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 .

II.1.3 Protocoale de adresare (ARP, RARP, BOOTP, DHCP)

Echipamentele conectate în rețea (plăci de rețea, modemuri etc) sunt descrise prin așa-numita **adresă fizică**, dată de producător. Aceasta este exprimată pe șase octeți, în format hexazecimal și este unică în lume, fapt asigurat de modul de alocare a adresei: primii trei octeți identifică firma producătoare (OUI - *Organizational Unique Identifier*) iar ultimii trei, cei mai puțin semnificativi, sunt alocați de către producător, echipamentului.

Adresa fizică se mai numește și **adresă MAC** întrucât este folosită pentru acces la mediul fizic de transmisie, pe subnivelul MAC al nivelului legăturii de date din modelul OSI.

Rutarea pachetelor în WAN nu se face pe baza adreselor fizice, ci pe a celor de rețea, conform ierarhiei stabilite prin sistemul numelor de domenii. Prin urmare, este necesară conversia adreselor de rețea în cele fizice și invers. Pe baza adreselor fizice și a celor de rețea se realizează încapsularea datelor pe nivelele OSI 2 și 3.

Un router are incorporate mai multe plăci de rețea, fiecare cu o adresă de rețea proprie. Adresa IP alocată interfeței ruterului prin care o rețea locală se conectează la WAN, trebuie să fie din clasa de adrese a LAN-ului. Această adresă este considerată ca adresă implicită a porții de acces în WAN (*default gateway*).

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

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

În suita de protocoale TCP/IP, se utilizează mai multe protocoale de adresare: ARP, RARP, BOOTP, DHCP.

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

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

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

Cererea ARP (*ARP Request*) este transmisă în rețea numai dacă adresa solicitată nu există în tabelul ARP. Pachetul cu cererea ARP conține adresa MAC de broadcast, adresa MAC a sursei, adresele IP ale sursei și destinației, precum și un cod de cerere ARP (Fig.II.6). Stația de destinație din rețeaua locală răspunde printr-un alt pachet (*ARP Reply*) adresat stației care a inițiat cererea, pachet care include adresa sa MAC.

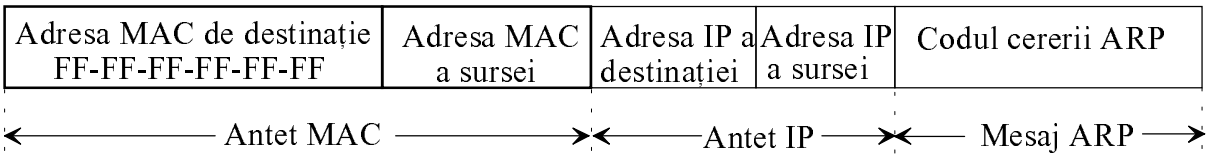

Fig.II.6 Formatul pachetului conținând cererea ARP

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

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

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

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

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

Pachetul RARP include adresele MAC ale sursei și destinației, adresa IP de broadcast, un câmp de adresă IP necompletat pentru adresa IP proprie și codul cererii RARP, conținut în memoria sa ROM (Fig.II.7). Serverul RARP răspunde cererii cu un pachet conținând adresa IP solicitată.

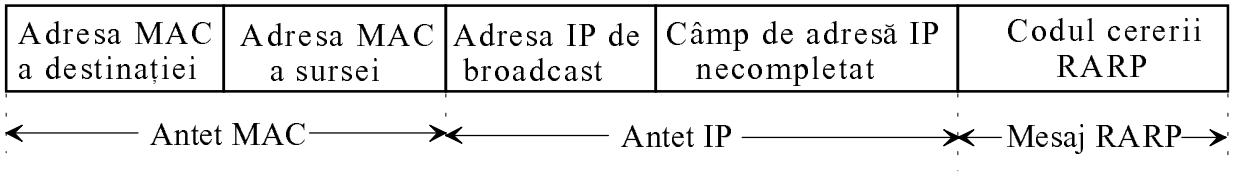

Fig.II.7 Formatul pachetului conținând cererea RARP

Observație

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

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

BOOTP a fost inițial proiectat pentru stațiile de lucru fără disc, pe care nu erau memorate informațiile de configurare IP. Pe serverul BOOTP există o bază de date în care se stochează adresele MAC ale stațiilor din LAN și adresele IP asociate fiecăreia, în mod static. Un calculator care folosește BOOTP, expediază cererea de aflare a adresei IP proprii (*BOOTP Request*) în rețea, prin broadcast (pe o adresă IP cu toți biții '1'). Serverul BOOTP transmite automat răspunsul (*BOOTP Reply*) în toată rețeaua prin broadcast, iar destinația 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, el furnizează sursei atât adresa sa IP, cât și adresele IP ale serverului și ruterului (*default gateway*) folosit de LAN.

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

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

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

Alocarea este rapidă și dinamică, protocolul fiinddeosebit de util pentru terminale mobile și pentru serviciul de roaming în WAN.

Observații

1. Întrucât DHCP alocă dinamic adresele IP și identificarea stațiilor se face pe baza numelor, apar probleme de actualizare a bazelor de date de pe serverele DNS. De aceea, se preferă utilizarea DHCP cu servere WINS (*Windows Internet Name Service*)
2. Deși ruterele nu suportă retransmisiile broadcast solicitate de ARP și RARP, ele permit aceste retransmisii în cazul BOOTP și DHCP, ceea ce facilitează comunicațiile dintre diverse LAN-uri.
3. Suplimentar față de metoda alocării dinamice, DHCP suportă și modul automat, și modul manual de alocare a adreselor într-o rețea TCP/IP. Modul automat presupune alocarea de adrese IP permanente nodurilor din LAN. În modul automat, DHCP este utilizat doar pentru intermedierea procesului de negociere a adresei, dintre administratorul de rețea și stația-gazdă.

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

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

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

II.1.4 Protocoale de transport (TCP,UDP)

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

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

Mesajul de pe nivelul aplicație este fragmentat în mai multe secvențe, pentru a nu depăși lungimea maximă admisă a unității de date transmise pe nivelul fizic (MTU - *Maximum transmission unit*). Datele sunt este încapsulate cu antetul TCP (Fig. II.8) și generate ca **segment TCP.** Acesta devine câmpul de date în datagrama IP. La recepție, TCP este responsabil de refacerea mesajului prin asamblarea corectă a tuturor secvențelor sale.

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

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

Numărul de confirmare (ACK n) specifică recepția corectă a secvențelor transmise și precizează numărul următoarei secvențe așteptate.

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

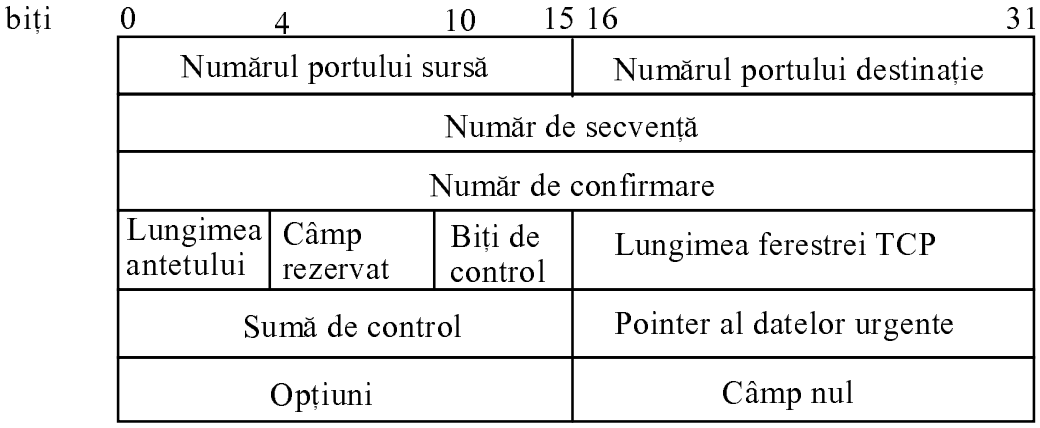

Fig.II.8 Formatul antetului TCP

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

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

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

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

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

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

FIN (*Final*) - specifică sfârșitul transmisiei.

Stabilirea unei conexiuni TCP se face în trei pași (*Three-Way Handshake Open Connection*), în care se folosesc acești biți pentru controlul fluxului și inițierea numerelor de secvență (SN) în ambele sensuri (Fig. II.9).

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

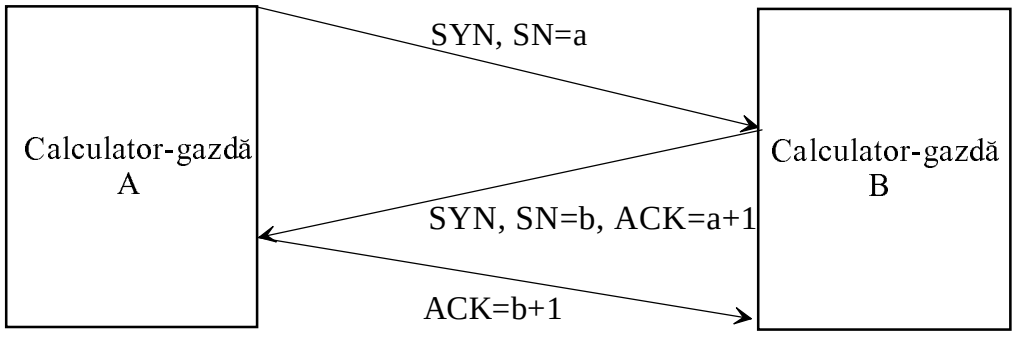

Fig. II.9 Algoritmul în trei pași de deschidere a conexiunii TCP

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

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

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

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

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

TCP folosește porturi de aplicație sau de protocol pentru a realiza comunicații simultane cu mai multe programe. Numerotarea porturilor de protocol se face global, în mod unic, pe întregul Internet și este descrisă în RFC 1700 (Tabel II.3). Aceste numere de protocol sunt utilizate atât de TCP, cât și de UDP.

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

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

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

Anumite numere de porturi de aplicații sunt utilizate numai de TCP.

Protocolul UDP (*User Datagram Protocol*) este considerat nesigur deoarece nu este orientat pe conexiune, nu utilizează mesaje de confirmare a recepției corecte, nu face retransmisia pachetelor eronate, nu permite controlul fluxului informațional și nu asamblează secvențele în cazul

Portul-sursă	Portul-destinație	Lungime	Sumă de control

Fig. II.10 Formatul antetului UDP

mesajelor fragmentate.

Avantajul acestui protocol este dat de viteza mare de procesare a datelor comparativ cu TCP.

Mesajul generat de nivelul aplicație formează împreună cu antetul UDP de 8 octeți o **datagramă UDP** (Fig. II.10).

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

Tabel II.3 Numerotarea porturilor logice de protocol

Protocol de aplicație din suita TCP/IP	Numărul portului alocat
Echo Protocol	7
Active Users	11
Daytime Protocol	13
FTP	21
SSH	22
Telnet	23
SMTP	25
TIME	37
RLP	39
NAME SERVER	42
NICNAME	43
DNS	53
BOOTP server	67
BOOTP client	68
TFTP	69
GOPHER	70
FINGER	79
HTTP*	80
POP2	109
POP3	110
Authentication Service*	113
UUCP Path Service*	117
NTP	123
NetBIOS Service	139
SNMP	161

* valabil numai pentru TCP

Observație

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

II.1.5 Protocolul Telnet

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

Acest protocol rezolvă incompatibilitățile dintre două sisteme implicate într-o conversație în rețea, prin folosirea conceptului de **terminal virtual de rețea** (NVT - *Network Virtual Terminal*), prin care se specifică anumite caracteristici de bază ale unui terminal simplu (*dumb*). De exemplu, VT100 este un NVT. Programele care comunică în rețea prin Telnet convertesc datele în formatul impus de NVT.

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

NVT ASCII utilizează numai o parte din secvențele de control definite de ASCII (Tabel II.4)

Tabel II.4 Secvențe de control NVT ASCII

Secvență de control	Cod hexazecimal	Semnificație
NUL	0x00	*no operation*
BEL	0x07	*bell*
BS	0x08	*backspace*
HT	0x09	*horizontal tab*
LF	0x0A	*line feed*
VT	0x0B	*vertical tab*
FF	0x0C	*form feed*
CR	0x0D	*carriage-return*

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

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

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

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

Utilizarea Telnet permite accesul de la distanță la stația de destinație.

Comanda de conectare pe un terminal din rețea folosind Telnet include fie adresa IP (*ipadd*) a terminalului pe care se dorește să se conecteze clientul Telnet, fie numele calculatorului, simplu dacă este în aceeași rețea sau incluzând numele domeniului Internet din care face parte dacă stația aparține altui segment de rețea. De asemenea, se poate specifica un nume echivalent (nickname) cu condiția ca acesta să fie inclus în baza de date de utilizatori de pe serverul de nume.

Este mai simplu de accesat o stație prin Telnet folosind numele prescurtat al terminalului sub forma unei combinații sugestive și accesibile de caractere (*nickname*), care poate fi definită printr-o comandă de asociere a acestuia cu adresa IP a stației respective (set).

Lista numelor calculatoarelor-gazdă incluse în baza de date poate fi afișată pe ecran cu comanda de vizualizare (show).

TTY (*TeleTYpe*) reprezintă denumirea echivalentă a terminalului virtual, fiind împrumutată din sistemul de operare UNIX.

Prin comanda de conectare sau comanda telnet, se creează temporar un TTY pentru serviciul respectiv și un alt TTY pentru portul accesat.

Conexiunea se realizează inițial cu parametrii impliciți pentru terminalul accesat, cu posibilitatea negocierii altor parametri pentru facilitarea comunicării.

Stabilirea tipului de terminal (de exemplu: dumb, vt100) accesat într-o sesiune Telnet se face prin comanda de definire a acestuia (set).

Se pot deschide mai multe sesiuni Telnet simultan.

Alte comenzi, valabile și pentru alte servicii de comunicații din Internet, sunt definite pentru

crearea serviciului (create), eliminarea serviciului (destroy), conectare (connect), deconectare (disconnect), reconectare (reconnect), vizualizare a sesiunilor, serviciilor sau parametrilor de terminal virtual (show).

Observații

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

2. Sintaxa comenzilor protocolului depinde de firma producătoare a echipamentelor.