

Capitolul 8

INTERNET

Ultimele decenii s-au caracterizat printr-o explozie informațională fără precedent în istoria omenirii, fapt ce a dus la creșterea importanței resurselor de comunicație.

Schimbul de informații reprezintă motivația existenței rețelelor de calculatoare interconectate, în cadrul cărora se detașează mediul de rețele extrem de complex constituit de Internet.

Noțiunea **internet** reprezintă o colecție de rețele separate fizic, interconectate pentru a forma o singură rețea logică. **Internet** (scris cu I mare) este rețeaua mondială ce interconectează rețelele din diferitele părți ale planetei într-o singură rețea logică, fig. 8.1.

Internet formează un mediu informațional și de calcul, oferind un volum imens de servicii și resurse: biblioteci și baze de date, fiind în același timp și o imensă comunitate de persoane din toate domeniile vieții economico-sociale, situate în diverse puncte geografice, care pot oricând să partajeze informații.

Mediul Internet este eterogen, nu este proprietatea unui guvern, a unei companii sau universități, nu este o singură rețea, ci un grup de rețele aranjate din punct de vedere logic într-o ierarhie, nu constituie o componentă software/ hardware de sine stătătoare și este utilizat zilnic de oameni de toate specializările și interesele imaginabile.

Internetul permite interconectarea calculatoarelor indiferent de platformă. Acest lucru a devenit posibil prin faptul că s-au stabilit o serie de reguli privind comunicația între calculatoare. Aceste reguli sunt denumite **protocoale** și definesc modul de lucru al aplicațiilor pentru a se face înțelese între ele. Dacă rețeaua la care suntem conectați este Internet, atunci vom depinde de o colecție de protocoale reunite sub denumirea TCP/IP. Suita TCP/IP este constituită dintr-o mulțime de protocoale, fiecare dintre ele asigurând transferul datelor în rețea într-un format diferit și cu opțiuni diferite. În funcție de necesitățile aplicației, putem utiliza unul sau altul dintre protocoalele suitei TCP/IP pentru transmiterea informațiilor pe Internet.

Câteva dintre beneficiile aduse de folosirea Internetului sunt:

– schimb rapid și comod de informații prin utilizarea unor servicii specializate ca: poșta electronică; transferul de fișiere, de imagini, a secvențelor audio și video; vizualizarea unor fișiere cu informații de tip text etc.;

– se pot primi informații și se pot face actualizări regulate ale subiectelor de interes prin intermediul listelor de distribuție prin e-mail (*mailing lists*) organizate pe subiecte de interes, fiecare membru al grupului primind automat informațiile care apar în rețea;

– e permis accesul la mii de arhive informaționale din întreaga lume, prin intermediul unor servere specializate în gestiunea și rezolvarea cererilor de vizualizare și expediere a componentelor arhivelor;

– se largesc posibilitățile de divertisment etc.

8.1. Istoricul Internetului

Precursorii rețelei mondiale numită Internet sunt două rețele apărute în Statele Unite: ARPANET a Departamentului Apărării al SUA și NSFNET a Fundației Naționale de Știință.

ARPANET

La mijlocul anilor '60, în plin Război Rece, Departamentul Apărării al SUA a vrut să creeze o rețea care să poată fi folosită în cazul declanșării unui război nuclear. În acea perioadă rețelele telefonice tradiționale cu comutare de circuite erau vulnerabile sub aspectul performanței – pierderea unei linii sau a unui comutator ducea la reducerea considerabilă a comunicărilor din rețea. Proiectul a fost dezvoltat de Agenția de Cercetare pentru Proiecte Avansate a Departamentului Apărării – ARPA.

Agenția a apelat la mai multe universități și firme pentru dezvoltarea acestui proiect. Proiectul inițial prevedea ca subrețeaua să fie constituită din minicalculatoare conectate prin linii de transmisie, astfel încât fiecare calculator să fie legat de cel puțin alte două calculatoare, pentru a asigura siguranța în funcționarea rețelei. În cazul în care unele linii sau calculatoare se defectau, mesajele puteau fi dirijate automat pe căi alternative.

Evoluțiile ulterioare au arătat că protocoalele ARPANET existente nu erau potrivite pentru a rula pe mai multe rețele. Astfel a apărut protocolul TCP/IP, care a fost proiectat special pentru comunicarea inter-rețele, obiectiv esențial în condițiile în care tot mai multe rețele de mici dimensiuni erau legate la ARPANET. Pentru a încuraja adoptarea noilor protocoale, ARPA a încheiat contracte cu Universitatea California din Berkeley, pentru integrarea protocoalelor în Berkeley Unix. Cercetătorii de la Berkeley au dezvoltat o interfață de programare cu rețeaua și au scris numeroase aplicații, utilitare și programe de administrare care să simplifice interconectarea. Aceste produse soft au răspuns necesităților concrete ale multor universități care dispuneau de câteva minicalculatoare conectate într-un LAN.

În anii '80, la ARPANET s-au conectat multe alte rețele. Pentru o accesare cât mai eficientă a calculatoarelor într-o inter-rețea de dimensiuni tot mai mari s-a creat sistemul numelor de domenii (DNS – *Domain Naming System*), care gestiona calculatoarele în domenii și punea în corespondență numele calculatoarelor cu adresele IP. DNS a fost ulterior preluat de Internet, ca un sistem de baze de date distribuit, generalizat, folosit pentru a memora informații referitoare la procedurile de atribuire a numelor.

În 1983, ARPANET conținea sute de calculatoare, era stabil și se bucura de succes. În acest moment, ARPA a încredințat administrarea rețelei Agenției de Comunicații a Apărării (DCA – *Defense Communications Agency*), care a izolat partea militară a rețelei într-o rețea numită Milnet și a prevăzut porți stricte între aceasta și subrețeaua de cercetare rămasă. Rețeaua Milnet există și astăzi.

În 1990, ARPANET era deja surclasat de rețelele mai moderne cărora le dăduse naștere; a fost închis și demontat, dar contribuția sa covârșitoare în crearea rețelei globale Internet rămâne actuală.

NSFNET

La sfârșitul anilor '70, ARPANET avea un impact enorm asupra cercetării universitare din SUA, deoarece permitea cercetătorilor să partajeze date și să colaboreze la diverse proiecte de cercetare. Cu toate acestea, nu toate universitățile aveau contracte de cercetare cu Departamentul Apărării, contracte necesare pentru conectarea la ARPANET. În încercarea de a realiza un acces universal, Fundația Națională de Știință din SUA (NSF – *National Science Foundation*) a organizat o rețea virtuală numită CSNET, care asigură suport pentru linii telefonice și avea conexiuni cu ARPANET și cu alte rețele.

În 1984, NSF a inițiat dezvoltarea unei rețele de mare viteză, succesoare a ARPANET-ului, care să fie deschisă tuturor grupurilor de cercetare din universități. Astfel, s-a constituit prima rețea de arie largă bazată pe TCP/IP, care conținea o subrețea asemănătoare cu cea din ARPANET, formată din 6 supercalculatoare aflate în orașe răspândite pe cuprinsul SUA. Ulterior, NSF a finanțat peste 20 de rețele regionale care s-au conectat la rețeaua principală, legând mii de universități, laboratoare de cercetare, biblioteci și muzee. Rețeaua astfel formată a fost denumită NSFNET.

Treptat, cererile tot mai numeroase de conectare la NSFNET au început să depășească posibilitățile de finanțare guvernamentale și, în plus, numeroase organizații comerciale interesate de conectare nu puteau realiza acest lucru din cauza statutului NSF. Primul pas spre comercializare a fost apariția corporației nonprofit ANS (*Advanced Networks and Services*), constituită de firmele MERIT, MCI și IBM. În 1990, ANS a preluat NSFNET și a înlocuit legăturile de comunicare crescând viteza de la 1,5 Mbps la 45 Mbps, formând ANSNET.

În decembrie 1991, Congresul SUA a autorizat crearea unei noi rețele naționale de cercetare și învățământ, NREN (*National Research and Educational Network*), care era un succesori mai rapid (funcționa la viteze de ordinul gigabiților) al NSFNET-ului. Obiectivul urmărit era o rețea națională la viteza de 3 Gbps, funcțională înainte de sfârșitul secolului, ca un prototip al unei super-magistrale informaționale.

Rețele comparabile cu NSFNET au apărut și în Europa, cum ar fi rețeaua EBONE axată pe cercetare sau EuropaNET – pe domeniul comercial. În plus, fiecare țară europeană are una sau mai multe rețele naționale (similare cu rețelele regionale NSF).

INTERNET

După 1 ianuarie 1983, TCP/IP a devenit unicul protocol oficial al ARPANET-ului, ceea ce a adus creșterea considerabilă a numărului de utilizatori, calculatoare și rețele conectate la ARPANET. Această creștere a devenit exponențială după integrarea rețelelor ARPANET și NSFNET. La mijlocul anilor '80, oamenii au început să privească inter-rețeaua ca o rețea globală de sine stătătoare și să o numească Internet.

Prin extinderea rețelei Internet din Statele Unite s-a format o rețea mondială Internet care permite unui număr extrem de mare de utilizatori din întreaga lume să aibă acces la un imens volum de informații depuse în baze informaționale aflate în noduri speciale ale rețelei și transferate folosind protocolul de referință TCP/IP.

Creșterea numărului de calculatoare conectate la Internet se datorează și conectării unor rețele deja existente (rețeaua de fizică spațială NASA, rețeaua de sisteme de calcul a IBM-ului etc.).

Calculatoarele personale se pot conecta la Internet, folosind o linie telefonică uzuală, un modem (pentru conversiile de date între formele analogică și digitală) și un program software folosit pentru realizarea comunicației. Aceste calculatoare primesc uzual o adresă IP temporară și pot avea acces la serviciile de informare și comunicare specifice Internet-ului prin schimburi de date cu alte calculatoare din Internet; transferurile de informații fiind intermediare de router-ul furnizorului de servicii la care sunt conectate.

Cele mai populare servicii disponibile în mediul Internet sunt:

- 1 **Poșta electronică (*E-mail*)** – permite transmiterea de mesaje private și de fișiere atașate mesajelor, uneia sau mai multor persoane.
- 1 **Liste de e-mail-uri (*Mailing List*)** – permite unui grup de oameni să poarte discuții de grup prin intermediul poștei electronice și oferă o modalitate de a distribui știri între membrii grupului.
- 1 **Grupuri de știri (*Usenet newsgroups*)** – permite discuții de grup folosind un sistem de servere de știri pentru stocarea mesajelor din peste 10000 de teme.
- 1 **Conversații în timp real (*chat online*)** – oferă o modalitate pentru derularea discuțiilor în timp real; participanții citesc mesajele scrise unul altuia, la interval de câteva secunde de când acestea au fost scrise.
- 1 **Conferințe de tip voce și video** – permit transmiterea de mesaje vocale, însoțite de imagini în timp real, precum și partajarea altor aplicații.
- 1 **WWW (*World Wide Web*)** este un sistem distribuit de pagini legate între ele, pagini ce pot conține text, imagini, sunete, video și alte tipuri de informații.
- 1 **Transfer de fișiere** – permite descărcarea fișierelor de pe servere publice de fișiere, inclusiv o mulțime de programe.

Caracterul academic, guvernamental și industrial pe care l-a avut Internetul, până în 1990, s-a transformat o dată cu apariția noii aplicații WWW (World Wide Web), care a adus în rețea milioane de utilizatori neprofesioniști.

WWW a fost inventat de fizicianul Tim Berners Lee de la CERN și a făcut ușor de folosit facilitățile existente. Prin programele de navigare (Mosaic, Netscape, Internet Explorer) apărute, WWW a făcut posibil ca un site să pună la dispoziție un număr de pagini de informație conținând text, imagini, sunete, video și legături între pagini (hipertext). Acest sistem s-a dovedit foarte util pentru informarea utilizatorului în domenii diverse. În scurt timp, au apărut diverse tipuri de pagini: hărți, tabele cu cotații de bursă, cataloage de bibliotecă, programe radio înregistrate, pagini personale etc.

Extinderea Internet-ului urmează o curbă exponențială, o dată cu creșterea performanțelor și accesibilității serviciilor oferite.

8.2. Modul de lucru al Internetului

Rețeaua Internet este o rețea cu comutare de pachete. Serverele din Internet sunt conectate între ele prin intermediul routerelor, legând rețele diferite de tip Ethernet, Token Ring, linii telefonice etc.

În vederea transmiterii datelor, mesajele sunt împărțite în componente de dimensiuni mai mici, numite pachete și care, pe lângă conținutul propriu-zis, au atașate informațiile de adresare necesare. Neavând legături directe cu toate celelalte routere, un router decide traseul optim pe care trebuie să-l urmeze un pachet până la destinație, folosind informația de adresă conținută în pachet.

Regulile folosite pentru a stabili cum și unde să se livreze pachetul sunt cuprinse în protocoale. Protocolul Internet (IP) este format dintr-un set de astfel de reguli, astfel că fiecare router va cunoaște ce trebuie să facă cu pachetele cu date care ajung la el. Protocolul IP folosește o schemă de adresare care face posibilă identificarea fiecărui calculator conectat la rețea prin intermediul unei adrese unice.

Identificarea mașinilor din Internet se realizează folosind adresele Internet sau adresele IP. Fiecare calculator conectat la Internet trebuie să aibă o adresă IP unică, pentru a putea comunica eficient cu celelalte calculatoare conectate la Internet. Adresele IP sunt segmentate într-o structură ierarhică și sunt formate din 4 numere cuprinse între 0 și 256, separate între ele prin puncte. Adresa Internet (IP) este memorată pe 4 octeți și este alcătuită din două părți: **adresa rețelei** din care face parte calculatorul și **adresa calculatorului**. Alegerea tipului de adresă se face în funcție de numărul de calculatoare și de gruparea acestora în diverse subrețele, ținând cont și de extinderile viitoare.

Astfel, adresele IP se împart în 3 clase, împărțire realizată în funcție de dimensiunile celor două câmpuri (adresa rețelei și adresa calculatorului):

1. **Adresele Internet de clasă A** sunt folosite pentru câteva sute de rețele care suportă mii de mașini și este alcătuită din 8 biți – adresa de rețea și 24 biți adresa calculatorului.

2. **Adresele Internet de clasă B** sunt folosite pentru câteva sute sau mii de mașini. Adresa din această clasă este alcătuită din 16 biți pentru adresa de rețea și 16 biți de adresa calculatorului.

3. **Adresele Internet de clasă C** pentru milioane de rețele care au maxim 256 de mașini fiecare. Această adresă este alcătuită din 24 biți adresa de rețea și din 8 biți – adresa calculatorului.

Adresa unei mașini vizibile din orice nod al Internet-ului se numește **adresă reală**. Din motive de securitate și legate de numărul extrem de mare de calculatoare din Internet, care nu pot fi referite în totalitate folosind adresele de 4 octeți, pentru adresarea calculatoarelor din rețelele locale se folosesc de obicei adrese false, care vor fi gestionate doar în interiorul rețelei respective de către serverul (serverele) acesteia, prin mecanisme specifice. Serviciile de bază de informare și comunicare din Internet sunt asigurate însă prin intermediul mașinilor cu adrese IP reale care pot fi servere de e-mail, servere de știri, servere web, servere ftp. Acestea pot fi „arodate“ rețelelor locale, asigurând și comunicarea cu calculatoarele din interiorul acestora prin intermediul unor protocoale adecvate.

Protocolul TCP preia informația ce trebuie transmisă și o împarte în mai multe părți cărora le atribuie câte un număr. Pentru a transmite prin rețea secvențele astfel obținute se folosește câte un plic TCP cu informația scrisă pe el. Plicul TCP este introdus apoi într-unul IP și este transmis în rețea. Imediat ce există informație de transmis într-unul din plicurile IP, rețeaua transportă acel plic prin liniile de comunicație. La receptor, un produs software care folosește TCP colectează plicurile, extrage datele și le ordonează după numărul fiecărui plic. Dacă lipsește ceva, cere transmițătorului să retransmită datele respective. După primirea tuturor datelor și aranjarea lor în ordinea corectă, ele se transmit unui program de aplicații ce folosește acest serviciu de comunicație.

Protocolul TCP creează impresia existenței unei conexiuni fizice directe între orice sursă și destinație.

În anumite situații, se poate folosi un protocol mai simplu, și mai ieftin decât TCP, numit UDP (*User Datagram Protocol*), dar acesta nu se ocupă de mesajele pierdute, și nici de menținerea datelor în ordinea corectă (mesajele transmise sunt scurte, iar dacă răspunsul nu apare într-un interval de timp prestabilit, mesajul va fi retransmis).

Conectarea unui calculator la Internet

Pentru ca un calculator să poată fi conectat la Internet trebuie folosit un furnizor de servicii (Internet Service Provider – ISP), care oferă, contra cost, unul sau mai multe conturi pentru conectare la Internet.

Un calculator este conectat la Internet dacă este legat la un alt calculator sau la o rețea care este la rândul ei conectată la Internet.

Există mai multe metode de conectare la Internet, fiecare necesitând diferite tipuri de echipamente hardware:

1. Conectare prin dial-up – presupune existența unui modem instalat pe calculator și a unei linii telefonice pentru conectarea la un calculator al furnizorului de servicii Internet. Majoritatea furnizorilor de servicii de tip dial-up permit conectarea la viteze de 14,4 kbps, 28,8 kbps și 56 kbps. Viteza de transfer a informațiilor depinde atât de viteza conexiunii, cât și de viteza suportată de modem. Folosind acest tip de conexiune, calculatorul se conectează numai atunci când se dorește utilizarea unui serviciu Internet, după care se deconectează.

2. Conectare folosind linii de tip ISDN, ADSL și linii telefonice dedicate

Unii furnizori de servicii Internet permit conectarea la viteze mai mari decât cele permise de liniile telefonice obișnuite. *Integrated Services Digital Network* (ISDN) și *Asymmetric Subscriber Digital Line* (ADSL) sunt două tipuri de linii telefonice digitale, de viteză mare care oferă o modalitate mai rapidă de conectare la Internet. Unele companii de telefonie oferă linii speciale de tip ISDN sau ADSL și echipamentele hardware speciale pentru conectarea calculatoarelor la aceste linii speciale.

ISDN este o linie telefonică îmbunătățită care poate fi utilizată atât pentru accesul rapid la Internet, cât și pentru convorbiri telefonice obișnuite. Folosind o singură linie se poate naviga pe Internet în timp ce se vorbește la telefon. ISDN este în totalitate digitală, acest lucru însemnând că nu mai e necesară transformarea semnalului din digital în analog pentru transmisie și invers la recepție.

ADSL este o tehnologie mai nouă și optimizează descărcarea fișierelor de volum mare pe calculator.

Dacă se dorește conectarea continuă a calculatorului la Internet, se utilizează, pentru conectarea calculatoarelor, linii telefonice închiriate. Există diferite viteze de transmisie a informațiilor pe aceste linii, cele mai răspândite fiind liniile de tip T1 care permit transferul informațiilor la viteza de 1,5 Mbps și T3 la viteza de 44 Mbps. Pot fi închiriate și fracțiuni ale liniei T1.

3. Conectare folosind cablu TV și DSS

Unele companii ce oferă servicii TV prin cablu oferă și accesul la Internet folosind același cablu și un modem special pentru conectarea la Internet.

DSS (*Digital Satellite Systems*) sau difuzarea informațiilor folosind sateliți, presupune utilizarea unei antene, a unui cablu coaxial, a unui adaptor special pentru calculator și a unui software dedicat pentru conectarea la Internet. Datele sunt recepționate la o viteză mare, *via* satelit, dar sunt transmise folosind o conexiune de tip dial-up.

4. WebTV

Web TV presupune folosirea unui televizor și nu a unui calculator pentru conectarea la Internet. WebTV este cea mai răspândită modalitate de conectare la Internet folosind un televizor și este dezvoltată, în parte, de Microsoft. Pentru utilizarea WebTV este necesară existența unui receptor WebTV care conectează televizorul la linia telefonică; ecranul televizorului va fi folosit pe post de monitor, telecomanda pentru navigare pe Web și tastatura pentru transmiterea și recepționarea mesajelor de poștă electronică.

Alegerea furnizorului de servicii Internet

Indiferent de modalitatea de conectare aleasă, aceasta presupune selectarea unui furnizor de servicii. Principalele criterii care trebuie avute în vedere la alegerea furnizorului de servicii sunt:

1 **Existența unui număr de telefon local** – majoritatea furnizorilor de servicii Internet oferă multe numere, pentru conectarea la Internet. Este de dorit ca furnizorul de servicii selectat să aibă și un număr local, pentru a nu apărea întârzieri și din cauza conectării la o centrală telefonică aflată la mare distanță.

1 **Prețul** – variază în funcție de viteza maximă permisă pentru conectare, de tipul abonamentului: cu conectare 24 ore din 24, 7 zile din 7 sau doar într-un anumit interval orar.

1 **Viteza de conectare și tipul de conectare acceptat.**

1 **Accesibilitate** – înaintea alegerii furnizorului de servicii este bine să vă interesați la alți abonați ai furnizorului dorit, dacă au probleme datorate imposibilității conectării la Internet, din cauza liniilor ocupate.

Există mai multe tipuri de servicii pe care le poate oferi un cont Internet:

1 **Căsuțe poștale de tip POP3** – aproape sigur contul de Internet va permite utilizarea serviciului de poștă electronică și va oferi una sau mai multe căsuțe poștale și adresele corespunzătoare, pe un server de tip POP3.

1 **Spațiu pentru un site Web** – multe conturi de Internet prevăd alocarea unui spațiu de mici dimensiuni pe un server Web, astfel încât se poate stoca un site Web propriu, accesibil de pe orice calculator conectat la Internet. Pentru un spațiu mai mare se percep, în general, taxe suplimentare.

1 **Găzduirea unui domeniu** – presupune existența unui nume de domeniu propriu; contul de poștă electronică și adresa site-ului Web vor aparține astfel propriului domeniu și vor fi stocate pe serverul furnizorului de servicii. Dacă se dorește crearea unui site Web mai mare sau a unuia sigur, a unor aplicații de comerț electronic sau sunt necesare opțiuni avansate pentru rularea scripturilor de pe site, trebuie utilizat un server propriu pentru găzduirea site-ului.

8.3. Sistemul de nume de domeniu

Este dificil de reținut și folosit adresa IP a calculatorului cu care dorim să conversăm. Din acest motiv, proiectanții Internet-ului au dezvoltat sistemul **DNS** (*Domain Name System*) care permite referirea calculatoarelor prin nume ca de exemplu *ftp.microsoft.com* sau *www.ase.ro*, în locul adresei IP a calculatorului.

DNS a fost creat pentru a putea aloca și gestiona pentru fiecare calculator conectat la Internet a câte un nume simbolic, asociat adresei IP a calculatorului respectiv. DNS este o metodă ierarhică, distribuită de organizare a spațiului de nume al Internetului.

8.3.1. Spațiul de nume

La început, Internetul utiliza un sistem structurat pe un singur nivel pentru a asigura nume calculatoarelor. Cu alte cuvinte, numele dat unui calculator nu reprezenta în nici un fel o relație între acesta și rețeaua căreia îi aparținea.

În perioada de început a Internet-ului, un astfel de sistem nu reprezenta o problemă – era vorba despre un număr redus de sisteme. O dată cu trecerea timpului, Internet-ul a crescut foarte mult ajungând astăzi să interconecteze zeci de mii de rețele, fiecare dintre acestea, la rândul ei, conținând o mulțime de calculatoare. Deoarece asignarea câte unei adrese unice pentru milioanele de calculatoare a depășit cu mult posibilitățile unei singure organizații, sistemul inițial de atribuire de nume calculatoarelor a evoluat într-un sistem ierarhic. Practic, astăzi, atribuirea de adrese unice cade în responsabilitatea mai multor companii și organizații, aflate pe diferite nivele ierarhice.

Prin sistemul numelor de domenii, într-un nume asignat unei mașini, există un număr variabil de domenii (cel mult 5), separate prin „.”; fiecare domeniu corespunde unui anumit grup, ultimul domeniu din nume având nivelul cel mai „înalt”. Domeniile se restrâng succesiv de la dreapta la stânga. Componentele numelor pot avea o lungime de maximum 64 de caractere, întregul nume nu poate să depășească 255 de caractere și nu se face distincție între literele mari și cele mici.

În vârful ierarhiei se află rădăcina. Ca și directorul rădăcină de pe un calculator, rădăcina sistemului DNS nu are nici un nume. Toate celelalte sisteme au câte un nume. În continuare, DNS-ul divizează fiecare domeniu în subdomenii. Nivelul imediat inferior rădăcinii DNS-ului este constituit din trei domenii:

1. *Arpa* – este un domeniu special care mapează adresele IP zecimale în nume de domenii și nu domeniile în adrese IP zecimale.

2. Domeniile organizaționale generice, reprezentate prin etichete alcătuite din trei litere, ca de exemplu *com*, *edu* sau *gov*.

3. Domeniile geografice reprezentate prin etichete alcătuite din două litere (codificarea țărilor) așa precum se specifică în documentul ISO 3166.

Grupul domeniilor organizaționale cuprinde șapte categorii de bază. În cadrul tabelului următor sunt prezentate domeniile organizaționale.

Domeniu	Descriere
Com	Organizații comerciale, de afaceri
Edu	Organizații educaționale, universități
Gov	Organizații guvernamentale din SUA
Int	Organizații internaționale

Mil Organizații militare din SUA
Net O rețea care nu se încadrează în nici una dintre celelalte categorii
Org O organizație ce nu se încadrează în nici una dintre categoriile enumerate

Sistemul ierarhic distribuie responsabilitatea atribuirii de nume la diferitele nivele ale ierarhiei. Astfel, *Internet Network Information Center* (InterNIC) se ocupă doar de domeniile generice. InterNIC transmite responsabilitatea atribuirii de nume diferitelor organizații. Fiecare organizație este responsabilă pentru o anumită porțiune a structurii arborelui DNS. Ariile de responsabilitate sunt numite **zone**. Organizațiile responsabile de o anumită zonă pot să treacă la divizarea zonei și să transmită responsabilitatea atribuirii numelor altor organizații. Această subdiviziune continuă până când se ajunge în situația în care o singură persoană poate să-și asume responsabilitatea atribuirii numelor într-o zonă bine definită. O astfel de persoană poartă numele de **administrator DNS**.

Unui nume DNS i se pun în corespondență mai multe informații decât strict adresa IP corespunzătoare: tipul gazdei (server de mail, server DNS etc.) și perioada de timp în care asocierea este valabilă. Unui PC conectat la Internet printr-un router al unui furnizor de servicii și folosind o linie telefonică, i se va atribui o adresă IP temporară, a cărei asociere cu calculatorul respectiv trebuie să fie valabilă doar pe durata conexiunii. În schimb, serverul furnizorului de servicii și serverele de e-mail sau web ale diverselor instituții, servere care trebuie să poată fi accesate oricând, trebuie să aibă adrese IP stabile. Mulțimea de informații pusă în corespondență cu o adresă IP se numește înregistrare de resurse.

Fiecărui domeniu i se asociază o multime de înregistrări de resurse care se poate reduce la adresa IP. De fapt, prin DNS se stabilește corespondența între numele de domenii și înregistrările de resurse corespunzătoare, reținute într-un fișier specific domeniului. Acest fișier va fi interogat pentru aflarea adresei IP a unui nume DNS. Practic, o înregistrare de resurse este un 5-uplu care conține: numele domeniului, timpul său de viață, tipul înregistrării (adresă IP, domeniu care acceptă poșta electronică, numele serverului de domeniu, nume de domeniu etc.) păstrat într-o formă codificată, clasa (informație Internet sau non-Internet) și o valoare dependentă de tipul înregistrării (un număr – adresă Internet, un nume de domeniu sau un șir de caractere care descrie elementul). Aceste informații se rețin pe serverele DNS în fișiere speciale.

8.3.2. Servere de nume

În sistemul DNS, serverele de nume sunt folosite pentru adresarea fișierelor de host-uri reținute de toate calculatoarele gazdă.

Fiecare server de nume va ști astfel adresele anumitor zone (de exemplu, într-o rețea locală) și adresele altor servere de nume. Folosirea unui singur server de nume pentru întreaga rețea nu este convenabilă. Astfel, solicitarea unei adrese poate fi rezolvată local sau prin intermediul altor servere de nume care cunosc acea adresă. Serverele de nume aflate la distanță vor reține în memorie înregistrările de resurse pe o durată proporțională cu timpul de viață din înregistrarea corespunzătoare. Responsabilitățile serverelor de nume se pot reprezenta sub forma unor structuri ierarhice în care informația despre nume și adresă se menține în mod distribuit, în cadrul serverului responsabil și nu în întreaga rețea.

8.3.3. Înregistrarea numelor de domenii

Pentru înregistrarea unui nume de domeniu este necesar un calculator conectat la Internet, căruia îi va fi asociat numele și alte două calculatoare gazdă, conectate și ele la Internet, care vor oferi serviciul de nume pentru domeniul înregistrat.

Gestiunea zonelor **edu**, **com**, **net** și **org** este asigurată de serviciile de înregistrare ale InterNIC, prin intermediul site-ului aflat la adresa www.internic.net.

Pentru înregistrare trebuie parcurși următorii pași:

1. Se verifică dacă numele domeniului care se dorește a fi înregistrat există deja; pentru aceasta se folosește secțiunea WHOIS de pe pagina principală a InterNIC.
2. Doar dacă domeniul solicitat nu există încă, se solicită furnizorului de servicii Internet să ofere serviciu de nume de domeniu pentru domeniul ales; de obicei acesta presupune plătitarea unui abonament.
3. Se completează formularul online aflat pe site-ul InterNIC; formularul conține informații despre numele, adresa, numerele de telefon și fax, adresa de e-mail, persoane de contact, adresele IP ale celor 2 servere de nume de domeniu.
4. Dacă toate informațiile introduse sunt corespunzătoare, InterNIC-ul trimite confirmarea înregistrării domeniului și factura pentru plata domeniului.

Pentru înregistrarea domeniilor în zonele corespunzătoare țărilor, zone de genul ro, us, uk etc. trebuie să se apeleze la organizațiile desemnate să gestioneze domeniul din țara respectivă. În România, de acest lucru se ocupă RNC (Romanian National Computer Network); adresa web care poate fi folosită pentru înregistrare de domenii în zona.ro, fiind www.rnc.ro. O listă cu organizațiile care gestionează domeniile corespunzătoare fiecărei țări se găsește la adresa www.iana.org.

8.3.4. Servere, clienți și porturi

Multe dintre calculatoarele gazdă aflate pe Internet oferă servicii altor calculatoare conectate la Internet. Calculatoarele care oferă servicii altor calculatoare sunt numite *servere*. Calculatoarele conectate la Internet care folosesc serverele pentru a obține informații se numesc *clienți*.

De exemplu, când calculatorul se conectează la Internet și programul de e-mail descarcă mesajele primite, de pe serverul de e-mail al furnizorului de servicii Internet, acest program este un client de poștă electronică.

Principalele tipuri de servere folosite în mediul Internet sunt:

1 **Serverele de poștă electronică** – gestionează mesajele recepționate și cele transmise. Mai precis, serverele de tip *Post Office Protocol* (sau POP3) stochează e-mail-urile sosite, iar serverele de tip *Simple Mail Transfer Protocol* (SMTP) gestionează e-mail-urile transmise. Clienții de e-mail primesc mesajele recepționate, transmit mesajele către un server de e-mail și permit citirea, scrierea, salvarea și imprimarea mesajelor.

1 **Serverele Web** stochează pagini web și transmit paginile ca răspuns la cererile provenite de la clienții web, adică de la browserele web.

1 **Serverele FTP (*File Transfer Protocol*)** stochează fișierele care pot fi transferate pe sau de pe un calculator care are instalat un client FTP.

1 **Serverele de știri** stochează articole cu informații pentru grup, informații care pot fi citite sau transmise prin intermediul unui client de știri.

1 **Serverele de IRC** permit comunicarea online în rețeaua Internet folosind un client IRC.

Un calculator gazdă poate rula mai multe tipuri de programe de tip server. Pentru a putea realiza acest lucru, fiecare tip de server răspunde pachetelor transmise unui port anume. Porturile sunt numerotate și folosirea lor este standardizată pe Internet. Cele mai răspândite porturi și serviciile corespunzătoare lor sunt:

Numărul portului

Serverul

21

FTP

23	Telnet
25	SMTP
80	WWW
110	POP3
194,6667	IRC
532	Usenet newsgroups

8.4. Poșta electronică

Poșta electronică sau e-mail-ul face parte din categoria aplicațiilor consacrate ale rețelelor de calculatoare, fiind utilizată de un număr din ce în ce mai mare de persoane. Poșta electronică s-a dovedit mult mai eficientă decât cea clasică, deoarece mesajele electronice ajung foarte repede la destinație și permit transmiterea unor informații de diverse tipuri.

La ora actuală, numărul mesajelor de poștă electronică îl depășește cu mult pe cel al scrisorilor clasice și asigură o comunicare eficientă între persoane, indiferent de localizarea lor geografică. Acest schimb rapid de idei constituie o premisă importantă pentru colaborarea între persoane și s-a dovedit extrem de util atât în cercetare și educație, cât și în industrie sau comerț.

Poșta electronică (*Electronic Mail* sau prescurtat *E-Mail*) este un sistem care permite unui utilizator individual să transmită un mesaj altui utilizator, mesajul fiind livrat într-o cutie poștală (*mail box*) unde destinatarul îl va găsi mai târziu. Din punct de vedere al emițătorului, pot exista unul sau mai mulți adresanți.

Avantajele poștei electronice sunt evidente: viteză, siguranță în expediere, posibilitățile de a adăuga textului imagini și sunet, apoi facilitatea de redirectare, și nu în ultimul rând posibilitatea de prelucrare și reexpediere a mesajelor.

Un sistem de poștă electronică este format din două componente principale: un client e-mail și un server e-mail. Un client e-mail este o stație de lucru sau PC pe care rulează un program numit agent utilizator. Acesta oferă interfața utilizatorului cu sistemul de poștă electronică și oferă facilități de a crea, trimite și recepționa mesaje (e-mail-uri), precum și posibilitatea gestionării acestora de fiecare utilizator.

Serverul e-mail trebuie să permită păstrarea mesajelor primite de toți utilizatorii care sunt înregistrați pe acest server. În plus, serverul trebuie să dispună de un pachet software – agent utilizator server– care să interacționeze cu agentul utilizator de pe fiecare client și care, în plus, trebuie să gestioneze transferul mesajelor e-mail pe Internet. Această componentă software este numită agent pentru transferul mesajelor și se ocupă cu trimiterea și recepționarea mesajelor e-mail către/de la alte servere e-mail care sunt conectate direct la Internet.

8.4.1. Concepte de bază

Poșta electronică nu operează cu concepte sofisticate. O parte dintre aceste concepte au fost preluate chiar de la sistemul de poștă clasic: cutia poștală, mesaj sau scrisoare, adresă expeditor, adresă destinatar.

8.4.1.1. Cutia poștală

Toate mesajele primite de un abonat pe serverul de e-mail la care este conectat sunt memorate în același fișier având numele dat de abonat, fișier care se numește cutie poștală de sistem – *system mailbox*.

După ce abonatul își verifică cutia poștală mesajele sunt transferate în cutia poștală personală aflată pe calculatorul de la care s-a conectat. Utilizatorul poate opta pentru păstrarea unei copii a mesajelor pe serverul de *e-mail*, sau pentru ștergerea acestora, o dată ce au fost transferate pe calculatorul personal.

Mesajele sunt păstrate, local, într-una dintre următoarele trei secțiuni, în funcție de proveniența lor:

- **Inbox**, mesajele primite,
- **Outbox**, mesajele expediate,
- **Trash**, mesajele șterse.

Se pot crea în plus și alte secțiuni care asemenea unui *folder* vor putea păstra mesajele salvate, copiate sau mutate aici de utilizator.

8.4.1.2. Mesajele

Termenul de mesaj înlocuiește foarte adesea termenul de scrisoare pentru că este mai cuprinzător. Prin e-mail se pot transmite alături de text și imagini, sunet, programe, elemente care în nici un caz nu pot fi interpretate ca scrisori.

Mesajul are două părți: antetul mesajului și conținutul (corpul) mesajului, iar programul de poștă electronică mai asociază implicit fiecărui mesaj un indicator de stare.

Antetul

Antetul este alcătuit dintr-o secvență standard de informații dintre care unele sunt introduse de operator obligatoriu sau opțional, iar altele sunt câmpuri cu valori implicite generate de programul de poștă electronică.

Câmpurile completate automat de programul de poștă sunt:

- **From:** – care conține adresa de e-mail a expeditorului;
- **data:** – la care este trimis mesajul;

Câmpurile care trebuie introduse de utilizator sunt următoarele:

- **To:** – adresa destinatarului, acest câmp e obligatoriu;
- **Subject:** – descrierea, pe scurt, a conținutului scrisorii; acest câmp este opțional;
- **Cc:** – *carbon copy*, în acest câmp se pot scrie adresele destinatarilor care vor primi copii identice ale mesajului, adrese separate prin virgulă; fiecare destinatar va vedea lista celorlalți corespondenți în antetul mesajului; este un câmp opțional;
- **Bcc:** – *blind carbon copy*, ca și în cazul *carbon copy*-urilor, destinatarii ale căror adrese sunt înscrise în acest câmp vor primi același mesaj, doar că, în acest caz, în antetul mesajului nu vor mai fi prezente și adresele celorlalți corespondenți.

Corpul mesajului

Acesta reprezintă textul propriu-zis al mesajului. Programele de poștă electronică dispun de un editor propriu cu un set minim de comenzi pentru redactarea și corectarea mesajelor.

Mesajele pot fi redactate *off-line* și cu editoare de texte obișnuite, de exemplu Word și apoi inserate în mesajul electronic prin tehnica „*cut & paste*“. Un text mai lung se poate salva într-un fișier ASCII și apoi atașat mesajului utilizând facilitatea „*File Attachment*“ disponibilă la mai toate programele de e-mail.

Vorbind de ultimele versiuni ale programelor de e-mail, acestea au de acum posibilitatea de a trimite și de a primi mesaje ce conțin elemente multimedia, secvențe HTML, așa cum apar ele pe Web.

Pentru creșterea vitezei de transmitere/recepție se poate opta numai pentru transmisia textului, adică opțiunea „*send plain text only*“.

Indicatorul de stare

Indicatorul de stare este un caracter creat și modificat automat de program pentru a informa utilizatorul despre natura mesajului și ultima operație de prelucrare suferită de mesajul respectiv. Putem ști dacă este vorba de un mesaj nou necitit, de un mesaj expediat ca răspuns, de un mesaj șters logic, de un mesaj care nu trebuie transmis mai departe, de un mesaj important, sau un mesaj care are un fișier atașat etc. Valorile sau simbolurile acestui indicator se afișează atunci când vizualizăm sumarul unei cutii poștale.

Tabela index

Toate mesajele dintr-o cutie poștală, standard sau creată de utilizator, sunt inventariate într-o tabelă distinctă, asociată implicit fiecărei cutii poștale, tabelă numită „index“ sau „sumar“. Aici se încrieu automat o serie de elemente de identificare ale mesajului preluate din antetul acestuia: adresa expeditorului sau a destinatarului, data, subiectul, precum și indicatorul de stare.

Toate programele de poștă electronică ne permit să afișăm și să parcurgem acest sumar pentru a selecta după dorință scrisoarea pe care dorim să o deschidem pentru a o citi integral.

8.4.1.3. Adresa e-mail

Singurul indiciu pe care îl are sistemul de e-mail pentru a livra un mesaj este adresa destinatarului. Aceasta este de forma: nume_utilizator@domeniu. Numele utilizatorului este numele contului pe care acel utilizator îl deține. Pe baza domeniului dintr-o adresă e-mail se poate transfera mesajul pe mașina destinatarului, iar pe baza numelui din adresă se realizează livrarea locală a mesajului în căsuța poștală a destinatarului. Iată un exemplu de adresă e-mail:

tsurcel@ ase.ro

unde:

tsurcel – este *user name*, numele de login al utilizatorului;

ase.ro – este *domain name*, numele complet al domeniului pentru referirea calculatorului la care este conectat PC-ul de la care operează utilizatorul.

În locul numelui complet al domeniului se poate folosi și adresa IP a calculatorului. De exemplu, adresa e-mail **tsurcel@sunu.rnc.ro** poate fi înlocuită cu adresa **tsurcel.@192.162.16.31** cu care este identică.

8.4.1.4. Aliasuri – nicknames

Alias-ul sau „porecla“ este un cuvânt care se folosește pentru a substitui adresa unui corespondent sau un grup de adrese de corespondenți. Scopul substituirii este evident acela de a se evita tastarea adreselor lungi de e-mail, și implicit eliminarea riscului de a greși. Automat, la expedierea mesajului aliasul este însă înlocuit cu adresa reală a destinatarului.

Definirea unui *alias* – *nickname*, se face în mod diferit de la un program de poștă la altul. *Alias*-urile sunt memorate alături de alte informații utile în agende de adrese ce pot fi vizualizate și actualizate.

8.4.2. Funcționarea sistemelor de e-mail

Sistemele de poștă electronică au uzual două componente: una care permite utilizatorilor să citească și să transmită scrisori, componentă formată din programe locale, numită „agent utilizator“, iar cea de-a doua, care transportă mesajele de la sursă la destinație, prin aplicații care se execută în fundal și transferă mesajele se numește „agent de transfer de mesaje“.

„Agenții“ utilizator sunt programe care acceptă o varietate de comenzi pentru compunerea și primirea răspunsului la mesaje și pentru manipularea cutiilor poștale. Aceste programe pot avea diferite tipuri de interfețe, de la cele bazate pe meniuri și icon-uri la cele care acceptă comenzi sub forma unor succesiuni de caractere introduse de la tastatură. Astfel că, deși modul lor de utilizare diferă, funcțiile oferite, referitoare la trimiterea și citirea mesajelor, sunt aceleași.

Se mai poate spune că agenții utilizator gestionează cutiile poștale, afișându-le conținutul și așteptând „comenzi“ referitoare la mesajele din cutiile poștale, pe care le execută. Aceste comenzi pot fi de următoarele tipuri: afișare de mesaj, trimitere de mesaj, răspuns la un mesaj, ștergere de mesaj, mutarea unui mesaj, deplasarea pe următorul mesaj, citirea unei noi cutii poștale, părăsirea sistemului de mail.

„Agenții“ de transfer al mesajelor de la emițător la receptor au rol de transport, de a stabili o conexiune de la mașina sursă la cea destinație și de a transmite mesajul. Funcționarea agenților de transfer nu necesită intervenția utilizatorilor sistemului de mail.

8.4.2.1. Programe de interfață cu utilizatorul

Există o mare varietate de programe care permit utilizatorilor să folosească sistemul de e-mail într-un mod extrem de accesibil. Aceste programe pot avea o interfață vizuală, specifică aplicațiilor Windows (Microsoft Outlook Express, Eudora), sau o interfață bazată pe meniuri și comenzi (utilitarul Pine sub Linux). Indiferent de modul de utilizare, aceste programe asigură funcții specifice referitoare la prelucrarea mesajelor de e-mail:

- a) redactarea și expedierea mesajelor;
- b) primirea și memorarea mesajelor;
- c) editarea și reexpediția mesajelor;
- d) gestiunea cutiilor poștale;
- e) gestiunea agendei de adrese;
- f) tipărirea mesajelor;
- f) asigurarea securității mesajelor.

Aceste funcții sunt disponibile prin comenzile sistemului de meniuri propriu fiecărui program de poștă electronică.

Redactarea și expedierea mesajelor

Această funcție permite utilizatorului să-și compună textul scrisorii de la tastatură și să-l expedieze la adresa de e-mail pe care a indicat-o în antetul scrisorii.

Orice program de poștă electronică are încorporat propriul editor de texte ce oferă inclusiv funcții de analiză lexicală. În plus, editorul de texte poate lucra cu o agendă de adrese unde utilizatorul, în dreptul aliasului, a trecut adresa completă de e-mail a acestuia.

Dacă dorim neapărat, putem redacta mesajul și cu un editor de texte clasic, dar ne complicăm. Versiunile recente ale multor programe de poștă electronică pot include și transmite într-o scrisoare și elemente multimedia, imagini animate și sunet.

Primirea și memorarea mesajelor

Este funcția complementară celei dintâi. Utilizatorul nu trebuie să inițieze nici o acțiune pentru a primi și a păstra mesajele adresate de alți corespondenți. El le va găsi pur și simplu în cutia poștală de pe serverul host. Deci, această funcție este total transparentă pentru utilizator. Acesta doar își verifică periodic cutia poștală, parcurgând lista mesajelor primite, după care le va citi și in extenso.

Editarea și reexpediția mesajelor

Editorul programului de poștă electronică ne permite tratarea conținutului mesajului ca pe orice text asupra căruia putem să operăm diverse corecții: adăugări, ștergeri, formatări, copieri, mutări de caractere, fraze, paragrafe.

Un mesaj primit se poate, în consecință, modifica și reexpedia celui ce ni l-a trimis. Programul de poștă electronică, la inițierea unui răspuns inversează automat adresele, expeditorul devenind acum destinatar, iar adresa noastră va apărea în câmpul de adresă a expeditorului.

Mesajele pot fi redirecționate către alți destinatari, în caz că se dorește ca mesajul să ajungă și la o altă adresă e-mail.

Gestiunea cutiilor poștale

Această funcție permite utilizatorului manipularea mesajelor, atât a celor primite cât și a celor trimise, prin comenzi specifice la nivel de fișier.

Avem posibilitatea de a vizualiza lista cutiilor poștale și sumarul mesajelor aflate în oricare cutie poștală. Utilizatorul își poate salva mesajele în fișiere ASCII pe hard-discul propriu, le poate șterge logic și fizic, le poate transfera dintr-o cutie poștală în alta. Oricând utilizatorul își poate crea sau șterge cutii poștale personale.

Gestiunea agendei de adrese

Agenda cu adrese, *address book*, grupează în ordine alfabetică numele, adresa de e-mail, precum și alte date ale corespondenților, persoane fizice sau firme. Este vorba despre adresa de acasă, telefon, fax, mobil sau adresa de la serviciu, departamentul, funcția și altele.

Orice persoană sau firmă inclusă în agendă este desemnată cu termenul de „contact“.

Prin gestiunea agendei cu adrese înțelegem operațiile de adăugare de noi persoane, de modificare sau chiar eliminare din agendă a datelor acestora. Desigur, e de ajuns un clic pe numele, aliasul, persoanei în agendă pentru a-i prelua adresa sa de e-mail și a-i trimite un mesaj.

Agenda de adrese poate fi disponibilă și în Windows Explorer, cu condiția să o importăm din Outlook Express.

Tipărirea mesajelor

Este o funcție obișnuită pe care o realizează toate programele de poștă electronică. Tipărirea la imprimantă este controlată prin intermediul unor setări software la care avem acces prin meniul comenzii *Print*.

Securitatea mesajelor

Securitatea mesajelor de poștă electronică a ridicat și ridică în continuare destule probleme. Există în acest sens și realizări deosebite în special în direcția criptării mesajelor, validării autenticității expeditorului, a semnăturii acestuia etc. Proiectul PEM – *Privacy Enhanced Mail* este una dintre realizările importante în acest sens prin care s-a impus un set de standarde care au permis scrierea de pachete de programe puternice, cum este pachetul de programe PGM – *Pretty Good Privacy* dezvoltat de Zimmermann în SUA și puternicul *Kerberos Authentication Server* realizat în cadrul proiectului Athena de cercetătorii de la MIT.

Programele obișnuite de poștă electronică folosesc un prim nivel de securitate furnizat de parola de acces pe serverul de interconectare și apoi parola de acces la cutia poștală. Utilizatorul își poate schimba parola de acces ori de câte ori dorește sau este forțat la anumite intervale de timp să o reînnoiască, schimbând cel puțin două dintre simbolurile utilizate în vechea parolă.

Majoritatea sistemelor de e-mail oferă facilități suplimentare față de cele enumerate mai sus. Astfel, utilizatorii sistemelor de e-mail își pot crea cutii poștale (*mail boxes*) sau foldere pentru păstrarea mesajelor primite și a celor transmise. Acestea pot fi gestionate prin comenzi speciale de creare și distrugere, inspectarea conținutului, inserare și ștergere de mesaje etc.

Se pot crea liste de adrese de poștă electronică (*mailing lists*) prin care mesajele să poată fi trimise unui grup de persoane: când se trimite un mesaj, se vor expedia copii identice pentru toate persoanele din listă.

Alte facilități evolute sunt: copiile la indigo, poșta de prioritate mare, poșta secretă (criptată) – înainte de trimiterea mesajului; acesta este codificat, iar la destinație se asigură posibilitatea decriptării lui, receptorii alternativi – pentru situații în care receptorul primar nu este disponibil.

Mesajele se înregistrează, iar inițiatorul poate verifica dacă un mesaj s-a transmis sau nu sau se poate realiza o notificare automată în cazul în care mesajele nu ajung la destinație. În plus, există facilități de tip *forward*, prin care pentru utilizatorii care se deplasează pe o anumită perioadă poșta își pot primi mesajele acolo unde se găsesc. De fapt, aceste funcții sunt rezultate ale acțiunii sistemului de transfer al mesajelor.

8.4.2.2. Sistemul de transfer al mesajelor

Modul în care mesajele ajung la destinație este transparent pentru utilizator; acest lucru este extrem de important, deoarece asigură o largă accesibilitate tuturor utilizatorilor.

Această componentă a sistemelor de e-mail asigură:

- 1 transferul mesajelor, respectiv transmiterea acestora de la emițător la receptor, pe baza unor conexiuni de rețea (create pentru emiterea mesajelor și eliberate ulterior). Transferul mesajelor se realizează automat, fără intervenția utilizatorului.
- 1 raportarea se referă la informarea emițătorului unui mesaj despre starea acestuia (dacă a fost livrat, respins, pierdut). Confirmarea primirii unui mesaj poate fi foarte importantă, în unele situații ea poate avea și semnificație juridică. În cazul în care un mesaj nu ajunge la destinație (are o adresă greșită sau nu se poate stabili o conexiune de rețea până la destinație în timp util), emițătorul va primi automat un mesaj de avertizare.
- 1 dispoziția este pasul final al comunicării și se referă la acțiunea realizată asupra mesajului de către receptor, după primirea lui (eliminarea înainte de citire, citire și ștergere, citire și salvare etc.). Prin intermediul agenților utilizator, sistemele de e-mail fac posibilă regăsirea și recitirea mesajelor anterior salvate, trimiterea lor mai departe (*forward*) sau alte operații de prelucrare a lor.

Funcțiile de bază a sistemului de transfer al mesajelor se realizează prin intermediul unor protocoale specifice. Cu toate că utilizatorul serviciului de e-mail interacționează nemijlocit doar cu clientul e-mail, se impun câteva precizări legate de protocoalele care asigură transferul mesajelor de pe un calculator pe altul, deoarece un utilizator poate fi pus în situația de a trebui să-și configureze un program client de e-mail. Transferul elementar al mesajelor între două mașini din Internet este realizat prin intermediul protocolului SMTP.

SMTP (*Simple Mail Transport Protocol*) – este protocolul consacrat de transport e-mail în Internet. În general, pentru trimiterea unui mesaj între două mașini din Internet se realizează o conexiune de tip SMTP care constă într-o etapă de autentificare și transferul efectiv. Din punctul de vedere al utilizatorului singura interacțiune cu acest protocol constă în specificarea numelui server-ului SMTP (server-ul care se va „ocupa“ de mesajele acestuia). Acest nume se obține de la administratorul de sistem.

Protocolul SMTP stabilește regulile după care funcționează un program (care rulează în background) care se execută pe mașina destinație a unei conexiuni TCP, având rolul de a accepta conexiunile și de a copia mesajele primite în cutiile poștale corespunzătoare. Dacă un e-mail nu poate fi livrat, se returnează transmițătorului un mesaj de eroare.

Livrarea finală a mesajelor

Adesea, utilizatorii lucrează pe PC-uri care nu sunt conectate direct la Internet, ci prin intermediul unor servere care pot primi și trimite mesaje de poștă electronică. Într-o asemenea situație, PC-urile trebuie să comunice cu un server de e-mail printr-un protocol de livrare.

Un protocol simplu, care permite aducerea mesajelor dintr-o cutie poștală aflată la distanță și depozitarea lor pe mașina utilizatorului, este **POP3 (Post Office Protocol)**. Acesta este protocolul uzual folosit pentru accesarea mail-urilor de pe un server de mail de către calculatoarele dintr-o stație locală. Așa după cum îi spune și numele, acest protocol lucrează pe principiul unei căsuțe poștale: programul client se conectează la anumite intervale de timp la server-ul POP3. La o conexiune sunt trimise mesajele din *outbox*-ul clientului și aduse mesajele noi de pe serverul de POP3. Autentificarea se realizează la nivel de utilizator, pe baza unei parole. Numele server-ului este furnizat de administratorul de sistem, la fel ca și numele contului POP.

Protocolul POP3 conține comenzi pentru conectarea și deconectarea utilizatorilor, aducerea și ștergerea mesajelor. De exemplu, în configurarea sistemului Outlook Express se va cere nu numai numele serverului de mail, ci și protocolul prin care stația locală comunică cu acesta.

IMAP (Interactive Mail Access Protocol) – protocol interactiv de acces la poșta electronică) este un protocol de livrare mai sofisticat, adoptat și el ca standard Internet. Acesta este proiectat pentru utilizatorii care folosesc mai multe calculatoare. Acest protocol funcționează pe principiul păstrării unui depozit central de mesaje pe serverul de e-mail, care poate fi accesat de fiecare mașină (mesajele nu se copiază pe mașina personală a utilizatorului).

DMSP (Distributed Mail System Protocol) – protocol distribuit pentru sistemul de poștă) este diferit de POP3 și IMAP prin faptul că nu presupune că toată poșta se află pe un singur server. Utilizatorii pot „descărca“ mesajele de pe server pe o stație de lucru, un PC sau un calculator portabil, apoi se pot deconecta de la server, citi mesajele și scrie răspunsurile, iar ulterior să se reconecteze, moment în care poșta se retransferă și sistemul se resincronizează.

Multe sisteme de livrare oferă facilități suplimentare, cum ar fi filtrarea mesajelor: la sosirea mesajelor se pot verifica anumite condiții și executa acțiuni corespunzătoare. Definirea unor astfel de reguli permite punerea în evidență a anumitor mesaje (de exemplu, de la o anumită persoană) sau eliminarea mesajelor nedorite chiar fără a fi afișate.

O altă caracteristică a sistemelor de livrare este posibilitatea de a trimite temporar poșta la o altă adresă, prin mecanisme de tip *forward*. Această facilitate este foarte utilă dacă într-o anumită perioadă, utilizatorul nu își poate accesa serverul uzual de mail, de exemplu, din cauza unor restricții de securitate.

8.5. FTP

FTP (*File Transfer Protocol*) este un protocol pentru transferul fișierelor. Protocolul HTTP utilizat de browsere pentru aducerea informațiilor codate HTML în calculatorul client este suficient pentru fișierele text și pentru imaginile asociate, deoarece aceste fișiere sunt, în general, de mici dimensiuni. Transferarea unor fișiere mari pune unele probleme de viteză și de siguranță a conexiunii, ceea ce face protocolul HTTP ineficient. În acest caz se utilizează protocolul FTP.

Protocolul FTP presupune împărțirea fișierului de transferat într-un număr de blocuri de dimensiune fixată și trimiterea acestor blocuri spre client. Pe calculatorul client are loc rearanjarea blocurilor în ordinea corectă, refăcându-se astfel fișierul original.

Principalele avantaje ale utilizării FTP-ului sunt viteza de transfer crescută și posibilitatea reluării unui transfer întrerupt din punctul în care a apărut întreruperea. În acest fel o legătură întreruptă nu presupune reluarea transferului de la început, realizându-se astfel o importantă creștere a vitezei de lucru.

În general, conectarea la un anumit server presupune deținerea unui cont pe calculatorul respectiv. În acest caz utilizatorul se identifică prin numele contului și parola, și ca urmare primește dreptul de a utiliza calculatorul respectiv pentru a copia fișiere pe și de pe server. Majoritatea serverelor FTP permit și conectarea limitată a celor care nu au cont pe calculatorul respectiv printr-o conexiune numită anonimă: numele de utilizator este *anonymous* sau *guest*, parola – adresa de e-mail. În acest caz, utilizatorul are drepturi de citire din anumite directoare, de obicei aflate toate în directorul *Pub* din rădăcină și, uneori drepturi de scriere într-un director numit *Upload*. Pentru copierea unui fișier de pe server pe calculatorul local se folosește termenul **download**, iar pentru transferul invers – **upload**.

FTP a fost utilizat inițial prin trimiterea de comenzi spre server într-o sesiune Telnet. Deși în ultimul timp au apărut programe care oferă o interfață grafică deosebită pentru a ușura lucrul cu comenzile FTP, folosirea comenzilor, în linie de comandă, este o metodă care poate fi aplicată indiferent de sistemul de operare sau dotarea cu programe a unui calculator conectat la Internet.

În sistemele Windows deschiderea unei sesiuni FTP se face lansând programul „ftp.exe“, interpretorul de comenzi FTP, aflat de obicei în directorul „Windows“ sau directorul „sistem“.

Clienții FTP sunt programe care oferă o interfață grafică simplă între utilizator și comenzile pe care le așteaptă serverul FTP. În acest mod utilizatorul nu este obligat să cunoască toate aceste comenzi, și în plus au avantajul de a se putea afișa în același timp mai multe informații despre server. În figurile 8.2, respectiv 8.3 este prezentată interfața programului WS_FTP, unul dintre cei mai răspândiți clienți FTP.

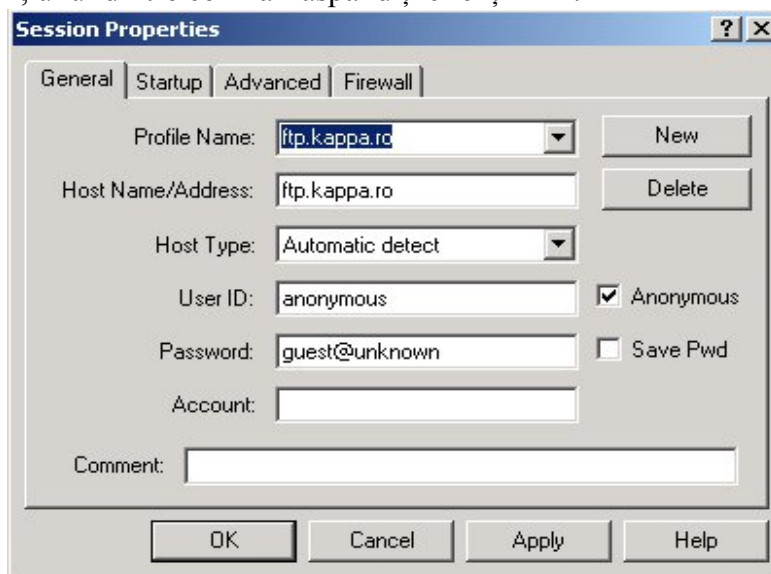


Fig. 8.2. Interfața de conectare a produsului WS_FTP

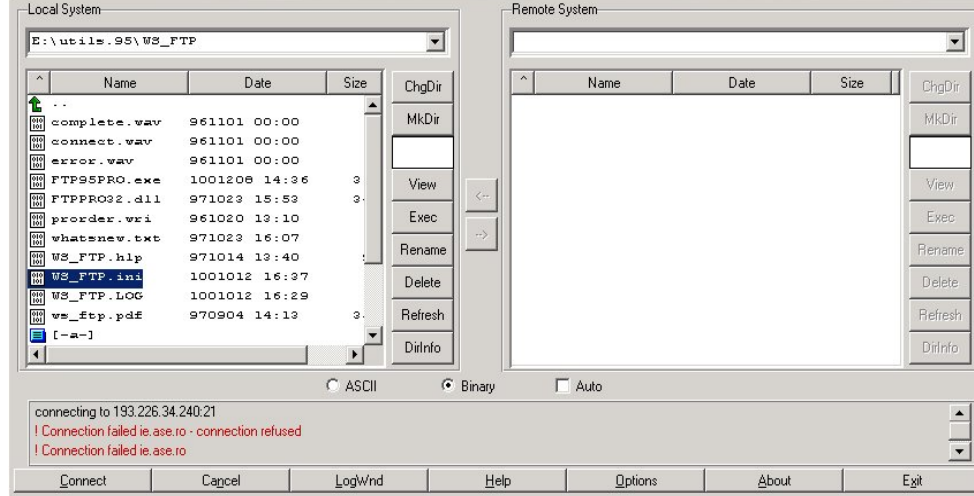


Fig. 8.3. Interfața de lucru a produsului WS_FTP

Browser-ele Web au posibilitatea de a accesa server-ele FTP. Adresa scrisă trebuie să indice faptul ca protocolul utilizat este FTP, ca în exemplul următor: <ftp://cronos.ase.ro/>. Se poate specifica și un nume de utilizator și o parolă, dar în acest mod de accesare a unui cont securitatea este minimă: ftp://nume_utilizator:parola@cronos.ase.ro. Browser-ul trimite comenzile FTP necesare, iar din răspunsul server-ului se obține o pagină în format HTML pe care o afișează.

În afara dezavantajului amintit, al lipsei securității parolei (oricine poate vedea parola), browser-ele nu oferă unul dintre avantajele transferului FTP: un transfer întrerupt nu poate fi reluat din punctul întreruperii. Acest lucru face ca browser-ele, deși oferă conexiuni FTP funcționale, să nu fie potrivite în cazul copierii unor fișiere de mari dimensiuni pe conexiuni de viteză redusă.

8.6. Grupuri de știri

Rețeaua de știri (*net news*) este una dintre cele mai populare aplicații ale rețelelor de calculatoare, asigurând informarea și comunicarea prin intermediul transmiterii și recepționării de mesaje din domeniile de interes corespunzătoare grupurilor de știri. Rețeaua tradițională de știri este denumită USENET și este diferită de Internet.

Un grup de știri creează un cadru pentru discuții pe teme bine determinate. La el subscriu persoanele interesate de acel subiect. Membrii unui grup de știri pot folosi un tip special de program (ca „agent utilizator”), care să permită citirea tuturor articolelor sau a mesajelor transmise într-un grup de știri. Acest program se numește cititor de știri (*news reader*) și realizează și transmiterea mesajelor într-un grup de știri: fiecare articol trimis unui grup de știri va fi transmis automat tuturor membrilor grupului, indiferent de localizarea lor geografică.

Durata transmisiei mesajelor de știri variază de la câteva secunde la câteva ore, în funcție de localizarea în rețea a emițătorului și receptorului. Deși au o implementare diferită, grupurile de știri au o funcționalitate similară cu listele de poștă electronică.

Recent, au apărut implementări alternative, care urmăresc aceleași obiective de informare și comunicare. Acestea se referă la produse software speciale care implementează liste de discuții și la trimiterea știrilor sub formă de mesaje de mail prin intermediul unor furnizori de servicii care permit subscrierea la diverse domenii de interes pe site-uri speciale.

8.6.1. Domenii clasice de interes în Usenet

Numărul foarte mare al grupurilor de știri din Usenet a determinat realizarea unei ierarhii, prin intermediul căreia să poată fi gestionate mai ușor. Oficial, ierarhiile de știri derivă din următoarele domenii principale:

- 1 **Alt** – arbore alternativ al ierarhiei oficiale, folosit pentru orice alte teme;
- 1 **Comp** – calculatoare, știința și industria calculatoarelor;
- 1 **Humanities** – literatură și științe umaniste;
- 1 **Misc** – domeniu mixt (temele care nu se încadrează în celelalte domenii);
- 1 **News** – gestiunea grupurilor de știri;
- 1 **Rec** – activități recreative, sport, muzică;
- 1 **Sci** – științe fizice și ingineresti;
- 1 **Soc** – aspecte sociale;
- 1 **Talk** – dezbateri, pamflete, polemici, argumentări.

În afară de ierarhiile oficiale, mai există ierarhii regionale sau pentru limbi diferite de cea engleză.

Fiecare dintre categoriile menționate mai sus se împarte în subcategorii, care se divid la rândul lor, pe același principiu ierarhic. Separarea categoriilor din specificarea completă a unui domeniu se face prin puncte (.). De exemplu, comp.lang se referă la limbaje de programare, iar comp.lang.c – la limbajul de programare C. Pot exista mai multe categorii de același nivel, care se pot înlocui între ele în specificările complete, astfel încât să se refere la subdomeniul dorit.

8.6.2. Programe pentru știri

Există numeroase programe de citire a știrilor (*news readers*) cu interfață de tip comandă sau vizuală. În cursul rulării, aceste programe verifică fișiere de informații specifice pentru a vedea cărui grup de știri îi aparține un anumit utilizator, apoi afișează o linie de rezumat pentru fiecare articol și așteaptă ca utilizatorul să selecteze unul sau mai multe articole pentru citire; acestea vor fi afișate pe rând. După ce au fost citite, ele pot fi salvate, șterse, tipărite etc.

Programele pentru știri permit utilizatorilor să subscrie sau să renunțe la subscrierea făcută la anumite grupuri de știri. De fapt, schimbarea unei subscrieri revine la editarea fișierului local în care apar grupurile de știri la care a subscris utilizatorul. În acest sens, se poate face o analogie între subscrierea la un grup de știri și urmărirea regulată, periodică a unei anumite emisiuni de televiziune sau radio.

Programele care gestionează grupurile de știri au și facilități de poștă electronică. Utilizatorul poate să compună mesaje și să le trimită către destinatarii doriți; peste cel mult o zi, mesajele vor ajunge la toți membrii grupului de știri respectiv. Un anumit mesaj se poate transmite, folosind o singură comandă, mai multor grupuri de știri. O altă facilitate este restricționarea distribuției geografice a poștei.

Pentru a reduce traficul de informații rezultat din numeroasele întrebări ale celor care subscriu la Usenet pentru prima dată, multe grupuri de știri și-au construit documente FAQ (*Frequently Asked Questions*), unele extrem de lungi și bine documentate, care încearcă să răspundă tuturor întrebărilor uzuale (ale începătorilor). Aceste documente sunt trimise prin poștă periodic sau la subscrierea unui nou utilizator, de către cei care le gestionează.

Deși majoritatea persoanelor folosesc numele real la transmiterea mesajelor, unele dintre ele doresc să rămână anonime, în special când transmit informații unor grupuri de știri controversate sau când trimit anunțuri cu caracter personal. Pentru a rezolva această problemă au apărut retransmițătorii anonimi (*anonymous remailers*), care sunt servere cu acces la mesajele de poștă electronică, cărora le schimbă câmpurile *Sender:*, *From:* și *Reply-To:*, astfel încât să includă referințe către retransmițător în loc de transmițător. Unele servere de acest tip asociază un număr fiecărui utilizator și folosesc acest cod asociat. Există modalități de regăsire a utilizatorului cu un anumit cod asociat, la care se poate apela în cazul în care comunicările intră sub incidența legii.

Implementarea grupurilor de știri în Usenet

Unele dintre grupurile de știri de mici dimensiuni sunt implementate ca liste de poștă electronică, astfel încât un mesaj trimis pe adresa listei va ajunge, într-o copie, la fiecare adresă din listă.

Această abordare nu este convenabilă pentru grupurile de dimensiuni mari, pentru că, prin numărul mare de mesaje transmise către diverse destinații, ar putea produce un blocaj al serverelor. De aceea, se preferă o altă implementare: fiecare site (campus universitar, companie sau furnizor de servicii Internet) care oferă serviciul de știri memorează mesajele sosite pe un server care funcționează și ca server de știri, într-un director (*news*) cu subdirectoare specifice (comp, sci etc.), care conțin la rândul lor subdirectoare. Cititorii accesează articolele de știri din subdirectorul corespunzător domeniului de interes. Această metodă are avantajul de a reține articolele de știri într-un exemplar unic în cadrul unui site, în subdirectorul corespunzător. După un anumit număr de zile, termenul de accesare a articolelor expiră și acestea sunt eliminate de pe disc.

Pentru a putea primi știri prin Usenet, fiecare site trebuie să aibă o sursă de știri (*newsfeed*) de la un alt site Usenet. Mulțimea serverelor de știri formează o rețea de noduri conectate prin legături care constituie, de fapt, rețeaua Usenet. Uzual, fiecare site își va testa sursa pentru a vedea dacă au apărut știri noi de la conectarea precedentă. Dacă da, ele vor fi colectate și depuse în subdirectorul adecvat din *news*. O altă modalitate, mai rar folosită, este ca o sursă să stabilească contactele cu serverele destinație când apar știri noi.

Protocolul folosit pentru transmiterea știrilor în Usenet se numește NNTP (*Network News Transfer Protocol*) și este similar cu SMTP; se bazează pe conexiuni TCP, funcționează pe modelul client-server și folosește comenzi de tip text. NNTP a fost proiectat pentru a realiza propagarea mesajelor de știri de la o mașină la alta și pentru a permite utilizatorilor conectați la un calculator care nu poate primi știri să le citească la distanță.

8.7. Securitatea transmisiei datelor

Pe măsura răspândirii aplicațiilor care presupun interconectarea calculatoarelor și a cunoștințelor despre protocoalele folosite în rețelele de calculatoare, pericolul interceptării și decodificării datelor în timpul transferării mesajelor în rețea a crescut, indiferent dacă transferul se face într-o rețea locală, într-un mediu format din mai multe rețele interconectate, sau în mediul Internet.

Au fost dezvoltate o serie de tehnici de securizare a datelor care atunci când sunt combinate oferă un înalt nivel de confidențialitate pentru informațiile transmise prin rețea. Aceste tehnici sunt:

1 **Integritatea datelor** – oferă siguranța receptorului că mesajul primit este identic cu cel emis;

1 **Secretizarea/confidențialitatea datelor** – protejează conținutul mesajului transmis în rețea împotriva citirii sau interceptării neautorizate;

1 **Autentificarea originii datelor**– permite receptorului mesajului să determine în mod sigur identitatea expeditorului;

1 **Nonepudierea** – garantează originea și integritatea tranzacției din punctul de vedere al expeditorului.

Integritatea și secretizarea sunt realizate prin intermediul **criptării datelor**, iar **autentificarea și nonepudierea** necesită schimbul unui set de mesaje criptate între cele două părți care comunică.

Criptarea datelor (sau **cifrarea datelor**) presupune ca partea emițătoare să prelucreze toate datele înaintea transmiterii, astfel încât dacă acestea sunt accidental sau intenționat interceptate în timpul transferului, să nu poată fi înțelese de interceptor. Datele trebuie să poată fi însă imediat **decriptate** sau **descifrate** de receptorul autorizat, pentru a obține mesajul inițial.

Majoritatea metodelor de criptare implică folosirea unor **chei de criptare** sau **criptografice** care trebuie să fie cunoscute numai de cele două entități care comunică. Înaintea criptării datelor, acestea sunt denumite **text-în-clar**, iar după criptare **text cifrat** sau codificat. Transformarea unui mesaj clar în mesaj cifrat poartă numele de **cifru**.

Securizarea datelor transmise în rețea se poate face realizând un **criptosistem**. Acesta este format dintr-unul sau mai mulți algoritmi de criptare, cheile folosite de algoritmi de criptare, un sistem de gestiune a cheilor, textul în-clar (textul original) și textul codificat.

Algoritmul de criptare este aplicat textului-în-clar și se obține textul cifrat. Textul cifrat este transmis la destinație unde se folosește algoritmul complementar pentru a obține textul în-clar transmis.

Securitatea unui sistem care folosește chei de criptare se bazează în special pe păstrarea secretă a valorii cheii, și nu atât pe ascunderea algoritmului folosit pentru criptare. Există mulți algoritmi puternici de criptare publici. Principala problemă a unui criptosistem este stabilirea unei modalități sigure de creare și de comunicare a cheii între cele două părți.

O altă problemă este autentificarea, în acest sens putând să apară două probleme:

1 Identitatea persoanei sau sistemului care realizează criptarea: mesajul este criptat de persoana care deține cheia la un moment dat. Acesta ar trebui să fie proprietarul cheii, dar dacă sistemul a fost „spart“ poate fi o persoană neautorizată.

1 Identitatea persoanei sau sistemului care a emis cheile de criptare: sistemul trebuie să răspundă la întrebarea: Cheile primite de cele două părți care comunică au fost create și transmise de proprietarul autorizat?

Alegerea unui algoritm de criptare trebuie să se facă presupunând că un mesaj transmis poate fi interceptat și salvat, astfel că „intrusul“ cunoaște contextul în care mesajul interceptat poate fi folosit adică tipul informațiilor schimbate. Scopul este alegerea metodei de criptare astfel încât un intrus chiar beneficiind de un calculator performant, să nu poată descifra textul codificat interceptat în timp util.

Există două tipuri de sisteme criptografice folosite astăzi:

1. criptografia cu cheie secretă (criptografia simetrică) – folosește aceeași cheie atât la cifrarea, cât și la descifrarea mesajelor. Aceste sisteme conduc la performanțe bune și sunt folosite pentru protecția datelor utilizatorilor. Securitatea criptării simetrice depinde de protecția cheii folosite, managementul acestora fiind un factor vital în securitatea datelor, iar procesul de distribuire sigură a cheilor este foarte dificil. În acest caz administrarea cheilor include:

- **generarea cheilor** -presupune existența de mijloace pseudoaleatorii de creare a succesiunii de biți ai cheii;
- **distribuția cheilor** – modul în care se transmit și se fac cunoscute cheile tuturor utilizatorilor cu drept de acces la informațiile criptate;
- **memorarea cheilor** – presupune stocarea sigură a lor pe un suport magnetic, de obicei criptate sub o altă cheie, numită cheie master.

Problema fundamentală a utilizării criptografiei în rețele este aceea a găsirii unor modalități de distribuire sigură, periodică a cheilor criptografice, acestea trebuind să fie schimbate cât mai des.

2. criptografia cu cheie publică (criptografia asimetrică) – folosește chei distincte de codificare și decodificare (dependente una de alta).

Una dintre chei, cheia privată este ținută secretă și este cunoscută doar de proprietarul ei. A doua cheie, cheia publică perechea cheii private este cunoscută partenerilor de dialog.

Nonrepudierea – folosirea sistemelor cu chei publice este utilă în garantarea identității emițătorului documentului electronic transmis. Se exploatează proprietatea duală a sistemelor cu chei publice în care nu numai că receptorul este capabil să decripteze toate mesajele pe care le primește (și care au fost criptate cu cheia publică), folosind cheia privată, dar în plus orice receptor poate decripta un mesaj criptat cu cheia privată a emițătorului folosind cheia publică a emițătorului.

Operațiile de criptare și de decriptare sunt realizate pe două nivele. Nivelul interior al criptării și decriptării este cel deja prezentat. La nivelul exterior emițătorul folosește propria cheie privată pentru a cripta mesajul original (textul-în-clar). Dacă receptorul poate decripta acest mesaj folosind cheia publică a emițătorului, acest lucru reprezintă dovada că emițătorul este cel care a inițiat de fapt trimiterea mesajului.

Relația matematică dintre cheile publică și privată permite emițătorului să creeze mesajul cu cheia sa privată și receptorului să decripteze mesajul cu cheia publică a emițătorului. Receptorul are astfel garanția că mesajul aparține emițătorului a cărui cheie publică a folosit-o pentru decriptare.

Autentificarea este necesară atunci când un client dorește să acceseze informații sau servicii de la un server din rețea. Înaintea acordării accesului clientului la informațiile de pe server, acesta trebuie să demonstreze că este un utilizator înregistrat. Odată autentificat îi este permis accesul utilizatorului la server. Procesul de autentificare poate fi realizat utilizând fie sistemul simetric fie cel asimetric.

Principiul general al **sistemului asimetric** este prezentat în figura 8.5.

Schema presupune că toți utilizatorii potențiali cunosc cheia publică a serverului S_p . Clientul creează mai întâi un mesaj conținând numele de utilizator al clientului, U , cheia publică a clientului C_p și indicatorul timp tc . Acesta din urmă indică timpul la care a fost creat mesajul și o înregistrare a acestuia este păstrată la client. Mesajul este apoi criptat utilizând S_p și trimis serverului (1).

Serverul mai întâi decriptează mesajul utilizând propria cheie secretă S_s și apoi încearcă să valideze numele de utilizator, verificând dacă există un utilizator cu numele U . Presupunând că acesta există, serverul trece la crearea unui mesaj de răspuns conținând: numele utilizatorului (U), indicatorul timpului clientului (tc) și un alt indicator de timp care precizează timpul la care a fost creat mesajul de răspuns de către server (ts). Serverul păstrează o înregistrare a acestuia și codifică mesajul utilizând cheia publică a clientului C_p . Apoi transmite mesajul criptat clientului (2).

La receptarea răspunsului, clientul mai întâi decriptează mesajul folosind propria cheie secretă C_s și dacă stabilește că valoarea tc conținută în mesaj este identică cu cea trimisă de el presupune că a fost autentificat de server. Urmează crearea și transmiterea unui nou mesaj conținând numele de utilizator al clientului și indicatorul de timp al serverului ts , mesaj ce are rolul de a aduce la cunoștință primirea mesajului. Noul mesaj este din nou criptat utilizând cheia publică a serverului S_p , și trimis serverului (3). Serverul îl decriptează folosind propria cheie secretă S_s și dacă stabilește că valoarea ts din mesajul recepționat este identică cu cea transmisă de el, se pregătește să accepte serviciul cerut de client.

În ambele cazuri, timpul la care mesajul a fost recepționat depășește valoarea indicatorului de timp din mesajul de răspuns corespunzător cu mai mult decât un interval de timp acceptabil definit de sistem, mesajul este exclus și accesul rămâne blocat.

Sistemul simetric

Sistemul cu cheie privată este folosit de sistemul **Kerberos** pentru a rezolva probleme de securitate. Kerberos oferă o modalitate de a verifica identitățile participanților la tranzacțiile dintr-o rețea neprotejată, realizată fără a ne baza pe verificarea făcută de sistemul de operare local, și presupunând că pachetele care circulă în rețea pot fi citite, modificate și inserate după dorință.

Mecanismul de bază pentru controlul securității adoptat de Kerberos este un set de tichete de criptare cunoscute sub denumirea de containere de control, folosite pentru controlul accesului la diferite servere care compun sistemul. Acesta include o serie de servere ale aplicației – servere de fișiere, servere de poștă electronică – și serverul sistem care distribuie biletele, cunoscut ca serverul de alocare a tichetelor. Toate mesajele schimbate între serverul de alocare a tichetelor și utilizator și între utilizator și serverele aplicației, sunt criptate folosind sistemul cu chei private, care sunt parte a tichetelor corespondente.

8.8. Gestiunea mesajelor de e-mail cu Outlook 2003

Programul Outlook 2003 cuprinde o diversitate de instrumente și caracteristici care se pot utiliza pentru a gestiona în mod eficient mai multe conturi de e-mail, de exemplu:

- se pot defini mai multe grupuri Send/Receive Groups, cu configurații separate ale conexiunilor pentru fiecare cont de e-mail.

- se pot defini reguli de prelucrare automată a mesajelor primite sau expediate.

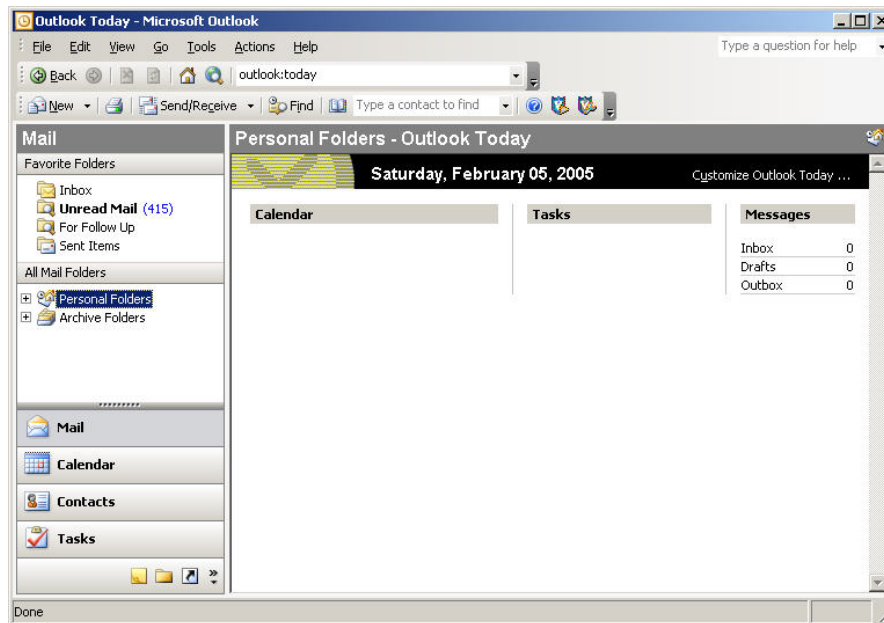


Figura 8.6. Fereastra aplicației Outlook 2003

Pentru utilizarea clientului de e-mail Outlook este necesară existența unui cont de e-mail accesibil prin protocoalele POP3, IMAP sau HTTP (pentru Hotmail) pe un server de e-mail. Contul de e-mail poate fi plătit la un furnizor de servicii Internet sau poate fi creat pe unul din numeroasele server gratuite care oferă conturi de e-mail (nu toate pot fi utilizate însă cu Outlook). Având la dispoziție informații precum numele contului, parola, numele serverelor de e-mail pentru transmitere și recepționare mesaje și modul de conectare la Internet, se poate configura un client de e-mail Outlook 2003. Configurarea conturilor se realizează din meniul Tools, opțiunea E-mail Accounts, de unde se alege opțiunea Add new e-mail account și prin intermediul unui Wizard sunt înregistrate pas cu pas toate setările legate de contul de e-mail. După configurarea contului de e-mail se poate folosi programul pentru trimiterea și recepționarea mesajelor.

În figura 8.6 este prezentată interfața aplicației Outlook 2003. Se observă structurarea acesteia în următoarele grupuri:

- gestiunea e-mail-urilor (Mail);
- gestiunea timpului (Calendar);

- gestiunea datelor de contact (Contacts);
- gestiunea activităților (Tasks).

Crearea, gestionarea și stocarea adreselor de e-mail. Outlook 2003 poate stoca adresele de e-mail și alte informații de utilizând grupul Contacts pentru stocarea informațiile de contact. Sunt permise adăugarea de informații de contact, precum numele și prenumele, adresa de e-mail, adresa de poștă, telefonul de acasă, de la serviciu etc. Informațiile de contact sunt disponibile și altor aplicații, cum ar fi Fax Console.

În ceea ce privește organizarea mesajelor de poștă electronică, sunt disponibile câteva directoare (foldere) prestabilite:

- Inbox – pentru mesaje primite
- Outbox – pentru mesaje ce urmează a fi trimise
- Sent Items – stochează mesajele transmise
- Draft – mesaje care urmează a fi trimise dar sunt nefinalizate
- Junk E-mail – pentru mesaje de e-mail nedorite (spam)

Trimiterea unui mesaj de e-mail se presupune scrierea adresei destinatarului și a mesajului propriu-zis și expedierea acestuia. Fereastra pentru mesaj se deschide selectând din meniul File opțiunile New și din aceasta opțiunea New Message.

Fereastra pentru mesaje noi (figura 8.7) este alcătuită din mai multe zone: o zonă pentru adrese, una pentru subiectul mesajului și o zonă pentru conținutul mesajului.

În zona de adrese sunt introduse adresa sau adresele de e-mail ale destinatarului mesajului. În această zonă există trei câmpuri:

- To: pentru adresa e-mail a destinatarului primar al mesajului. Pot fi scrise mai multe adrese, despărțite prin spațiu liber sau prin punct și virgulă (,);
- CC (Carbon Copy): pentru adresa sau adresele la care se va trimite o copie a mesajului, destinatarul primar putând observa acest lucru;
- BCC (Blind Carbon Copy): pentru adresa sau adresele la care se va trimite o copie a mesajului, fără ca destinatarul primar să observe acest lucru;

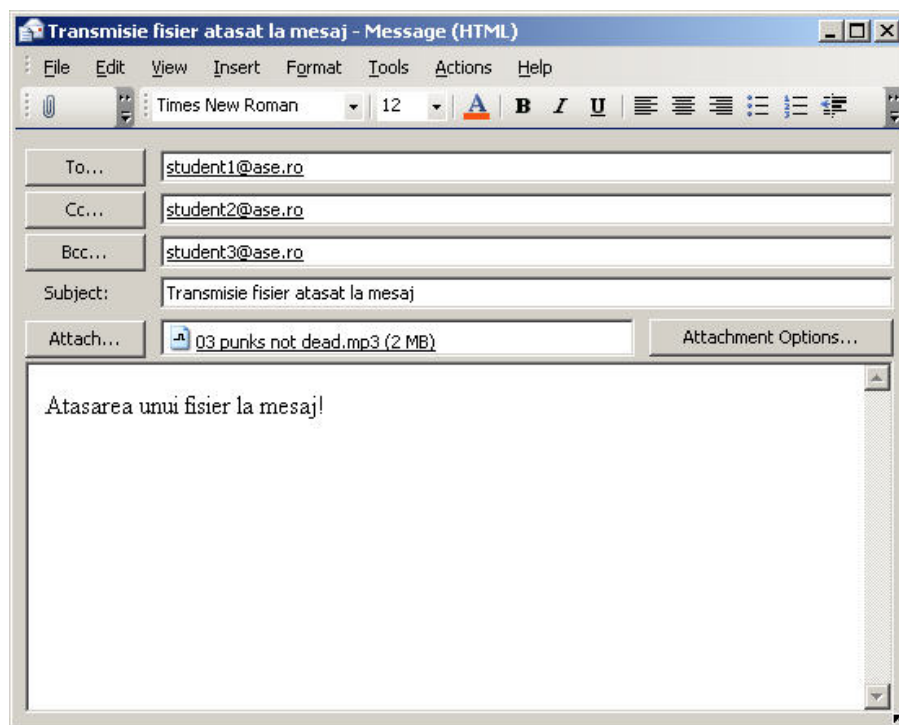


Figura 8.7. Fereastra Outlook pentru mesaje noi

În zona Subject se scrie pe scurt subiectul mesajului iar în zona de mesaj se scrie mesajul propriu-zis.

Există posibilitatea de a atașa fișiere la mesaj, caz în care va fi disponibilă o zonă de atașamente și un buton Attach prin care se pot atașa noi fișiere.

După scrierea adresei și compunerea mesajului, acesta se poate trimite executând clic pe butonul Send de pe bara de instrumente din fereastră, iar mesajul este plasat în folderul Outbox și în funcție de setările existente, mesajul este trimis imediat sau după apăsarea butonului Send/Receive de pe bara de instrumente.

O altă modalitate de a trimite un mesaj este ca răspuns la un mesaj de e-mail primit (Reply).

Primirea mesajelor e-mail. După conectarea la furnizorul de servicii Internet se execută clic pe Send/Receive de pe bara de instrumente Outlook. Se va deschide o casetă de stare și mesajele e-mail noi vor fi recepționate de Outlook. Mesajele noi vor fi salvate în folderul Inbox și vor apărea cu caractere aldine (bold). Pentru a putea citi un mesaj se execută clic pe

acesta, iar conținutul va apărea în panoul Preview din partea dreaptă a ferestrei Outlook. Pentru a deschide mesajul într-o fereastră separată, se execută dublu clic pe mesaj.

Pentru a răspunde unui mesaj se selectează mesajului și se apasă butonul Reply sau Reply to All de pe bara de instrumente Outlook. Se deschide astfel fereastra de mesaj nou unde adresa sau adresele de răspuns apar în casetele potrivite, iar în fața subiectului s-a adăugat Re:, care reprezintă abrevierea de la Regarding împrumutată de la scrisorile de afaceri și de la rapoarte, pentru a arăta că acesta este un răspuns și textul mesajului original, apar și ele în fereastra pentru răspuns. Se scrie răspunsul mesajului deasupra mesajului original în zona pentru mesaj. Mesajul original poate fi păstrat sau se poate șterge. Apoi se expediază mesajul în mod asemănător trimiterii unui mesaj nou.

În cazul în care se dorește retrimiteria unui mesaj recepționat se selectează mesajul și se apasă butonul Forward. Conținutul mesajului va fi copiat în zona de mesaj a ferestrei de mesaje noi care va fi deschisă automat. Înaintea subiectului mesajului original este plasată prescurtarea Fwd:. După completarea adresei destinatarului mesajul se transmite ca orice alt mesaj.

Alegerea unui format al mesajelor. Atunci când se compune un mesaj sau se efectuează clic pe butonul Reply, programul Outlook permite alegerea unui format din trei formate de mesaje distincte și anume:

- Plain Text, care transmite numai literele, cifrele și simbolurile din setul de caractere utilizat pentru a crea mesajul. Outlook înlătură, în acest caz, orice formatare, inclusiv culorile, fonturile și figurile atunci când expediază mesajul;
- Rich Text permite specificarea fonturilor, culorilor, marcajelor și a altor atribute ale textului, cu o restricție majoră: numai destinatarii care utilizează programul Outlook sau un alt client Exchange vor putea vizualiza corect aceste informații formatare;
- HTML, care oferă aceleași opțiuni de formatare ca și formatul Rich Text, plus capacitatea de a specifica stiluri, de a numerota automat rândurile și de a adăuga reguli pe orizontală. Deoarece formatul aflat la bază este același ca al unei pagini Web, se pot defini grafice de fundal și se pot insera imagini în mesaj. Majoritatea programelor moderne de tip client de e-mail pe Internet sunt capabile să citească mesaje în format HTML. În cazul în care programul client de e-mail al destinatarului nu poate interpreta formatul HTML, acesta afișează o versiune a mesajului

sub formă de text simplu, cu o atașare care poate fi vizualizată cu orice navigator Web.

Atunci când se creează un mesaj nou, programul Outlook utilizează formatul prestabilit Rich Text. Pentru a alege oricare din cele trei formate acceptate, acesta se selectează din meniul Format. Atunci când se răspunde la un mesaj folosind Reply, programul Outlook ignoră preferințele specificate ca prestabilite și utilizează formatul mesajului inițial.

Specificarea gradului de importanță al mesajelor. Pentru ca un mesaj, după ce a fost compus și livrat unui server, să fie tratat în mod special, adică să i se acorde sau nu o mai mare importanță, trebuie să fie configurat astfel:

- Se apasă pe butonul Options care deschide caseta de dialog Message Options;
- în secțiunea Message Settings se utilizează lista derulantă Importance pentru a modifica aceste câmpuri de la configurația lor prestabilită (cu gradul de importanță Normal) la Low (scăzut) sau High (înalt) (figura 8.8). Destinatarul e-mail-ului va observa în lista de mesaje o săgeată în jos, de culoare albastră, pentru mesajele Low Importance și semnul exclamării, de culoare roșie, pentru mesajele High Importance.

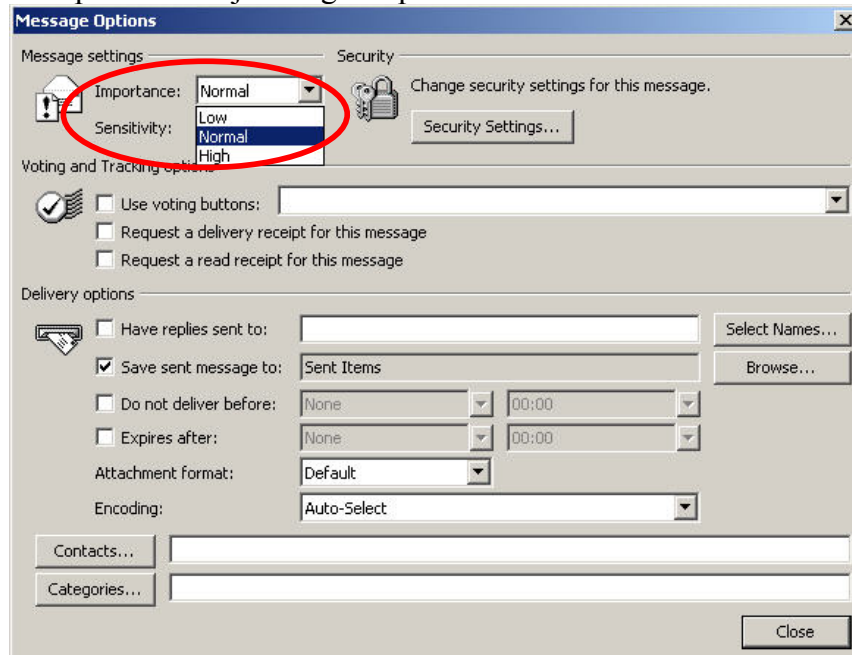


Figura 8.8. Setarea priorității mesajelor

Atașamente e-mail. Atașamentele mesajelor e-mail reprezintă o metodă simplă de trimitere și primire a fișierelor prin Internet. Când se primește un fișier atașat, el trebuie mai întâi salvat. În funcție de clientul de e-mail accesul la fișierele atașate se realizează prin pictograme și legături în cadrul mesajului (așa cum se întâmplă cu Outlook) sau prin salvarea fișierelor într-un director prestabilit pe discul utilizatorului (Eudora Light) etc. Spre deosebire de celelalte versiuni de Outlook care acceptau orice tip de fișier atașat la un mesaj e-mail, Outlook 2003 (după experiența atacurilor cu viruși special scriși pentru acest program) refuză să permită accesul la atașări unor anumite tipuri de fișiere. Ele sunt clasificate pe două niveluri de pericolozitate, pe primul nivel fiind fișierele executabile, scurtăturile, scripturile, bazele de date Access și alte obiecte care pot fi considerate purtătoare de viruși și sunt căutate la primirea mesajului într-o listă de extensii stocată în baza de date Registry. Dacă extensia se află pe lista respectivă, este posibil ca programul Outlook să vă forțeze să salvați fișierul înainte de a-l deschide sau să vă interzică accesul la atașament, astfel:

- atunci când programul Outlook găsește un fișier de nivel 1, afișează în panoul Info un mesaj care anunță că a blocat accesul la un fișier căruia i se afișează nume complet;
- atunci când programul Outlook găsește un fișier de nivel 2, obligă la salvarea sa pe hard disc.

Atașările pe care Outlook le consideră sigure apar în panoul Preview și în ferestrele mesajelor, în care este afișată o pictogramă și un nume pentru fiecare fișier atașat. Aceste detalii apar în linia Attachments, imediat după câmpul Subject. Pe o pictogramă de atașare se poate efectua clic dreapta mouse și utiliza meniurile contextuale pentru a deschide, tipări, salva și șterge atașarea respectivă.



Figura 8.9. Avertisment la trimiterea de atașamente considerate nesigure

În cazul în care se încearcă trimiterea unui fișier considerat nesigur, programul Outlook avertizează asupra riscului ca atașamentul să nu poată fi accesat de alți clienți Outlook (figura 8.9).

Utilizarea semnăturilor. Programul Outlook permite crearea unei semnături reprezentată de un scurt bloc de text (și opțional, elemente grafice sau cod HTML), care identifică utilizatorul, și eventual furnizează și alte informații despre utilizator. Cu ajutorul programului Outlook ca editor de mesaje, se pot crea una sau mai multe semnături (care pot fi de tip text, Rich Text sau HTML) pentru a fi utilizate în cadrul mesajelor de ieșire. Etapele de bază în crearea unei semnături sunt:

1. Se selectează din meniul Tools, Options și din foaia Mail Format se apasă pe butonul Signatures și din noua fereastră care se deschide se apasă pe butonul New;
2. În caseta de dialog Create New Signatures se introduce o denumire descriptivă a semnăturii și se specifică dacă se creează de la zero sau pe baza unei semnături sau a unui fișier existent;
3. Se continuă cu Next până la caseta de dialog Edit Signature unde se introduce textul care va fi utilizat pentru semnătura personală (figura 8.10).
4. Pentru a adăuga eventuale formătări textului selectat se folosesc opțiunile Font și Paragraph;
5. Se apasă butonul Finish pentru a salva semnătura.

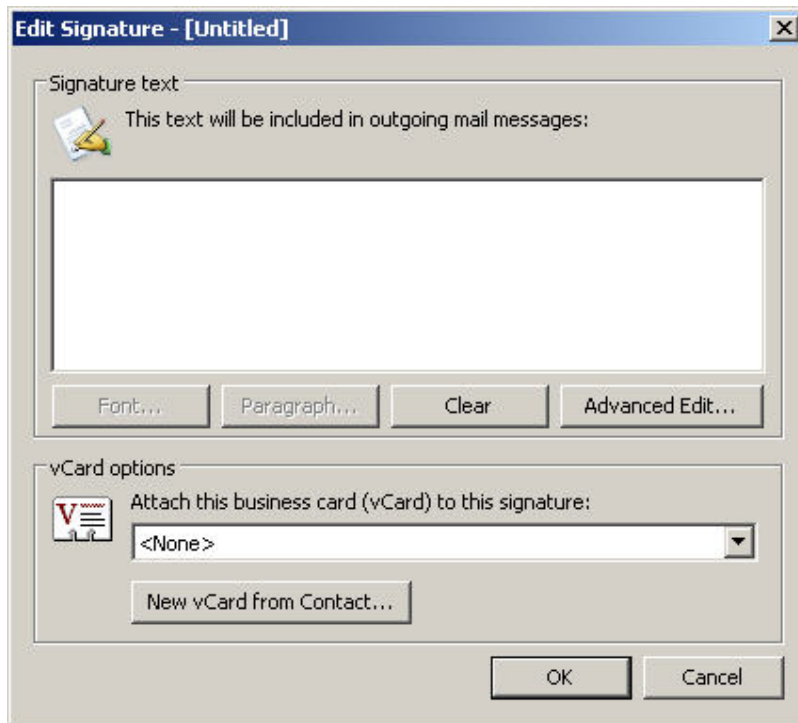


Figura 8.10. Fereastra de editare a semnăturilor digitale

Atunci când se specifică o semnătură prestabilită în foaia Mail Format din caseta de dialog Options, programul Outlook adaugă automat textul respectiv la sfârșitul fiecărui mesaj pe care îl creați. Dacă se utilizează Word ca editor de mesaje, atunci semnătura poate fi creată folosind Tools, Options, General, E-mail Options.

Configurarea notificărilor. Programul Outlook poate să notifice utilizatorul în diverse moduri atunci când acesta primește un mesaj nou. Tipurile de notificări sunt:

- emiterea unui sunet și schimbarea, pentru puțin timp, a formei indicatorului mouse-ului la primirea unui nou mesaj. Aceasta reprezintă forma cea mai subtilă de notificare. Pentru a modifica oricare dintre acestea, este necesar să se selecteze Tools, Options, urmat de clic pe Preferences, pe butonul E-mail Options și pe butonul Advanced E-mail Options (figura 8.11);
- notificare mai persistentă o constituie pictograma care apare în zona de notificare din dreapta barei de aplicații. O pictogramă de forma unui plic plasată aici anunță primirea unui nou mesaj e-

mail. Efectuarea unui dublu clic pe pictogramă deschide folderul Inbox și permite citirea mesajelor.

- forma cea mai evidentă de notificare este un mesaj pop-up care apare pe ecran atunci când sosește un mesaj nou (Desktop Alert).

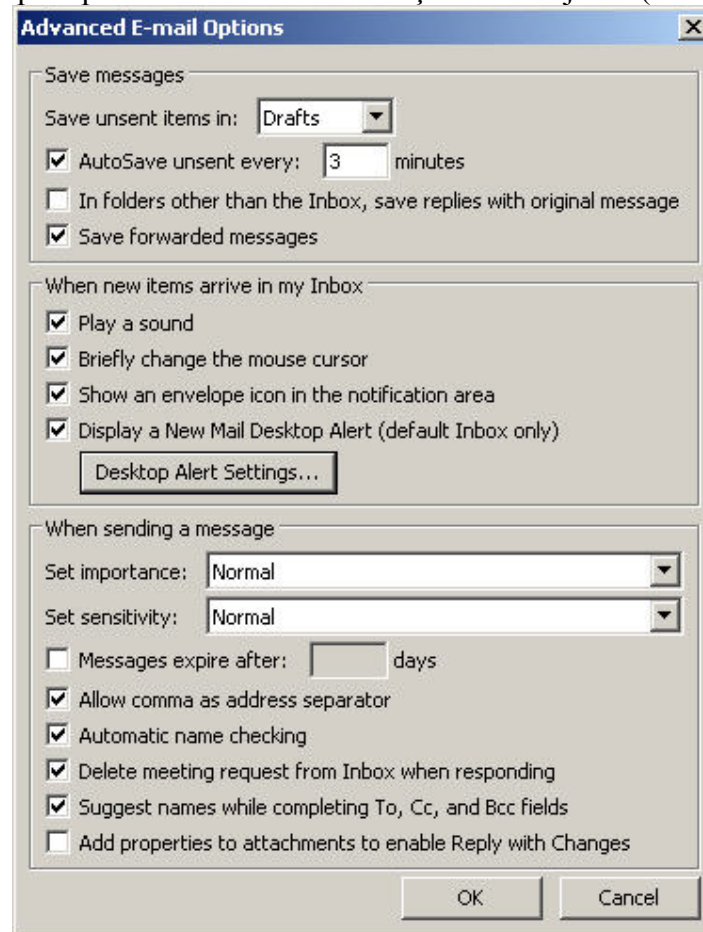


Figura 8.11. Fereastra de setare a opțiunilor pentru mesaje

Organizarea mesajelor de e-mail. Pentru a lansa instrumentul de bază pentru organizarea mesajelor dintr-un folder, se selectează folderul respectiv și din meniul Tools se selectează opțiunea Organize. Panoul Organize, care se va plasa chiar deasupra ferestrei mesajului (figura 8.12), permite crearea unui anumit tip de regulă pentru sortarea corespondenței către sau de la o anumită adresă. Sunt utile trei dintre opțiunile prezentate aici:

- selectarea unor mesaje și apoi efectuați clic pe opțiunea Using Folders pentru a crea o regulă care mută corespondența de la expeditorul mesajului respectiv, într-un folder specificat; această opțiune este utilă pentru tratarea mesajelor care sunt primite ca urmare a abonării la o anumită listă poștală; în anumite cazuri este nevoie de definirea unei reguli Sent To; această opțiune este adecvată atunci când numele expeditorului diferă de fiecare dată, dar destinatarul este întotdeauna același
- opțiunea Using Colors permite asocierea de culori expeditorilor de mesaje.
- opțiunea Using Views schimbarea modului de vizualizare a mesajelor; de exemplu zona de vizualizare a mesajelor poate fi poziționată jos sau la dreapta sau poate să fie dezactivată;

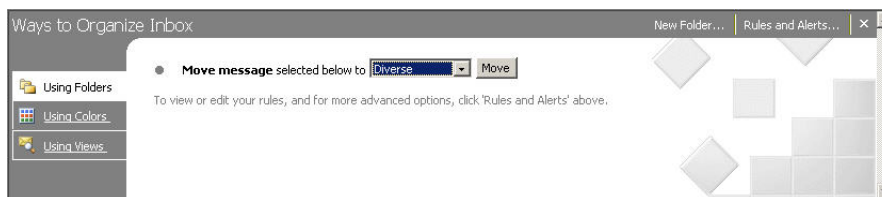


Figura 8.12. Organizarea mesajelor din foldere

Utilizarea filtrelor Outlook pentru mesaje. Programul Outlook are filtre încorporate care încearcă să identifice conținutul mesajele nedorite (spam). Aceste filtre utilizează liste de attribute cunoscute și cuvinte cheie comune ambelor tipuri de mesaje nedorite. Activarea filtrelor automate se realizează din meniul Actions, submeniul Junk E-Mail opțiunea Junk E-Mail Options (figura 8.13).

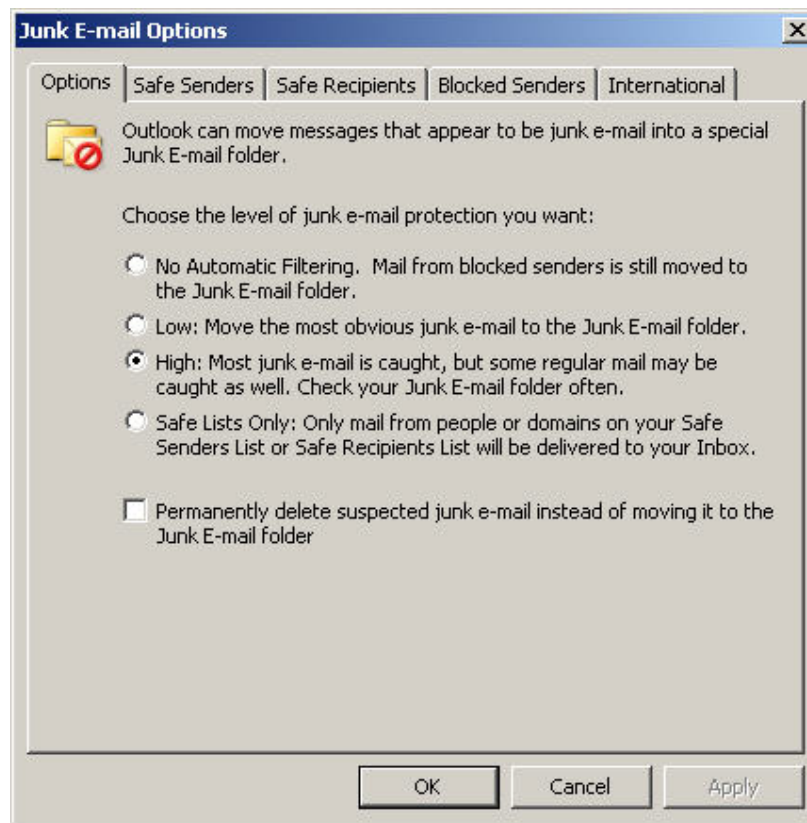


Figura 8.13. Opțiunile pentru Junk E-mail

Există posibilitatea de a stabili reguli pentru mesaje de e-mail care sosesc. Fereastra de definire a regulilor se activează din meniul Tools, opțiunea Rules and Alerts (figura 8.14). Regulile constau din criterii și acțiuni.

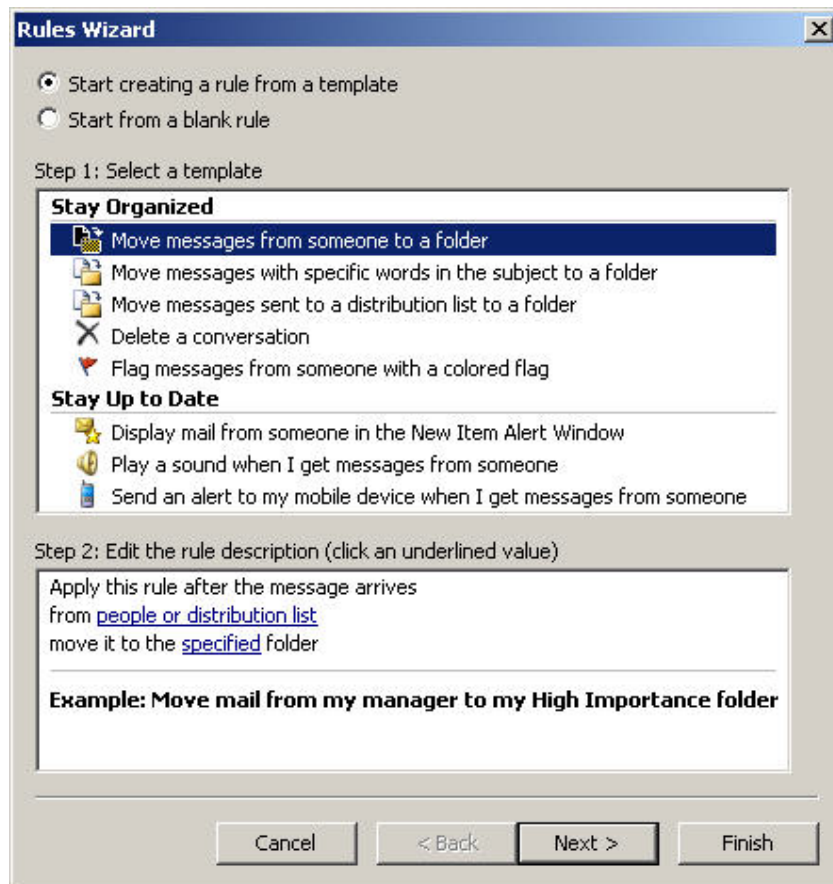


Figura 8.14. Stabilirea de reguli pentru mesaje

Criteriile se definesc în funcție de adresa destinatarului sau a expeditorului sau a existenței unor cuvinte în câmpul Subject sau în cadrul mesajului. În cazul identificării unor mesaje care corespund criteriilor stabilite, asupra acestora pot fi executate o serie de acțiuni (mutare, ștergere, marcare mesaj etc.). După definirea regulilor acestea sunt salvate și pot fi activate sau dezactivate.