unor blocuri de date (datagrame) între surse şi destinații identificate prin adrese cu lungime fixă. În cazul datagramelor foarte mari, protocolul IP realizează, dacă este cazul, fragmentarea şi reasamblarea în vederea transmiterii prin orice rețea. Nu dispune de mecanisme care să asigure securitatea serviciului sau controlul fluxului de informații. Este apelat de protocoalele superioare pentru transferul prin rețea al datelor, apelând la rândul lui la protocoalele rețelei locale pentru transportul datelor către un echipament local. Acest echipament local (adiacent) poate fi destinația finală a pachetelor de date sau poate fi un nod intermediar al sistemului de comunicații (*router*), care trebuie să redirecționeze datele.

Modul de funcționare a protocolului IP este următorul:
- aplicația pregăteşte datele şi le transmite nivelului Internet al software-ului de rețea,
- nivelul Internet adaugă acestor date un antet (*header*), conținând adresa de destinație,
- datagrama rezultată este transmisă interfeței de rețea, care adaugă la rândul ei un antet şi transmite întreg cadrul către primul nod intermediar al rețelei de comunicații, care va efectua rutarea pachetului,
- la recepție, un nod intermediar va decide după adresa de destinație prezentă în antet care este subrețeaua şi, implicit, următorul nod intermediar către care trebuie redirecționat pachetul,
- în cadrul destinației finale, antetul este înlăturat şi datagrama se transmite nivelului Internet, de unde este transmis nivelului aplicație.

Din acest mod de funcționare se pot deduce următoarele reguli privind mecanismele de rutare:
- fiecare datagramă este direcționată către cel mai apropiat nod intermediar, *router* sau *gateway*,
- operația de rutare constă în determinarea nodului intermediar următor (adiacent) care la rândul lui poate redirecționa datagramele către destinația finală. Acest tip de rutare este numit *hop-by-hop routing* şi nu permite determinarea întregii secvențe de noduri intermediare.
- destinația imediat următoare poate fi un alt *router* sau chiar destinația finală.
- decizia privind destinația imediată este luată pe baza informațiilor existente în cadrul tabelei de rutare. Această tabelă este menținută de fiecare *router* şi conține asocieri de tipul *destinație finală - destinație următoare* (next hop).
- la primirea unei datagrame, *router*-ul caută în tabela de rutare înregistrarea corespunzătoare destinației finale. Dacă această înregistrare este găsită, datagrama se transmite către următoarea destinație specificată în ruta respectivă.
- tabela de rutare poate fi actualizată în următoarele moduri:
    - prin rute statice, introduse de administratorul rețelei. Orice echipament de rețea (*host* sau *router*) conține o aşa-numită rută statică implicită (*default*), utilizată pentru redirecționarea datagramelor atunci când nu este găsită nici o înregistrare care să corespundă cu adresa finală.
    - prin rute directe, care sunt create automat de echipamentul de rețea (*host* sau *router*) în momentul în care se specifică adresele IP şi măştile de subrețea pe interfețele echipamentului. În acest mod se realizează asocierea între destinația imediată şi interfața fizică prin care poate fi atins următorul nod de rutare.
    - prin rute dinamice, schimbate între *router*-ele adiacente prin intermediul protocoalelor specializate. Utilizând mecanismele de rutare dinamică, un *router* transmite *router*-elor învecinate întreaga tabelă de rutare, constând în rute statice, rute directe şi rute dinamice „învățate" de la alte *router*-e. Cele mai cunoscute protocoale de rutare dinamică sunt: RIP (*Routing Information Protocol*), versiunile 1 şi 2, utilizat frecvent în rețele private, OSPF (*Open Short Path Finding*), IGRP (*Internal Gateway Routing Protocol*), BGP (*Border Gateway Protocol*, utilizat în rețeaua *Internet* pentru rutarea infomațiilor între furnizorii de servicii).

2.4 Nivelul transport

Este un nivel intermediar care delimitează nivelul *hardware* de nivelul *software*. Unitatea de date este *segmentul*. Oferă un set standard de servicii, independent de tipul rețelei utilizate: transfer sigur de date pe o rețea de comunicații considerată nesigură, corectarea erorilor când această operație nu se realizează pe nivelurile inferioare, negocierea calității serviciului. Sarcina principală a nivelului transport este aceea de refacere a fluxului de date la destinație, deoarece un pachet poate fi segmentat în mesaje mai mici, cu rute diferite prin rețeaua de comunicații.

În cazul utilizării protocolului IP pe nivelul rețea, sunt disponibile două protocoale la nivelul transport:

- TCP, *Transmission Control Protocol*
    - este un protocol bazat pe conexiune, în care pentru fiecare pachet transmis se aşteaptă o confirmare din partea echipamentului de destinație.
    - transmisia următorului pachet nu se realizează dacă nu se primeşte confirmarea pentru pachetul transmis anterior.
- UDP, *User Datagram Protocol*
    - este folosit în situațiile în care eficiența şi viteza transmisiei sunt mai importante decât corectitudinea datelor, de exemplu în rețelele multimedia, unde pentru transmiterea către clienți a informațiilor de voce sau imagine este mai importantă viteza (pentru a reduce întreruperile în transmisie) decât calitatea.
    - este un protocol fără conexiuni, semnalarea erorilor sau reluărilor fiind asigurată de nivelul superior,
    - datele transmise nu sunt segmentate.

2.5 Nivelul sesiune

Permite stabilirea de conexiuni (sesiuni) între aplicațiile existente pe echipamentele dintr-o rețea. Prin urmare, este orientat către problemele specifice aplicațiilor, mai puțin pentru comunicația efectivă, siguranța acesteia fiind asigurată de nivelurile inferioare.

Nivelul sesiune execută următoarele funcții principale:

- gestiunea dialogului între aplicații,
- sincronizarea între aplicații,
- gestiunea şi raportarea erorilor.

În cazul aplicațiilor IP, nivelul sesiune este utilizat şi pentru identificarea aplicațiilor instalate pe acelaşi echipament de rețea, identificat în cadrul rețelei printr-o adresă IP unică. Pentru identificare, o aplicație utilizează o valoare întreagă, cuprinsă între 1 si 65535, numită port de comunicație. De exemplu:

- Telnet: portul 23,
- FTP: portul 21,
- HTTP: portul 80 sau 8080,
- SNMP: porturile 161 şi 162,
- SMTP (transmisie email): portul 25,
- POP (recepție email): portul 110.

2.6 Nivelul prezentare

Îndeplineşte funcții legate de reprezentarea datelor, conversii, criptare, compresie etc. Stabileşte sintaxa pentru datele transmise prin rețea.

2.7 Nivelul aplicație

Acest nivel defineşte protocoalele specifice aplicațiilor. Cele mai uzuale aplicații definte la acest nivel sunt:

- terminale virtuale: Telnet,
- transfer de fişiere: FTP (*File Transfer Protocol*),

- poştă electronică,
- SMTP (*Simple Mail Transfer Protoco*l),
- POP (*Post Office Protocol*),
- Aplicații web (prezentare, baze de date etc.) cu HTTP (H*yper Text Transfer Protocol*)
- Administrare şi monitorizare: SNMP (S*imple Network Management Protocol*).

3. Monitorizarea rețelelor

Scopul principal al monitorizării unei rețele este urmărirea permanentă a stării de funcționare a echipamentelor de comunicație sau a echipamentelor destinate anumitor servicii, simultan cu urmărirea disponibilității şi încărcării canalelor de comunicație. Informația rezultată din monitorizarea unei rețele trebuie să asigure un suport pentru identificarea şi depanarea rapidă a defectelor.

Pentru implementarea acestor funcții se utilizează două protocoale specializate:
- ICMP, Internet Control Message Protocol
- SNMP, Simple Network Management Protocol

ICMP este un protocol care funcționează la nivelul 3 al modelului OSI (nivelul rețea), nefiind necesară utilizarea unui protocol de transport (TCP sau UDP) sau a unui port de comunicație. Acest protocol permite încapsularea în interiorul cadrului IP a unor informații, care o dată ajunse la destinația specificată, determină generarea unui răspuns către sursa ICMP, din care se poate deduce timpul de răspuns pe un canal de comunicație (de exemplu, mesajul rezultat în urma lansării comenzii *„ping"* în linia de comandă, în fereastra DOS a sistemului de operare *Windows*).

Parametrii ICMP pot fi astfel configurați încât să determine generarea unui răspuns din partea fiecărui echipament de comunicație tranzitat de pachetele ICMP (comenzile *tracert*, *ping route*), obținându-se şi o imagine a traseului fizic corespunzător canalului de comunicație. În cazul în care nodul de destinație sau un nod tranzitat nu răspunde la un pachet ICMP, este asociat un mesaj de eroare, care poate oferi informații utile în stabilirea cauzelor pentru care nu poate fi atinsă o destinație (cale de comunicație nefuncțională, rute IP necorespunzătoare etc.).

SNMP este un protocol care funcționează la nivelul de aplicație al modelului OSI şi cuprinde una sau mai multe stații de administrare şi mai multe elemente de rețea administrabile (*server*, *switch*, *hub*, *router* etc.).

Un echipament administrabil este format din două componente principale:
- un agent SNMP, prin intermediul căruia sunt stabilite regulile de transfer a informațiilor între echipamentul administrabil şi stația de administrare,
- o colecție de obiecte (*Management Information Base*, MIB) în care sunt gestionate informațiile referitoare la elementele componente ale echipamentului administrabil.

Colecția MIB conține următoarele informații:
- starea sistemului şi a dispozitivelor care compun echipamentul (interfețe de rețea),
- statistici despre performanțele sistemului (memorie, procesor, *buffer*-e),
- statistici ale traficului pe interfețe, erori la nivel logic sau fizic,
- parametri de configurare (adrese IP, rute etc.).

La nivelul echipamentului administrabil, agentul SNMP execută următoarele operații:
- colectează informații despre starea şi componentele sistemului şi actualizează obiectul corespunzător din colecția MIB,
- răspunde cererilor (interogărilor) efectuate de stația de administrare,
- raportează stației de administrare evenimentele speciale (critice) prin intermediul alarmelor SNMP (*traps*),
- oferă administratorului acces direct pe echipament sau la un dispozitiv al acestuia.

Alarmele SNMP se împart în două categorii:
- standard: raportează către stația de administrare următoarele evenimente speciale:
    - activarea/dezactivarea interfețelor de rețea,
    - repornirea echipamentului, la cald sau la rece,

- erori de autentificare.

- enterprise: pot genera semnalizări suplimentare despre: modificarea configurației echipamentului sau încercări de configurare, probleme în funcționarea protocoalelor de rutare dinamică, semnalizări privind depăşirea pragurilor pentru tensiunea de alimentare sau pentru parametrii ambientali (temperatură, umiditate etc.).

O comparație între cele două protocoale utilizate pentru monitorizare şi administrare este prezentată în tabelul următor:

ICMP	SNMP
Oferă o imagine de ansamblu a stării de funcționare a unei rețele: echipamente sau interfețe de rețea funcționale sau nu, gradul de încărcare a canalelor de comunicație.	Oferă informații detaliate asupra unor parametri de comunicație importanți: gradul de încărcare efectiv la nivelul tuturor interfețelor de rețea ale unui echipament, şi eventualele erori de transmisie/recepție, gradul de încărcare al procesorului şi al memoriei RAM. Starea unei interfețe (*up*, *down*, *loopback*) şi dacă această stare este provocată de disfuncționalități ale rețelei sau este o stare administrativă (impusă de administratorul de rețea).

Starea generală a rețelei nu este raportată în timp real, ci numai la intervale regulate, corespunzătoare momentelor de interogare a rețelei.	Starea generală a rețelei este raportată în timp real, prin intermediul alarmelor care sunt transmise în momentul producerii unui eveniment. Excepție fac situațiile în care echipamentul este oprit sau se dezactivează interfața corespunzătoare canalului de comunicație prin care se transmit şi alarmele SNMP. Aceste evenimente nu pot fi puse în evidență decât cu ajutorul protocolului ICMP.
Permite identificarea segmentelor de rețea care alcătuiesc canalul de comunicație dintre sursă şi destinație.	Permite realizarea topologiilor de rețea şi identificarea anumitor tipuri de echipamente, prin obținerea informațiilor referitoare la adresele IP alocate şi a tabelelor de rutare utilizate. Acest lucru este posibil numai dacă sistemul de monitorizare cunoaşte toate comunitățile de citire ale echipamentelor care compun o rețea.
Oferă informații utile despre eventualele disfuncționalități, informații care, interpretate corect, pot ajuta la descoperirea cauzelor care provoacă aceste probleme (adrese IP sau rute incorecte, canale de comunicație congestionate etc.)	Oferă multe informații detaliate cu privire la problemele apărute în cadrul unei rețele, la nivelul echipamentelor sau canalelor de comunicație, însă, de foarte multe ori, aceste probleme afectează chiar căile de comunicație prin care se obțin aceste informații sau se transmit alarme SNMP.

Din compararea caracteristicilor celor două protocoale reiese că utilizarea combinată a acestora constituie soluția optimă de monitorizare şi administrare a rețelelor, fiind posibilă astfel atât raportarea detaliată a funcționării echipamentelor (inclusiv în format grafic), prin utilizarea protocolului SNMP cât şi menținerea unei imagini minimale a stării de funcționare a rețelei, prin intermediul protocolului ICMP, în cazul în care este afectată funcționarea agentului SNMP.

4. Administrarea rețelelor

Administrarea rețelei locale presupune:
- monitorizarea rețelei Ethernet şi a traficului,
- asigurarea, menținerea şi controlul securității rețelei locale,
- colaborarea în vederea remedierii nefuncționalităților echipamentelor cu firma care asigură service-ul în limitele contractuale şi rezolvarea diverselor disfuncționalități apărute în exploatarea curentă,
- gestiunea corectă e elementelor de bază ale rețelei locale (adrese IP, echipamente de comunicații, aplicații specifice),
- menținerea la standarde corespunzătoare a calității rețelei din punct de vedere al configurărilor.

În arhitectura rețelei, *server*-ele sunt maşinile cu importanța cea mai mare. Ele stochează baze de date, au componente ale aplicațiilor care rulează în sistem, dețin un rol important în sistemul de comunicație şi dispun de resurse *hardware* importante.

Server-ul are în componență subansamble redundante pentru asigurarea toleranței la defectare şi disponibilității permanente în funcționare. Funcțiile pe care un server trebuie să le ofere:
- servicii în rețea: dns, ftp, nfs, telnet, mail, etc.
- găzduirea de resurse comune pentru mai mulți utilizatori,
- asigurarea serviciilor către utilizatori pentru o perioadă de timp cât mai îndelungată.

Administrarea sistemului de operare instalat pe *server* presupune:
- monitorizarea funcționării şi menținerea în stare de funcționare,
- asigurarea, menținerea şi controlul securității server-ului,
- colaborarea în vederea remedierii nefuncționalităților echipamentelor cu firma care asigură service-ul în limitele contractuale şi rezolvarea diverselor disfuncționalități apărute în exploatarea curentă,
- gestionarea sistemului de operare, a bazelor de date şi a aplicațiilor (verificări software şi hardware, stabilirea unui plan de backup şi restore, gestionarea spațiului pe disc etc.),
- gestiunea versiunilor sistemului de operare, a bazelor de date şi a aplicațiilor care rulează pe server etc.

Stațiile de lucru (clienții) necesită în general un set de activități de administrare similare celor ale *server*-elor, şi anume:
- monitorizarea funcționării şi menținerea în stare de funcționare,
- colaborarea în vederea remedierii nefuncționalităților echipamentelor cu firma care asigură service-ul în limitele contractuale şi rezolvarea diverselor disfuncționalități apărute în exploatarea curentă,
- gestionarea sistemului de operare şi a aplicațiilor instalate (verificări software şi hardware, politica de backup şi restore, gestiunea spațiului pe disc, antiviruşi etc.) etc.

Pentru asigurarea unei corecte gestionări a sistemelor, se recomandă păstrarea unui jurnal (*log file*) în care să se noteze toate elementele semnificative atunci când se face o modificare în rețea (de natură *hardware* sau *software*, cum ar fi: schimbări de adrese, adăugări de noi calculatoare, reconfigurarea BIOS-ului, actualizarea şi/sau instalarea de programe, etc.).

Pentru protecția datelor se recomanda urmărirea unei politici de *backup*. Periodic, este indicat să se salveze datele pe *server* şi/sau pe alte calculatoare. În cazul extrem când sistemul de operare a fost grav afectat, se poate face re-instalarea de pe CD-urile de *backup* (urmată de reluarea procedurilor de personalizare, moment în care un jurnal care conține setările corecte este de mare folos).

5. Noțiuni de bază pentru utilizarea echipamentelor

După ce au fost puse în funcțiune, calculatoarele au fost sigilate. Accesul în interiorul carcasei se face doar prin distrugerea acestui sigiliu şi este permisă doar personalului care efectuează *service*, care va re-sigila echipamentul după intervenție.

Pentru perioade mai îndelungate de nefuncționare (de exemplu în timpul vacanțelor) calculatoarele vor fi oprite şi deconectate de la alimentarea cu curent electric. Acest lucru este valabil şi pentru celelalte echipamente: *server*, *hub*, *router*, *modem*, *imprimantă*, *scanner* etc.