Rețele de calculatoare pentru gestiunea afacerilor

Introducere

Cartea de față se adresează studenților doctoranzi din domeniul Administrarea afacerilor și se dorește a fi o sumară, dar nu superficială, trecere în revistă a fundamentelor rețelelor de calculatoare, atât de răspândite în prezent, atât în spațiul public cât și privat. Formele în care întâlnim rețelele de calculatoare ne pot bulversa, ni se solicită parole și nu știm pentru ce, ceea ce putem face ușor din rețeaua cablată a companiei nu putem face din rețeaua wireless a aceleași companii. Cu laptop-ul nostru putem accesa, de acasă, rețeaua companiei sau instituției unde lucrăm, dar din aeroport sau de la Mall nu, deși nu am făcut nicio modificare la calculator.

Încercăm să deslușim, în paginile ce urmează, tainele rețelelor de calculatoare, într-un limbaj accesibil oricui nu are studii superioare de specialitate. Cu puțină imaginație, oricine a parcurs acest material, ar trebui să găsească răspunsul la problemele enunțate mai sus. și totuși….e nevoie de câteva minime cunoștințe care, în prezent, sunt furnizate de majoritatea programelor de studii din învățământul superior: Informatică, Bazele tehnologiei informației sau orice disciplină echivalentă. Aceste cunoștințe sunt necesare pentru că noțiuni ca bit, octet, bandă, sistem de operare, proces și altele, sunt folosite fără a mai fi explicate (nici nu ar fi posibil în cadrul acestui material). De asemenea, cunoștințe elementare de algebră booleană sunt necesare pentru a înțelege clasificarea rețelelor și interconectarea lor iar, în felul acesta, să înțelegem de ce nu este posibil să avem o rețea imensă de calculatoare ci se preferă interconectarea mai multor rețele de dimensiuni mai mici.

Deoarece Web-ul este serviciul cel mai utilizat în rețelele de calculatoare, ultimele două capitole realizează o trecere în revistă principalelor concepte ale limbajului HTML și respectiv ale limbajului CSS.

Parcurgerea prezentului material ar trebui să asigure unui manager, fie el al unei instituții publice sau al unei companii private, cunoștințele fundamentale care să îi permită să comunice eficient cu personalul compartimentului IT din subordine și, de ce nu, să conceapă și implementeze o strategie de dezvoltare bazată pe rețele de calculatoare.

Autorul

1 Rețele de calculatoare

Odată cu dezvoltarea industriei de calculatoare personale și introducerea lor pe scara largă în tot mai multe firme, instituții de învățământ și ale administrațiilor, necesitatea schimbului de fișiere între calculatoarele aceleași firme sau instituții a apărut tot mai evidentă. Tot o necesitate a devenit utilizarea în comun a resurselor hardware și software ale organizației – imprimante, modemuri, medii de stocare, aplicații software – de către mai mulți utilizatori. Copierea și plimbarea fișierelor pe CD-uri sau stick-uri de memorie între calculatoare, chiar în interiorul aceleași încăperi nu este o soluție, pentru că este greoaie și consumatoare de timp, iar instalarea de imprimante și/sau modemuri la toate calculatoarele este costisitoare. Soluția o constituie legarea tuturor calculatoarelor într-o rețea. Prin intermediul rețelei este posibil un schimb rapid și sigur de informații (fișiere, mesaje) între diverșii utilizatori precum și utilizarea rațională a periferiei. Mai mult, prin intermediul rețelei este posibilă realizarea de teleconferințe, inclusiv video, cu o parte sau cu toți membrii rețelei. Putem defini rețeaua ca *un sistem de două sau mai multe calculatoare, conectate între ele și capabil să transfere date între acestea*.

1.1 Clasificarea rețelelor de calculatoare

Rețelele de calculatoare pot fi clasificate după mai multe criterii.

1.1.1 După aria de cuprindere

Din punct de vedere al vecinătății în care se află calculatoarele, rețelele sunt:

- rețele locale (LAN - Local Area Network)
- rețele de campus (CAN – Campus Area Network)
- rețele metropolitane (MAN – Metropolitan Area Network)
- rețele extinse (WAN – Wide Area Network)

Inițial clasificarea împărțea rețelele de calculatoare doar în LAN și WAN, ulterior adăugându-se acestora și celelalte tipuri. Rețelele locale sunt cele în care calculatoarele se află relativ aproape unul de altul, în aceeași încăpere sau clădire. Unii autori clasifică rețelele LAN în două subtipuri, rețele personale PAN (Personal Area Network) și casnice, HAN (Home Area Network). Rețelele personale interconectează echipamente sau dispozitive de uz personal, la distanță de câțiva metri: telefon mobil cu laptop, telefon mobil cu dispozitiv hands-free. Rețelele casnice interconectează echipamentele dintr-o locuință. De cele mai multe ori rețelele PAN și HAN sunt rețele fără fir (wireless).

În rețelele CAN, calculatoarele sunt dispuse într-o arie limitată, cum ar fi un campus sau o bază militară. Rețelele metropolitane acoperă o arie mult mai mare decât rețelele de campus, interconectând rețelele locale din clădiri îndepărtate ale unei metropole. Rețelele extinse acoperă teritorii mari, la nivel de țări sau continente.

1.1.2 După topologie

Din punct de vedere a modului de conectare fizică a echipamentelor de rețea (topologie), distingem următoarele topologii:

1. Rețea de tip magistrală

La acest tip de rețea toate calculatoarele sunt legate la cablul principal al rețelei, așa cum se arată în Figura 1. În felul acesta toate calculatoarele au acces egal la magistrală, care nu poate fi ocupată decât dacă este liberă la momentul când un calculator inițiază o transmisie. Pentru obținerea accesului la magistrală este nevoie de un mecanism de arbitrare, care poate fi centralizat sau distribuit. Atunci când un calculator transmite date către un alt calculator, el ocupă magistrala în totalitate, altă comunicație ne mai putând fi posibilă până le eliberarea magistralei. În felul acesta viteza reală de comunicare scade cu creșterea numărului de calculatoare conectate (în limbaj de specialitate se spune că lățimea de bandă - capacitatea de transport a datelor - este partajată între calculatoare)

Pentru optimizarea funcționării rețelelor de tip bus, cablul magistrală este închis pe capete cu niște dispozitive speciale numite *terminale*.

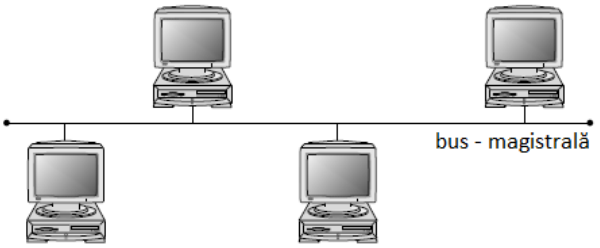


Figura 1 Rețea de tip magistrală

Deoarece funcționarea rețelei este dependentă de traficul de pe magistrală, întreruperea cablului magistrală în orice punct duce la scoaterea din funcție a rețelei, ceea ce este un dezavantaj. Avantajele rețelei de acest tip sunt legate de cost, care este cel mai redus și de posibilitatea extinderii prin adăugare progresivă de noi stații de lucru. În ultimul timp s-a renunțat la această topologie, locul ei fiind luat de una mai fiabilă, topologia de tip stea.

2. Rețea de tip stea

La acest tip de rețea legătura între calculatoare se face prin intermediul unor concentratoare (HUB-uri sau switch-uri) care au rolul de a distribui semnalele către toate calculatoarele din rețea. În felul acesta se elimină dezavantajul prezent la rețelele magistrală; întreruperea unui cablu afectează doar stația în cauză, restul rețelei continuând să funcționeze,

Figura 2. Extinderea rețelei de tip stea se face relativ ușor, adăugând concentratoare noi, așa cum se poate vedea în **Figura 3.**

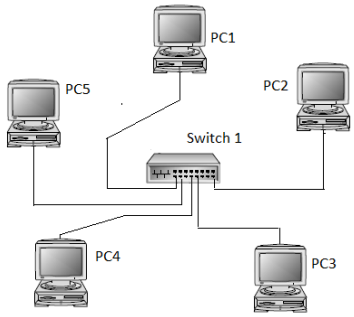


Figura 2 Topologie de rețea stea

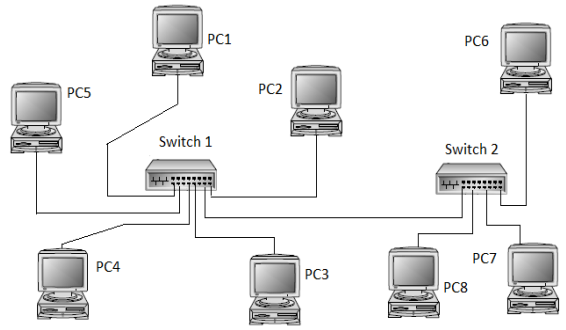


Figura 3 Topologie stea extinsă

Dezavantajul îl reprezintă costul, care pentru rețele cu multe calculatoare, peste 16-20, este mare din cauza costului ridicat al concentratoarelor de mare capacitate.

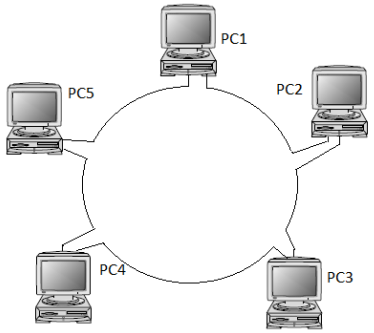


Figura 4 Topologie inel (ring)

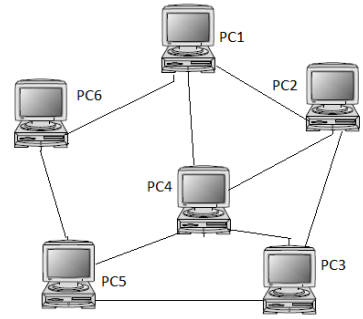


Figura 5 Topologie plasă (mesh)

Pe lângă cele două tipuri, mai există două tipuri de rețea, mai puțin răspândite: rețea în inel (ring) și plasă (mesh), Figura 4, Figura 5. Ambele topologii au ca scop eliminarea dezavantajului creat de întreruperea magistralei la topologia *bus*.

1.1.3 După natura mediului de comunicație

Din acest criteriu distingem a) rețele cablate și b) rețele fără fir (wireless).

La rețele cablate mediul de comunicație îl constituie conductoare electrice din cupru sau conductoare optice – fibra optică. Conductoarele electrice diferă funcție de topologia rețelei. Spre exemplu, în cazul rețelei de tip *bus* cablul este de tip coaxial, asemănător celui folosit la televiziunea prin cablu. Deoarece există o singură pereche de fire disponibilă pentru schimbul de date (firul central și cămașa metalică, Figura 6), comunicația se face în mod semi duplex: un calculator nu poate decât să transmită sau să recepționeze la un moment dat.

La topologiile de tip stea se folosește un cablu cu fire răsucite, în care o pereche de fire este folosită pentru transmitere iar alta pentru recepție. În felul acesta un calculator poate să transmită și să recepționeze în același timp, cu efect benefic asupra vitezei medii de transmitere. Cablurile cu fire răsucite sunt de două tipuri, ecranate (STP – Shielded Twisted Pairs) sau neecranate (UTP – Unshielded Twisted Pairs), ambele având 4 perechi de fire răsucite din care se folosesc doar două, Figura 7.

Cablurile de cupru permit viteze de la 10 Mb/s la 1 Gb/s. Pentru viteze mai mari se folosesc cabluri cu fibră optică.

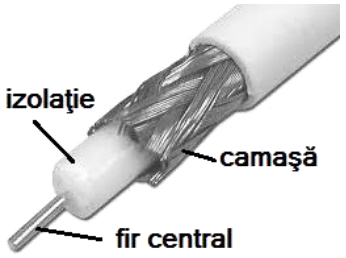


Figura 6 Cablu coaxial

Figura 7 Cablu UTP

În ceea ce privește rețelele fără fir, wireless, acestea sunt de mai multe tipuri, în funcție și de aria de cuprindere. Rețelele de telefonie mobilă (GSM) sunt un exemplu de rețele fără fir de tip WAN, cele din hoteluri sau aeroporturi sunt rețele wireless locale. În continuare ne vom referi doar la rețelele wireless locale, cunoscute și sub numele de Wi-Fi[1], care sunt de două tipuri, cu infrastructură și fără infrastructura sau ad-hoc.

În rețelele cu infrastructură, accesul la rețeaua locală, și prin ea la Internet, este asigurat de un echipament numit Access Point (punct de acces -

[1] Wireless-Fidelity, după termenul High Fidelity folosit în electroacustică

AP) care este conectat prin fire la rețeaua locală cablată. AP creează o zonă de radiație electromagnetică, numită HotSpot, în interiorul căreia orice echipament cu interfață wireless se poate conecta la rețeaua locală, Figura 8. În funcție de modul în care este setat AP-ul, accesul la rețea poate fi deschis (Open) sau securizat. Accesul deschis este folosit în spațiile publice, ca cele amintite mai sus. El este foarte nesigur deoarece permite accesul egal tuturor calculatoarelor aflate în aria de acoperire și astfel, un utilizator rău intenționat, dotat cu un laptop și software adecvat, poate intercepta comunicația dintre oricare alt utilizator și AP. Pentru a putea fi identificat, un HotSpot poartă un nume, SSID[2], care este vizibil tuturor celor aflați în aria de acoperire.

În instituții și companii, accesul la AP se face securizat, cu ajutorul unei parole (passphrase). Pentru a se putea conecta la rețeaua wireless, utilizatorul trebuie să cunoască parola pe care i-o furnizează administratorul rețelei. În felul acesta doar cei autorizați se pot conecta la rețea. Parola este folosită de calculatorul utilizatorului și de către AP pentru a cripta datele schimbate între acestea. Astfel, chiar dacă datele pot fi interceptate de către un terț, ele nu pot fi descifrate.

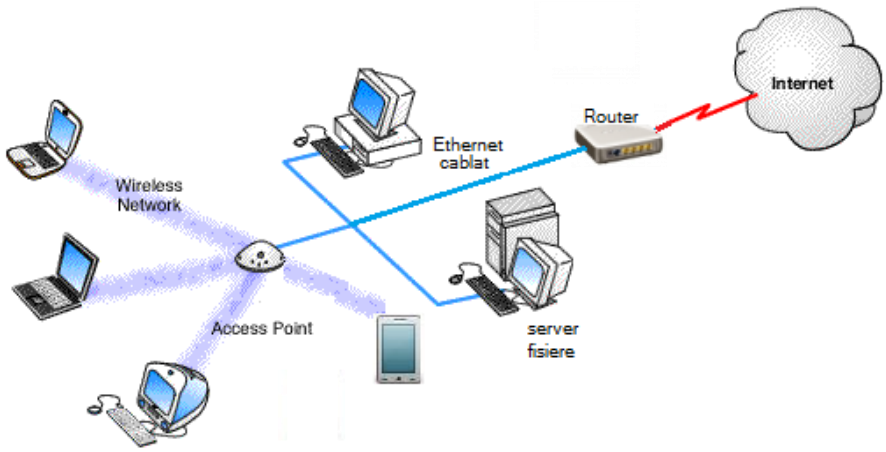


Figura 8 Rețea wireless cu infrastructură

În prezent, cele mai folosite metode de securizare pentru AP-uri sunt WPA și WPA2 (Wi-Fi Protected Access).

Rețelele ad-hoc nu au nevoie de nicio infrastructură, putând fi organizate pe loc între două sau mai multe calculatoare echipate cu interfețe wireless. Pentru a se putea interconecta, toate calculatoarele trebuie setate cu același SSID, iar pentru a asigura protecția comunicației vor trebui securizate cu unul

[2] Service Set Identifier

din protocoalele WPA sau WPA2. Figura 9 ilustrează setarea SSID-ului și alegerea tipului de securitate pe un calculator cu sistem de operare Windows7.

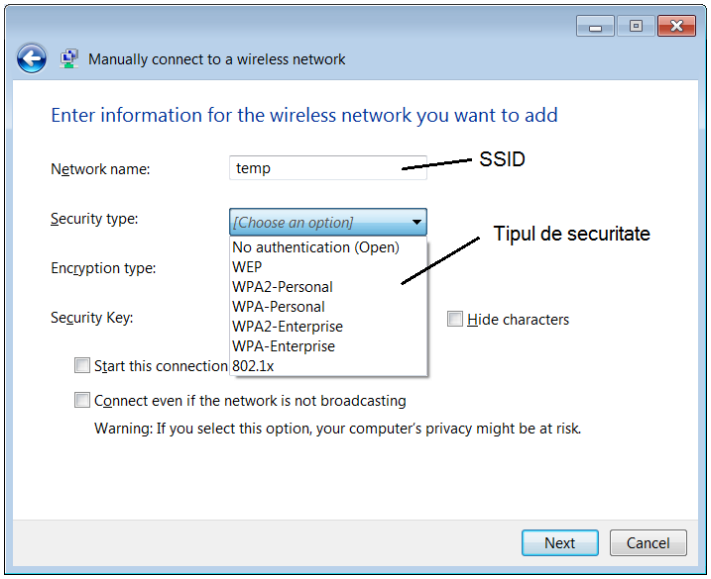


Figura 9 Configurarea unei rețele ad-hoc pe Windows7

1.1.4 După arhitectură

Din punct de vedere al arhitecturii rețelele de tip LAN sunt de două tipuri:

- rețele client/server
- rețele peer- to- peer

În rețelele client/server calculatoarele se împart două categorii, serverele - calculatoare puternice care coordonează folosirea în comun a resurselor și asigură serviciile de bază pentru rețea, și respectiv stațiile de lucru, care sunt clienți pentru servere. Stațiile de lucru sunt calculatoarele pe care lucrează utilizatorii și care, în general, au putere de calcul mult mai redusă decât a serverului.

Într-o rețea de acest tip pot exista unul sau mai multe servere, dintre care unul este responsabil cu autentificarea clienților. Ele sunt configurate pentru a răspunde cât mai rapid cererilor clienților, pentru o stabilitate ridicată și pentru a asigura o bună protecție a datelor în rețea. Deoarece serverele trebuie să poată rezolva cererile simultane ale mai multor clienți sistemul de operare al acestora trebuie să fie unul special destinat acestui scop, cum ar fi Novell NetWare, Windows Server, Unix sau Linux. Cu cât un server este accesat de mai mulți clienți concomitent iar sarcinile sunt mai complexe, cu atât scade viteza cu care stațiile sunt deservite. În Figura 10 este reprodusă structura unei rețele de tip

client /server. De reținut că liniile din desen nu reprezintă conexiuni fizice, ci legături logice; topologia unei rețele cu arhitectură client/server poate fi oricare din cele enumerate anterior.

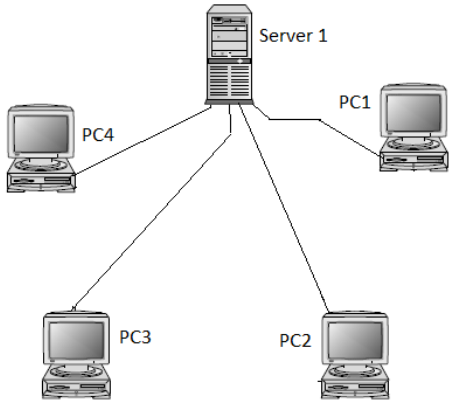


Figura 10 Rețea client/server

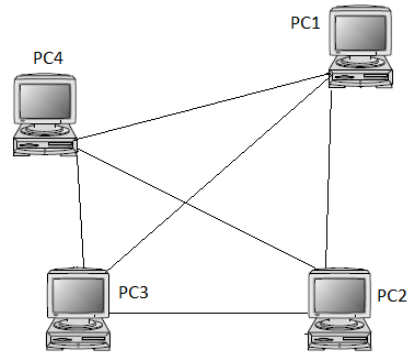


Figura 11 Rețea peer- to- peer

Prin server desemnăm, în funcție de context, atât mașina pe care rulează aplicațiile server cât și aplicațiile server însele. Mașinile au putere de calcul foarte mare, comparativ cu stațiile de lucru, de regulă sunt multiprocesor, au hard discuri de mare capacitate conectate în matrici RAID[3], pentru a asigura redundanța datelor stocate.

Spre deosebire de rețelele client/server, în rețelele *peer- to- peer* stațiile nu accesează un server pentru îndeplinirea unei anumite sarcini, ci toate sunt privite în mod egal. Unitățile de disc ale calculatoarelor sunt folosite în comun, fiecare stație putând pune la dispoziție fișiere, directoare, discuri, imprimante, comportându-se ca server temporar.

Și în cazul acestui tip de rețea, dacă una din stații este solicitată de alte stații din rețea, stații din rețea, viteza de lucru pentru lucrările proprii scade. În

Figura 11 este reprezentată o rețea de tip *peer- to- peer.*

Pentru rețele de tip peer - to - peer nu este nevoie de un sistem de operare dedicat. Sistemele de operare Windows XP, Vista și 7 și 8 au incluse funcționalitățile necesare acestui tip de rețea, ceea ce constituie un avantaj.

[3] Redundant Array of Independent Disks

1.1.5 După logica rețelei (protocolul LAN)

Spre deosebire de clasificarea rețelelor sub aspect topologic, care arată cum se plasează și interconectează calculatoarele în rețea, clasificarea sub aspectul logic are în vedere modul în care se desfășoară comunicația între calculatoare prin intermediul suportului fizic.

Pentru funcționarea rețelei aceasta se bazează pe o stivă de protocoale, care comunică între ele, cu scopul de a asigura transmisia datelor de la o aplicație de pe calculatorul sursă, la mediul de transmisie și invers, de la mediu de transmisie la aplicație, la calculatorul destinație. Protocoalele s-au dezvoltat în strânsă legătură cu sistemele de operare pentru serverele de rețea, astfel că protocolul ales trebuie să fie potrivit (în sensul acceptării) sistemului de operare. Cele mai cunoscute 3 tipuri de protocoale pentru rețea sunt listate mai jos alături de sistemele de operare care folosesc aceste protocoale:

- IPX/SPX[4] Novell NetWare, Windows Server[5]
- NetBEUI Windows Server, OS/2 LAN Server
- TCP/IP UNIX, Windows Server

Protocolul TCP/IP este constituit, de fapt, dintr-o suită de protocoale, care operează la niveluri diferite în stiva de protocoale a modelului OSI: TCP (Transmission Control Protocol) și IP (Internet Protocol) (a se vedea secțiunea 1.2). Deși a fost conceput pentru Internet, protocolul TCP/IP este folosit și în rețele locale. De fapt, orice rețea locală care este conectată la Internet trebuie să utilizeze protocolul TCP/IP. Un LAN care folosește protocoale și servicii specifice Internetului se numește *Intranet*

La nivelul cel mai de jos, cel al legăturii cu mediul de transmisie, cel mai utilizat protocol este Ethernet. Popularitatea lui se datorează costului mic, simplității și vitezei mari de operare.

1.2 Modelul de referință OSI

Diversitatea de implementare concretă a rețelelor este extrem de mare și derivă din necesitățile specifice ale fiecărei firme. Oricare ar fi însă modul de configurare al rețelei, ea trebuie să asigure compatibilitatea între programele de pe fiecare calculator și echipamentele hardware ce fac legătura între calculatoare. *Organizația Internațională pentru Standarde* (ISO) a propus un model, cu valoare de recomandare, cunoscut sub numele de modelul OSI (*Open*

[4] Internetwork Packet Exchange/Sequenced Packet Exchange
[5] Începând cu Windows NT Server și ulterioare, 2000, 2003…2016 Server.

Systems Interconnection - interconectarea sistemelor deschise), Figura 12, care se dorește a fi un cadru pentru proiectarea protocoalelor de rețea.

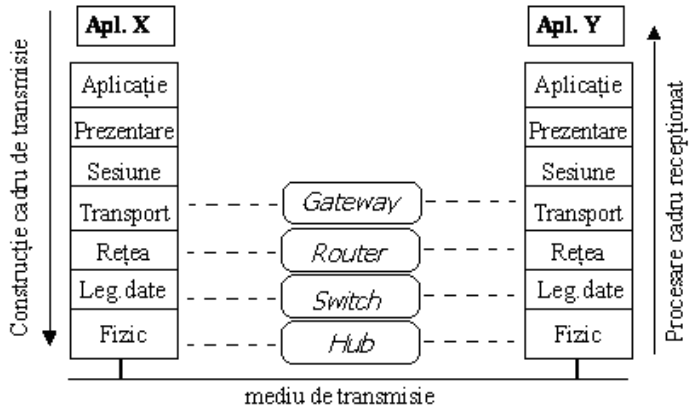


Figura 12 Modelul de referință OSI

După cum se poate vedea modelul este construit pe șapte nivele. Fiecare nivel, până la cel de aplicație, se bazează pe nivelul imediat inferior pentru a realiza o serie de funcții specifice și pentru a „ascunde" detaliile acestor funcții nivelelor superioare. Cele șapte nivele și funcțiile lor sunt sintetizate după cum urmează:

1. nivelul fizic este constituit din cablurile de legătură, echipamentele concentratoare, amplificatoarele și plăcile de interfață cu rețeaua; este partea palpabilă a oricărei rețele. Se ocupă cu transmisia nestructurată de șiruri de biți prin mediul fizic.
2. nivelul de date este cel care răspunde de transferul fiabil de date prin legătura fizică. Asigură sincronizarea, controlul erorilor și fluxului de date care sunt constituite în pachete (cadre).
3. nivelul de rețea este cel care asigură independența nivelelor superioare de tehnologia folosită pentru transmisie. Răspunde de stabilirea, menținerea și terminarea conexiunii.
4. nivelul de transport asigură corectitudinea recepționării informațiilor provenite de la celelalte stații de lucru. Prin canalele de transmisie (cablu sau radio) semnalele pot suferi alterări, pe care nivelul de transmisie trebuie să le corecteze.
5. nivelul de sesiune asigură mecanismul de control al dialogului între aplicații.
6. nivelul de prezentare asigură independența aplicațiilor față de diferențele în reprezentarea datelor (sintaxa)

7. nivelul de aplicație asigură accesul la mediul OSI a proceselor de aplicație.

Nivelele 5-7 sunt, de regulă, implementate în aplicații. Fiecare nivel funcționează cu protocoale specifice, însă unele protocoale de aplicație, cum sunt FTP, SMTP sau HTTP acoperă și nivelele de sesiune și prezentare.

1.3 Tehnologia Ethernet

1.3.1 Fundamente

Termenul Ethernet se referă la o familie de rețele locale reglementate de standardul IEEE 802.3 care definește ceea ce este cunoscut ca protocolul CSMA/CD (Carrier Sense Multiple Access with Collision Detection – Acces Multiplu cu Sesizarea Purtătoarei și Detecția Coliziunilor). Patru viteze de transmitere a datelor sunt până în prezent definite pentru operarea pe fibră optică sau pe cablu cu fire torsadate.

- 10 Mbps -10Base-T Ethernet
- 100 Mbps - Fast Ethernet
- 1000 Mbps - Gigabit Ethernet
- 10 Gigabit Ethernet

Deși au fost propuse tehnologii alternative, Ethernet a supraviețuit ca o tehnologie importantă, fiind utilizată în prezent de circa 85% din rețelele locale de PC uri din lume. Aceasta se datorează următoarelor caracteristici importante ale protocolului:

- este ușor de înțeles, implementat, administrat și întreținut
- permite realizarea rețelelor la un cost redus
- asigură o flexibilitate extinsă pentru instalarea rețelelor
- garantează interconectarea și operarea cu succes a produselor conforme cu standardul, independent de producătorul acestora.

1.3.1.1.1 Ethernet normal, rapid și ultrarapid

Rețelele Ethernet sunt de mai multe tipuri și fiecare tip are o denumire codificată. Iată câteva dintre acestea:

1. **10BASE5—Thick Ethernet or Thicknet** Este versiunea standardizată de către IEEE (Institute of Electronic and Electrical Engineers) a rețelei Ethernet originale, care funcționează cu cablu coaxial.
2. **10BASE2—Thin Ethernet, Thinnet, or Cheapernet** O versiune mai ieftină a tipului 10BASE5, introdusă pentru reducerea costurilor și complexității de cablare. Funcționează tot pe cablu coaxial, dar mai

subțire în diametru, de unde si denumirea *Thin Ethernet*. Este, de asemenea, standardizată de IEEE.[6]

3. **10BASE-T**, este o soluție nouă, complet diferită de cele anterioare, de asemenea standard IEEE, și care folosește ca suport de comunicație două perechi de fire răsucite și neecranate (cablu UTP), asemănătoare cablului telefonic. Pe o pereche se transmite, pe cealaltă se recepționează.
4. **10BASE-F** se referă la trei tipuri diferite de specificații pentru suport de fibră optică:
    - **10BASE-FL** (Fiber Link – legătură de fibră) a fost proiectat pentru a înlocui un standard mai vechi, (Fiber Optic Inter-Repeater Link) și este compatibil cu acesta din urmă. Este cel mai popular standard pe fibră. Când lucrează intercalat cu FOIRL lungimea unui segment este de circa 1000m iar când este utilizat exclusiv lungimea poate ajunge la 2000m [7].
    - **10BASE-FP și 10BASE-FB** sunt învechite și nu se mai utilizează. P înseamnă pasiv iar B înseamnă backbone.
5. **Fast Ethernet 100BASE-T** este asemănător cu 10BASE-T doar că viteză este de 10 ori mai mare. Are trei niveluri de implementare, toate parte a standardului IEEE 802.3u:
    - 100BASE-TX, care utilizează două perechi de fire din cablu UTP de categoria 5 sau din cablu STP de tip 1 și este cel mai popular pentru conexiunile *pe orizontală*;
    - 100BASE-FX, care folosește două fibre optice și este foarte popular pentru conexiunile *pe verticală* sau la backbone;
    - 100BASE-T4, folosește patru perechi de fire din cablu de categoria 3 or superioară. Nu este un standard foarte comun.
6. **Gigabit** sau **1000-Mb Ethernet** este standardizat IEEE (IEEE 802.3z) și cuprinde trei standarde pentru tipurile de suportul fizic: **1000BASE-SX Fiber** (fibră pentru conexiuni pe orizontală) cu varianta **1000BASE-LX Fiber** (fibră pentru conexiuni pe verticală sau la magistrala de campus – *campus backbone*), **1000BASE-CX Copper** (cablaj Copper-Twinax), și **1000BASE-T**.

1.3.2 Cum se decodifică aceste denumiri

Convenția de nume adoptată de IEEE pentru Ethernet este următoarea:

[6] IEEE 802.3

[7] http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/nums12.htm

Primul număr (10, 100, 1000) indică viteza de transmitere în megabiți (Mb) pe secundă.

Al doilea termen indică tipul de transmisie: BASE = banda de bază; BROAD=broadband – bandă largă.

Ultimul termen indică lungimea segmentului: 5 înseamnă 500m

În noile versiuni ale standardului IEEE, cifrele sunt înlocuite de literele. De exemplu, 10BASE-T înseamnă cablu UTP pentru realizarea legăturilor, 10BASE-FL înseamnă fibră optică pentru legături.

1.3.3 Scurt istoric

Standardul Ethernet original a fost dezvoltat ca o rețea experimentală pentru cablu coaxial în 1970 de către compania Xerox, pentru a opera la o viteză de 3 Mbs folosind un protocol cu acces prin detecția purtătoarei și detecția coliziunilor pentru rețele LAN cu cerințe de trafic sporadic dar greu. Succesul lui a făcut ca în 1980 să se elaboreze specificațiile versiunii 1.0 a protocolului Ethernet de 10 Mbs de către un consorțiu format din trei companii: Digital Equipment Corporation, Intel Corporation, și Xerox Corporation.

Standardul original IEEE 802.3 s-a bazat, și a fost foarte asemănător, pe specificațiile Ethernet Versiunea 1.0. Standardul definitiv a fost publicat ca standard definitiv în 1985, de atunci numeroase suplimente ale acestuia fiind elaborate pentru a ține pasul cu dezvoltările tehnologice și a-l face compatibil cu noile medii de rețea cu viteză mare de transmitere.

1.3.4 Elementele rețelelor Ethernet

Rețelele locale Ethernet se compun din nodurile de rețea și mediile de interconectare. Nodurile de rețea se împart în două clase principale:

- Echipamente terminale pentru date (DTE – Data Terminal Equipment), dispozitive care sunt fie sursa fie destinația cadrelor de date. DTE sunt, în mod obișnuit, dispozitive ca PC uri, stații de lucru, servere de fișiere sa de tipărire, care sunt numite, global, stații finale.
- Echipamente de comunicație (DCE – Data Communications Equipment), dispozitive intermediare de rețea care recepționează și trimit mai departe cadre de-a lungul rețelei. DCE sunt fie dispozitive de sine stătătoare cum ar fi repetoare, switch-uri și router-e, fie interfețe de comunicație cum ar fi adaptoare de rețea sau modem-uri.

În continuare echipamentele de comunicație de sine stătătoare sunt numite fie noduri intermediare fie DCE. Interfețele de rețea vor fi numite NIC (Network Interface Card).

Ca medii de transmitere se folosesc în mod curent două tipuri de cabluri cu fire de cupru, UTP și STP și câteva tipuri de cabluri de fibră optică.

1.3.5 Topologii și structuri de rețele Ethernet

Rețelele LAN suportă multe configurații, dar indiferent de mărime și complexitate toate sunt o combinație a trei structuri de interconectare de bază sau blocuri constructive de rețea.

Cea mai simplă structură este interconectarea punct la punct, reprezentată în Figura 13. Numai două noduri de rețea sunt implicate iar conexiunea poate fi DTE la DTE, DTE la DCE sau DCE la DCE. Conexiunea prin cablu punct la punct mai este cunoscută sub numele de legătură de rețea. Lungimea maximă admisă a legăturii depinde de tipul cablului sau metode de transmisie folosită.

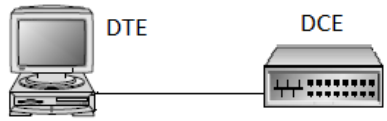


Figura 13 Conexiune punct la punct

Rețelele originale Ethernet au fost implementate cu structură magistrală din cablu coaxial, așa cum este arătat în Figura 14.

Lungimea segmentului era limitată la 500m, la acesta putând fi conectate până la 100 de stații. Segmentele individuale pot fi conectate prin intermediul repetoarelor, cu condiția ca între oricare stații ale rețelei să nu existe mai multe căi.

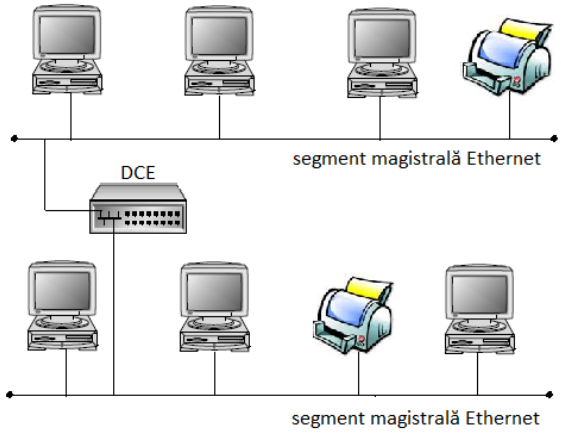


Figura 14 Interconectarea segmentelor de rețea

Deși noile rețele LAN au abandonat tehnologia magistrală, mai există în exploatare rețele mai vechi care funcționează pe această topologie. Începând cu

anul 1990 opțiunea s-a îndreptat spre topologia stea, a cărei configurație este reprodusă în Figura 15.

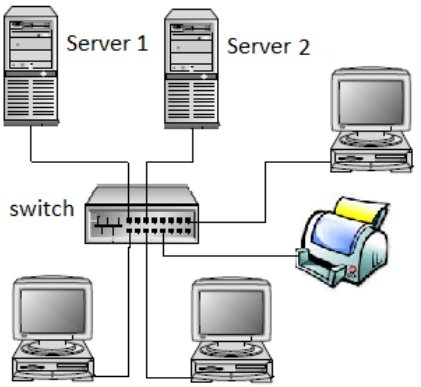


Figura 15 Rețea Ethernet, client-server, cu topologie stea

Piesa centrală a rețelei de tip stea este concentratorul (hub sau repetor multiport) sau switch-ul (comutator). Cablurile UTP, intens folosite în prezent, limitează lungimea segmentului la 100 m, însă topologia stea este suficient de flexibilă pentru a elimina această restricție, prin legarea în cascadă a mai multor switch-uri.

Fiecare legătură a topologiei stea este o legătură punct la punct și realizată fie cu cabluri cu fire torsadate fie cu fibră optică.

1.3.6 Corespondența dintre modelul IEEE 802.3 și modelul OSI

Figura 16 ilustrează nivelele logice ale standardului IEE 802.3 și relația lor modelul de referință OSI. Se observă că nivelul legăturilor de date din modelul OSI este împărțit în două subnivele IEEE 802 și anume: subnivelul MAC (Media Acces Control) și subnivelul MAC-client. Nivelul fizic al modelului IEEE 802.3 corespunde nivelului fizic din modelul OSI. Subnivelul MAC-client poate fi unul din următoarele:

- Control al legăturilor logice (LLC – Logical Link Control), dacă unitatea este una DTE. Acest subnivel asigură interfațarea dintre MAC Ethernet și nivelele superioare din stiva de protocoale a stației finale. Subnivelul este definit de standardele IEEE 802.3
- Puntea (bridge), dacă unitatea este una DCE. Punțile asigură interfațarea între rețelele LAN (LAN to LAN) care utilizează același protocol, de exemplu Ethernet-Ethernet, precum și protocoale diferite, de exemplu Ethernet- Token Ring. Punțile sunt definite de standardele IEEE 802.1.

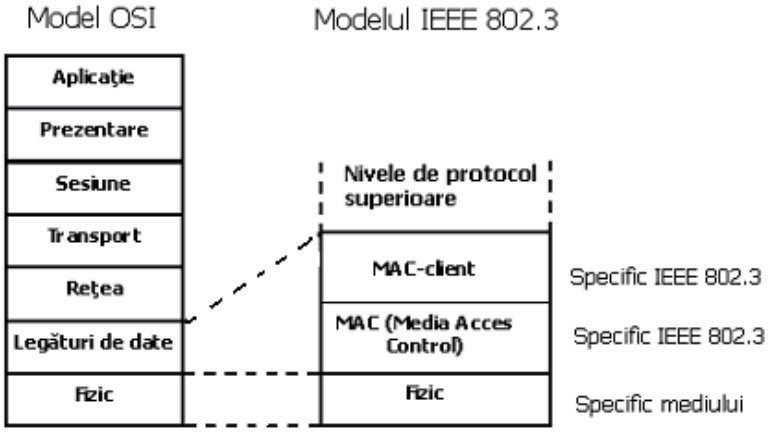


Figura 16 Corespondenta între standardul IEEE 802.3 și modelul de referință OSI

Subnivelul MAC are două funcții principale:

- încapsularea datelor, incluzând asamblarea cadrelor înainte de transmisie și prelucrarea/detecția erorilor pe durata recepției și după recepție.
- controlul accesului la mediul de transmisie, incluzând inițierea transmisiei cadrelor și recuperarea lor în cazul eșuării transmisiei.

1.3.7 Formatul cadrelor Ethernet de bază

Standardul IEEE 802.3 definește un format de bază al cadrului de date, care este cerut de toate implementările MAC, și câteva formate suplimentare opționale care sunt folosite pentru a extinde posibilitățile protocolului de bază. Formatul cadrului de bază conține 7 câmpuri aranjate ca în Figura 17.

1. Preambulul (PRE) – conține 7 octeți. Preambulul este o secvență de biți 1 și 0 care spune stațiilor receptoare că sosește un cadru și asigură o modalitate de sincronizare a porțiunilor cadrului recepționat cu fluxul de biți.
2. Separatorul început de cadru (SOF - Start-of-frame delimiter) conține 1 octet de forma 10101011 care indică începutul cadrului.
3. Adresa de destinație (DA – Destination Address) conține 6 octeți. Ea indică ce stație sau stații trebuie să recepționeze cadrul. O adresă de destinație poate indica fie o adresă individuală (corespunzătoare unei singure stații) sau o adresă „multicast” corespunzătoare unui grup de stații. O adresă având toți biții 1 se referă la toate stațiile din rețeaua LAN, și poartă numele de adresă „broadcast”.

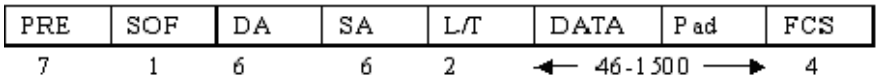


Figura 17 Structura unui cadru Ethernet standard

Fiecare dispozitiv Ethernet fabricat (NIC, hub, switch sau router) conține o adresă unică de 48 de biți – 6 octeți, numită adresă MAC sau adresă fizică. Ea este atribuită de fabricant și primii trei octeți identifică fabricantul iar următorii trei octeți modelul și numărul de ordine al adaptorului. Un exemplu de adresă MAC, exprimată convențional în hexazecimal, este: 00-A0-D2-A4-41-1E. Adresa sursei (SA – Source Address) conține, de asemenea, 6 octeți și indică adresa stației care transmite cadrul Este întotdeauna o adresă individuală.

4. Lungime/tip (L/T – Length/Type) conține 2 octeți. Dacă valoarea acestui câmp este mai mică sau egală cu 1500 atunci câmpul indică numărul de octeți de date conținut de cadru iar dacă este mai mare decât 1536 atunci valoarea câmpului indică un tip opțional de cadru, tipul particular fiind identificat prin chiar valoarea câmpului.
5. Data (DATA) este o secvență de n octeți de orice valoare, unde n este mai mic sau egal cu 1500. Dacă lungimea datelor este mai mică decât 46 atunci câmpul DATA trebuie extins prin adăugarea unui număr de octeți (Pad) pentru a aduce lungimea câmpului la 46 de octeți.
6. Suma de control a cadrului (FCS) conține 4 octeți. Ei conțin o valoare care reprezintă suma de control CRC (cyclic redundancy check) pe 32 de biți a tuturor biților cadrului, mai puțin cei conținuți în câmpurile PRE, SOF și FCS. Înainte de trimiterea unui cadru stația transmițătoare calculează suma de control și o memorează în câmpul FCS. Stația care recepționează cadrul face aceeași operație și compară rezultatul cu valoarea din câmpul FCS. Dacă valoarea calculată diferă de cea din câmpul FCS se consideră că s-a produs o eroare de transmitere și cadrul este abandonat.

Reamintim faptul că această structură de cadru este valabilă numai pentru Ethernet de bază, pentru Gigabit Ethernet el având o structură diferită și o lungime de 416 sau 520 octeți.

1.3.8 Transmisia cadrelor

Când subnivelul LLC al unei stații primește o cerere de transmitere de cadru însoțită de adresă și datele propriu-zise de la nivelul de Rețea, subnivelul LLC începe secvența de transmitere prin transferul datelor de la LLC în buferul de cadru al MAC. Subnivelul LLC face următoarele operații:

- Preambulul și separatorul de început de cadru sunt inserate în câmpurile PRE și SOF

- Adresele destinației și sursei sunt inserate în câmpurile de adrese
- Octeții de date LLC sunt numărați și rezultatul este inclus în câmpul Length/Type
- Octeții de date LLC sunt inserați în câmpul Data. Dacă numărul lor este mai mic decât 46, un șir pad de octeți este inserat până la 46

O valoare de control FCS este generată pe câmpurile DA, SA, Length/Type și Data și este adăugat la sfârșitul câmpului Data.

După ce cadrul este asamblat modul în care el este transmis depinde de modul de operare: semiduplex sau full-duplex. Standardul IEEE 802.3 cere ca subnivelul MAC al Ethernet să suporte modul semiduplex în care MAC poate fie transmite fie recepționa un cadru dar nu poate face ambele operații odată. Modul full-duplex este o funcționalitate opțională care permite MAC să transmită și să recepționeze cadre în același timp.

1.3.8.1 Transmisia semiduplex - Metoda de acces CSMA/DC

Protocolul CSMA/CD a fost inițial dezvoltat ca un mijloc prin care două sau mai multe stații ar putea împărți un mediu de comunicație comun într-un mediu fără comutare în care protocolul nu cere arbitraj central, acces token sau atribuire de interval de timp pentru permisiunea de transmitere. Fiecare MAC Ethernet determină singur când poate trimite un cadru.

Regulile de acces CSMA/CD pot fi rezumate după acronimul protocolului:

- *Carrier sense* – sesizarea purtătoarei: fiecare stație ascultă traficul pe mediul de transmisie pentru a determina când apar decalaje între transmisiile cadrelor.
- *Multiple access* –acces multiplu: stațiile pot începe transmisia oricând dacă detectează că rețeaua este liberă (nu există trafic).
- *Colision detect* – detectarea coliziunilor: când două sau mai multe stații din aceeași rețea CSMA/CD încep transmisia aproximativ în același timp, șirul de biți de la stațiile transmițătoare vor interfera (intră în coliziune) unele cu altele și transmisiile vor deveni neinteligibile. Dacă se întâmplă acest lucru fiecare din stațiile transmițătoare trebuie să fie capabilă să detecteze apariția coliziunii înainte de încheierea transmisiei cadrului propriu. Stațiile vor aștepta un timp qvasi-aleatoriu înainte să încerce reluarea transmiterii cadrului.

1.4 Interconectarea rețelelor de calculatoare

Problema interconectării rețelelor a apărut ca o consecință a dezvoltării companiilor și instituțiilor care dețineau rețele de calculatoare. Necesitatea

folosirii în comun a resurselor informatice de către diferitele sucursale sau agenții ale aceleași companii, aflate în localuri diferite, cu rețele proprii, de multe ori diferite ca topologie și tip, a impus găsirea unor soluții pentru conectarea acestor rețele. Pe de altă parte, creșterea dimensiunii unei rețele, prin creșterea numărului de calculatoare conectate conduce, așa cum am menționat mai sus, la scăderea vitezei de răspuns a rețelei. De aici a apărut necesitatea fragmentării rețelei în rețele mai mici, care să fie ulterior interconectate. În felul acesta viteza în interiorul fiecărei rețele crește, conexiunea dintre rețele fiind folosită numai pentru transmiterea de informații între calculatoarele aflate în rețele diferite. Pentru a face posibilă interconectarea rețelelor este nevoie de un nou sistem de adrese, prin care să poată fi identificată rețeaua și, în cadrul rețelei, calculatorul (host-ul). Adresele rețelelor trebuie să fie unice, ca și adresele host-urilor în cadrul rețelei. În mod clar adresele MAC nu satisfac această cerință. Pe lângă sistemul de adrese este nevoie și de un protocol de comunicație care să știe să utilizeze aceste adrese și să dirijeze corect datele dintr-o rețea in alta. Un astfel de protocol este IPS/SPX (Internetwork Packet Exchange/ Sequenced Packet Exchange) implementat de Novell[8]. Adresele IPX constau într-o adresă de rețea, de lungime fixă de 32 de biți, și adresa de host, de lungime 48 biți, care este identică cu adresa MAC.

Un alt sistem de adresare este adresarea IP, folosită de protocolul TCP/IP (Transmission Control Protocol/Internet Protocol). În prezent funcționează, în paralel, două versiuni de adrese IP, IPv4 și IPv6. Protocolul TCP/IP s-a impus ca standard în Internet, fiind folosit și în rețelele intranet.

Conectarea rețelelor se realizează prin intermediul unor echipamente speciale numite routere și gateway-uri. Router-ele sunt echipamente de dirijare a traficului de date care realizează conexiuni la un nivelul de rețea din modelul OSI. Ele identifică destinația pachetelor de date și le dirijează din rețea în rețea până la destinație. Gateway-urile permit conectarea LAN-urilor care utilizează protocoale complet diferite, la toate nivelurile de comunicație. Funcționează la nivelul de transport în modelul de referință OSI.

1.5 Protocolul TCP/IP

De la inventarea lor, acum trei decenii, eterogenitatea rețelelor a crescut prin dezvoltarea unei palete diverse de tehnologii ca Ethernet, Token Ring, Fiber Distributed Data Interface (FDDI), Integrated Services Digital Network (ISDN) sau Asynchronous Transfer Mode (ATM). Protocoalele Internet s-au

[8] http://www.protocols.com/pbook/novel.htm

dovedit a fi cea mai bună realizare pentru interconectarea acestei varietăți de tehnologii LAN sau / și WAN.

Suita de protocoale Internet nu include numai specificațiile pentru nivelele inferioare (ca TCP și IP) ci și specificații pentru aplicații comune ca poșta electronica (e-mail), emularea terminalelor (telnet) și transferul de fișiere (FTP), vezi Figura 18.

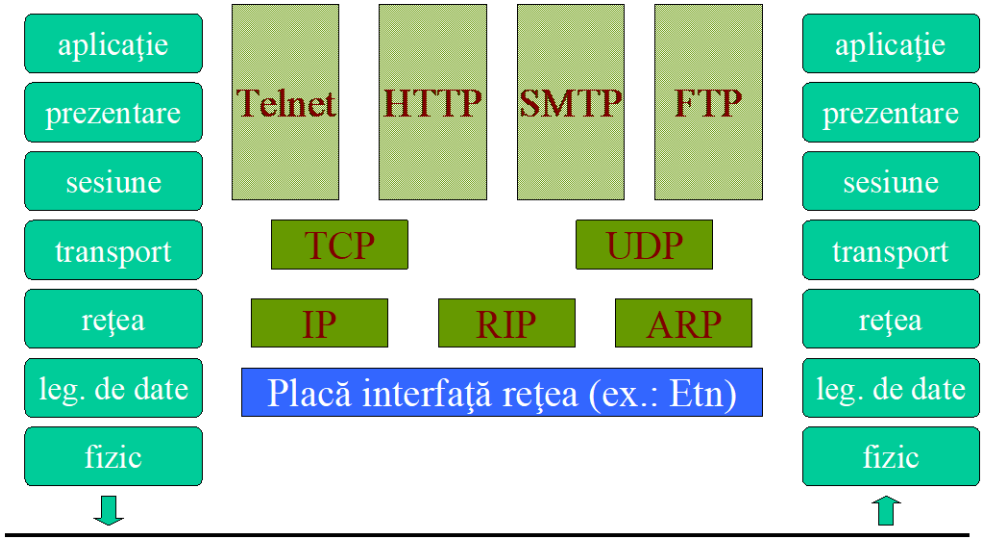


Figura 18 Relația dintre suita protocoalelor Internet și modelul de referință OSI

Protocoalele Internet sunt suita de protocoale cel mai larg implementată în echipamentele de calcul și comunicație ale producătorilor. Orice producător de computere oferă astăzi suport pentru cel puțin o parte din suita protocoalelor Internet

1.5.1 Tehnologia TCP/IP

Această secțiune descrie aspectele tehnice ale protocoalelor TCP, IP și a celor cu care interacționează și a mediilor în care aceste protocoale operează. Deoarece principalul obiectiv al capitolului îl reprezintă rutarea (o funcție a nivelului 3), discuția protocolului TCP (protocol de nivel 4) va fi scurtă.

Suita de protocoale TCP/IP cuprinde o sumă de protocoale pentru prelucrarea datelor în procesul de comunicație:

- TCP (Transmission Control Protocol) comunicația între aplicații
- UDP (User Datagram Protocol) comunicația simplă între aplicații
- IP (Internet Protocol) comunicarea între computere
- ICMP (Internet Control Message Protocol) pentru erori și statistici

- DHCP (Dynamic Host Configuration Protocol) pentru adresare dinamică
- ARP (Address Resolution Protocol)

TCP folosește o conexiune fixă (se spune că este orientat pe conexiune) și folosește pentru comunicarea între aplicații.

Când o aplicație vrea să comunice cu alta prin intermediul protocolului TCP, ea trimite o cerere de comunicație la o adresă precisă. După sincronizarea celor două aplicații, TCP inițiază o comunicație full-duplex între cele două aplicații, care va ocupa linia dintre cele două computere până când una dintre aplicații va închide comunicația.

UDP este asemănător cu TCP dar mai simplu și, în consecință, mai puțin fiabil.

IP este un protocol neorientat pe conexiune și folosește pentru comunicația între computere. Fiind un protocol orientat pe datagrame și nu pe conexiune, el nu solicită pre-existența unei conexiuni înainte de trimiterea datelor. În acest fel IP reduce nevoia de linii de comunicație. IP sparge mesajele (datele, în general) în pachete mai mici, independente, și le trimite către alte computere prin Internet. IP este responsabil de rutarea fiecărui pachet către destinație. Pentru a desăvârși această sarcină fiecare computer care folosește protocolul TCP/IP trebuie să aibă atribuită o adresă IP.

1.5.2 Adrese IP

În prezent există două scheme de adrese IP, una pe 4 octeți (IPv4) și alta pe 16 octeți (IPv6). Cea de a doua, mai puțin răspândită dar aflată în plin proces de generalizare, a fost elaborată pentru a crește numărul de adrese IP disponibile și pentru a îmbunătăți schema pe 4 octeți. În continuare ne vom ocupa de adresele pe 4 octeți care cunosc cea mai mare utilizare în prezent.

O adresă IP este formată din 32 de biți sau 4 octeți. Convențional ea se scrie prin valoarea zecimală a fiecărui octet, cu punct între acestea, de exemplu: 80.96.120.5 sau 172.20.0.1. Cum fiecare octet poate lua valori de la 0 la 255 (în zecimal), rezultă că adresele IP valide pot fi în intervalul 0.0.0.0 și 255.255.255.255, ceea ce corespunde unui număr de 2^{32} adrese, adică circa 4,3 miliarde. În fapt, datorită unor restricții impuse de către IANA (Internet Assigned Numbers Authority – Autoritatea pentru atribuirea numerelor în Internet) doar o parte din aceste adrese sunt publice și/sau valide, numărul real fiind de circa 3,2 miliarde. Aceasta și pentru că anumite intervale de adrese sunt rezervate pentru alte destinații și nu pot fi atribuite în rețeaua Internet iar altele sunt rezervate pentru uzul exclusiv în rețelele locale. Acestea din urmă se numesc adrese *private*, în timp ce restul adreselor valide în rețeaua Internet sunt

adrese *publice*. Adresele private nu sunt rutabile și de aceea pot fi atribuite doar computerelor din rețelele locale. Iată câteva exemple de intervale de adrese private:

10.0.0.0 - 10.255.255.255

127.0.0.0 - 127.255.255.255

172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255

Întreg spațiul adreselor IP este divizat în 5 clase notate cu litere de la A la E, din care doar primele 3 au utilizare publică. Ideea care a stat la baza împărțirii adreselor în clase este că orice adresă IP să fie formată din două părți: prima parte să reprezinte adresa rețelei iar partea a doua să reprezinte adresa host-ului în rețea. S-a convenit ca pentru clasa A primul octet să reprezinte numărul rețelei iar restul de trei octeți să reprezinte adresa host-ului. Primul bit al primului octet trebuie să fie 0.

La clasa B primii doi octeți dau adresa rețelei iar ultimii doi adresa host-ului. Prefixul pentru primul octet din adresa rețelei trebuie să fie 10. În fine, la clasa C primii trei octeți dau adresa rețelei iar ultimul octet furnizează adresa host-ului. Prefixul primului octet al adresei rețelei trebuie să fie 110. O altă convenție este ca nicio adresă, fie ea de rețea sau de host, să nu aibă toți biții cu valoarea 0 sau 1.

Situația este sintetizată, pentru toate clasele, în Tabelul 1

Tabelul 1 Clasele adreselor IPv4

Clasa	**prefix**	**Adresa început**	**Adresă sfârșit**
A	0	1.0.0.1	127.255.255.254
B	10	128.0.0.1	191.255.255.254
C	110	192.0.0.1	223.255.255.254
D	1110	224.0.0.1	239.255.255.254
E	1111	240.0.0.1	255.255.255.254

Clasele D si E sunt clase speciale, care nu au utilizare publică, în sensul că adresele din aceste clase nu sunt alocate clienților și serverelor în mod obișnuit. Adresele din clasa D sunt folosite pentru *multicasting*. Multicast-ul este un mecanism de definire a unui grup de noduri de rețea către care se trimit simultan pachete de date folosind adresarea IP. Multicast-ul este folosit în principal de rețelele de cercetare. Clasa E este o clasă rezervată pentru destinații speciale. Host-urile care folosesc adrese din aceste clase nu vor putea comunica corect. O situație aparte o reprezintă adresa 255.255.255.255 din clasa E

folosită pentru broadcasting în rețelele locale. Un pachet IP cu această adresă va fi recepționat de către toate nodurile rețelei locale dar nu și de alte host-uri din Internet. Din acest motiv procedeul se numește broadcast limitat. și tot din acest motiv nu este permis ca toți biții din adresa rețelei și/sau a host-ului să fie 1. Asupra acestor aspect vom reveni. Să vedem cum se formează numărul rețelei și numărul host-ului. În cazul rețelelor din clasa A, primul octet desemnează rețeaua iar primul bit are valoarea 0. Aceasta înseamnă că cea mai mică adresă posibilă se obține când toți biții sunt 0 iar cea mai mare când toți biții sunt 1, cu excepția primului care rămâne 0, vezi Figura 19.

Bit	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**Valoarea în zecimal**
	0	0	0	0	0	0	0	0	→ 0
	0	.	.	.	.	.	.	.	
	0	1	1	1	1	1	1	1	→127

Figura 19 Determinarea numărului rețelelor din clasa A

Pentru că nu se admit valori 0 și 255 (toți biții 0 sau 1) pentru numărul rețelei și/sau host-ului rezultă că cea mai mică adresă IP validă din clasa A este 1 iar cea mai mare 127. Pentru numărul host-ului rămân ultimii 3 octeți, valorile posibile fiind in intervalul 0.0.0 – 255.255.255. Din motivul arătat adresele valide sunt cu două mai puține, cele corespunzătoare situațiilor în care toți biții sunt 0 sau 1. Rezultă că spațiul adreselor valide este 0.0.1 - 255.255.254, de unde și valorile din Tabelul 1. Concluzia este că în clasa A sunt un număr de 127 de rețele și 16777214 hosturi în fiecare rețea.

Pentru rețelele din clasa B, primii 2 octeți din adresa IP sunt alocați numărului rețelei iar ultimii 2 numărului host-ului. Primii doi biți ai primului octet fiind rezervați pentru prefixul rețelei, rămân 14 biți pentru stabilirea numărului rețelei.

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**		**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**Valoarea zecimală**
1	0	0	0	0	0	0	0	.	0	0	0	0	0	0	0	0	→ 128.0
1	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	
1	0	1	1	1	1	1	1	.	1	1	1	1	1	1	1	1	→191.255

Figura 20 Determinarea spațiului adreselor de rețea pentru clasa B

Numărul total de rețele din această clasă este de 2^{14} = 16384, din care adrese valide sunt cu două mai puțin, adică 16382, iar numărul de host-uri din fiecare rețea este de 2^{16} – 2 = 65534. Figura 20 arată modul de determinare a spațiului adreselor de rețea pentru clasa B. Raționamentul se poate repeta pentru clasa C unde primii 3 octeți sunt rezervați pentru numărul rețelei iar ultimul

pentru numărul host-ului. Se găsește că adresa cea mai mică pentru o rețea din clasa C este 192.255.255 iar cea mai mare 223.255.255, numărul total de adrese de rețea fiind 2097152. Fiecare rețea poate conține 2^8 –2 = 254 de host-uri.

În spațiul adreselor valide sunt rezervate blocuri de adrese care diminuează, așa cum am mai spus, numărul adreselor disponibile pentru public. Astfel, în clasa A, domeniul de la 0.0.0.0 la 0.255.255.255 nu este un domeniu public[9], spațiul 127.0.0.0 la 127.255.255.255 este rezervat pentru *loop back* (un bloc de date trimis cu o adresă din acest spațiu trebuie să se întoarcă la host-ul care a trimis aceste date), spațiul 192.168.0.0 – 192.168.255.255 din clasa C este rezervat pentru rețele locale care nu au acces la Internet. O listă a adreselor rezervate poate fi găsită în [10].

Se obișnuiește ca intervalele de adrese să se scrie și sub forma `adresa_bază/nr_biti` în care `adresă_bază` este cea mai mică adresă din interval iar `nr_biți` indică numărul biților care desemnează adresa rețelei. Spre exemplu spațiul 128.0.0.0/16 indică faptul că primii 16 biți (2 octeți) desemnează rețeaua și nu se modifică în intervalul de adrese, doar ultimii 2 octeți putându-se modifica. Acest spațiu poate fi scris ca interval de la 128.0.0.0 la 128.0.255.255.

1.5.3 Fundamentele rutării IP

Considerăm o mică rețea care folosește protocolul TCP/IP și adaptoare de rețea Ethernet. Rețeaua are doar 3 calculatoare (noduri de rețea) iar adresa rețelei este 194.42.101. Valoarea primului octet ne arată că este vorba de o rețea din clasa C, în care primii trei octeți desemnează numărul rețelei iar ultimul numărul host-ului din rețea. Astfel, cele trei calculatoare din rețea pot primi orice număr între 1 și 254 cu condiția ca acestea să fie diferite. Să admitem că cele 3 calculatoare notate A, B, C au numerele 1, 2 și respectiv 3. În Figura 21, numărul host-ului este evidențiat cu caractere aldine în interiorul adresei IP .

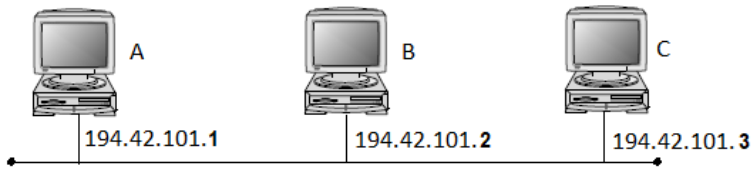


Figura 21 O rețea din 3 calculatoare

[9] http://www.iana.org/assignments/ipv4-address-space
[10] http://www.rfc-editor.org/rfc/rfc3330.txt

Fiecare nod are o adresă Ethernet (adresa MAC a adaptorului de rețea din fiecare calculator), adresă care este unică și este exprimată în formă hexazecimală printr-un număr de 6 octeți separați prin cratimă (ex. 00-10-DC-14-7C-5A). Adresa FF-FF-FF-FF-FF-FF este o adresă rezervată, folosită pentru broadcasting, așa cum se va vedea imediat. Ne punem următoarea întrebare: să presupunem că nodul A vrea să trimită un pachet de date nodului C pentru prima oară și că el cunoaște adresa IP a nodului C. De unde știe nodul A care este adresa Ethernet a nodului C?

Este posibil să se determine adresa MAC pe baza adresei IP prin utilizarea un mecanism cunoscut sub numele de „Protocol de Rezoluție a Adreselor" (ARP – Address Resolution Protocol) care permite descoperirea dinamică a adreselor Ethernet[11]. Protocolul ARP trimite un cadru de date special, de interogare, pe adresa MAC: FF-FF-FF-FF-FF-FF care va fi recepționat de toate nodurile din rețea - broadcast în rețea. În exemplul considerat, cadrul este recepționat de nodurile B și C. Un cadru de interogare arată cam așa:

Adresă IP sursă:	Adresă Ethernet sursă:
194.42.101.1	00-10-DC-49-8A-20
Adresă IP țintă:	Adresă Ethernet țintă:
194.42.101.2	FF-FF-FF-FF-FF-FF
Adresă IP țintă:	Adresă Ethernet țintă:
194.42.101.3	FF-FF-FF-FF-FF-FF

Fiecare calculator care recepționează cererea de interogare o analizează și răspunde cu un mesaj de forma:

Răspuns nodul B

Adresă IP sursă: 194.42.101.2
Adresă Ethernet sursă: 00-27-AE-49-FF-A4
Adresă IP țintă:194.42.101.1
00-10-DC-49-8A-20

Răspuns nodul C

Adresă IP sursă: 194.42.101.3
Adresă Ethernet sursă: 00-16-7E-3C-FB-44
Adresă IP țintă:194.42.101.1
00-10-DC-49-8A-20

[11] ftp://ftp.rfc-editor.org/in-notes/rfc1180.txt

Răspunsurile nodurilor B și C sunt recepționate de nodul A care completează, în memoria cahche, o tabelă de corespondențe între adresele IP și adresele MAC ale calculatoarelor din rețea, de genul:

Adresă IP:	Adresă Ethernet:
194.42.101.1	00-10-DC-49-8A-20
194.42.101.2	00-27-AE-49-FF-A4
194.42.101.3	00-16-7E-3C-FB-44

Acest tabel se păstrează un timp limitat in memoria cache și are rolul de a reduce traficul generat de cererile ARP. Înainte de a trimite un cadru de date, interfața caută în tabela din memoria cache și numai dacă nu găsește corespondența efectuează o cerere ARP. Când se adaugă un nou nod în rețea acesta nu are nici o intrare în tabelul de corespondențe a nodului A până când:

a) sistemul de operare a calculatorului pornit spune interfeței de rețea să trimită un pachet de anunțare a prezenței în rețea;

b) apare necesitatea transmiterii unui pachet de date de la A la noul nod. Dacă se inițiază un astfel de transfer, protocolul ARP va completa tabelul cu o nouă linie.

În felul acesta am răspuns și întrebării pe care ne-am pus-o anterior, cum poate determina nodul A adresa MAC a nodului C, către care dorește să trimită un pachet de date.

Mai trebuie să specificăm că nu este posibil să se determine adresa Ethernet din adresa IP pe baza unui algoritm pentru că adresa IP este atribuită de administratorul de rețea, care poate să o modifice în funcție de nevoile rețelei, în timp ce adresa MAC este una ce ține de hardware-ul calculatorului. Un calculator căruia i se înlocuiește adaptorul de rețea Ethernet cu un altul va avea aceeași adresa IP dar o altă adresă MAC. Protocolul ARP este responsabil de reactualizarea conținutului tabelei de corespondențe în această situație. Dacă nu era deja clar până acum, mai facem precizarea că fiecare calculator din rețea dispune de o asemenea tabelă de corespondențe pe baza căreia știe cărui calculator din rețeaua Ethernet să trimită datele atunci când cunoaște adresa IP a calculatorului țintă.

Să vedem acum ce se întâmplă în cazul a două rețele Ethernet diferite interconectate. Elementul de interconectare este un router, care poate fi un echipament de sine stătător sau calculator care are două interfețe, câte una în fiecare din cele două rețele, și rulează un program de rutare. Să considerăm că nodul C este nodul comun celor 2 rețele, așa cum este ilustrat în Figura 22.

Vom presupune că rețeaua a doua este din aceeași clasă și are numărul 194.42.102.

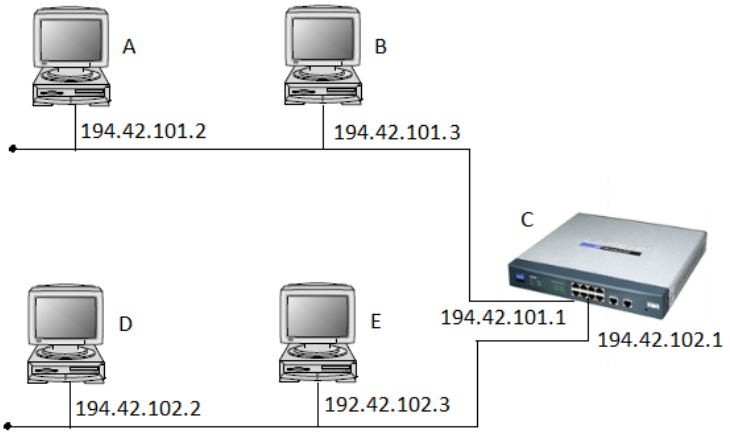


Figura 22 Conectarea a două rețele printr-un router

Router-ul alege calea potrivită pentru pachetele din rețea pe baza adreselor IP de destinație ale pachetelor pe care le primește pe cele două interfețe și pe baza unei tabele de rutare. Dacă nodul A trimite un pachet nodului E, el trebuie mai întâi să îl trimită pe interfața nodului C din rețeaua în care se află A. Pe baza tabelei de rutare, care în acest caz este foarte simplă, router-ul trimite pachetul pe interfața din rețeaua în care se află nodul E. Nodul C determină adresa Ethernet a nodului E folosind protocolul ARP, așa cum s-a arătat mai devreme. Deși nu este o regulă, în practică, interfețelor router-ului li se alocă adresele cele mai mici din clasa respectivă, pentru a nu stânjeni alocarea adreselor pentru celelalte noduri.

1.5.3.1 Rutare directă și indirectă

Rutarea directă a fost evidențiată în primul exemplu, când nodul A comunică cu nodul C, iar în al doilea exemplu e folosită pentru comunicarea între nodurile A și B sau între D și E. Dacă pachetul nu necesită trimiterea mai departe (forwarding), cum ar fi situația în care adresa IP de destinație are același număr de rețea, se folosește rutarea directă. Rutarea indirectă se folosește când *adresele rețelelor sursă și destinație sunt diferite*. Din această cauză pachetul trebuie trimis mai departe de către un nod care știe cum să găsească destinația. În exemplul în care A vrea să trimită un pachet lui E, pentru ca A să știe cum poate pachetul să ajungă la E, nodul A are nevoie de o informație care să îi spună cărui nod să trimită pachetul pentru a ajunge la E. Acest nod se numește *gateway* sau router între cele două rețele. Nodul C trebuie definit ca gateway implicit (default gateway) pentru toate nodurile din cele două rețele. Toate pachetele care sunt destinate unui nod care nu face parte din

rețeaua proprie sunt trimise către gateway-ul implicit. Cum gateway-ul are două interfețe, câte una pentru fiecare rețea, cu adrese IP diferite, nodurile din cele două rețele vor avea setate ca gateway implicit adresa IP a interfeței care face parte din rețeaua respectivă. Astfel nodurile A și B vor avea ca gateway implicit adresa IP 194.42.101.**1** în timp ce nodurile D și E adresa IP 194.42.102.**1**. Tabela de rutare din gateway-ul implicit este setată astfel încât să trimită corect mai departe pachetele.

1.5.3.2 Rutarea statică și dinamică

Rutarea statică se realizează utilizând tabele de rutare preconfigurate care rămân valabile un timp nedefinit, până când sunt modificate manual. Este forma elementară de rutare si presupune ca toate computerele din rețea să aibă adresele IP configurate static. Acest lucru obligă ca fiecare calculator să rămână în rețeaua lui, chiar dacă își schimbă fizic locul. Dacă unul din computere trebuie mutat în cealaltă rețea atunci trebuie reconfigurat cu setul de adrese IP din rețeaua nouă iar tabela de rutare modificată astfel încât să reflecte noua situație.

Rutarea dinamică folosește protocoale speciale de rutare care permit actualizarea automată a tabelelor de rutare cu router-ele știute ca router-e pereche. Aceste protocoale sunt grupate după apartenența lor la protocoale pentru gateway interne (IGPs) sau externe (EGPs). Protocoalele gateway interne se folosesc pentru a distribui informațiile de rutare în interiorul unui sistem autonom (AS). Un AS este un sistem de router-e în interiorul domeniului administrat de o autoritate. Exemple de protocoale gateway interne sunt OSPF[12] și RIP[13]. Protocoalele gateway externe sunt folosite pentru rutarea între sistemele autonome (rutare inter-AS) astfel încât fiecare sistem autonom să știe cum să ajungă la altele prin Internet. Exemple de protocoale gateway externe: EGP și BGP [14]

1.6 Rutarea IP avansată

1.6.1 Masca de subrețea

Când se setează fiecare nod cu adresa de rețea trebuie specificată și masca de subrețea (netmask). Masca de subrețea folosește pentru a specifica care parte din adresa IP este aferentă numărului rețelei și care numărului hostului. Acest lucru se realizează printr-o operație logică și (AND) la nivel de bit, între adresa

[12] ftp://ftp.rfc-editor.org/in-notes/rfc2328.txt
[13] ftp://ftp.rfc-editor.org/in-notes/rfc2328.txt
[14] ftp://ftp.rfc-editor.org/in-notes/rfc1812.txt

IP și masca de rețea. Rezultatul indică numărul rețelei. Rețelele din clasa A au masca 255.0.0.0, cele din clasa B au masca 255.255.0.0 iar cele din clasa C au masca 255.255.255.0. În exemplul în care nodul A trimite un pachet nodului E, nodul A știe că E nu se află în aceeași rețea cu nodul A pentru că aplicând masca adresei IP a nodului A rezultă adresa 194.42.102, care este adresa celeilalte rețele, Figura 23.

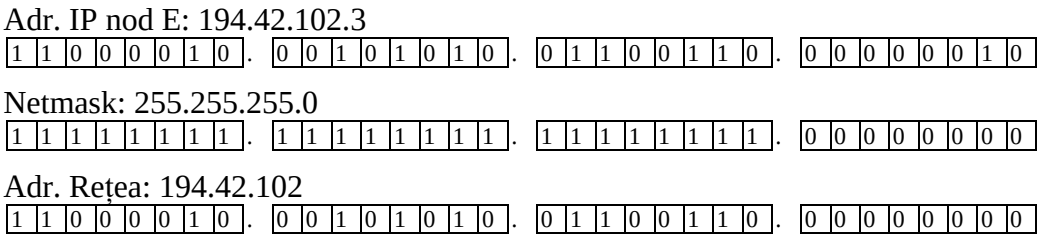


Figura 23 Determinarea adresei de rețea din adresa IP cu ajutorul măștii de rețea

Masca de subrețea devine mai importantă când se utilizează adresarea „fără clasă” (classless). Pentru a vedea cum stau lucrurile în acest caz, să considerăm următoarea situație: un administrator de rețea deține spațiul de adrese de clasă C, de la 194.127.64.1 - 194.126.64.254, ceea ce înseamnă 254 de adrese de host în rețeaua cu numărul 194.127.64/24. El trebuie să creeze, folosind aceste adrese, 3 rețele independente. Aceste rețele care rezultă sunt *pseudo-rețele* și le vom numi în continuare *subrețele*, deoarece ele aparțin aceleași rețele de clasă C. Cum se procedează în asemenea situație? Soluția este modificarea măștii de subrețea, astfel că ea nu va mai avea valoarea uzuală 255.255.255.0 ca la rețelele din clasa C, ci o valoare convenabilă, pe care urmează să o stabilim.

Să ne imaginăm că din cei 8 biți ai adresei hostului am aloca un număr de biți, cei mai semnificativi, pentru numărul subrețelei. Asta înseamnă că ultimii 8 biți nu mai reprezintă o adresă de host, ci o combinație între adresa subrețelei și adresa hostului. Deoarece vrem să facem n=3 subrețele, din ultimul octet vom rezerva pentru adresa de subrețea, cel mai mic număr m biți pentru care $2^m \geq n$. În situația de față m=2 satisface inegalitatea de mai sus deoarece $2^2=4>3$. Rezultă situația ilustrată în Tabelul 2 pentru adresele IP de subrețea.

Tabelul 2 Adresele IP posibile ale subrețelelor

Nr. subre-țelei	Adresa IP subrețea (binar)	Domeniul adreselor IP posibile în subrețea
0	11000010.01111111.01000000.00	194.127.64.1 - 194.127.64.62
1	11000010.01111111.01000000.01	194.127.64.65 - 194.127.64.126
2	11000010.01111111.01000000.10	194.127.64.129 - 194.127.64.1
3	11000010.01111111.01000000.11	194.127.64.193 - 194.127.64.254

Pentru adresa hosturilor din fiecare subrețea rămân 6 biți disponibili, adică fiecare subrețea poate conține maxim 2^6-2 = 62 stații. Masca de subrețea se obține din masca standard pentru clasa C, la care, pe pozițiile rezervate numărului subrețelei se scrie 1. În situația de față, primii doi biți din ultimul octet al măștii de subrețea vor avea valoarea 1, în loc de valoarea standard 0. Prin urmare, masca de subrețea este, pentru toate calculatoarele:

11111111.11111111.11111111.11000000 sau, în zecimal, 255.255.255.192.

Conectarea stațiilor și interconectarea rețelelor se face așa cum este ilustrat în Figura 24.

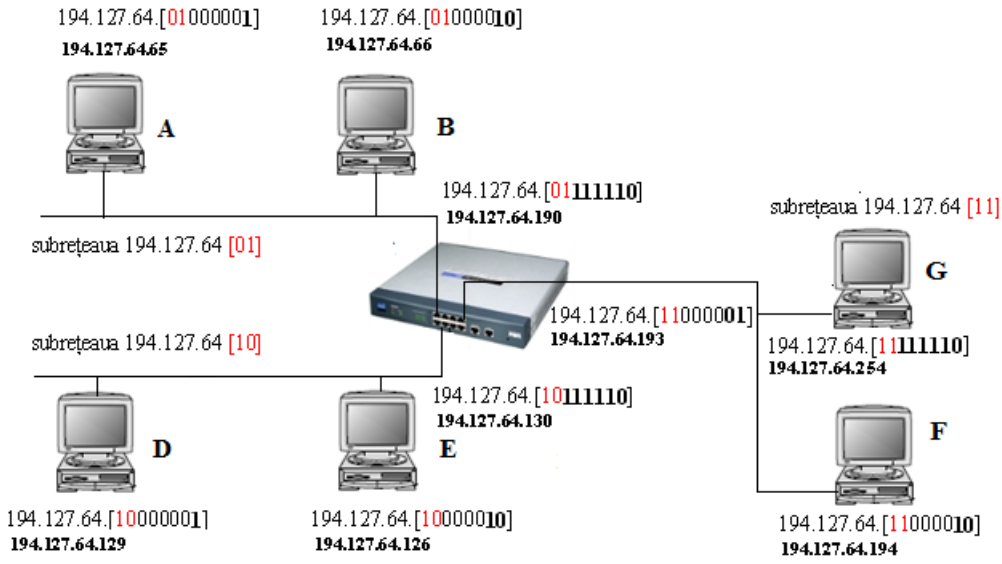


Figura 24 Conectarea subrețelelor

Fiecare nod din această rețea, compusă din 3 subrețele, trebuie să aibă setată o tabelă de rutare care să îi spună ce trebuie să facă cu fiecare pachet de date care au o adresă IP de destinație specificată. Pentru nodurile A, B, D și E tabelele sunt simple, pentru că orice pachet care are altă destinație decât un calculator din subrețeaua proprie va fi trimis gateway-ului implicit. Tabela de rutare este mai complicata pentru C, unde pachetul care vine de pe o interfață poate fi dirijat spre alte două interfețe, funcție de adresa IP a destinației.

1.7 Alocarea adreselor IP

Adresele IP, atât cele pe 4 cât și cele pe 6 octeți, sunt gestionate, la nivel global de IANA (Internet Assigned Numbers Authority). Pentru o mai bună

administrare ea a delegat atribuțiile altor 5 organizații (numite și registraturi Internet), la nivel regional, astfel:

- AfriNIC (African Network Information Centre) – regiunea Africa
- APNIC (Asia Pacific Network Information Centre) – regiunea Asia/Pacific
- ARIN (American Registry for Internet Numbers) – regiunea America de Nord
- LACNIC (Regional Latin-American and Caribbean IP Address Registry) – America Latină și câteva insule din Caraibe
- RIPE NCC (Réseaux IP Européens) – regiunea Europa, Orientul mijlociu și Asia Centrală.

Acestea atribuie blocuri de adrese IP din toate clasele. Utilizatorii mici nu se vor adresa autorității regionale pentru achiziția unui sau mai multor blocuri de adrese. Doar marii distribuitori de servicii Internet, marile companii, organizații guvernamentale pot cumpăra blocuri mari de adrese pe care apoi le revând mai micilor furnizorilor de servicii Internet (ISP – Internet Service Provider), firmelor și instituțiilor statului. Cel mai mic bloc de adrese este cel din clasa C, care conține 254 de adrese pentru o rețea. Dacă necesarul unei firme este mai mic atunci ea poate negocia cu ISP-ul fragmentarea blocului în subrețele „fără clasă", așa cum am arătat în secțiunea precedentă. Trebuie menționat, încă o dată, că utilizarea adreselor publice este obligatorie pentru toate computerele care au acces la Internet. Pentru o rețea izolată, care folosește protocolul TCP/IP, se pot folosi fără restricții adrese private. Există o metodă, pe care o vom arăta-o la momentul potrivit, prin care și aceste calculatoare, cu adrese IP private, pot avea acces la o bună parte din serviciile Internet. În continuare vom vedea cum se atribuie adresele IP într-o rețea locală.

Odată intrată în posesia blocului de adrese firma trebuie să se îngrijească de atribuirea lor calculatoarelor din rețeaua proprie. Sunt două posibilități: atribuirea statică și atribuirea dinamică.

1.7.1 Atribuirea statică a adreselor IP

Atribuirea statică presupune ca administratorul de rețea să seteze, pe fiecare calculator în parte, adresa IP a calculatorului, a măștii de rețea, a gateway-ului implicit și a serverelor DNS. El trebuie să țină evidența riguroasă a tuturor adreselor folosite pentru a nu genera conflicte de adrese în rețea. Dacă rețeaua este izolată (fără acces la Internet și fără conectare cu o altă rețea) atunci sunt suficiente adresele IP ale calculatoarelor și măștile de rețea. Pentru setarea statică a adresei pe un calculator care utilizează Windows XP, procedați astfel:

1. dați clic dreapta pe pictograma My Network Places de pe desktop și selectați *Properties* din meniul contextual. Se va deschide fereastra care conține toate conexiunile pe care le puteți realiza; tipic, dacă aveți o singură placă de rețea, va apare pictograma unei singure conexiuni. Ca regulă, vor apărea atâtea conexiuni câte plăci de rețea aveți pe calculator, Figura 25.

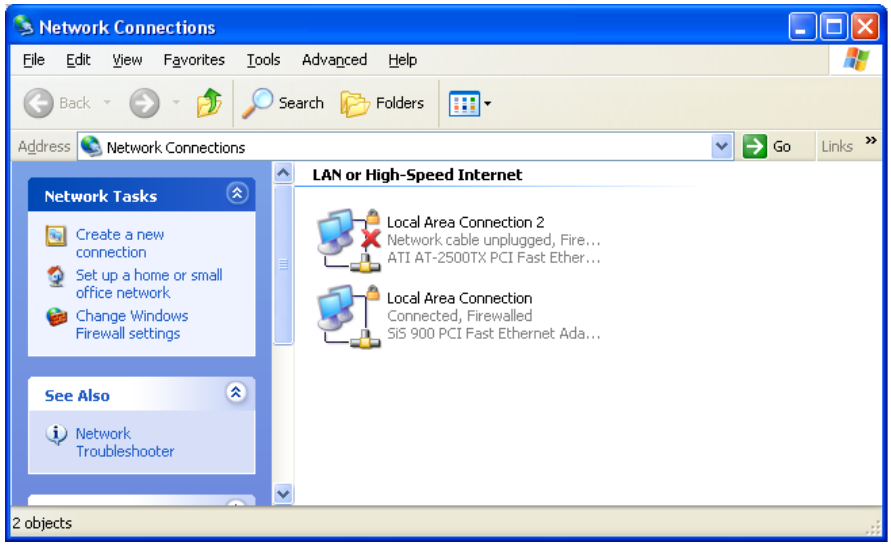
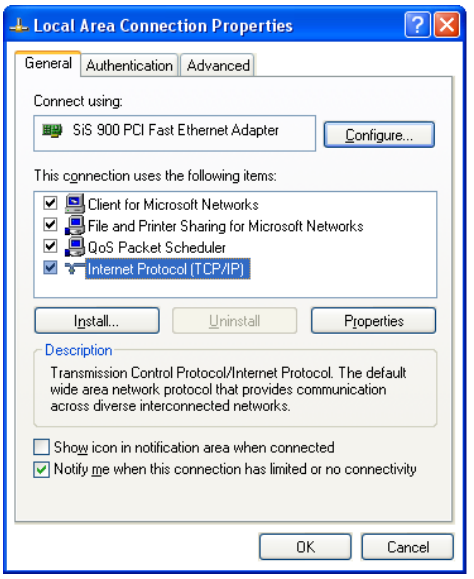


Figura 25 Fereastra Network Connections conține atâtea conexiuni câte plăci de rețea sunt în computer.

2. dați clic dreapta pe conexiunea pe care vreți să o utilizați, dacă aveți mai multe și selectați *Properties*. Asigurați-vă că aveți cablul UTP conectat la respectiva placă și nu la alta. Se va deschide fereastra din Figura 26a din care selectați *Internet protocol (TCP-IP)*. Apăsați butonul *Properties*.
3. în noua fereastră care se deschide, Figura 26b, selectați opțiunea *Use the following IP address*. Completați câmpurile cu datele furnizate de administratorul rețelei sau ISP. În exemplu s-a considerat o adresă dintr-o clasă privată.
4. apăsați butonul OK, succesiv, în ferestrele care au fost deschise pentru a aplica setările și a le închide.
5. verificați aplicarea setărilor deschizând o fereastră de comandă (*Start – Programs – Accessories – Command Prompt*). Tastați comanda *ipconfig /all*, apăsați *Enter* și citiți rezultatul. Acesta trebuie să arate ca în Figura 27 .

a) 

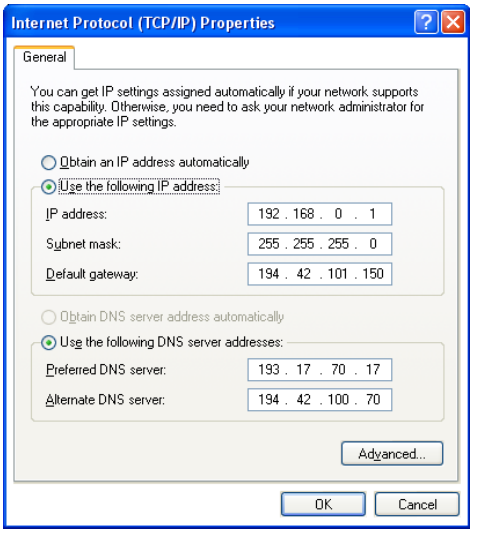
b) 

Figura 26 Fereastra cu a) componentele de rețea instalate b) setarea statică a adreselor IP

Operațiile trebuie repetate pe fiecare calculator din rețea, singurul câmp care diferă fiind cel al adresei IP. Cu aceasta setarea adreselor s-a încheiat.

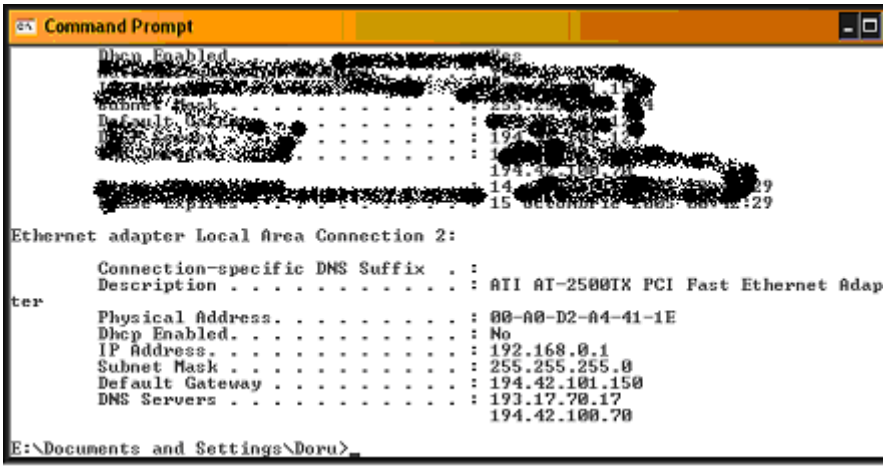


Figura 27 Adresele IP cu care a fost configurată conexiunea

1.7.2 Alocarea dinamică a adreselor IP

La rețelele cu multe computere, peste 50, alocarea statică nu mai e o soluție deoarece administrarea rețelei se îngreunează excesiv. O metodă

eficientă este alocarea dinamică, la pornirea calculatorului, a tuturor adreselor IP de care acesta are nevoie pentru a funcționa în rețea. De această problemă se ocupă protocolul DHCP (Dynamic Host Configuration Protocol) și serverul DHCP. Orice calculator conectat la rețea, când este pornit, lansează o cerere, de tip broadcast, de descoperire DHCP prin care dorește să afle dacă există un server DHCP în respectiva rețea. De regula, serverul DHCP, dacă există, este conectat la aceeași rețea pe care o deservește, dar sunt cazuri când gateway-ul unei rețele poate fi programat să trimită mai departe (forward) cererea de descoperire, dacă serverul DHCP se află în altă rețea. Există două moduri de alocare dinamică a adreselor în care se poate ține sau nu cont de adresele MAC ale adaptoarelor de rețea. În primul caz alocarea se face pe baza unui tabel de corespondență între adresele MAC și adresele IP cu care trebuie setate computerele din rețea. Acest mod se asigură un grad sporit de securitate al rețelei deoarece un computer care nu are adresa MAC a adaptorului de rețea inclusă în tabela de alocare nu va fi configurat cu adresele IP corespunzătoare. Al doilea mod atribuie adresa IP a host-ului și celelalte adrese IP oricărui calculator conectat la rețea, ignorând adresele MAC, în limita spațiului de adrese disponibil. Această metodă este folosită atunci când securitatea rețelei este asigurată prin alte metode sau este mai puțin importantă. Pentru a funcționa alocarea dinamică este necesar ca în rețea să existe un server DHCP. Acesta poate fi un computer distinct, de preferință, dar poate fi și un computer al unui utilizator care rulează aplicația server. În ambele situații serverul DHCP trebuie să fie pornit pe toată durata cât este solicitat accesul la rețea. Pe calculatoarele din rețea nu mai trebuie setată nici o adresă IP, ci este suficient ca ajunși în etapa din Figura 26 b să alegeți opțiunea *Obtain an IP address automatically*.

Dacă adresele pe care le utilizați sunt adrese publice toate calculatoarele vor avea acces la Internet, indiferent dacă adresele au fost setate static sau dinamic.

1.8 Accesul calculatoarelor cu IP privat la Internet

Problema accesului la Internet cu adrese IP private a apărut din mai multe motive. Existau firme care aveau rețea de calculatoare TCP/IP cu adrese IP private și care, la momentul construirii rețelei, nu au avut în vedere necesitatea conectării la Internet. Ulterior, ele și-au modificat optica, luând în calcul posibilitatea de a avea acces la Internet, din interiorul rețelei. Pe de altă parte, epuizarea adreselor IP publice din clasa IPv4 a impus necesitatea găsirii unor soluții care să permită accesul la Internet a calculatoarelor cu adrese IP private. În sfârșit, adresele publice costă, achiziționarea unei adrese publice pentru fiecare calculator din rețeaua firmei este neeconomică. Rezolvarea o constituie serverul NAT (Network Address Translator), care, cel mai adesea, funcționează

împreună cu un router. Un server NAT are alocate un număr *n* de adrese IP publice, prin care comunică în Internet, și un număr *m* de adrese private, către rețeaua companiei, cu *n*<*m*. Astfel, compania nu trebuie să achiziționeze *m* adrese publice, câte una pentru fiecare calculator, ci doar *n* adrese, *n* fiind mai mic decât *m*. Când un calculator din rețeaua privată trimite o cerere în Internet, serverul NAT „caută" o conexiune publică liberă și înaintează cererea pe respectiva conexiune, după care eliberează conexiunea, pentru a putea fi reutilizată de alte calculatoare. Totodată reține adresa IP și portul calculatorului care a trimis cererea și către cine s-a făcut respectiva cerere. Când sosește răspunsul, serverul NAT caută în memorie cine a făcut cererea și trimite răspunsul pe adresa IP privată corespunzătoare. Cu alte cuvinte, adresa privată a fiecărui calculator este translată într-o adresă publică, rutabilă.

Figura 28 prezintă o modalitate de conectare a 4 calculatoare cu adrese IP private, la Internet, folosind un server NAT cu adrese IP publice.

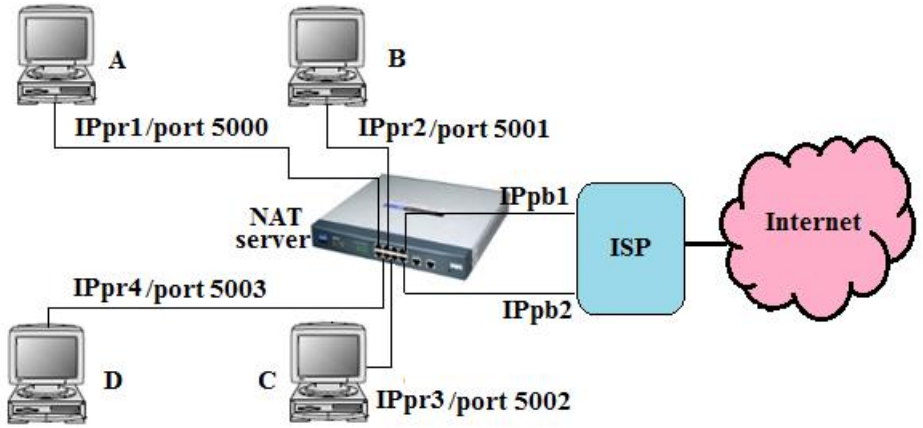


Figura 28 Conectarea la Internet a patru calculatoare cu adrese IP private, printr-un server NAT cu două adrese IP publice

Un caz particular îl reprezintă situația în care numărul conexiunilor publice este *n*=1, adică se utilizează o singură adresă IP publică. Este cazul celor mai multe rețele casnice (HAN) și al firmelor mici, cu câteva zeci de calculatoare. În funcție de numărul de calculatoare din rețeaua privată se determină și banda necesară pe conexiunea publică, care trebuie să fie cu atât mai mare cu cât numărul de calculatoare este mai mare. Pentru o rețea privată cu până la 10 calculatoare, o viteză a conexiunii publice de 100Mb/s este suficientă.

Toate routere-le wireless de uz general includ un server NAT, deoarece ele alocă adrese IP private (de regulă în domeniul 192.168.0.0 - 192.168.255.255), pe care le rutează pe o conexiune IP publică.

1.9 Accesul la infrastructura Internet

Infrastructura rețelei Internet este formată de suportul de comunicații de mare viteză, numit *backbone* (coloana vertebrală a Internetului), constituit din cabluri de fibră optică și canele de comunicație prin satelit. La backbone, proprietate a marilor companii de telecomunicație, sunt conectați marii furnizori de servicii Internet - ISP. Aceștia, la rândul lor conectează alți furnizori mai mici de servicii, care asigură servicii pentru persoane fizice, instituții de stat sau firme private. Dacă până acum câțiva ani utilizatorii casnici se conectau, de regulă, la ISP printr-o legătură telefonică normală și un modem (echipament care asigură adaptarea în vederea comunicării dintre calculatoare și suportul fizic de comunicație) în prezent aceștia sunt conectați în principal prin intermediul cablurilor TV (CATV) sau liniilor telefonice speciale ADSL (Asymetric Digital Subscriber Line). Adaptarea la mediul de comunicație folosit de ISP se face cu niște echipamente dedicate, media-convertoare sau modemuri. Vitezele asigurate de liniile telefonice obișnuite sunt modeste, între 33-56Kb/s, insuficient pentru conținutul actual al site-urilor Web sau pentru transfer de fișiere mari. Conectarea prin CATV sau ADSL asigură viteze mult superioare 20 Mb/s…200Mb/s. În locurile izolate conexiunea poate fi asigurată prin unde radio, wireless, dar stabilitatea conexiunii este afectată de condițiile meteorologice și existenta unei vizibilități directe între antena ISP și antena clientului.

Instituțiile, firmele, campusurile universitare, au calculatoarele conectate într-o rețea locală care, prin intermediul unui router și o conexiune de mare viteză (sute de Mb/s ;și chiar 1 Gb/s) este conectată direct la ISP. În Figura 29 se exemplifică modul în care un utilizator casnic și o rețea locală se conectează la un ISP, iar acesta, la rândul lui, printr-o linie de mare viteză are acces la Internet prin unul din punctele de acces (NAP- Network Access Point).

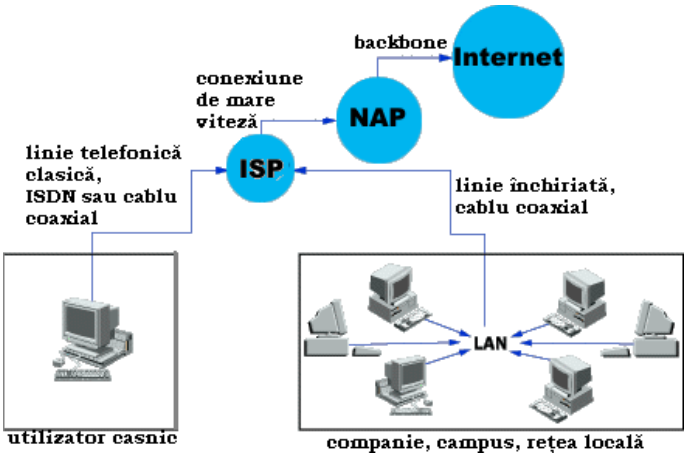


Figura 29 Conectarea utilizatorilor casnici și a rețelelor locale la Internet

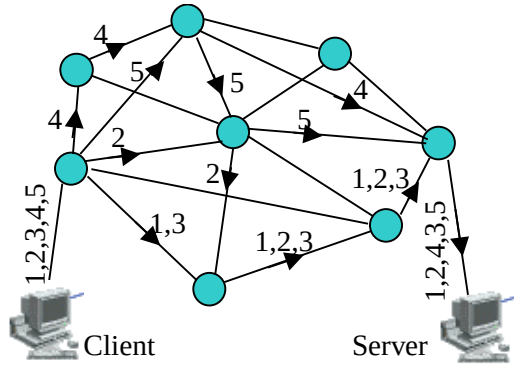
Calculatoarele conectate la Internet pot fi împărțite în două mari clase, servere și clienți. Calculatoarele care pun la dispoziție anumite servicii (WWW, FTP, E-mail) sunt servere iar calculatoarele care se conectează la acestea pentru a folosi respectivele servicii sunt clienți. Un calculator, ca mașină, poate găzdui mai multe aplicații server, el putând fi, în același timp, și server WWW și FTP sau e-mail.

Mai mult, este posibil ca același calculator să fie, în același timp, și server – furnizând un anumit tip de serviciu clienților, de exemplu WWW, dar și client, fiind conectat și beneficiind de serviciile altui server, de exemplu FTP.

Un server are întotdeauna o adresă IP fixă, în timp ce clienții au, de regulă, adrese IP variabile. Aceasta deoarece serviciile oferite de servere trebuie să fie oferite mereu de la aceeași adresă, dar accesarea serviciilor poate fi făcută de la orice adresă.

Este important de știut că, spre deosebire de o legătură telefonică clasică între doi abonați, unde o dată stabilit circuitul el rămâne același până la întreruperea convorbirii, în cazul conexiunilor prin Internet lucrurile stau complet diferit: fiecare pachet de date TCP/IP care circulă prin Internet este dirijat de către router-e, spre destinație, pe calea cea mai fiabilă, care asigură un umăr minim de erori și viteză maximă. Astfel, este posibil ca pachete aparținând aceluiași mesaj să parcurgă căi diferite până la destinație. Pentru utilizatori acest lucru este transparent, ei neștiind pe ce cale a plecat sau a sosit fiecare din pachetele care alcătuiesc informația. De remarcat că la destinație pachetele pot să nu ajungă în ordinea în care au fost transmise sau să nu ajungă toate; este rolul protocolului TCP (nivelul 4 din modelul OSI) să reconstituie

succesiunea inițială a pachetelor și să ceară retransmiterea celor pierdute sau recepționate cu erori.



Desenul din

Figura 30 poate clarifica acest mod de funcționare, numit „cu comutare de pachete”. Considerând că informația a fost descompusă în cinci pachete, numerotate de la 1 la 5, pe fiecare ramură a rețelei formată din nodurile Internet în care se află router-e este trecut numărul pachetului care a tranzitat respectiva cale.

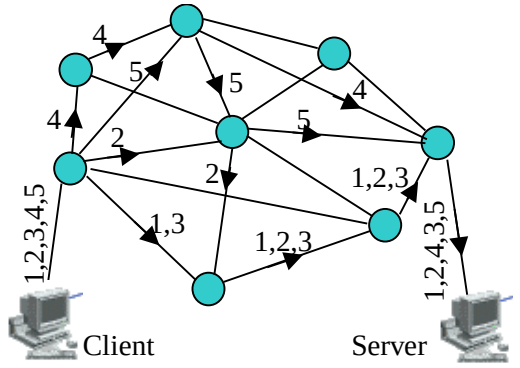


Figura 30 Rutele parcurse de cele cinci pachete care compun informația transferată între client și server

Calculatorul care recepționează pachetele reface informația și o va prelucra în consecință, în raport cu conținutul acesteia; dacă este o cerere de la un client o va trata și va răspunde, dacă este răspunsul unui server informația va fi pusă la dispoziția utilizatorului. Un alt lucru important de știut este acela că pentru a se putea înțelege, atât serverul cât și clientul trebuie să utilizeze același protocol de aplicație pentru a putea comunica. Protocolul de aplicație nu trebuie confundat cu protocolul de transport (TCP/IP), el este specific fiecărui tip de serviciu, FTP pentru transfer de fișiere, SMTP pentru e-mail, HTTP pentru web, etc.

Acesta este, în linii mari, modul în care funcționează Internetul. În realitate lucrurile sunt mult mai complicate, deoarece sistemul este astfel conceput încât scoaterea din serviciu a unei anumite părți a lui să nu afecteze funcționarea întregului. Acesta este, de fapt, și principalul rol al rutării.

1.10 Servicii pentru rețele locale

Utilitatea rețelelor locale este mai bine pusă în valoare prin intermediul unor servicii pe care acestea le oferă. Între acestea, cele mai cunoscute și utilizate sunt:

- Servere de autentificare (Authentication servers)
- Servicii de directoare (Directory services)
- Protocol de configurare automată a host-urilor (Dynamic Host Configuration Protocol (DHCP))
- Sistem de nume de domeniu (Domain Name Systems (DNS))
- Poștă electronică (e-Mail)
- Tipărire (Printing)
- Sistem de fișiere de rețea (Network file system)

Pentru că despre unele servicii am vorbit deja (DNS), iar altele urmează să fie prezentate în capitolul următor (DNS, e-Mail), vom prezenta, pe scurt, esența celorlalte servicii de rețea:

Serverele de autentificare, folosesc pentru autentificarea utilizatorilor sau a altor servere în rețea. Utilizatorii aflați la distanță sau serverele, trebuie să se autentifice la serverele de autentificare pentru a câștiga drepturi în rețea. Dacă autentificarea reușește, utilizatorul primește o cheie criptografică cu care va cripta informațiile transmise în rețea. Autorizarea reprezintă baza pentru 3 funcții indispensabile accesului autorizat la rețea:

- Autorizarea - determinarea drepturilor care pot fi acordate unui utilizator sau server care se autentifică
- Intimitatea (privacy) - păstrarea caracterului confidențial al informațiilor vehiculate, față de ceilalți utilizatori ai rețelei
- Non-repudierea - imposibilitatea negării unei acțiuni întreprinse ca urmare a autorizării în sistem.

Cel mai frecvent mecanism de autentificare este bazat pe parolă, dar mai sunt folosite și Kerberos și criptografia cu chei publice

Serviciile de directoare, asigură pe accesul la informații pe baza unor hărți de resurse. Hărțile pot fi privite ca niște tabele, care pe o coloană conțin nume iar pe alta valori. Serviciul de directoare permite regăsirea valorilor pe baza numelor. Este posibil ca un nume să aibă mai multe valori asociate, așa

cum un anumit cuvânt de dicționar poate avea mai multe înțelesuri. Un utilizator nu trebuie să știe adresele fizice ale resurselor pe care dorește să le folosească ci doar numele lor, pe baza cărora serviciul de directoare va localiza respectivele resurse.

Serviciile de tipărire sunt asigurate de serverele de tipărire, care sunt fie echipamente hardware, fie programe care rulează pe un calculator la care este conectată o imprimantă. Serviciul dă posibilitatea utilizatorilor îndepărtați să tipărească documente la o imprimantă aflată în altă locație, pentru ei sau pentru alții. Serviciile de tipărire gestionează sarcinile de tipărire primite de la utilizatori, pentru a se evita conflictele.

Sistemele de fișiere de rețea permit accesul diverșilor utilizatori de pe computere diferite, la fișiere stocate pe mai multe calculatoare din rețea. Accesul nu se face direct, la nivel fizic, ca în cazul rețelelor peer-to-peer, ci prin intermediul rețelei, pe baza unui protocol. În acest fel este posibil să se restricționeze accesul pentru unii utilizatori, pe baza unei liste de control al accesului (ACL).

2 Servicii Internet

Rețeaua Internet a oferit, în etapele sale de început, trei servicii: FTP – File Transfer Protocol, Telnet – conectare la distanță și e-mail. Ulterior s-au adăugat și alte servicii, Usenet, IRC, Gopher și, cel care a contribuit decisiv la „explozia” lui, serviciul WWW.

Serviciul FTP permite transferul de fișiere între calculatoarele utilizatorilor îndepărtați și servere dedicate (servere FTP). În funcție de permisiunile utilizatorilor, transferul poate fi unidirecțional, numai de la server la client, sau bidirecțional. De asemenea accesul poate fi deschis, pentru oricine (modul anonim), caz în care, de regulă, transferul este unidirecțional, sau autentificat, cu parolă, pentru clienții serverului, situație în care transferul este, tot de regulă, bidirecțional. Administratorul poate modifica permisiunile oricărui utilizator, acordându-i drepturi mai restrânse sau mai extinse. Serviciul este foarte util pentru lucrul la distanță, când utilizatorul poate stoca pe server ultimele versiuni ale documentelor sau programelor sale. Este intens folosit pentru actualizarea conținutului paginilor Web.

Serviciul Telnet, tot mai puțin utilizat astăzi, din motive de securitate, permite utilizatorilor unui server să se conecteze de la distanță la server și să lucreze pe el, ca și când ar fi conectați direct, prin rețeaua locală. În prezent se folosesc variante ale Telnet-ului care utilizează protocoale securizate pentru

conectare (Putty, pentru utilizatorii sistemelor de operare Windows, SSH pentru utilizatorii Linux).

Serviciul IRC (Internet Relay Chat) este folosit pentru chat (pălăvrageală), pe Internet. Servere dedicate găzduiesc „camere" de discuție, în care se poate alătura oricine. Utilizatorii trebuie să aibă instalat pe calculatoarele lor un client pentru acest serviciu. Foarte popular a fost clientul mIRC. Discuțiile fiind nemoderate iar caracterul lor „foarte deschis" pot să nu fie agreate de multe persoane. Odată cu îmbunătățirea funcțiilor oferite de aplicațiile de mesagerie instantanee (IM), cum ar fi Skype sau Yahoo Messenger, popularitatea IRC a scăzut.

Serviciul Usenet este unul foarte asemănător cu actualele forumuri de discuții, dar cu o mare și importantă deosebire: forumul nu este găzduit de un server la care se conectează toți utilizatorii care doresc să contribuie, ci dimpotrivă, sistemul este descentralizat. Utilizatorii sunt conectați la servere diferite, care schimbă mesajele între ele.

2.1 Serviciul DNS

Este un serviciu folosit de orice utilizator, al oricărui alt serviciu, în mod transparent, fără ca măcar acesta să conștientizeze acest lucru. Rolul serviciului este de a face conversia adreselor utilizate, sub formă de nume, în adrese IP.

După cum am arătat, calculatoarele conectate la Internet comunică între ele pe baza adreselor IP, care sunt unice. Pentru utilizatorul uman este extrem de greu, dacă nu imposibil, să memoreze un număr mare de adrese IP. Pentru el este mult mai comod să folosească nume prietenoase, care să sugereze spațiul în care este localizată resursa: usv.ro, emag.ro, facebook.com etc. Acestea sunt nume de domenii, care conțin două componente: numele domeniu de top (ro, com, org, edu, info) și numele domeniului propriu-zis (sau de nivel 2). Numele domeniului de top este ultimul, separat prin punct de numele de domeniu propriu-zis. Sunt două mari categorii de nume de domenii de top, generice (com, net, org etc) și regionale (ro, it, us, jp). Prima categorie indică natura serverelor din domeniul respectiv (com=comercial, edu=educational, org=organizație), fără nicio referire la localizarea geografică; a doua categorie indică țara, fără nicio indicație cu privire la natura serverelor (ro=România, jp=Japonia etc.). În cadrul fiecărui domeniu de top se pot înregistra oricâte domenii de nivel 2 (propriu-zise), dar diferite ca denumire. De asemenea, într-un domeniu pot exista subdomenii, care au un nume ce precede și se separă cu punct de numele de domeniu: seap.usv.ro. Se realizează, astfel, o structură ierarhică, precum cea din Figura 31, în vârful căreia se află domeniul rădăcină, care nu are nume.

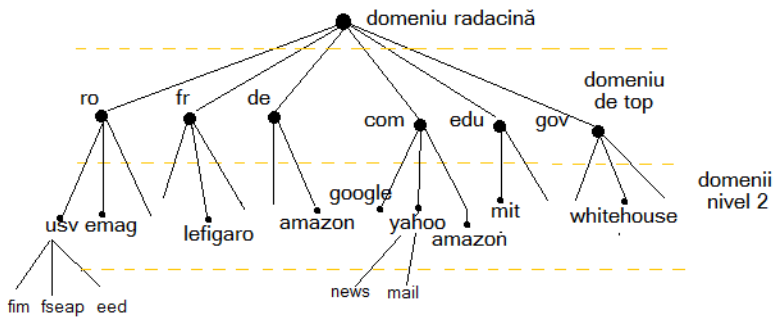


Figura 31 Organizarea ierarhică a domeniilor

Fiecare domeniu este responsabil de toate numele de domeniu subordonate.

Domeniul deține unul sau mai multe servere DNS care păstrează corespondența între adresele IP ale serverelor subordonate și numele lor. Adresele acestor servere DNS sunt configurate în toate host-urile din domeniul respectiv. Să presupunem că un utilizator din subdomeniul *fim* al domeniului *usv.ro* dorește să acceseze serverul web al subdomeniului *seap* din același domeniu *usv.ro*. După ce utilizatorul scrie adresa www.seap.usv.ro și apasă tasta Enter, calculatorul său va lansa o cerere de rezolvare a adresei IP a serverului www.seap.usv.ro către serverul DNS a domeniului *usv*, cu a cărei adresă a fost configurat.

Acesta va căuta în tabela sa de corespondențe și va răspunde clientului cu adresa IP corespunzătoare. Abia în acest moment cererea de afișare a paginii web de pe serverul www.seap.usv.ro va fi trimisă către adresa IP a serverului, respectiv 80.96.120.12.

O altă situație este cea în care în un utilizator din domeniul *yahoo.com* dorește să acceseze serverul www.seap.usv.ro. Calculatorul său va lansa cererea de rezolvare către serverul DNS intern al domeniului yahoo, care nu va găsi corespondența căutată în tabelele sale. Acesta va trimite, mai departe, cererea către serverul DNS autoritativ[15], al domeniului *com*. Nici acesta nu găsește adresa și trimite cererea, mai departe, serverului DNS a domeniului rădăcină, tot autoritativ. Acesta determină că adresa este din domeniul de top *ro* și trimite cererea către serverul DNS a domeniului de top *ro*. Aici nu se găsește corespondența căută, dar se găsește că adresa aparține domeniului *usv* iar

[15] Serverele autoritative păstrează evidența serverelor de pe nivelul inferior, subordonate. Serverele recursive interoghează serverele de pe nivelele superioare pentru a afla adresa IP a serverelor din alte domenii.

cererea este înaintată serverului DNS din domeniul *usv*. Abia aici se determină adresa IP a serverului www.seap.usv.ro care este trimisă la serverul DNS care a fost interogat primul de către client (server intern, recursiv). Acesta trimite răspunsul, sub forma adresei IP clientului care a lansat cererea. Server DNS recursiv, care primește rezolvarea, memorează pentru o perioadă de timp, rezultatul rezolvării. În felul acesta, dacă apare o nouă cerere din același domeniu, nu mai este necesară reinterogarea serverelor DNS pe toată calea descrisă. Pentru a nu încărca inutil memoria serverelor DNS, dacă într-un interval de timp nu apar alte cereri de rezolvare, echivalențele memorate temporar vor fi șterse. Practic, singurele informații permanente sunt cele corespunzătoare serverelor din subordine. Ilustrarea funcționării sistemului este reprodusă în Figura 32.

Important de reținut că și sistemele de operare, și navigatoarele Web memorează adresele IP și numele de domenii în memoria lor *cache*. În felul acesta se elimină interogările DNS pentru adrese care au fost anterior accesate.

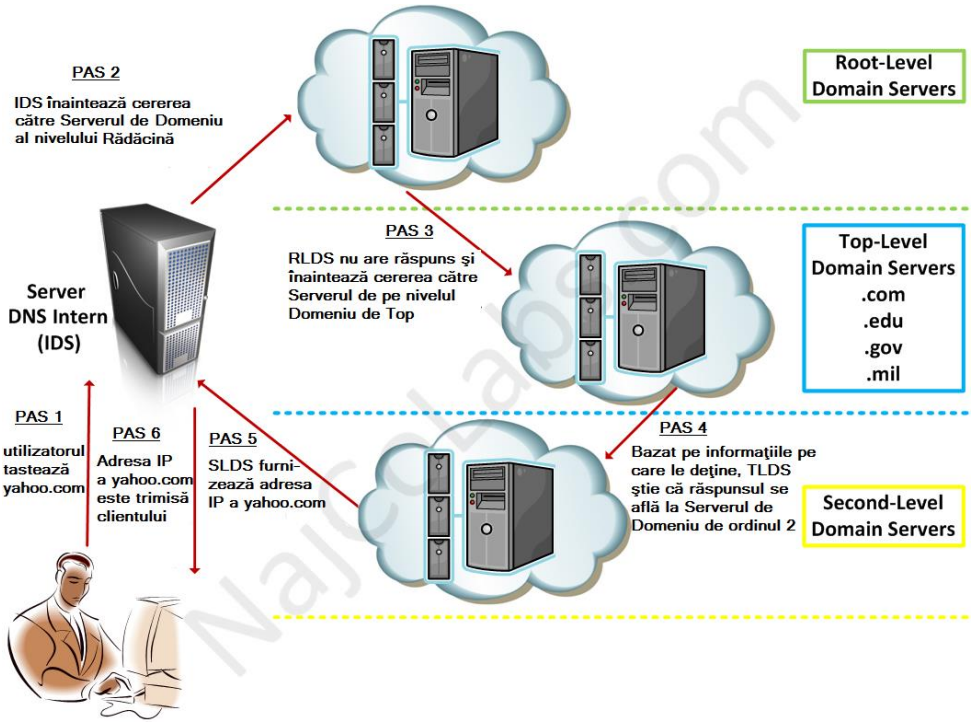


Figura 32 Ilustrarea funcționării sistemului de servere DNS (prelucrare după najcolabs.com**)**

2.2 Serviciul WWW

Dintre toate serviciile pe care Internetul le pune la dispoziție, cel mai folosit este, de departe, serviciul WWW – World Wide Web. În continuare este prezentat, succint, acest serviciu.

2.2.1 Scurtă istorie

Începuturile WWW datează din anul 1989 când la Laboratorul de Cercetări de Fizică Nucleară (CERN) din Geneva s-a cristalizat ideea conceperii unui sistem de transmitere a informațiilor între diferitele echipe, aflate la distanță una de alta, bazat pe Hypertext. Un an mai târziu, în octombrie 1990 proiectul a fost prezentat iar după numai două luni au început să se contureze primele rezultate. Munca a demarat cu elaborarea unui program capabil să interpreteze limbajul Hypertext, numit browser. În anul 1991, după eliminarea mai multor neajunsuri în funcționare, Web-ul a fost pus la punct și a devenit funcționabil. Anul 1992 a fost un an al dezvoltării, browser-ul Web a devenit disponibil prin intermediul FTP iar Web-ul a fost prezentat publicului și organizațiilor cele mai diverse[16].

Dacă în noiembrie 1992 existau 26 servere Web în întreaga lume, în octombrie 1993 numărul lor a depășit 200. Aceasta și datorită faptului că între timp au devenit disponibile alte două browsere, unul al firmei MacIntosh iar altul al firmei Mosaic, acesta din urmă proiectat pentru mediul Windows. În anul 1994 s-au depus eforturi pentru securizarea Web-ului în scopul asigurării confidențialității datelor vehiculate (corespondențe, cărți de credit, acces la resurse protejate, etc.). Pentru dezvoltarea pe mai departe a Webului, în anul 1994 s-a produs fuziunea dintre CERN și MIT (the Massachusetts Institute of Technology) deoarece cerințele în resurse materiale, dar și umane, depășeau posibilitățile laboratorului CERN.

Ce este astăzi Web-ul este lesne de constatat: informații, mesagerie, afaceri, comerț, artă, divertisment sunt numai câteva dintre activitățile ce se derulează sub semnul acestui serviciu.

2.2.2 Protocoale și limbaje în WWW

Funcționarea WWW se bazează, în esență, pe doi piloni: protocolul și limbajul (sau codul).

Protocolul este acel produs software (sau mai simplu program) care asigură tranzacția între clienți și servere. Protocolul pentru Web este HTTP

[16] http://info.cern.ch/

(HyperText Transfer Protocol) care, în desfășurarea unei tranzacții, tratează 4 faze:

- Conectarea
- Cererea
- Răspunsul
- Deconectarea

Serverele care găzduiesc pagini Web se numesc servere Web sau http, iar aplicațiile cu ajutorul cărora ne conectăm la respectivele servere, pentru a vizualiza paginile găzduite se numesc, generic, clienți Web sau *browser*-e Web (pe scurt browser sau navigator).

În faza de conectare, browser-ul încearcă să se conecteze cu serverul. Această stare este identificată prin faptul că pe bara de stare a ferestrei browser-ului apare mesajul „Conecting to…..”. Dacă conectarea nu se poate realiza, după un timp oarecare browser-ul returnează un mesaj de informare asupra acestui fapt. Acest mesaj nu trebuie confundat cu mesajele de eroare returnate de servere ca urmare a unor erori survenite în scrierea corectă a adreselor Web sau inexistenței documentelor solicitate pe serverul accesat.

Dacă conexiunea s-a realizat browser-ul trimite o cerere către server. Această cerere specifică ce tip de protocol este utilizat (implicit este HTTP dar poate fi și FTP, Gopher sau WAIS) și ce obiect (document Web sau alt tip de fișier) se caută.

Presupunând că serverul a recepționat și interpretat corect cererea (în caz contrar se va genera un mesaj de eroare) atunci se trece la a treia fază, răspunsul. În funcție de browser-ul utilizat pe bara de stare apare un mesaj care confirmă citirea răspunsului de la server. Ca și în cazul cererii, răspunsul specifică protocolul folosit dar mai conține o serie de informații care sunt afișate pe bara de stare indicând ce anume se întâmplă în fiecare moment pe perioada transferului, Figura 33.

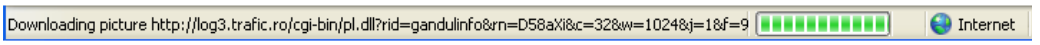


Figura 33 Bara de stare a browser-ului *Internet Explorer 7* la un moment al încărcării unei pagini web

Când transferul s-a încheiat se produce deconectarea de la server.

În funcție de obiectul încărcat, browser-ul va iniția acțiuni diferite, fie va afișa textul dacă obiectul este un simplu fișier ASCII (text), va lansa un viewer pentru fișiere grafice (GIF, JPG) sau va lansa un player pentru fișiere audio / video, fie va salva pe disc obiectul sub formă de fișier.

Limbajul este un limbaj care descrie modul în care informația conținută în documentele Web trebuie afișată. În Internet limbajul standard este HTML (Hyper Text Markup Language, limbaj de marcare a hipertext-ului). Documentele HTML conțin text, imagini, sunet și linkuri (legături) către alte documente. Limbajul HTML având posibilități variate de formatare a documentului valorifică ingeniozitatea celui care îl creează (web master sau web designer), rezultatul fiind documente cu mare impact la utilizator.

2.2.3 Browsere Web

2.2.3.1 Generalități

Browserele Web, sau clienții web, sunt programe destinate serviciului Web al Internetului. Ele rulează pe calculatoarele client din rețea și permit vizualizarea documentelor HTML, citirea poștei electronice prin intermediul interfeței Web sau transferul de fișiere de pe servere FTP. În prezent sunt patru browsere cu mare răspândire pentru PC-uri: Mozilla Firefox (FF) al fundație Mozilla, Chrome al companiei Google, Internet Explorer (IE) al firmei Microsoft, și Opera al firmei Opera Software. Opțiunea pentru unul sau altul ține mai mult de obișnuință deoarece diferențele sunt nesemnificative pentru utilizatorul obișnuit. Datorită implementărilor diferite ale limbajului HTML și limbajelor pentru scripturi (JavaScript, Jscript, VBscript), același document Web poate apărea diferit în ferestrele diferitelor browsere. Indiferent de browser-ul utilizat, acesta trebuie să asigure obligatoriu câteva elemente de interfață cu utilizatorul. În cele ce urmează se vor face referiri la Firefox, unul din cele mai folosite si apreciate navigatoare.

Toate ferestrele browserelor dispun de câteva elemente comune care vor fi explicate în cele ce urmează:

Câmp pentru introducerea adresei: are aspectul unei casete text în care se introduce de la tastatură adresa sau locația documentului căutat. Adresa se introduce in format URL (Uniform Resource Locator - locator uniform de resurse), care conține numele protocolului (sau schema), numele domeniului sau adresa IP, portul și calea către fișier, după modelul:

[protocol][hostname][port][pathname]

Protocol-ul este implicit HTTP. Dacă se dorește alt protocol acesta trebuie specificat. Întotdeauna numele protocolului este urmat de două puncte „:”. Pe lângă protocolul implicit, alte protocoalele utilizate sunt: file: (fișier local), ftp: (FTP), mailto: (E-mail), news: (Usenet news) și gopher: (Gopher). După numele protocolului urmează un număr variabil de slash-uri “/” – două

slashuri dacă se utilizează HTTP:, FTP: sau News:, trei slashuri pentru file: și nici unul pentru mailto: sau Gopher:.

Hostname sau ***numele domeniului:*** a fost definit în secțiunea anterioară. ***Port***-ul, este numărul portului dedicat protocolului utilizat, pe serverul către care se face cererea. Multe protocoale au definite ca implicite numerele porturilor, cum ar fi: 21 pentru FTP, 70 pentru Gopher, 80 pentru World Wide Web, 119 pentru Usenet news, 8080 pentru serverele proxy. De aceea el poate fi omis din conținutul URL când se folosește unul din protocoalele de mai sus pe portul standard.

Pathname sau ***calea***, reprezintă calea către document, și se specifică asemănător cu modul de specificare a căii în Windows, cu deosebirea că în loc de backslash "\" se folosește slash "/".

Un exemplu. Site-ul web al organizației IANA este http://www.iana.org. Dacă doriți să accesați documentul care conține descrierea domeniilor generice de nivel 1 va trebui să introduceți adresa *http://www.iana.org/gtld/gtld.htm*. Calea către documentul *gtld.htm* este *gtld/gtld.htm*.

După introducerea adresei se apasă tasta Enter pentru a informa navigatorul să trimită cererea la adresa indicată.

Observații:

Numele protocolului și al domeniului nu sunt „Case Sensitive", adică pot fi scrise atât cu litere mari (Capitals) cât și cu litere mici sau combinații ale acestora, dar calea este „Case Sensitive" și trebuie specificată ca atare. Dacă în calea de mai sus s-ar fi scris "GtLd.htm" atunci serverul ar fi răspuns cu un mesaj de eroare, care atenționează asupra faptului că fișierul respectiv nu poate fi găsit.

În exemplul de mai sus s-a omis protocolul, care este http:, deoarece browser-ul consideră acest protocol ca implicit.

Butoane de navigare servesc pentru răsfoirea paginilor care au fost deschise, asemenea unei cărți. Butoanele au forma unor săgeți, orientate spre stânga pentru înapoi și spre dreapta pentru înainte. Din pagina curentă, dacă se acționează butonul Back se încarcă pagina anterior vizualizată, iar după aceasta se poate reveni la pagina inițială acționând Forward. La Firefox, dacă se dă click dreapta pe oricare din butoanele de navigare, se deschide lista cu paginile vizitate, din care se poate alege oricare, fără a fi nevoie să se acționeze repetat butoanele *Back* sau *Forward*.

Tot în această categorie pot fi incluse alte două butoane: *Stop, Refresh* și *Home*. Butonul *Refresh* folosește pentru reîncărcarea pagini curente dacă

operația anterioară a eșuat ori a fost întreruptă de utilizator. El este, de asemenea, util în cazul în care se editează un document HTML și se dorește previzualizarea acestuia. După orice modificare făcută în sursa documentului și salvată, pentru a se vedea efectul modificării trebuie reîncărcat documentul cu ajutorul butonului de reîmprospătare. La navigatorul Firefox aspectul butonului *Refresh* se schimbă pe durata încărcării unei pagini, luând aspectul literei X, cu funcția *Stop*. Butonul *Stop* folosește pentru oprirea încărcării paginii accesate. Odată terminată încărcarea paginii, butonul Stop revine la starea și aspectul inițiale. Butonul *Home*, care are aceeași denumire în majoritatea browser-elor, folosește pentru încărcarea paginii definite de utilizator ca pagină implicită.

Fereastra navigatorului Firefox, versiunea 37, este reprodusă în Figura 34. Se poate observa că față versiunile anterioare bara de meniuri este mult diminuată, din dorința de a mări cât mai mult suprafața activă a ferestrei. Ea poate fi afișată sau ascunsă, la dorința utilizatorului, făcând click dreapta cu mouse-ul pe bara de titlu a ferestrei navigatorului și alegând *Menu Bar* din meniul contextual. Ca toate navigatoarele moderne, Firefox oferă posibilitatea navigării în *taburi* (sau file), mult mai comodă față de navigarea ăn ferestre diferite.

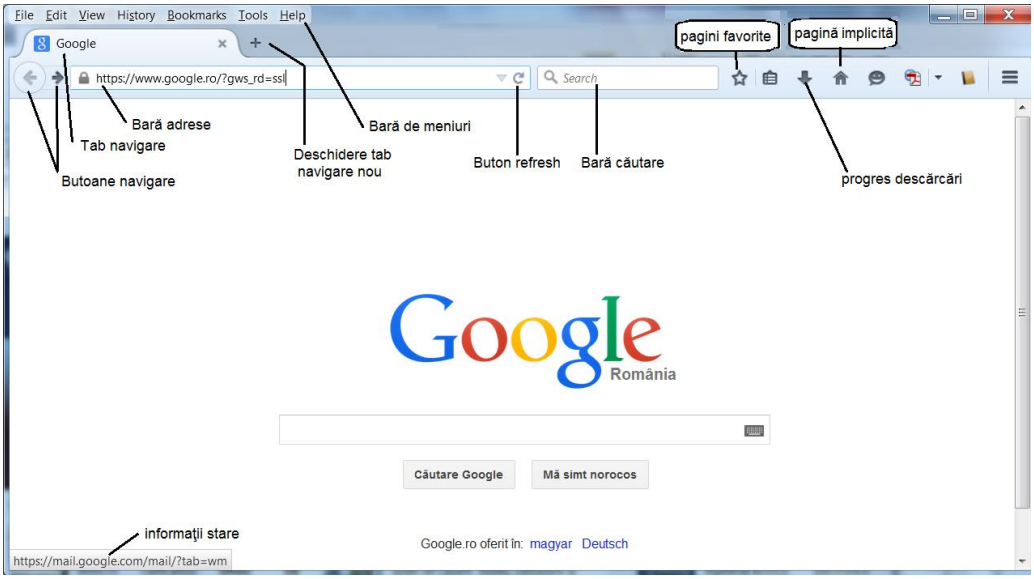


Figura 34 Fereastra Mozilla Firefox

2.2.3.1.1 Personalizarea navigatorului Firefox

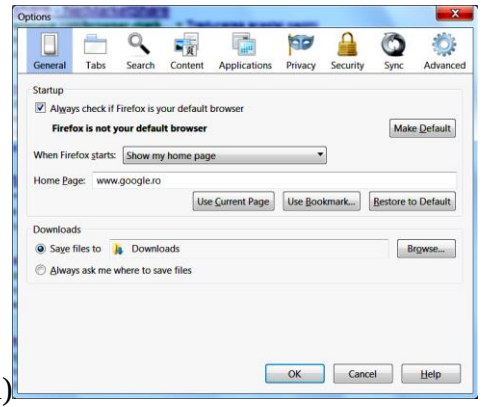
Setarea paginii implicite (Home Page)

Pentru a seta pagina implicită a navigatorului (cea care se încarcă la apăsarea butonului *Pagină implicită*) faceți click pe butonul *Tools* de pe bara de

instrumente și alegeți *Option* din meniu. Se va deschide fereastra de dialog din Figura 35, din care alegeți butonul General. În câmpul *Home page* scrieți adresa paginii pe care doriți să o faceți pagină implicită. Apăsați butonul *Ok* pentru salvare. Dacă pagina este deja încărcată, apăsați butonul *Use Current Page* și apoi butonul Ok. Apăsând butonul *Restore to Default* stabiliți ca pagină implicită pagina Firefox. Puteți stabili și pagina cu care se deschide navigatorul, care poate fi diferită de pagina implicită

Tot în această secțiune puteți stabili folderul în care să se descarce fișierele de pe Internet (implicit este Downloads).

Pentru stabilirea motorului de căutare folosit de bara de căutare, alegeți butonul *Search* și, mai întâi, selectați sau deselectați motoarele de căutare din listă, apoi cu butonul *Default Search Engine* alegeți motorul implicit.

a) 

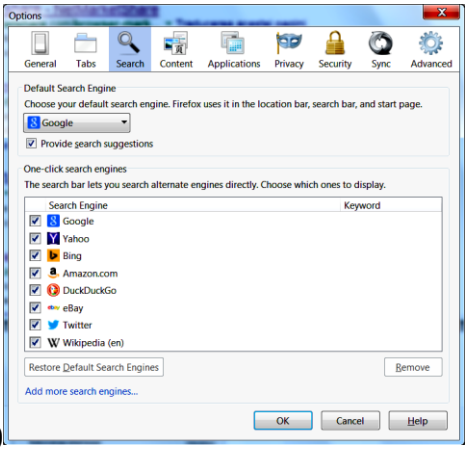
b) 

Figura 35 Tabelele *General* și *Content* ale ferestrei de dialog Internet Options

Istoricul navigării

Atunci când navigați pe Internet, navigatorul memorează adresele introduse în bara de adrese și linkurile activate în cursul navigării. Se constituie astfel un *istoric al navigării*, accesibil prin apăsarea săgeții din capătul din dreapta al barei de adrese. Acesta este diferit de istoricul navigării în cadrul unei sesiuni, care este disponibil la apăsarea săgeții din dreptul butoanelor *Forward* și *Back* și care se șterge la închiderea ferestrei browser-ului. Accesul altei persoane la istoricul navigării poate fi considerat ca o încălcare a intimității.

De asemenea, în timpul navigării, se memorează conținutul paginilor vizitate sub forma unor fișiere temporare pe calculatorul dumneavoastră. Această operație se face cu scopul de a accelera încărcarea paginilor pe care le-ați mai vizitat anterior, furnizând elementele de conținut la o viteză mult mai

mare din fișierele memorate în loc să fie aduse de pe site-ul web cu viteza limitată a conexiunii. și accesul unor alte persoane la fișierele temporare poate fi considerat un atac la intimitate deoarece devoalează conținutul paginilor vizitate.

Este posibil ca navigatorul să memoreze datele pe care le introduceți în formularele de pe anumite pagini web, cum ar fi numele de utilizator și parola de autentificare la serverul de e-mail. Acest lucru este un real pericol deoarece dă posibilitatea altor persoane să folosească datele memorate pentru a accesa site-uri web in contul dumneavoastră.

Pentru a stabili ce elemente doriți să fie memorate de navigator, alegeți butonul *Privacy* și selectați, din pagina care vă este afișată, elementele care doriți să fie memorate.

Datele memorate pot fi șterse alegând *History* din bara de meniuri și, apoi, *Clear History*. Din fereastra care se deschide selectați elementele pe care doriți să le ștergeți, apoi, din butonul de ștergere alegeți intervalul de timp pentru care faceți ștergerea (ultima oră, ultimele patru ore, ziua curentă sau ștergerea tuturor datelor). Apăsați butonul *Clear Now* și așteptați până la închiderea ferestrei, Figura 36.

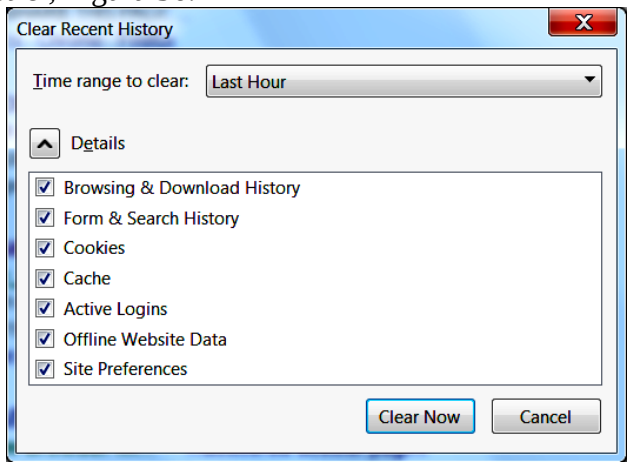


Figura 36 Ștergerea istoricului

2.2.3.2 Navigarea cu ajutorul browser-ului

Prin navigare pe Internet se înțelege acțiunea de explorare a resurselor puse la dispoziție de Internet. Așa cum am arătat mai sus browser-ul de Internet este mijlocul prin care acest lucru este posibil. Pentru a accesa un anumit document găzduit de un server Web adresa (mai corect URL-ul) acestuia trebuie scrisă în câmpul de adrese, după care se apasă tasta *Enter*

De regulă documentele nu sunt izolate ci grupate tematic în ceea ce se numesc *site*-uri. Fiecare site are o pagină principală (home page), cea care este afișată atunci când în caseta de adresă nu se specifică numele fișierului și calea. Numele paginii principale este, de regulă, *index.html* dar sunt servere care au definite și alte nume pentru pagina principală, cum ar fi *index.htm, index.php, default.htm, main.htm*. Spre exemplu, numele paginii principale a Facultății Științe Economice și Administrație Publică din Universitatea "Ștefan cel Mare" Suceava este index.php. Dacă în caseta de adresă se introduce www.seap.usv.ro sau www.seap.usv.ro/index.php browser-ul va afișa aceeași pagină, adică index.php. Pe lângă pagina principală un site mai conține și alte pagini Web precum și fișiere imagine, sunet, executabile. De cele mai multe ori fișierele care alcătuiesc site-ul se află pe același server dar este posibil ca anumite pagini sau fișiere să fie găzduite de alte servere Internet.

După apăsarea tastei *Enter*, browser-ul va căuta să se conecteze la serverul al cărui nume a fost specificat în adresă. Dacă serverul nu poate fi contactat (nu există, este temporar inaccesibil) utilizatorul primește un mesaj de eroare. Dacă serverul a putut fi contactat atunci acesta va încerca să satisfacă cererea, adică să expedieze documentul solicitat către calculatorul care a făcut cererea. Dacă documentul este găsit, acesta va fi afișat în fereastra browser-ului. Dacă documentul nu este găsit, atunci serverul va răspunde cu un mesaj de eroare care va fi, de asemenea, afișat de browser.

Într-un document Web există porțiuni de text (cuvinte) sau zone de imagine deasupra cărora cursorul mouse-ului își schimbă aspectul luând forma unei mâini cu degetul arătător ridicat. Respectivele cuvinte, care de obicei sunt afișate cu altă culoare decât restul textului și sunt subliniate, sau porțiuni de imagine reprezintă legături (hyperlinks) spre alte documente Web sau fișiere. Dacă faceți click pe butonul stâng al mouse-ului când cursorul se află deasupra unei legături, atunci browser-ul va stabili o conexiune spre serverul care găzduiește respectivul document sau fișier și, dacă legătura reușește, va lansa cererea. Dacă documentul solicitat există atunci serverul îl va trimite și va fi afișat de browser, în aceeași fereastră sau într-o fereastră nouă. Dacă cererea se referă la un fișier oarecare, atunci browser-ul va răspunde funcție de natura fișierului:

- dacă este un fișier imagine de tipul suportat (jpg, jpeg, gif, png) acesta va fi afișat,
- dacă este un alt tip de fișier (imagine -tiff, bmp, audio -mp3, video -mpeg, executabil -exe, MSOffice - Word, Excel) browser-ul va încerca să lanseze aplicația asociată tipului respectiv de fișier, de exemplu Paint, Media Player, Real Player, Winamp, MSWord sau să lanseze în execuție fișierul executabil. Dacă nu poate lansa respectiva aplicație atunci sunteți atenționa asupra posibilității salvării fișierului pe discul local.

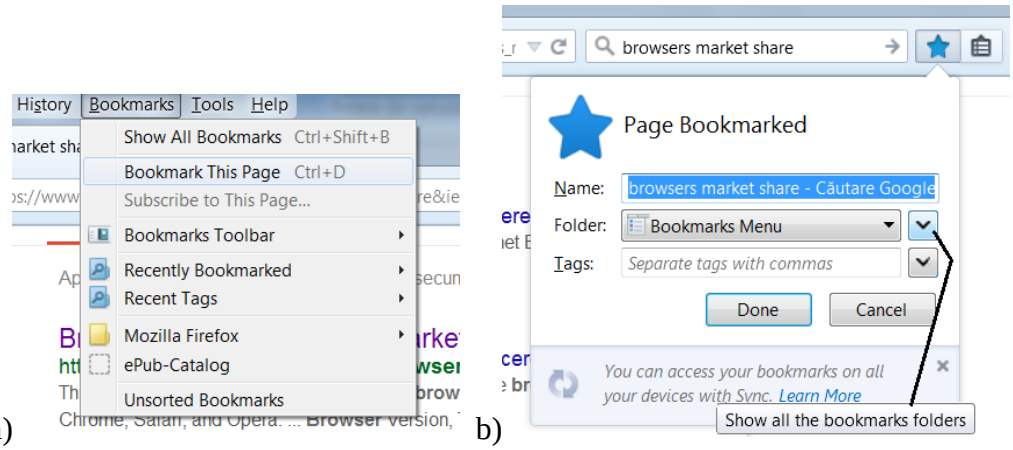
Folosind butoanele de navigare *Back* și *Forward* puteți reveni la paginile anterior vizitate, fără a mai fi nevoie de introducerea adresei de la tastatură. Dacă doriți abandonarea unei operații în curs apăsați pe butonul *Stop* de pe bara de instrumente. Pentru reîmprospătarea informației de pe ecran apăsați butonul *Refresh*.

Adresele accesate sunt memorate de navigator și dacă doriți să reveniți rapid la una dintre ele, apăsați butonul din capătul din dreapta al barei de adrese (triunghiul cu vârful în jos). Sub caseta de adrese se desfășoară lista adreselor care au fost introduse din care se poate alege cea dorită. În timpul scrierii adresei, sub bara de adrese se desfășoară o altă listă care conține adrese pe care Internet Explorer le propune pe baza primelor caractere din adresă care au fost tastate. și de aici se poate alege adresa dorită, dacă există..

2.2.3.2.1 Administrarea listelor de preferințe

Dacă o anume pagină prezintă un interes deosebit pentru dumneavoastră și doriți să o aveți la îndemână pentru a fi accesată rapid, o puteți adăuga în lista de preferințe (Bookmarks). Pentru aceasta, având pagina încărcată și afișată în navigator, apăsați butonul *Bookmarks* din bara de meniuri. Se va deschide o listă de articole, Figura 37a, din care alegeți *Bookmark This Page* sau apăsați combinația de taste *Ctrl + D*. Pagina va fi adăugată la lista *Bookmarks*.

Pentru a nu obține o listă foarte lungă este bine să organizați această listă creând dosare pe diverse subiecte în care să memorați paginile legate de subiectele respective. Pentru crearea unui dosar nou apăsați butonul *Show all the bookmarks folders*, Figura 37b. Conținutul acestei secțiuni se modifică și puteți să salvați pagina în alt dosar sau să creați un dosar nou.



a) b)

Figura 37 Meniul *Bookmarks* permite adăugarea paginilor la lista de preferințe, cu posibilitatea organizării paginilor salvate.

Administrarea listei de preferințe (redenumirea dosarelor, adăugarea sau ștergerea lor, modificarea conținutului dosarelor) o puteți face din meniul *Bookmarks*, alegând *Show All Bookmarks*. Navigatorul vă va pune la dispoziție o interfață în care puteți face aceste operații.

2.2.3.2.2 Stabilirea setului de caractere

Este posibil ca atunci când deschideți pagini scrise în altă limbă decât engleză să vedeți caractere neinteligibile în text, în special în locul diacriticelor, ceea ce vă va îngreuna substanțial citirea. Aceasta se întâmplă deoarece la crearea paginii a fost folosit un sistem de codare a diacriticelor diferit de sistemul pe care îl folosește navigatorul. Dacă pagina conține informații despre setul de caractere folosit, navigatorul se va plia pe acel set și redarea va fi corectă. Datorită unor greșeli de proiectare a paginii, informațiile despre setul de caractere pot fi greșite (nu există consistență în folosirea setului de caractere declarat) sau pot lipsi.

Figura 38 Neconcordanța între codificarea caracterelor paginii și a cea folosită la decodificare de navigator

Din acest motiv navigatorul va afișa eronat anumite secțiuni ale paginii, , Figura 38, sau chiar întreaga pagină dacă nu poate determina ce set de caractere utilizează pagina.

Puteți determina browser-ul să folosească setul potrivit alegând din bara de meniuri opțiunea *View* și apoi *Character Encoding*. În ultima perioadă, majoritatea paginilor create în alte limbi folosesc seturi de caractere *Unicode*. Dacă navigatorul nu reproduce corect toate caracterele, deși are stabilit ca set

implicit de redare tot *Unicode*, va trebui să încercați alte codificări. Pentru limba română, ca și pentru orice altă limbă central europeană, alegeți *Central European (ISO)* sau *Central European (Windows)*. Orice set de caractere stabilit în această secțiune va determina navigatorul să ignore meta informațiile din pagină. Opțiunea *Auto-Detect* determină navigatorul să stabilească setul de caractere pe baza meta informațiilor sau, în lipsa lor, pe baza altor elemente din document.

2.2.3.2.3 Modificarea dimensiunii fonturilor și conținutului

Puteți mări sau micșora conținutul paginii, text și imagini, apăsând tasta *Ctrl* și apoi tasta + pentru a mări, respectiv - pentru a micșora. Alternativ puteți apăsa tasta Ctrl și roti butonul din mijloc al mouse-ului.

2.2.3.2.4 Tipărirea paginilor Web

Tipărirea se face apăsând combinația de taste *Ctrl + P* sau din meniul *File* cu opțiunea *Print*.

Previzualizarea documentului poate fi făcută din meniul *File* cu opțiunea *Print Preview*. Față de versiunile anterioare IE7 aduce o îmbunătățire substanțială prin interfața intuitivă și o serie de noi funcționalități.

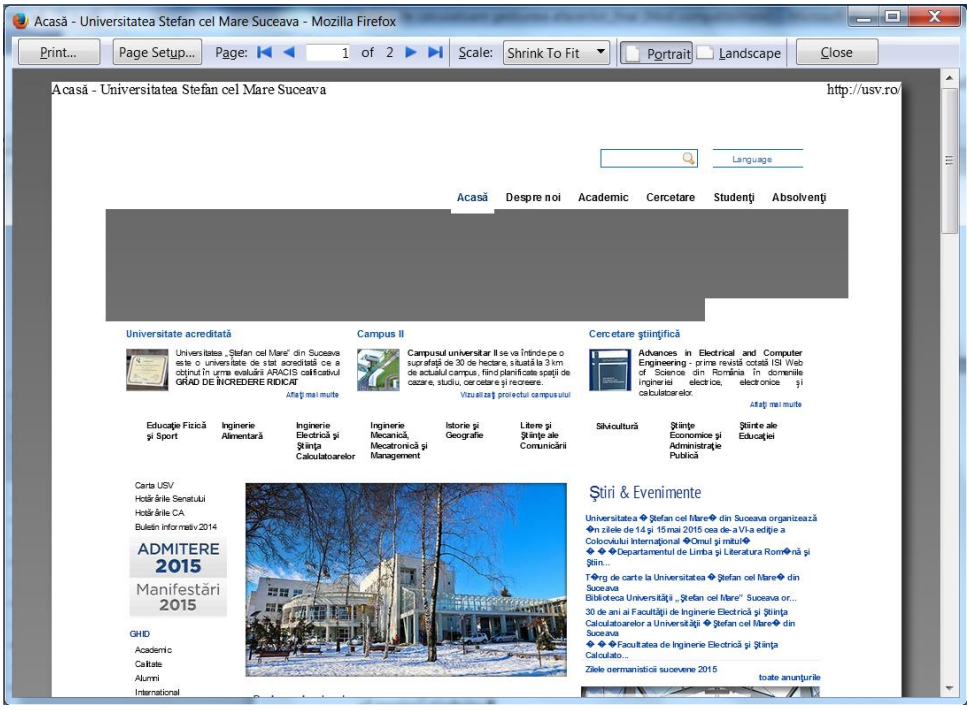


Figura 39 Fereastra de tipărire oferă utilizatorului o interfață intuitivă

Astfel, opțiunea *Shrink to fit* (strânge pentru a potrivi), permite încadrarea paginii afișate pe ecran în formatul stabilit al paginii tipărite. Se deschide o fereastră cu aspectul celei din Figura 39, care este destul de intuitivă pentru a mai necesita informații suplimentare.

2.2.3.2.5 Salvarea paginilor Web

Puteți salva paginile web pentru a avea acces la conținutul acestora offline - atunci când nu mai dispuneți de o conexiune Internet (de exemplu in avion sau tren). Din meniul *File* alegeți *Save Page As*. În fereastra de dialog care se deschide, Figura 40, în câmpul *File name*: tastați un nume sugestiv pentru fișier. Din lista *Save as type*: alegeți formatul dorit.

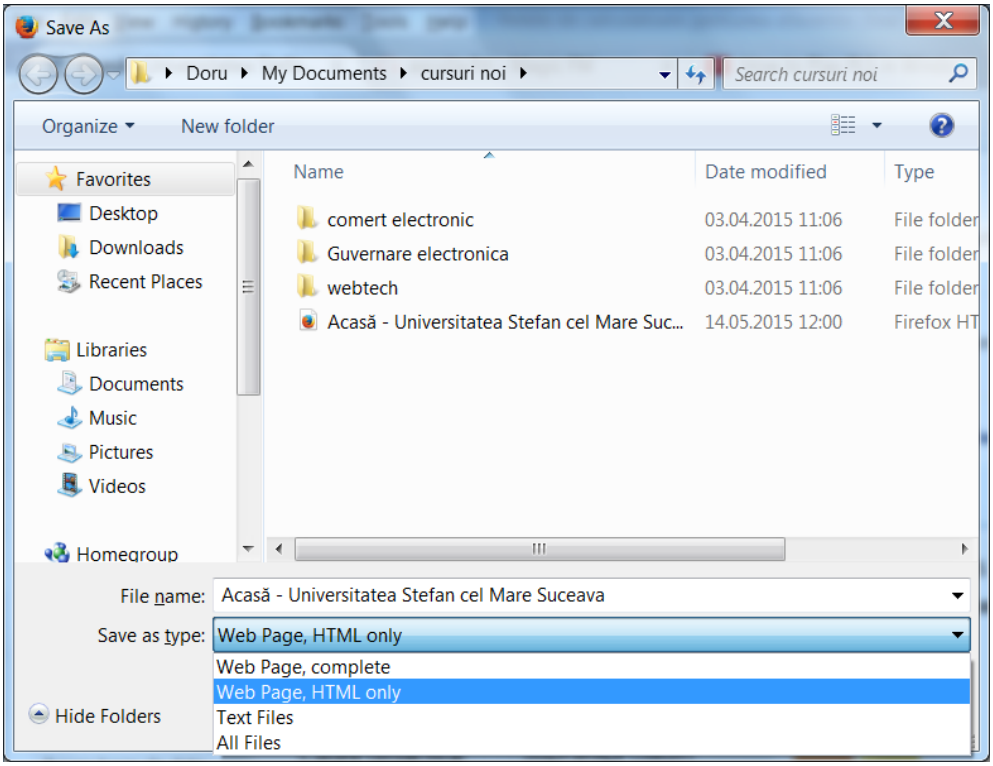


Figura 40 Fereastra *Save Webpage* permite salvarea paginii în multiple formate

Iată o scurtă descriere a formatelor disponibile:

- Webpage, complete (*.htm,*.html) - păstrează formatul original (htm sau html) salvând elementele conținute în pagină (imagini, scripturi, etc.) în dosare asociate fișierului salvat.

- Web Page HTML only (*.htm,*.html) – Salvează textul cu legături (hyperlins) dar fără formatări, culori pentru fundal și text
- Text files (*.txt)- salvează doar informația text, neformatat, fără legături.

2.2.3.2.6 Copierea textului, imaginilor și legăturilor dintr-un document Web

Puteți copia textul dintr-o pagină Web și utiliza într-un editor de text selectând textul respectiv și folosind comenzile de copiere: combinația de taste *Ctrl* + C sau comanda *Copy* din meniul contextual. Textul copiat în clipboard îl puteți lipi apoi în orice editor de text sub Windows. Dacă folosiți MSWord vă recomand ca lipirea să o faceți folosind comanda *Paste Special* din meniul *Edit* și nu cu simplu *Paste* sau *Ctrl*+V. Evitați astfel copierea formatului HTML din pagina Web în pagina Word, copiere care vă poate da mare bătaie de cap la formatarea finală a documentului Word.

În ceea ce privește imaginile inserate în document, acestea pot fi salvate sub formă de fișier grafic astfel: poziționați cursorul mouse-ului pe imagine, dați click pe butonul drept al mouse-ului și alegeți comanda *Save Image As…* iar din fereastra de dialog care se deschide alegeți dosarul / unitatea de disc unde doriți să salvați și dați un nume fișierului. Pentru salvarea imaginilor care servesc ca fundal (background) poziționați cursorul oriunde pe suprafața fundalului, faceți click dreapta și din meniul contextual alegeți comanda *View Background Image*. Odată imagine afișată o salvați ca pe orice altă imagine.

Pentru a copia adresa unei legături din pagină poziționați cursorul pe legătură, dați click dreapta și din meniul contextual selectați *Copy Link Location*. Adresa este copiată în clipboard și o puteți apoi lipi în orice editor de text sub Windows sau în orice casetă text dintr-un formular Web.

2.3 Poșta electronică (E-Mail)

Poșta electronică este un serviciu al Internetului intens folosit în comunicarea și transmiterea de informații între grupuri de persoane. Are câteva avantaje, comparativ cu poșta tradițională: timpul de livrare a mesajului, notificarea expeditorului cu privire la eventualele probleme de livrare, posibilitatea atașării unor fișiere, costul redus.

Prin e-mail se transmite text, posibil formatat HTML, la care se pot atașa fișiere cu conținut divers (documente, imagini, sunet, programe).

Ca orice serviciu Internet, funcționarea poștei electronice se bazează pe clienți și servere. Rolul serverelor este de a păstra conturile (căsuțele poștale)

clienților, primirea și transmiterea mesajelor de la și către clienți, transmiterea și primirea mesajelor către alte servere de e-mail din Internet.

Un server de e-mail este, de regulă, asociat unui domeniu/subdomeniu: usv.ro, seap.usv.ro, yahoo.com, edu.ro etc. Un utilizator care are un cont pe un server aparținând unui domeniu oarecare este identificat printr-o adresă de e-mail, de forma *username@domeniu.topdomeniu*. În același domeniu/subdomeniu nu pot exista doi utilizatori cu același username.

Un cont constă într-un spațiu de memorie rezervat pe disc, care este împărțit în câteva dosare (foldere): Inbox – locul de depozitare a tuturor mesajelor primite; Sent – dosar în care se pot păstra, la opțiunea utilizatorului, copii ale mesajelor expediate; Trash – dosar în care sunt trimise toate mesajele șterse din celelalte dosare. În funcție de furnizorul de servicii de e-mail, contul mai poate avea câteva dosare, printre care Spam sau Junk – dosar în care sunt trimise mesajele identificate ca SPAM de filtrele aplicației și Drafts – dosar în care sunt păstrate ciornele mesajelor neexpediate. Pe lângă acestea, utilizatorul poate crea propriile dosare, pentru a putea organiza mai bine mesajele.

Accesul utilizatorului la contul său se poate face fie direct, la serverul de e-mail, prin intermediul unui client de e-mail, fie indirect, prin intermediul unei interfețe web, pusă la dispoziție de furnizorul de servicii de e-mail, Figura 41.

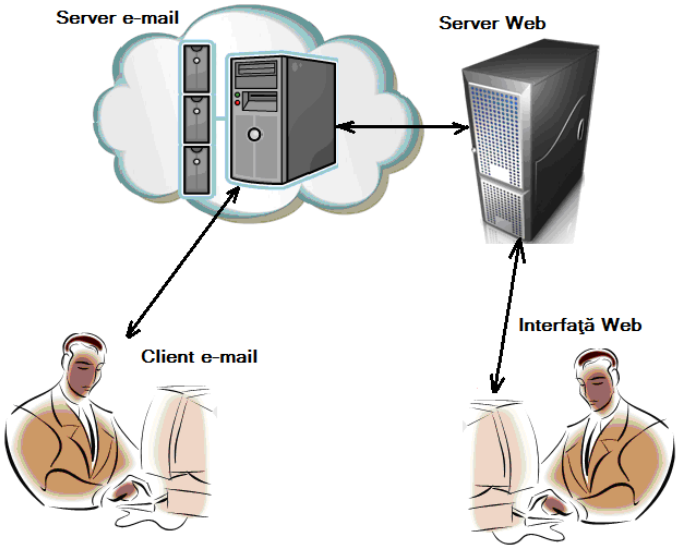


Figura 41 Accesul la contul de e-mail a doi utilizatori, cu client de e-mail și prin interfață web

Clienții de e-mail (MS Outlook, MS Outlook Express, Mozilla Thunderbird, Evolution) oferă mai multe facilități în gestionarea și manipularea mesajelor, dar prezintă dezavantajul că trebuie instalați și configurați pe

calculatorul utilizatorului. Pe de altă parte, interfețele Web asigură accesul la poșta electronică de oriunde există acces la Internet și un navigator Web.

2.3.1 Accesul cu clienți de e-mail

Un client de e-mail se poate conecta la server folosind protocoale specifice acestui serviciu. Pentru a trimite mesajul de la client la server este utilizat protocolul SMTP (Simple Mail Tranfer Protocol). Același protocol este utilizat de serverele de e-mail pentru a transmite mesajele de la unul la altul.

Pentru citirea mesajelor de pe server, clientul de e-mail poate folosi unul din protocoalele POP3 (Post Office Protocol, versiunea 3) sau IMAP (Internet Message Access Protocol). Pentru sistemele proprietare se folosesc protocoalele specifice, puse la dispoziție de acestea, cum ar fi Microsoft Exchange sau Lotus Notes/Domino.

Funcționarea serviciului de e-mail și protocoalele folosite este redată în Figura 42. În imagine este redată situația în care cei doi clienți utilizează serviciul de e-mail din rețelele locale din care fac parte și serverele. În practică, de multe ori, accesul la e-mail se face din alte rețele, situație în care conexiunea cu serverul se face prin rețeaua Internet.

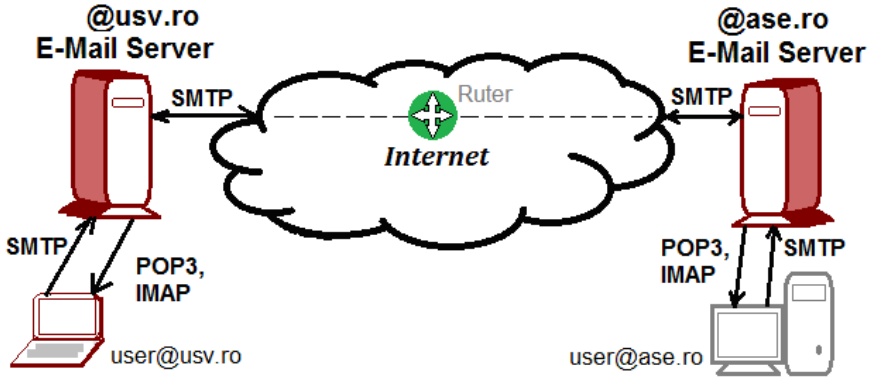


Figura 42 Funcționarea serviciului de e-mail și protocoalele utilizate de către clienții de e-mail

Diferența dintre protocoalele POP3 și IMAP constă în aceea că primul descarcă toate mesajele din dosarul Inbox pe calculatorul clientului, într-un dosar local, numit tot Inbox, eliberând spațiul de pe server. Acest fapt dă posibilitatea citirii mesajelor și offline, după deconectarea de la Internet. Protocolul IMAP afișează doar lista mesajelor din Inbox, citirea lor făcându-se prin descărcarea pe calculatorul local a unor copii ale acestora, ele rămânând pe server. Se asigură astfel accesul clientului la cont de pe mai multe calculatoare.

Utilizatorii pot manipula mesajele pe server, mutându-le dintr-un dosar în altul, ștergându-le sau chiar mutându-le de pe server pe calculatorul local.

Clienții de e-mail creează, la instalare, dosare locale cu aceleași denumiri sau funcții cu cele de pe server, și unele suplimentare, cum ar fi Outbox. Acesta păstrează mesajele scrise offline și sunt transferate pe server după conectarea la acesta. Mai mult, un client de e-mail poate gestiona mai multe conturi, pe servere diferite sau pe același server. Spre exemplu, o persoană angajată ca secretar la o firmă poate avea două adrese de e-mail pe serverul firmei, una personală și alta pentru birou: *user@firma.ro* și *office@firma.ro*.

Clientul de e-mail, configurat cu cele două conturi, va afișa conținutul fiecărui cont, iar dacă protocolul utilizat este POP3, mesajele din Inbox-urile celor două conturi vor fi transferate în dosarul Inbox local. Utilizatorul poate răspunde la orice mesaj folosind oricare din cele două conturi. Fereastra clientului Mozilla Thunderbird este reprodusă în Figura 43.

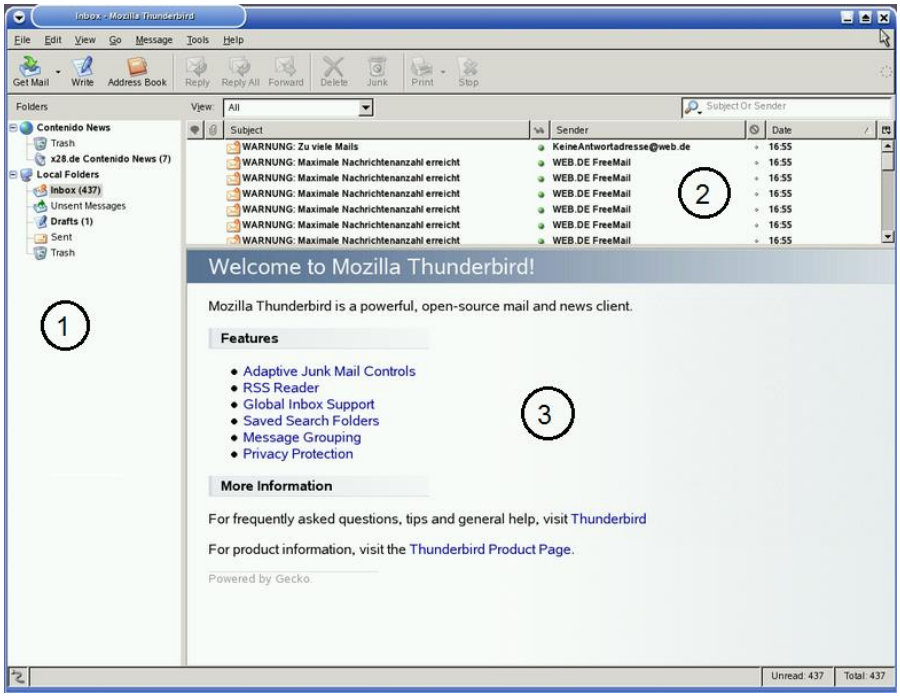


Figura 43 Fereastra clientului de e-mail Mozilla Thunderbird

Ea este împărțită în 3 cadre: cadrul 1 afișează toate dosarele de pe server și pe cele locale. În cadrul 2 este afișată lista mesajelor din dosarul selectat în cadrul 1. Cadrul 3 oferă o previzualizare a mesajului selectat în cadrul 2. Pentru deschiderea mesajului într-o fereastră proprie, se dă dublu click pe respectivul mesaj.

Orice mesaj electronic conține mai multe câmpuri: *From* – adresa de e-mail a expeditorului, *To* – adresa de e-mail a destinatarului, *Subject* – subiectul mesajului, *Body* (corpul mesajului) – conținutul efectiv al mesajului. Câmpul *To* poate conține mai multe adrese de e-mail, separate prin virgula sau punct și virgulă. În această situație mesajul va fi trimis tuturor destinatarilor din lista conținută de câmpul *To*. Există și câmpuri opționale, *Cc* (Carbon copy – copie la indigo) în care se pot trece, de asemenea, adresele de e-mail ale altor destinatari și *Bcc* (Blind carbon copy), în care se trec adresele de e-mail ale destinatarilor, adrese care nu sunt dezvăluite celorlalți destinatari.

Printre facilitățile pe care clienții de e-mail le oferă utilizatorilor se numără și posibilitatea filtrării mesajelor, atașării de semnături, solicitarea confirmării deschiderii mesajului de către destinatar, stabilirea unei valori pentru importanța mesajului, crearea de liste de destinatari.

Filtrarea mesajelor constă în stabilirea unor reguli după care mesajele vor fi sortate dacă îndeplinesc anumite criterii. Astfel este posibil ca mesajele primite să nu intre toate în Inbox ci să fie direcționate spre alte dosare. Criteriul poate avea în vedere oricare din câmpurile *From*, *Subject*, *Body*. Dacă unul din aceste câmpuri conține sau începe cu un cuvânt pe care îl stabilim noi, mesajul respectiv va urma regula pe care o stabilim pentru acest criteriu. Spre exemplu, dacă dorim ca facturile electronice, primite prin e-mail, de la furnizorul nostru de telefonie mobilă, să nu fie amestecate cu restul mesajelor din Inbox, creăm un dosar numit „Facturi electronice”, notăm adresa de e-mail de la care sosește mesajul cu factura, să zicem support@mobilpay.ro și stabilim următorul set criteriu/regulă: **criteriul**: dacă *From* conține support@mobilpay.ro, atunci aplică **regula**: mută mesajul în dosarul *Facturi electronice*.

Atașarea semnăturii este o facilitate care permite definirea unor semnături pentru același cont sau conturi diferite, care pot fi atașate, după caz, cu un singur click, la finalul mesajului, înainte de trimitere.

Solicitarea confirmării deschiderii mesajului constă în activarea unui câmp, înainte de trimitere, prin care destinatarului i se cere, atunci când deschide mesajul, să confirme, cu un click, primirea lui. Cum destinatarul are posibilitatea să refuze confirmarea primirii, facilitatea se bazează pe buna credință a destinatarului.

Nu toate mesajele pe care le trimite cineva sunt la fel de importante pentru el; expedierea unei oferte noi este mai importantă decât răspunsul la un mesaj de rutină. Există 3 nivele de prioritate: ridicat, normal și scăzut. Expeditorul poate stabili, înainte de expediere, care este importanța mesajului (pentru el, nu pentru destinatar, care poate să aibă altă scară de valori).

Atunci când în mod frecvent anumite mesaje sunt trimise aceloraşi destinatari, este util ca aceştia să fie grupaţi într-o listă, cu un nume sugestiv. De exemplu, toţi clienţii pot fi grupaţi în lista *clienti*, furnizorii în *furnizori*, prietenii în *prieteni*. Atunci când compunem un mesaj pentru clienţi, în câmpul *To* vom scrie numele listei, în loc să trecem, adresă cu adresă, adresele de e-mail ale clienţilor.

2.3.2 Accesul cu interfaţa Web

Spre deosebire de clienţii de e-mail, care trebuie instalaţi pe calculatorul utilizatorului, oferindu-i toate facilităţile doar de pe acel calculator, interfaţa Web permite accesul la contul de e-mail de oriunde există acces la Internet şi un navigator Web. Marii furnizori de servicii de e-mail (Yahoo, Microsoft, Google) oferă interfeţe Web pentru accesul la conturile găzduite de serverele lor. Yahoo oferă o interfaţă complexă, intuitivă, cu o funcţionalitatea apropiată de a clienţilor de e-mail, Figura 44, în timp ce Google oferă o interfaţă minimalistă, mai puţin intuitivă dar foarte fiabilă şi rapidă, Figura 45.

Oricum, anumite acţiuni, cum ar fi crearea unui filtru, reprezintă o aventură în ambele cazuri, pentru cine nu este familiarizat cu cele două interfeţe, Figura 46.

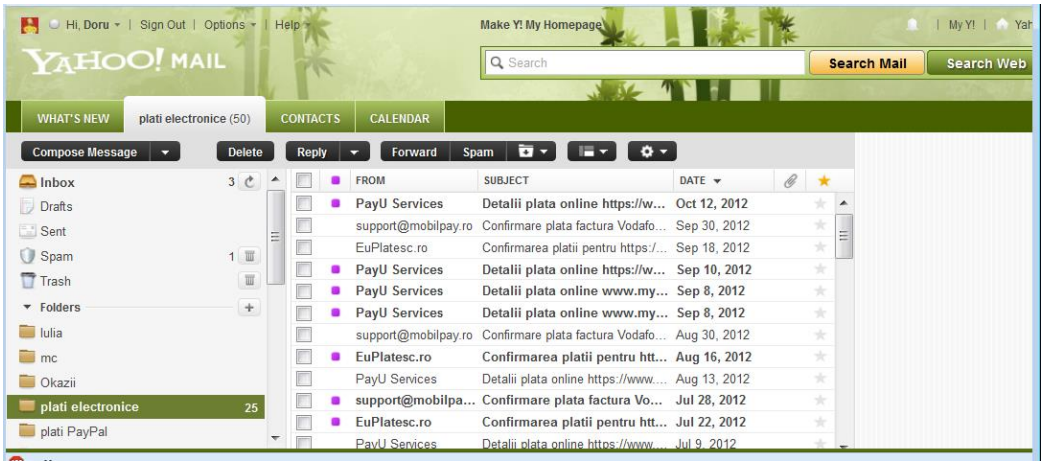


Figura 44 Interfaţa Web pentru accesul la contul Yahoo Mail

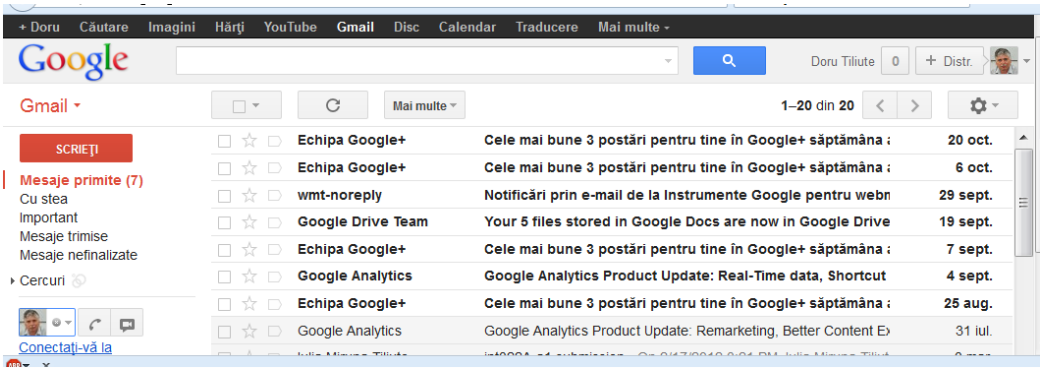


Figura 45 Interfața Webmail, de la Google este minimalistă, orientată mai mult pe text și mai puțin pe grafică

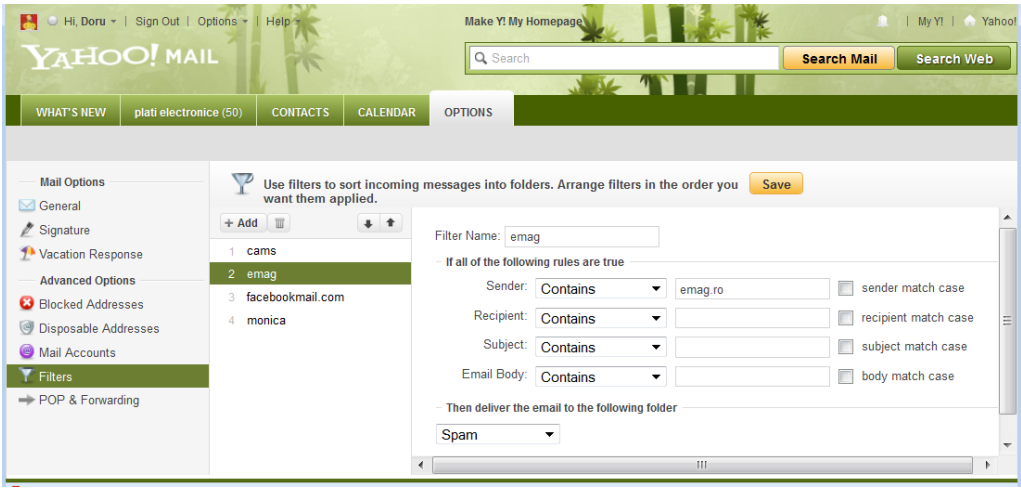


Figura 46 Interfața pentru crearea unui filtru pe Yahoo Mail

2.4 Serviciul FTP

Serviciul FTP este foarte important pentru gestiunea la distanță a fișierelor de pe server. Dacă într-o rețea locală Windows avem posibilitatea accesului la fișierele de pe alte calculatoare prin funcția File Sharing, acest lucru nu mai este posibil într-o rețea WAN. Din acest motiv, pe mașinile care trebuie să pună la dispoziție fișiere care să poată fi accesate la distanță, se instalează un server FTP. Fiecare utilizator trebuie să aibă un cont pe serverul FTP, care garantează accesul și permisiunile la anumite fișiere și directoare de pe server. În anumite situații serverul FTP poate da acces public, doar pentru citire, doar pe baza unei adrese de e-mail valide. Accesul în acest mod se numește „anonim” (anonymous), iar utilizatorul trebuie să introducă drept nume de utilizator chiar *anonymous*. Dar regula este să se evite accesul anonim din

motive de securitate a rețelei; modul normal este cel autentificat, cu nume de utilizator și parolă. Pentru a ne putea conecta la serverul FTP avem nevoie de un client FTP. Clienții FTP sunt fie în linie de comandă fie cu interfață grafică. Unii sunt gratuiți, alții comerciali. Atât sistemul de operare Windows cât și Linux includ un client FTP de tip linie de comandă, cu același nume, *ftp*. Ei sunt destul de greoi în utilizare deoarece necesită cunoașterea comenzilor ftp.

2.4.1 Clientul Windows ftp

Clientul se lansează din fereastra Command Prompt, cu comanda *ftp*. Se deschide o conexiune cu comanda *open*, urmată de numele serverului sau adresa IP a acestuia. După furnizarea datelor de autentificare, dacă utilizatorul are acces, apare mesajul *Login successful*. Pentru a putea vedea conținutul directorului utilizatorului se folosește comanda ls, cu opțiunea –l (long). Rezultatul este o listă detaliată cu fișierele și directoarele conținute. În Figura 47 se dă un exemplu de conectare autentificat la serverul FTP cu adresa 80.96.123.238, folosind clientul *ftp* din Windows. Detaliile sunt tabelate, iar în continuare vom explica ce reprezintă fiecare coloană.

Pe prima coloană este afișată o secvență de 10 caractere în forma trwxrwxrwx. Primul caracter reprezintă tipul fișierului: dacă fișierul este un director (sună ciudat pentru un utilizator de Windows, dar pentru sistemele de operare Unix sau Linux aceasta este terminologia) atunci pe prima poziție din șir este afișată litera d, dacă este un link către alt fișier, va fi afișată litera l iar dacă este un fișier propriu-zis, este afișată cratima -.

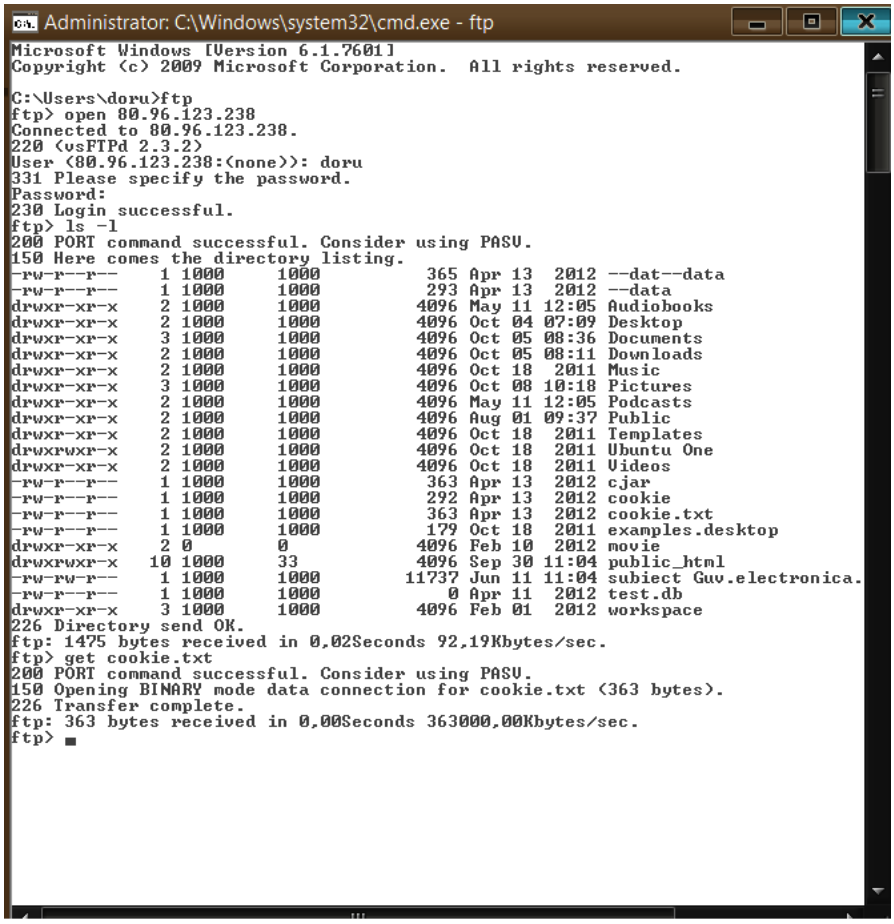


Figura 47 Clientul FTP al SO Windows 7, exemplu de conectare și descărcare fișier

Următoarele 9 caractere sunt împărțite în trei grupe care afișează permisiunile fișierului pentru trei categorii de utilizatori. Primele 3 caractere indică permisiunile proprietarului fișierului, următoarele 3 caractere pe cele ale grupului (din care proprietarul poate face sau nu parte) iar ultimele 3 pe cele ale publicului.

Permisiunile se referă la drepturile pe care fiecare categorie de utilizatori le are asupra fișierului. Astfel dreptul de citire este evidențiat de litera r (read), cel de scriere de litera w (write) iar cel de execuție de litera x (execute) – pentru fișierele executabile.

```
      t  rwx  rwx  rwx
     /     |     \     \
tip fișier  proprietar  grup  public
```

Întotdeauna permisiunile sunt afișate în această ordine, rwx. Dacă în locul oricărei litere apare semnul cratimă –, aceasta însemnă ca pentru categoria respectivă de utilizatori permisiunea nu există (nu are dreptul respectiv). Spre exemplu șirul drwxr--r-- ne arată că este vorba despre un director în care proprietarul are toate drepturile, în timp ce grupul și publicul nu au decât drept de citire. Acest mod de organizare permite un bun control al securității informațiilor de pe server prevenind accesul neautorizat la date.

Pe următoarea coloană este afișat un număr care indică numărul de fișiere conținute de directorul respectiv. Dacă directorul este un fișier atunci numărul este 1. Pe următoarele 2 coloane sunt afișați identificatorii atribuiți proprietarului și grupului de către sistemul care găzduiește serverul FTP. Pe sistemele Unix/Linux, funcție de distribuția utilizată, numerele sub 100 (499 Red Heat Linux, 999 Debian Linux) sunt atribuite unor procese interne ale sistemului iar cele peste aceste valori sunt atribuite utilizatorilor care au conturi create pe sistem. Superuser-ul are Id-ul 0.

Următoarea coloană afișează dimensiunea fișierului/directorului, în octeți, iar următoarea, data ultimei modificări a fișierului. Ultima coloană conține numele fișierului.

Principalele comenzi FTP sunt date în Tabelul 3. Lista completă a comenzilor se poate obține tastând ? în clientul *ftp*.

În mod evident utilizarea clienților în linie de comandă nu este comodă, putând fi, cel mult, o soluție „de avarie”. Din fericire există destui clienți cu interfață grafică. E dificil de făcut o clasificare a lor, depinde mult de obișnuința fiecărui utilizator. Se disting, însă, printre cei gratuiți, doi clienți de foarte bună calitate: FileZilla și Fire FTP. Primul este un client propriu-zis, disponibil pentru toate sistemele de operare importante iar al doilea este un supliment (add-on) pentru navigatorul Mozilla Firefox (asta însemnă că nu poate fi folosit de sine stătător).

Tabelul 3 Lista principalelor comenzi FTP

comanda	**semnificația**
?	Solicitare ajutor despre comenzile FTP acceptate de server
ascii	Setează modul ASCII de transfer al fișierelor
binary	Setează modul binar de transfer al fișierelor (se folosește la transferul fișierelor non-ASCII.)
bye	Părăsește aplicația FTP (ca și quit)
cd	Schimbă directorul de pe server
close	Închide conexiunea cu serverul dar mediul FTP rămâne deschis

delete	Șterge un fișier din directorul curent de pe server
dir	Afișează o listă completă (cu toate proprietățile) a fișierelor din directorul curent
get	Copie un fișier de pe server pe calculatorul local
help	Cere o listă a tuturor comenzilor FTP disponibile
lcd	Schimbă directorul de pe calculatorul local (client)
ls	Listează numele fișierelor din directorul curent de pe server
mkdir	Creează un nou director în directorul curent de pe server
mget	Copie mai multe fișiere de pe server pe calculatorul local; utilizatorul este solicitat să răspundă cu Y/N înainte de transferul fiecărui fișier.
mput	Copie mai multe fișiere de pe calculatorul local pe server; utilizatorul este solicitat să răspundă cu Y/N înainte de transferul fiecărui fișier.
open	Deschide conexiunea cu serverul
put	Copie un fișier de pe calculatorul local pe server
pwd	Afișează directorul curent de pe server
quit	Părăsește aplicația FTP (ca și bye)
rmdir	Șterge un director din directorul curent de pe server

2.4.2 Clientul Fire FTP

Suplimentul se descarcă de pe Internet, căutând din fereastra meniului Suplimente a Firefox după numele suplimentului. Se apasă butonul Instalează și după terminarea descărcării se repornește navigatorul. În meniul Dezvoltator Web[17] se selectează Fire FTP și se va deschide fereastra din Figura 48, în care apăsați butonul *Create an account*.

[17] În versiunile 13 şi ulterioare

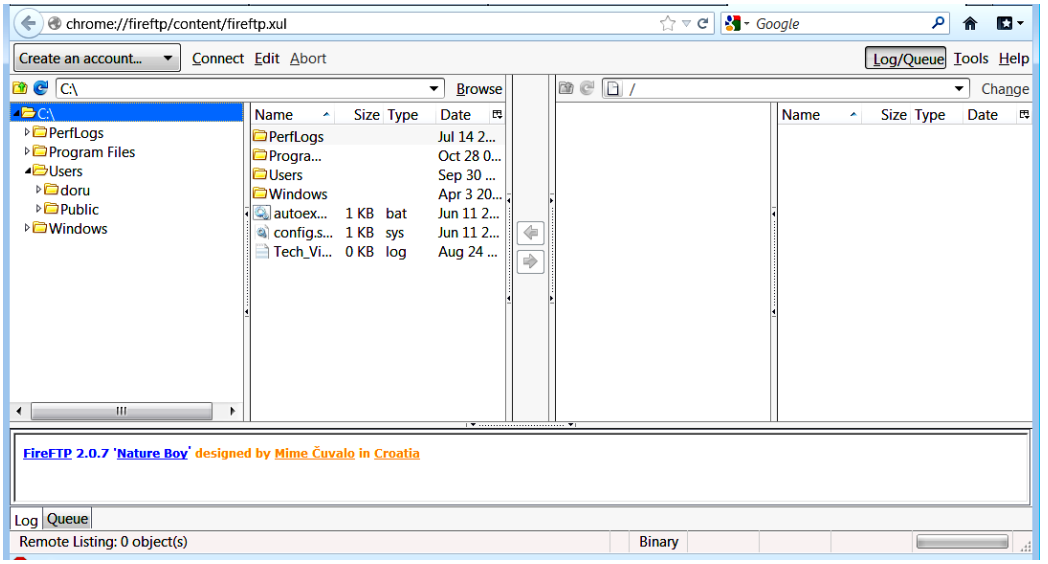
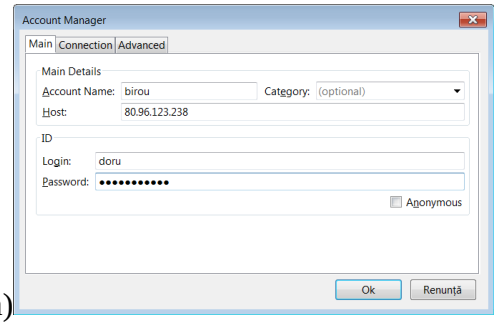


Figura 48 Fereastra suplimentului Fire FTP, după instalare

Se va deschide fereastra cu aspectul din **Error! Reference source not found.**a, în care se introduc datele solicitate: un nume pentru cont (pot fi gestionate mai multe conturi, pe același server sau servere diferite), numele sau adresa IP a hostului (gazdei serverului FTP), numele și parola utilizatorului. Pentru accesul anonim se selectează caseta Anonymous. Dacă conexiunea este securizată va trebui ca în tabela *Connection* să alegem din lista *Security* tipul de securitate utilizat, Figura 49b.

a)



b)

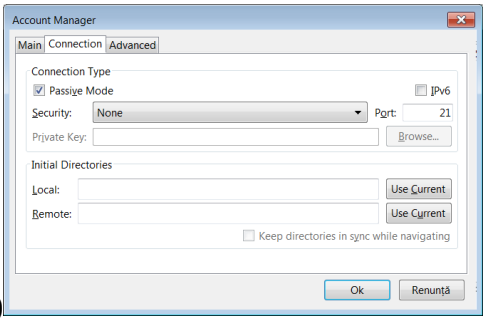


Figura 49 Ferestrele de configurare a contului

În secțiunea *Initial Directories* se pot seta directoarele care vor fi listate, mediat după conectare, de pe calculatorul local și de pe server.

Se dă *Ok* și în fereastra principală se apasă butonul *Connect*. Conținutul directorului stabilit ca implicit, va fi afișat în cadrul din dreapta, ca în Figura 50.

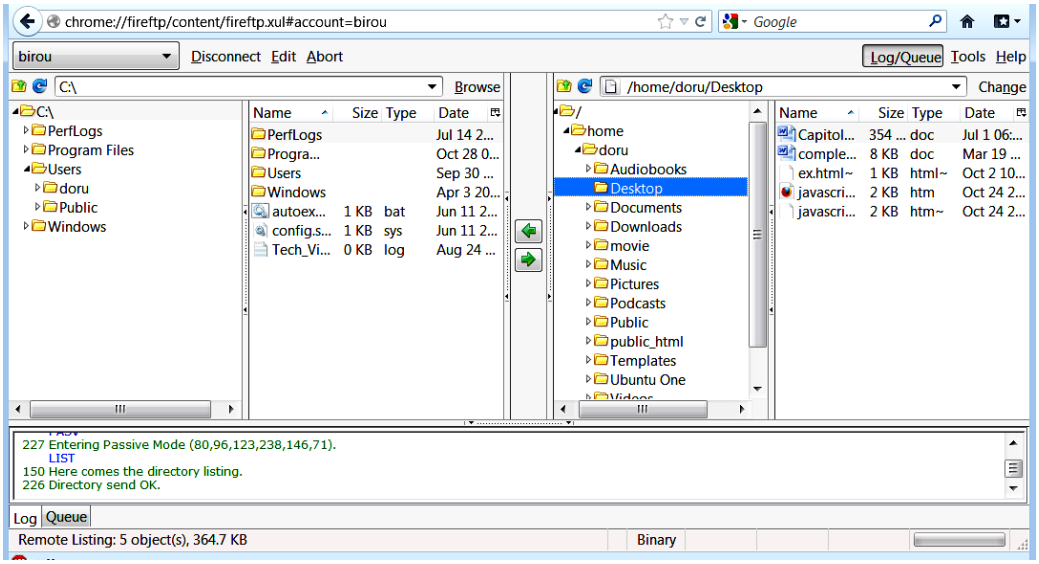


Figura 50 Fereastra clientului Fire FTP, după conectarea la server

Din acest moment utilizarea clientului este banală: pentru a transfera un fișier sau director de pe calculatorul local pe server sau invers, se selectează respectivul fișier sau director și se trage în sensul dorit. Dacă locația fișierului nu este vizibilă, se face click pe pictograma directorului pentru a-i detalia conținutul și tot așa, până sursa sau destinația devin accesibile.

Sub cele două cadre principale se află un cadru orizontal în care sunt afișate mesajele schimbate de client cu serverul FTP. Acestea pot fi utile în cazul apariției unor probleme de conectare sau transfer. Astfel, e posibil ca deși conectarea să se fi realizat cu succes, actualizarea unui fișier pe server să nu fie posibilă din cauza lipsei permisiunilor de scriere.

Deconectarea de la server se face prin apăsarea butonului *Disconnect*.

3 HTML

Limbajul HTML (HyperText Markup Language) este limbajul folosit la creare paginilor Web. El nu este un limbaj de programare ci unul de marcare, care „spune” navigatorului Web cum anume să redea conținutul unei pagini. Ideal ar fi ca toate navigatoarele Web - Internet Explorer, Mozilla Firefox, Chrome și celelalte, să redea în mod identic aceeași pagină, deoarece conține aceleași marcaje sau instrucțiuni pentru redare. În practică lucrurile stau puțin diferit, deși în ultimii ani s-au făcut multe progrese în privința interpretării unitare și conform cu specificațiile a majorității elementelor care alcătuiesc o pagină Web. Specificațiile sunt elaborate de un consorțiu internațional, World