II

PROTOCOALE DE COMUNICAȚII

II.1 SUITA DE PROTOCOALE TCP/IP

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

Protocoalele din această familie sunt ierarhizate pe cele patru nivele ale modelului TCP/IP (Fig. II.1). Protocoalele de pe nivelele superioare ale stivei beneficiază de serviciile furnizate de protocoalele de pe nivelele inferioare.

Numele acestei suite de protocoale este dat de protocolul de rețea (IP) și cel de transport (TCP). Totuși suita include mai multe protocoale deosebit de utile pentru furnizarea serviciilor Internet:

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

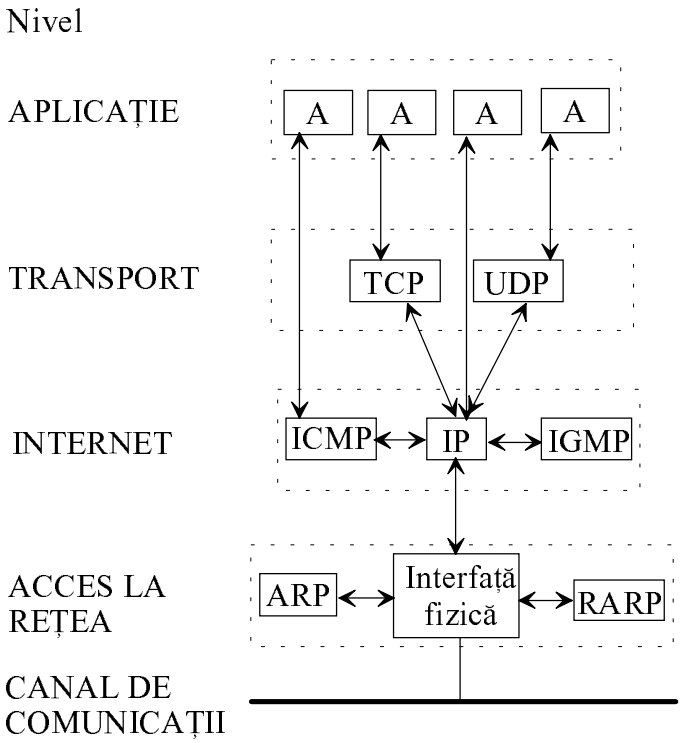


Fig.II.1 Comunicații între protocoalele din stiva TCP/IP (A= aplicatie)

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

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

ICMP (*Internet Control Message Protocol*) - protocol de nivel rețea care transportă mesaje de control și de eroare, referitoare la capacitatea sistemului de a transmite pachetele de date la destinație fără erori (RFC 792). Protocolul ICMP comunică direct cu aplicațiile, fără a accesa TCP sau UDP.

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

ARP (*Address Resolution Protocol*) - comunică la cerere, pe baza adresei IP a unui echipament, adresa fizică (MAC) de 6 octeți a acestuia (RFC 826). Tabelele ARP sunt stocate în memoria RAM a echipamentului (calculator, router etc). Se pot face echivalări sugestive între numele unei persoane și adresa MAC a echipamentului, respectiv între adresa poștală și adresa IP, care permit localizarea destinației unui mesaj.

RARP (*Reverse Address Resolution Protocol*) - furnizează la cerere adresa IP dată unui echipament cu adresa MAC, pe baza unor tabele (RFC 903).

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

Din figura II.1, se observă că un protocol de aplicație (A) poate comunica direct cu IP, dar în acest caz este nevoie să includă funcțiile de transport în propriul program de aplicație.

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

FTP (*File Transfer Protocol*) - protocol de transfer al fișierelor între calculatoare, mai precis un limbaj comun care permite comunicarea între orice sisteme de operare (DOS, UNIX etc) folosind programe FTP pentru client și server. FTP folosește TCP pentru transferul sigur al datelor (RFC 959).

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

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

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

SMTP (*Simple Mail Transfer Protocol*) - permite diferitelor calculatoare care folosesc TCP/IP să comunice prin poșta elelctronică (*e-mail / electronic-mail*). Acest protocol stabilește conexiunea punct-la-punct între clientul SMTP și serverul SMTP, asigură transferul mesajului prin TCP, înștiințează utilizatorul despre noul mesaj primit după care se desface legătura (RFC 821).

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

BOOTP (*BOOTstrap Protocol*) - este apelat de un utilizator pentru a-și afla adresa IP. Acest protocol folosește UDP pentru transportul mesajelor. Un calculator care folosește BOOTP, expediază un mesaj în rețea prin broadcast (pe o adresă IP cu toți biții '1'). Serverul de BOOTP

retransmite mesajul în toată rețeaua (*broadcast*) iar destinația își recunoaște adresa MAC și preia mesajul. Acest protocol nu poate lucra într-un sistem de alocare dinamică a adreselor IP, dar spre deosebire de RARP, acesta furnizează sursei atât adresa sa IP, cât și adresele IP ale serverului și ruterului (*default gateway*) folosit de LAN (RFC 951).

DHCP (*Dynamic Host Configuration Protocol*) - succesor al protocolului BOOTP, permite utilizarea unui număr limitat de adrese IP de către mai mulți utilizatori. Clientul solicită serverului DHCP o adresă IP. Acesta îi alocă o adresă dintr-un domeniu de adrese cunoscut, eventual îi furnizează și masca de rețea. Alocarea este rapidă și dinamică. Deși ruterele nu suportă transmisiile broadcast solicitate de ARP și RARP, ele permit aceste transmisii în cazul BOOTP și DHCP ceea ce facilitează comunicațiile dintre diverse LAN-uri.

HTTP (*HyperText Transfer Protocol*) - protocolul propriu al Web-ului, folosit de utilizatorii *web* și de serverele WWW pentru transferul unor fișiere de tip text, imagine, multimedia, în format special (*hypertext*), prin intermediul unui limbaj special HTML (*HyperText Markup Language*) folosind interfețe grafice pentru utilizatori (GUI - *Graphic Unit Interface*).

NTP (*Network Time Protocol*) - sincronizează ceasurile interne din două sau mai multe calculatoare, cu precizie de 1 - 50 ms față de timpul standard oficial (RFC 1305).

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

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

Datele circulă în stiva de protocoale de sus în jos, în cazul transmisiei, și de jos în sus, spre aplicații, la recepție. Datele sunt încapsulate la fiecare nivel de modulul software asociat protocolului după care sunt transmise nivelului inferior.

De exemplu, în cazul folosirii TCP ca protocol de transport pentru o aplicație rulată într-o rețea de calculatoare, încapsularea datelor se realizează în mai multe etape, la trecerea de pe un nivel pe altul, conform figurii II.2.

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

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

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

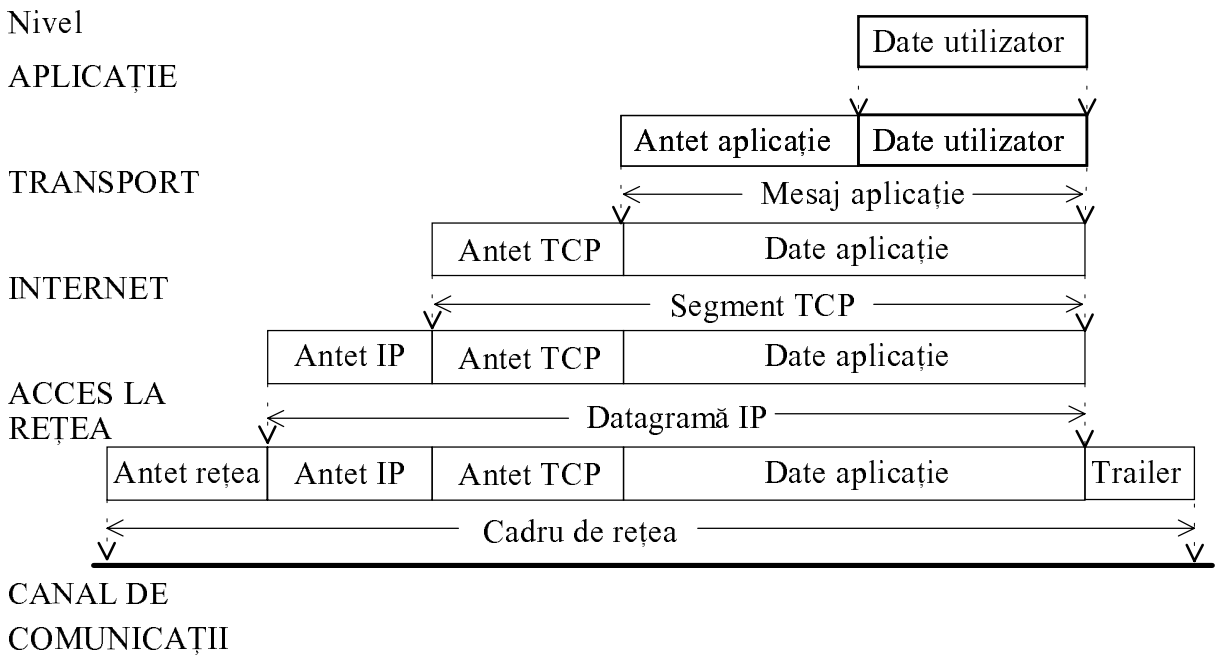


Fig.II.2 Încapsularea datelor în stiva TCP/IP folosind TCP

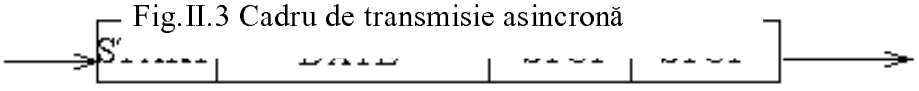
Unitatea generată de nivelul de transport este încapsulată cu un antet IP într-o **datagramă IP**, denumită uneori și pachet IP.

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

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

În cazul comunicațiilor asincrone, se transmit unități de date individuale (5 - 8 biți), încapsulate cu un bit de **start** de nivel '0' logic (*low*) și biți de **stop** (1; 1.5 sau 2 biți), de nivel '1' logic (*high*). În intervalele de **pauză de transmisie**, se menține nivelul logic '1'. Este posibilă introducerea în cadrul datelor a unui bit de paritate (impară, pară etc) pentru detecția unui număr impar de erori de transmisie.

Fig.II.3 Cadru de transmisie asincronă



II.1.1 Protocolul INTERNET. Adresarea IP

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

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

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

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

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

Formatul datagramei IP este prezentat în fig. II.4. Datele sunt precedate de un antet (*header*) de 20 sau 24 octeți, care include anumite câmpuri în care se specifică tipul de serviciu efectuat, gradul de securitate a transmisiei, detalii privind fragmentarea respectiv reasamblarea mesajelor de mari dimensiuni.

Semnificațiile câmpurilor din antetul IP sunt următoarele:

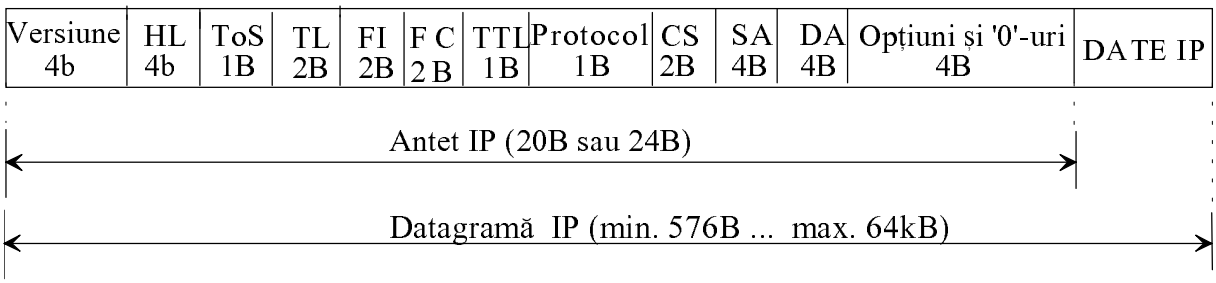


Fig. II.4 Formatul pachetului IP

Versiunea IP - este importantă pentru evitarea incompatibilității sistemelor.

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

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

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

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

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

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

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

1 ICMP

2 IGMP

6 TCP

8 EGP (*Exterior Gateway Protocol*)

17 UDP

89 OSPF (*Open Shortest Path First*).

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

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

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

"Opțiuni" și '0'-uri - reprezintă un câmp opțional folosit pentru diagnosticare (de exemplu, folosind PING - *Packet InterNetwork Groper*), securizare sau setare a rutelor. Acest câmp este

completat eventual cu zerouri astfel că lungimea header-ului crește cu 4 octeți atunci când se introduc diverse opțiuni.

ADRESAREA IP

O adresă IP este exprimată pe 4 octeți, în format zecimal cu puncte. Aceasta conține identificatorul de rețea (N - *network)*, eventual de subrețea (S - *Subnetwork*) care include echipamentul-gazdă și identificatorul plăcii de rețea a acestuia (H - *Host*). Identificatorul (ID - *IDentifier*) de rețea precede identificatorul plăcii de rețea. Adresa IP astfel formată este alocată în mod unic în Internet de InterNIC (*Internet Network Information Center*).

Schema de adresare IP este structurată pe cinci clase de adrese, diferențiate în funcție de lungimea câmpului alocat rețelei dar și prin prefixul binar utilizat (Tabel II.1) stabilit pe baza unui cod-prefix.

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

Tabel II.1 Clasele de adrese IP

Clasa de adrese	Lungimea adresei rețelei (B)	Prefix binar fix	Domeniul de valori al primului octet	Lungimea ID-ului de rețea (b)	Lungimea ID-ului gazdei (b)	Numărul de calculatoare - gazdă adresabile	Număr de rețele adresabile
A	1	0	0 - 127	7	24	16 777 214	126
B	2	10	128 - 191	14	16	65 534	16 382
C	3	110	192 - 223	21	8	254	2 097 150
D	(multicast)	1110	224 - 239	-	-	-	-
E	(rezervată)	11110	240 - 247	-	-	-	-

În aceeași rețea se folosește un singur ID de rețea dar ID-uri de gazdă diferite. Se spune că adresele de clasă A, B sau C sunt de tip *unicast* deoarece identifică în mod unic gazda.

Simbolic adresele IP pot fi scrise astfel:

1. adrese de clasă A:

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

2. adrese de clasă B:

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

3. adrese de clasă C:

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

De exemplu, rețeaua cu 4 calculatoare având adresele IP: 192.110.12.1; 192.110.12.2; 192.110.12.3; 192.110.12.4 are identificatorul de rețea 192.110.12.0.

Administrarea în mod unic a întregului spațiu de adrese din Internet este practic imposibilă, fiind vorba de circa 4 miliarde de adrese. De aceea s-a procedat la divizarea acestuia în rețele mai mici, cu număr redus de adrese care sunt administrate local de ISP (*Internet Service Provider*). Acest fapt a determinat reducerea numărului de adrese din Internet la circa 3,7 miliarde dar nu constituie un dezavantaj major deoarece alocarea adreselor se poate face dinamic, nu static (adresare fixă a gazdelor), numai pentru utilizatorii activi la un moment dat din rețea. Adresarea în interiorul LAN-ului poate fi făcută cu adrese locale alocate de administratorul de rețea și nu prin DNS, adrese care nu au legătură cu adresele IP reale date de DNS rețelei respective.

Observații

1. Adrese IP se alocă și unor interfețe fizice din echipamentele de comunicație (de exemplu, unui router i se pot aloca mai multe adrese IP, întrucât are mai multe interfețe de comunicație).

2. Pentru aplicații care necesită adresarea multicast se utilizează adrese de clasă D, în baza protocolului IGMP. Există adrese de grupuri prestabilite (*well-known*) de către IANA (*Internet Assigned Numbers Authority*) subordonată societății ISOC (*Internet SOCiety*) care coordonează funcționarea întregului Internet. Exemple de adrese multicast permanente (conform RFC 1112):

224.0.0.1 multicast către toate sistemele dintr-un LAN.

224.0.0.2 multicast către toate ruterele dintr-un LAN.

224.0.0.5 multicast către toate ruterele OSPF dintr-un LAN.

224.0.0.9 multicast pentru toate ruterele RIP-2 dintr-un LAN.

224.0.1.1 multicast pentru protocolul NTP (*Network Time Protocol*).

3. În multe cazuri chiar și 254 de adrese reprezintă un număr prea mare pentru o rețea de calculatoare locală. Se impune atunci partajarea unei clase de adrese (A, B, C) în mai multe subclase alocate **subrețelelor** (*subnetwork*) cu un anumit număr de utilizatori. Identificarea subrețelei se face în câmpul identificatorului gazdei, prin biții cei mai semnificativi. Numărul biților utilizați pentru identificatorul de subrețea, respectiv pentru ID-ul gazdelor, este restricționat la **minimum doi,** întrucât combinațiile de biți identici '1' sau '0' sunt rezervate.

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

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

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

Se pot forma 30 subrețele fiecare cu maximum 6 utilizatori.

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

Rutarea pachetelor prin Internet presupune că la nivelul ruterelor externe se citește adresa rețelei (fără ID-ul gazdei), iar la nivelul ruterelor interne se extrage adresa subrețelei. Pentru aceasta se folosesc **măști de rețea** (*network mask*) pe care le aplicăm adresei IP a destinației pentru a selecta ID-ul rețelei, respectiv **măști de subrețea** (*subnetwork mask*) pentru determinarea adresei subrețelei. În acest scop, se efectuează operația 'ȘI' logic (AND), bit cu bit, între adresa IP a destinației și mască. Masca de rețea sau de subrețea se obține prin impunerea valorii '1' tuturor biților din câmpul rețelei, respectiv a subrețelei, și '0' pe toate pozițiile din câmpul gazdei.

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

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

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

Exemplul 1

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

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

Adresa acestei rețele este 192.110.12.0.

Exemplul 2

Pentru adresa IP 170.202.112.23, de clasă B, se aplică masca de rețea 255.255.0.0 rezultând adresa rețelei: 170.202.0.0.

Exemplul 3

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

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

Masca de subrețea este: 11111111.11111111.11111111.11111000 sau 255.255.255.248.

Pentru aflarea numărului de identificare a gazdei în rețea sau subrețea, se aplică o combinație binară echivalentă măștii de rețea sau subrețea negate pe care o vom denumi simplu **masca negată** (*wild card*), având toți biții '0' în câmpul rețelei și subrețelei, respectiv '1' în câmpul gazdei.

Exemplul 4

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

00000000.00000000.00000000.00000111

iar în format zecimal cu puncte rezultă 0.0.0.7.

Prima subrețea formată are adresa 192.110.12.8 și clasa de adrese pentru calculatoarele-gazdă 192.110.12.9 ... 192.110.12.14. Adresa de broadcast a subrețelei este 192.110.12.15.

A doua subrețea are adresa 192.110.12.16, clasa de adrese a gazdelor 192.110.12.17 ... 192.110.12.22 și adresa de broadcast 192.110.12.23 ș.a.m.d. Similar se stabilesc adresele tuturor subrețelelor formate.

Observații

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

2. Adresele IP ale interfețelor echipamentelor de comunicație (gateway, firewall, router) prin care se transportă pachetele între LAN și WAN, mai sunt denumite și **adrese de transport**. În general, este indicat ca unui echipament de comunicație să i se aloce o clasă de adrese separată. Rutarea pachetelor se va face pe baza tabelelor de rutare în care sunt stabilite rutele între adresele de transport.

3. Pentru lărgirea spațiului de adrese din Internet s-a propus folosirea **IPng** (*IP next generation*) sau IPv6 care, spre deosebire de IPv4, folosește adrese de 128 de biți, ordonate ierarhic; elimină broadcast-ul în favoarea multicast-ului; include în cadrul IP un header cu lungime fixă

conținând informații strict necesare rutării pachetelor, altele fiind incluse în subheadere; suportă modul automat de alocare a adreselor IP; permite autentificarea și criptarea datelor; prevede un sistem de priorități privind transmisia care să faciliteze transmisiile multimedia (voce, audio, video).

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

APLICAȚII

1. Un calculator cu adresa 193.214.32.125 dorește să transmită în rețeaua locală un mesaj prin broadcast. Ce adresă IP a destinației utilizează? Care este adresa de broadcast pentru această rețea?

2. Administratorul de rețea transmite utilizatorilor din rețea un mesaj prin broadcast. Dacă adresa IP a sursei este 172.100.94.1care este adresa IP a destinației?

3. Sursa cu adresa IP 173.100.94.1 transmite un mesaj calculatorului cu adresa 192.100.10.120. Ce mască de rețea se aplică la nivelul ruterelor?

4. Unui LAN i se alocă ID-ul de rețea 193.125.117.0. Administratorul constată că îi sunt necesare subrețele cu maximum 30 utilizatori.

a. Câte subrețele poate forma?

b. Ce mască de subrețea se utilizează ?

c. Ce mască de rețea se aplică ?

d. Care sunt adresele subrețelelor respectiv clasele de adrese ale calculatoarelor-gazdă din fiecare subrețea?

e. Ce adrese de broadcast se utilizează în fiecare subrețea formată?

5. Pentru o adresă IP 203. 192.45.16 se folosește masca de subrețea 255.255.255.192. Determinați:

a. numărul de biți utilizați pentru ID-ul subrețelei;

b. numărul de subrețele existente în acest LAN;

c. adresele subrețelelor;

d. măștile de rețea, de subrețea și masca negată;

e. clasele de adrese și adresa de broadcast pentru a treia subrețea (în ordine crescătoare a adreselor de subrețea).

II.1.2 DNS - Sistemul numelor de domenii Internet

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

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

Numele nodurilor din Internet sunt compuse din mai multe **etichete** separate prin puncte (de exemplu, etc.tuiasi.ro), fiecare etichetă reprezentând numele unui **domeniu Internet** în care este inclus calculatorul respectiv. Un domeniu Internet este definit pe baza unor caracteristici de activitate sau de localizare, folosind o diagramă de tip 'arbore', cu un nod 'rădăcină' și mai multe nivele de ierarhizare (Fig. II.5).

Pe primul nivel, DNS este împărțit în trei domenii:

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

2. **grupul generic** al organizațiilor, cuprinzând șapte categorii de bază, fiecare asociată unei etichete compusă din trei caractere (Tabel II.2).

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

Tabel II.2 Grupul generic din Internet

Etichetă	Descrierea domeniului
`com`	organizație comercială
`edu`	organizație educațională
`gov`	organizație guvernamentală (rezervat S.U.A.)
`int`	organizație internațională (rezervat S.U.A.)
`mil`	organizație militară
`net`	rețea propriu-zisă neinclusă în alte categorii
`org`	alte organizații (cu specific noncomerial, nonguvernamental etc)

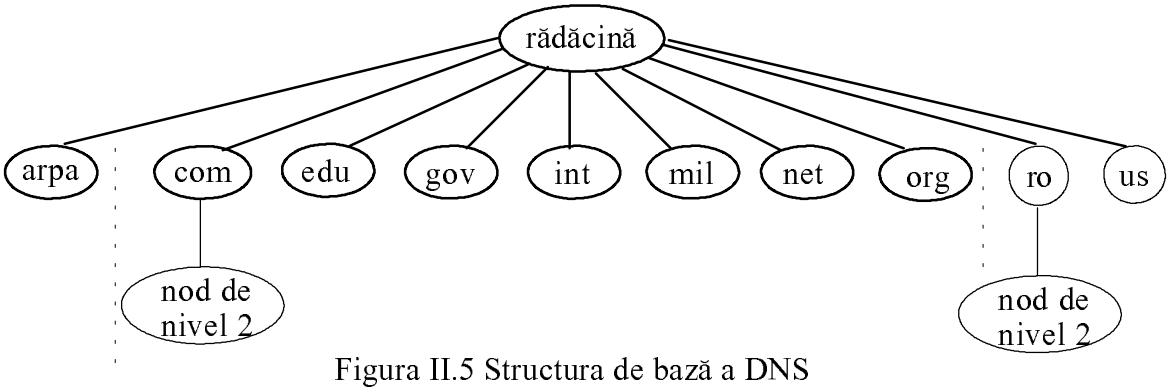


Figura II.5 Structura de bază a DNS

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

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

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

Programul-client pentru translarea numelor de domenii Internet apelează o funcție de translare a adreselor (de exemplu, *gethostbyaddr, gethostbyname*), care deschide un canal de comunicație cu programul-server DNS, transmite cererea și după ce primește de la server informația despre adresa respectivă, închide canalul și transmite informația programului-client.

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

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

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

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

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

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