

CAPITOLUL 5

SISTEME DE OPERARE ÎN REȚEA

5.1 Protocoalele TCP/IP

TCP/IP reprezintă un grup de protocoale a cărui denumire este dată de principalele sale standarde, TCP (Transmission Control Protocol) și IP (Internet Protocol). Aceste protocoale pot fi folosite pentru comunicații în cadrul oricărui set de rețele interconectate. Viabilitatea tehnologiei TCP/IP a fost verificată la o scară foarte mare. Protocoalele TCP/IP stau la baza unei mari rețele, numite Internet, care a început cu mai bine de 25 de ani în urmă cu rețeaua ARPA (Advanced Research Projects Agency), ulterior denumită și DARPA (Defense Advanced Research Projects Agency) și care acum regroupează zeci de mii de rețele, utilizând același ansamblu de protocoale, pentru a oferi o interfață unică utilizatorilor lor. Software-ul de rețea, înglobând o mare parte din protocoalele TCP/IP, este disponibil pe o gamă largă de calculatoare care folosesc diferite sisteme de operare.

Dintre serviciile de aplicații oferite utilizatorilor de rețeaua Internet cele mai frecvent folosite sunt poșta electronică (e-mail), transferul de fișiere, WWW și conexiunea la un calculator distant (remote login). Permanent noi servicii sunt oferite utilizatorilor. La nivelul transport se asigură atât servicii cu conexiune cât și servicii fără conexiune.

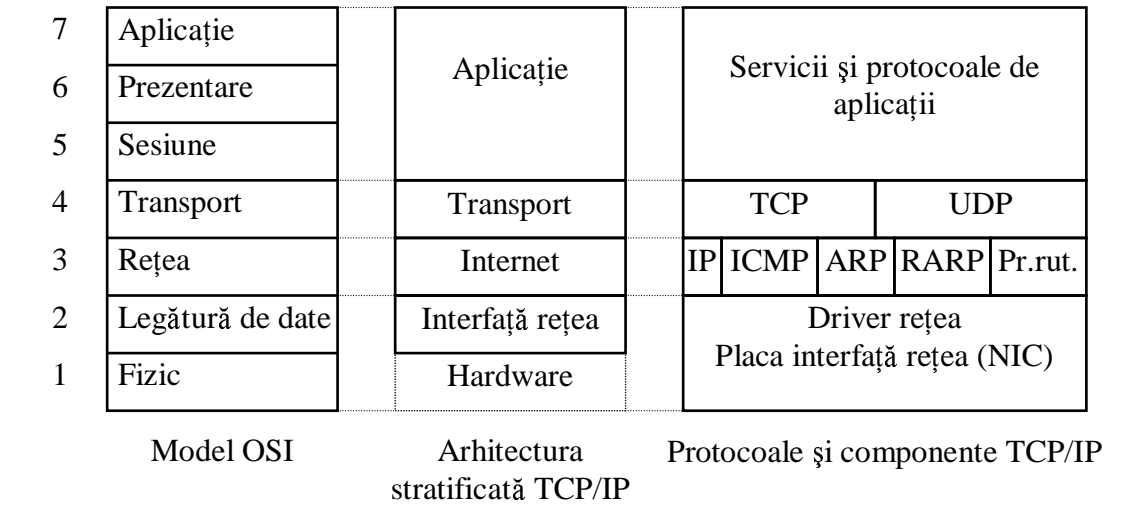
Autoritatea supremă care dirijează evoluția rețelei Internet este o organizație constituită din membri voluntari, numită Internet Society (ISOC). În cadrul acestei organizații există un consiliu, numit Internet Architecture Board (IAB), care are responsabilitatea tehnică a evoluției rețelei. El aprobă standarde noi, alocă resurse și ia decizii privind rețeaua.

Un alt organism, IEFT (Internet Engineering Task Force), are sarcina de a dezbate, periodic, probleme pe termen scurt: publică rapoarte și documentație, sugerează acceptarea unor idei propuse pe bază de voluntariat sau propune adoptarea unor noi standarde.

Documentația Internet, inclusiv standardele, este publicată sub forma unor documente RFC (Request for Comments). Documentul RFC 1540, intitulat Internet Official Protocol Standards, detaliază lista tuturor documentelor RFC.

5.1.1 Arhitectura TCP/IP

Arhitectura stratificată a unei rețele TCP/IP este prezentată, prin comparație cu modelul OSI, în figura 5.1.



TCP - Transmission Control Protocol	ICMP - Internet Control Message Protocol
UDP - User Datagram Protocol	ARP - Address Resolution Protocol
IP - Internet Protocol	RARP - Reverse Address Resolution Protocol

Figura 5.1 Arhitectura TCP/IP

Protocoalele TCP/IP sunt conceptual organizate în patru nivele care se sprijină pe un al cincilea nivel, reprezentat de circuitistica necesară pentru transmiterea semnalelor de date.

Nivelul cel mai de jos dintre cele patru, numit interfață rețea, face ca funcționarea nivelului imediat superior, numit internet și echivalent nivelului rețea din modelul OSI, să nu depindă de rețeaua fizică utilizată pentru comunicații și de tipul legăturii de date. O interfață rețea poate fi constituită dintr-un driver rețea, când sistemul este conectat la o rețea locală, sau un subsistem mai complex care utilizează un anumit protocol al legăturii de date (epre exemplu HDLC, atunci când rețeaua utilizează comutatoare de pachete).

O rețea individuală TCP/IP poate fi o rețea locală, utilizând diferite protocoale de subnivel MAC (802.3, 802.4, 802.5 etc), poate fi o rețea care folosește legături de date de mare distanță de tipul circuitelor punct la punct închiriate sau comutate, cu un suport fizic oarecare.

Un concept fundamental al unei rețele globale TCP/IP, rezultate din interconectarea unor rețele cu tehnologii diferite, este acela că, din punct de vedere al rețelei globale, orice sistem de comunicații capabil să transfere pachetele contează ca o singură rețea, indiferent de caracteristicile sale. Protocoalele TCP/IP tratează toate rețelele la fel. În esență, protocoalele TCP/IP definesc o rețea abstractă care nu ține seama de detaliile rețelelor fizice componente.

Interconectarea rețelelor fizice se realizează prin intermediul rutelor. Stabilirea rutelor se face luând ca bază rețeaua de destinație. În felul acesta volumul informației necesare pentru rutare depinde de numărul rețelelor interconectate și nu de numărul sistemelor din rețea.

Nivelul interfață rețea acceptă mesajele de la nivelul internet și le pregătește pentru transmiterea pe un anumit tip de legătură de date (rețea fizică). Pe de altă parte, nivelul interfață rețea analizează fiecare cadru recepționat de placa NIC și determină, după biții de control ai cadrului, care este protocolul de nivel internet căruia trebuie să i se transmită datele din cadrul recepționat.

Nivelul internet realizează funcțiunile de rutare și de releu pentru transmiterea pachetelor de la sistemul sursă la sistemul destinație. La acest nivel se utilizează mai multe protocoale, dintre care se remarcă potocolul Internet (Internet Protocol - IP) care asigură un serviciu de transmitere a datelor fără conexiune.

Protocolul ICMP (Internet Control Message Protocol) folosește serviciile IP (mesajul ICMP ocupă câmpul de date al IP), asigurând un mecanism prin care ruterii și sistemele din rețea comunică informații privind situațiile de funcționare anormală.

Protocolul ARP (Address Resolution Protocol) permite unui sistem să determine adresa fizică (MAC) a unui alt sistem din aceeași rețea fizică cunoscând adresa IP (de nivel rețea) a acestuia.

Protocolul RARP (Reverse Address Resolution Protocol) permite unui sistem să-și obțină, atunci când n-o cunoaște, adresa IP proprie.

Nivelul transport asigură comunicația între programele de aplicație. O astfel de comunicație este numită adesea comunicație cap - la - cap. Nivelul transport poate regla

fluxul datelor, poate asigura livrarea datelor fără erori și în secvență. La nivelul transport fluxul datelor ce trebuie transmise se împarte în pachete și fiecare pachet este trecut, împreună cu adresa de destinație, către nivelul internet pentru transmisiune. Când mai multe programe de aplicație beneficiază, în același sistem, de serviciile rețelei, nivelul transport trebuie să accepte datele de la acestea și să le treacă spre nivelul inferior, adăugând fiecărui mesaj informația necesară pentru identificarea programelor de aplicație.

Sunt folosite două protocoale de transport: UDP (User Datagram Protocol) și TCP (Transmission Control Protocol). Protocolul UDP asigură un serviciu fără conexiune folosind IP pentru transportul mesajelor. Acest protocol, mai simplu decât TCP, nu garantează livrarea mesajului la recepție fără erori, fără pierderi, fără duplicate, în ordinea în care au fost emise. Programele de aplicație care utilizează UDP ar trebui să-și asume responsabilitatea deplină pentru soluționarea acestor aspecte ale transmisiunii. Protocolul TCP asigură un serviciu cu conexiune, garantând livrarea corectă, în ordine, a mesajelor la recepție.

La elaborarea unui program de aplicație se alege protocolul de transport în funcție de necesitățile impuse de aplicație.

Nivelul aplicație asigură utilizatorilor rețelei, prin intermediul programelor de aplicație, o gamă largă de servicii. Dintre acestea cele mai frecvent folosite sunt SMTP (Simple Mail Transfer Protocol), FTP (File Transfer Protocol), Telnet Remote Login, SNMP (Simple Network Management Protocol), WWW.

Protocolul SMTP este folosit pentru transferul mesajelor de poștă electronică. Utilizatorul poate transmite mesaje sau fișiere altui utilizator conectat la Internet sau la un alt tip de rețea, având însă o conexiune cu Internet.

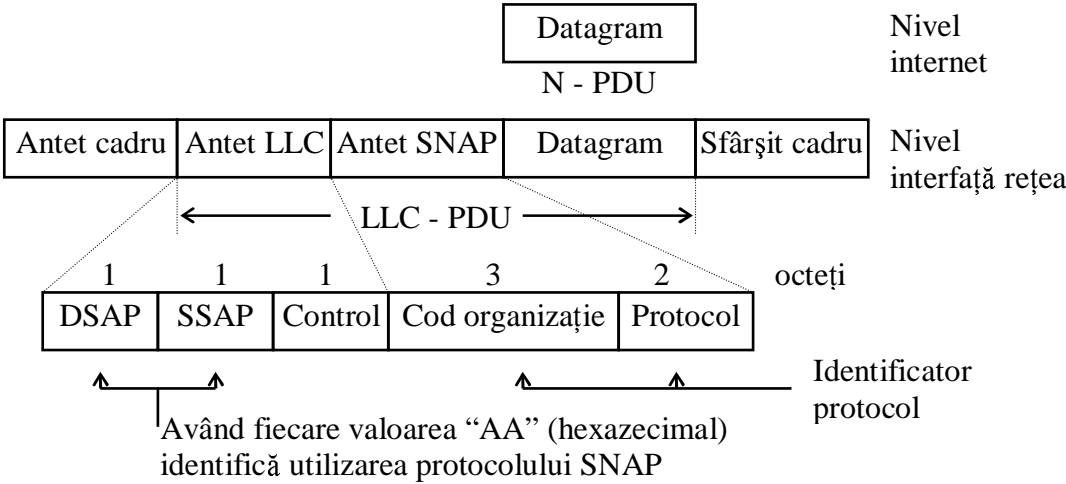
Protocolul FTP permite utilizatorilor transferul de fișiere, în ambele sensuri, între un sistem local și unul distant. Fișierele pot conține fie texte (caractere ASCII sau EBCDIC), fie date pur binare.

Protocolul Telnet permite unui utilizator să se identifice într-un sistem distant prin intermediul sistemului local. Acest protocol stabilește o relație client - server între sistemul local (client) și aplicația Telnet distantă (server), permițând deci funcționarea unui sistem local în regim de terminal virtual conectat la un sistem distant.

Protocolul SNMP este folosit pentru administrarea de la distanță a echipamentelor de interconectare a rețelelor.

5.1.2 Nivelul interfață rețea (legătură de date)

Data fiind, din punct de vedere fizic, diversitatea rețelelor ce pot fi interconectate prin TCP/IP, arhitectura TCP/IP nu specifică utilizarea unui anumit protocol de nivel legătură de date. Există totuși standarde (RFC) pentru suport Ethernet (RFC 894), suport IEEE 802 (RFC 1042), suport X.25 (RFC 877) și pentru alte tipuri de suport.



SNAP - Sub-Network Access Protocol
DSAP (SSAP) - Destination (Source) Service Access Point
Valoarea "03" (hexazecimal) în câmpul de control LLC indică informație nenumerotată

Figura 5.2 Structura generală a unui cadru

Unitățile de date primite de la nivelul internet (rețea), numite datagrame (datagrams) în cadrul protocolului IP, sunt încapsulate, în cazul în care sistemul se află într-o rețea LAN, în cadre cu structura corespunzătoare tipului de rețea (802.3, 802.4, 802.5, FDDI etc.). Figura 5.2 arată structura generală a unui cadru, evidențiind câmpul unității de date primite de la nivelul internet (N - PDU) și informațiile de protocol ce trebuie adăugate de subnivelele LLC și MAC.

5.1.3 Nivelul internet (rețea)

- Adresele de rețea IP -

În versiunea 4 a grupului de protocole TCP/IP adresele de nivel rețea sunt compuse din patru octeți, lungime considerată insuficientă pentru a permite subadresări particulare.

Tip adresă	Identificator rețea	Identificator sistem
---------------	------------------------	-------------------------

Figura 5.3 Structura adresei IP

Adresa (Fig. 5.3) se compune dintr-un prefix, specificând clasa rețelei și, totodată, delimitarea câmpurilor identificatorilor de rețea și de sistem, urmat de identificatorul rețelei și de identificatorul sistemului în rețeaua respectivă. Sunt definite patru clase de adrese, specificate de primii biți ai primului octet (Fig. 5.4).

A	0XXXXXXXX			
	Identificator rețea	Identificator sistem		
B	10XXXXXXXX	XXXXXXXXXX		
	Identificator rețea		Identificator sistem	
C	110XXXXXX	XXXXXXXXXX	XXXXXXXXXX	
	Identificator rețea			Identificator sistem
D	1110XXXXX			
	Adresă multidestinatari			

Figura 5.4 Formatul adreselor IP

Adresele din clasa A au în prima poziție bitul 0. Ceilalți șapte biți ai primului octet identifică rețeaua fizică. Pot fi până la 126 rețele care utilizează adrese din clasa A (adresele 0 și 127 nu sunt utilizate). Deoarece o adresă din clasa A are 24 biți pentru a identifica un sistem, o rețea din această clasă poate avea practic un număr aproape nelimitat de sisteme.

Adresele din clasa B au în primele două poziții dibitul 10, următorii 14 biți identifică rețeaua, iar ultimii 16 biți identifică sistemul. Pot exista, interconectate, până la $2^{14} - 2$ rețele, fiecare cu până la $2^{16} - 2$ sisteme.

Adresele din clasa C încep cu tribitul 110, următorii 21 biți identifică rețeaua, iar ultimii opt biți identifică sistemul în fiecare rețea. Pot fi până la $2^{21} - 2$ rețele cu adrese de acest tip, fiecare rețea cu până la 254 sisteme.

Adresele din clasa D încep cu grupul 1110 în primele patru poziții și sunt utilizate pentru difuzarea mesjelor de la un sistem către un grup de sisteme din rețeaua globală.

Uzual adresa unui sistem este prezentată prin echivalentul zecimal al fiecărui octet:

IP 23.8.124.73 = 0010111.00001000.01111100.01001001

Masca asociată unei rețele permite determinarea rețelei (identificator) căreia aparține un sistem când se cunoaște adresa de rețea a sistemului: operația logică ȘI, aplicată bit cu bit adresei sistemului și măștii are ca rezultat identificatorul rețelei. Masca unei rețele va avea biți 1 în octeții corespunzători identificatorului rețelei și în rest biți 0. De exemplu, pentru o rețea în clasa B masca va fi 255.255.0.0:

ȘI 128.35.12.30 → 10000000.00100011.00001100.00011110
 255.255.0.0 → 11111111.11111111.00000000.00000000
 128.35.0.0 → 10000000.00100011.00000000.00000000

În tabelul de mai jos sunt prezentate domeniile de valori pentru identificatorii de rețea corespunzători primelor trei clase, precum și măștile rețelelor.

Clasa rețelei	Structura identificatorului de rețea	Domeniul de valori pentru identificatorul rețelei	Masca rețelei
A	0xxxxxxx/0/0/0	1 – 126	255.0.0.0
B	10x...x/x...x/0/0	128.1 – 191.254	255.255.0.0
C	110x..x/x...x/x...x/0	192.0.1 – 223.255.254	255.255.255.0

După cum se poate observa, clasa rețelei se poate recunoaște după primul octet:

1 – 126 clasa A; 128 – 191 clasa B; 192 – 223 clasa C.

- Subrețele IP –

O rețea poate fi divizată în subrețele (după localizarea sistemelor unei companii); pentru identificarea subrețelor se utilizează un număr de biți, dependent de numărul subrețelor, din primele poziții ale identificatorului de subsistem. Spre exemplu, fie o rețea clasa A, cu 5 subrețele. Masca pentru rețele din clasa A este 255.0.0.0.

Masca pentru subrețele este:

255.224.0.0 = 11111111.11100000.00000000.00000000

Cei trei biți care identifică fiecare subrețea pot fi: 100(00000) = 128; 110(00000) = 192; 101(00000) = 160; 011(00000) = 96; 010(00000) = 64.

Adresele de difuziune, specificând faptul că pachetul este adresat tuturor sistemelor dintr-o rețea, au toți biții identificatorului de sistem egali cu 1.

Clasa A, permițând un număr redus de rețele, este atribuită rețelei Arpanet. Adresele din clasele B și C, permițând un număr mult mai mare de rețele, sunt atribuite organizațiilor individuale. Pentru a asigura identificatori de rețea unici în toată lumea,

această atribuire de adrese este asigurată de o autoritate centrală. De fapt, o adresă IP, specificând o rețea și un sistem conectat la acea rețea, nu specifică un anumit calculator, ci o conexiune la rețea. Un ruter, spre exemplu, interconectând mai multe rețele, va avea mai multe adrese IP distincte, câte una pentru fiecare rețea la care este conectat

Adresa de rețea și adresa hardware fizică a plăcii NIC instalate într-un sistem sunt distincte. Protocoalele de la nivelul rețea ale grupului TCP/IP asigură metode de conversie între adresele de rețea de 32 biți și adresele fizice (MAC) utilizate pe o legătură de date particulară.

- Protocolul IP -

Protocoalele care operează la nivelul internet (rețea), asigurând servicii protocoalelor operând la nivelul transport, realizează rutarea și comutarea pachetelor (datagrams) prin rețelele de comunicații din care se compune rețeaua globală Internet. Principalul protocol de la acest nivel este protocolul IP (Internet Protocol). El rutează pachetele prin rețelele interconectate, îndeplinind și funcțiuni de segmentare a pachetelor și de reasamblare a lor. Celelalte protocoale care operează la același nivel internet contribuie la realizarea funcțiunii de rutare îndeplinite de IP. În operația de rutare protocolul IP folosește adresa de rețea (adresa IP) conținută în pachetul IP. Fiecare pachet este o entitate independentă, fără legătură cu vreun alt pachet. Protocolul IP nu garantează livrarea pachetelor către destinatar, motiv pentru care se spune că serviciul furnizat de acest protocol este nefiabil, fără a însemna însă o calitate scăzută a acestuia. Dacă este necesar, în funcție de aplicație, nivelul imediat superior, prin protocolul TCP, asigură fiabilitatea corespunzătoare.

Fragmentarea pachetelor și apoi reasamblarea lor la destinație sunt funcțiuni necesare pentru a respecta dimensiunea cadrelor impusă de protocolul utilizat la nivelul legătură de date, specific fiecărui tip de rețea.

Formatul pachetelor IP este prezentat în figura 5.5. Structura pachetelor se bazează pe cuvinte de 32 biți, lungime corespunzătoare procesoarelor ARPANET inițiale. În continuare se va prezenta semnificația câmpurilor unui pachet.

- Versiune - Identifică versiunea protocolului IP care generează pachetul. În prezent este utilizată versiunea 4 a protocolului.

- Lungimea antetului - Indică lungimea antetului măsurată în cuvinte de 32 biți. Lungimea minimă a antetului corespunde cazului când acesta nu conține câmpul opțiuni și este 5 (20 octeți).

4 biți	4 biți	8 biți	16 biți	
Versiune	L. antet	Tipul serviciului	Lungimea totală	
Identificare			Fanioane	Decalajul fragmentului (13 b)
Durata de viață		Protocol	Secvența de verificare a antetului	
Adresa de rețea (IP) a sursei				
Adresa de rețea (IP) a destinației				
Opțiuni + biți de completare				
Date				

Figura 5.5 Formatul pachetului IP

- Tipul serviciului (ToS - Type of service) - Arată calitatea serviciului cerut pentru transportul pachetului în rețea. Primii trei biți din câmpul ToS specifică prioritatea pachetului, permițând sursei să indice importanța fiecărui pachet, dar, în general, ruterii ignoră acest câmp. Calitatea serviciului cerut este exprimată prin intermediul următorilor trei biți, prin care se pot solicita întârziere mică, eficiență în transmisiune (referitor la debit - throughput) și fiabilitate. Acest câmp poate influența ruterii în alegerea unei căi spre destinație dar, așa cum s-a mai menționat, protocolul IP nu garantează calitatea cerută pentru transportul datelor. Ultimii doi biți nu au încă o semnificație.
- Lungimea totală - Acest câmp specifică lungimea totală a pachetului, măsurată în octeți, incluzând atât antetul cât și datele.
- Identificare, Fanioane și Decalajul fragmentului - Controlează fragmentarea și reasamblarea pachetelor. Desigur, transmisiunea pachetelor ar fi eficientă dacă fiecare pachet generat de o sursă ar putea fi inclus în întregime într-un cadru pentru a traversa rețeaua spre destinație. Dar fiecare tip de rețea impune o anumită limită superioară pentru lungimea cadrului. Spre exemplu, rețeaua Ethernet limitează cadrul la 1500 octeți de date, unele rețele publice de date limitează cadrul la 128 octeți etc. Limitarea dimensiunii pachetelor la cea mai mică limită superioară admisă în rețea ar face transmisiunea ineficientă. Din această cauză protocolul IP lasă sursei latitudinea să aleagă dimensiunea pachetului corespunzător constrângerilor impuse de legătura de date la care ea este conectată, iar o divizare a fiecărui pachet în fragmente se realizează în ruter atunci când urmează să traverseze o rețea care admite dimensiuni mai mici.

Reasamblarea pachetelor se face la destinație. Fiecare fragment are același format ca și un pachet complet.

Câmpul "Identificare" conține un număr care identifică pachetul. Când un ruter fragmentează un pachet câmpul Identificare trebuie copiat în antetul fiecărui fragment. În felul acesta la destinație se poate ști, ținând seama și de adresa sursei, cărui pachet aparține fiecare fragment.

Câmpul "Decalajul fragmentului" (Fragment offset) indică, pentru fiecare fragment, numărul grupurilor de câte 8 octeți transmise deja din pachetul căruia îi aparține fragmentul respectiv.

Prin cei trei biți din câmpul "Fanioane" (Flags) se poate semnaliza interdicția de fragmentare a pachetului (când sursa impune această restricție) și dacă, în cazul unui fragment, este sau nu ultimul din pachet. Câmpul "Lungimea totală" indică, în cazul unui fragment, lungimea fragmentului și nu a pachetului din care face parte.

- Durata menținerii în viață (Time to live) - Arată cât timp, în secunde, i se permite unui pachet să rămână în rețea. În acest câmp sursa care generează pachetul indică un timp maxim de supraviețuire a pachetului. Echipamentele care prelucrează pachetul (ruterii) la trecerea sa prin rețea spre destinație decrementează, fiecare, mărimea înscrisă în acest câmp cu o unitate. În plus, în cazurile în care ruterii sunt suprasolicitați și prelucrează cu întârziere pachetele, se face o decrementare suplimentară corespunzătoare timpului de așteptare. Când mărimea înscrisă în acest câmp ajunge la zero ruterul elimină pachetul și transmite către sursă un mesaj de eroare. Limitarea timpului de supraviețuire în rețea evită circulația la nesfârșit a pachetelor.

- Protocol - Identifică protocolul de nivel superior (transport: TCP sau UDP) asociat pachetului. Pentru protocolul TCP identificatorul este 6 iar pentru UDP este 17.

- Secvența de verificare a antetului - Permite verificarea corectitudinii (integrității) valorilor din antet. Acest câmp este determinat prin prelucrarea antetului, considerat ca o succesiune de întregi, fiecare alcătuit din 16 biți. Fiecare ruter calculează secvența de verificare și o compară cu cea din antet.

- Câmpurile de adrese - Conțin adresele de rețea (IP) de câte 32 biți fiecare, a sistemului sursă și a sistemului destinație. Aceste câmpuri nu sunt modificate la trecerea pachetelor prin ruteri.

- Opțiuni - Acest câmp are o lungime variabilă (maximum 40 octeți) și este rezervat pentru a introduce unele funcțiuni de control privind rutarea, securitatea rețelei și altele.

În acest câmp pot fi introduse mai multe opțiuni. Fiecare opțiune este specificată printr-un cod de opt biți ce poate fi urmat de un octet care indică lungimea și de mai mulți octeți de date pentru respectiva opțiune. Pentru ca acest câmp să aibă dimensiunea egală cu un multiplu de 4 octeți se folosesc biți de completare.

- Câmpul datelor - Are o lungime variabilă, dar un număr întreg de octeți. Limitele pentru dimensiunea unui pachet, inclusiv antetul, sunt 576 octeți minimum și 65.535 octeți maximum.

Așa cum s-a arătat, adresele Internet (IP), cu o lungime de patru octeți, constau din două părți: o parte care identifică rețeaua la care este conectat sistemul și o alta care identifică conexiunea prin care sistemul se leagă la rețea. Un sistem de extremitate sau un ruter, care are mai multe conexiuni fizice la o rețea sau la mai multe rețele, are câte o adresă distinctă pentru fiecare dintre conexiunile sale. Adresele Internet pot fi folosite și pentru referirea la rețele, în mod convențional adresa unei rețele având toți biții părții rezervate conexiunii cu valoarea 0.

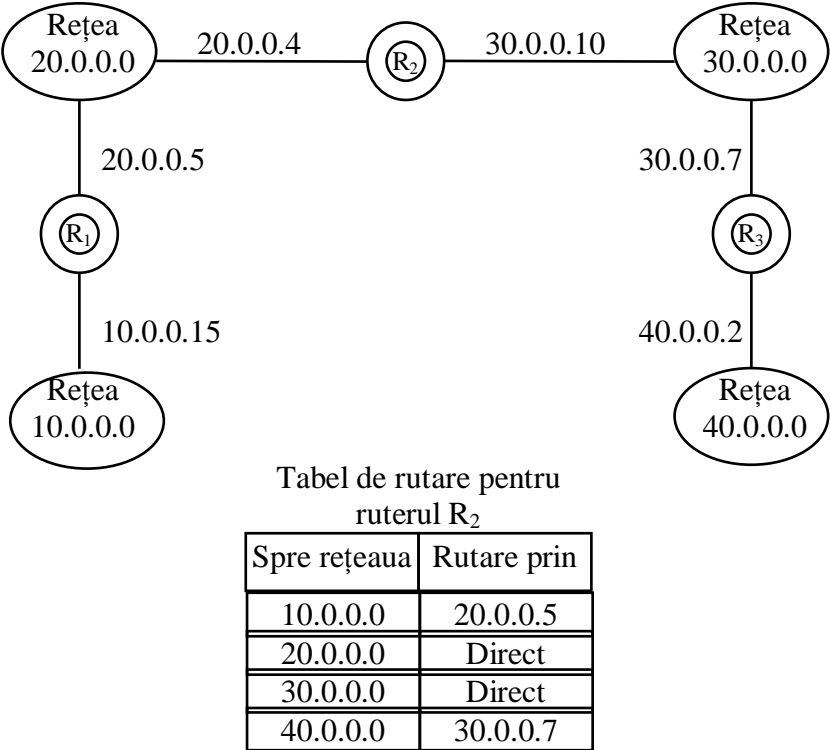


Figura 5.6 Rețea Internet formată din patru rețele și trei routeri

Transmiterea unui pachet între două sisteme aflate în aceeași rețea fizică (legătură de date LAN) nu implică utilizarea ruterilor. Sistemul sursă include pachetul într-un cadru și transmite cadrul la adresa fizică, de subnivel MAC, ce corespunde adresei de rețea a sistemului destinatar. Faptul că sistemul destinatar se află conectat la aceeași rețea fizică este constatat de către sistemul sursă prin extragerea părții de rețea a adresei IP de destinație și compararea cu partea de rețea a propriei (sau propriilor) adrese IP. Rutarea pachetelor în cazul în care cele două sisteme, sursă și destinație, nu se află conectate la aceeași legătură de date se realizează prin intermediul ruterilor care, în acest scop, utilizează tabele de rutare.

Tabelul de rutare al unui ruter conține perechi (N,R), în care N este adresa IP a rețelei de destinație iar R este adresa IP a primului ruter pe calea spre rețeaua N. În figura 5.6 se prezintă ca exemplu patru rețele conectate prin trei ruteri și tabelul de rutare al ruterului R₂.

Fiecare sistem are de asemenea un tabel de rutare în care se specifică adresa IP a celui mai apropiat ruter, care este un ruter conectat la aceeași legătură de date.

De remarcat însă că, în timp ce în tabelele de rutare sunt trecute numai adresele IP și deciziile de rutare se iau numai pe baza adresei rețelei de destinație, transmiterea pachetelor de la sistemul sursă la un ruter, de la un ruter la altul și de la un ruter la sistemul de destinație se face prin intermediul cadrelor, folosind adresele fizice ale ruterilor și, în final, a sistemului destinatar. Permanent însă, în pachetul transportat de un cadru se află adresele IP ale sistemelor sursă și destinație.

Inițializarea tabelelor de rutare și adaptarea lor permanentă la condițiile de funcționare ale rețelei se fac cu ajutorul unor protocoale prin intermediul cărora ruterii schimbă informații de rutare.

Din grupul protocoalelor de rutare TCP/IP fac parte:

- protocoale intradomeniu: RIP (Routing Information Protocol), Hello, OSPF (Open Shortest Path First Protocol);
- protocoale interdomenii: EGP (Exterior Gateway Protocol).
- **Protocolul ICMP -**

Așa cum s-a menționat, protocolul IP furnizează un serviciu fără conexiune. Fiecare pachet trece din ruter în ruter pentru a ajunge de la sistemul sursă la sistemul destinație.

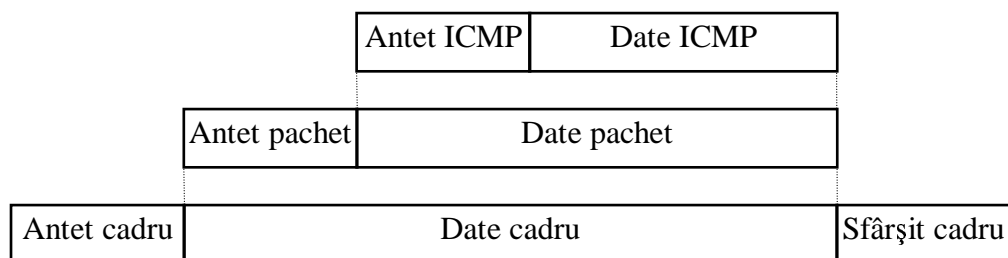


Figura 5.7 Încapsularea mesajului ICMP

Protocolul IP nu garantează livrarea fiecărui pachet la destinație, dar utilizează un mecanism (protocol) care permite oricărui ruter să semnaleze sistemului sursă o situație anormală apărută în rutarea unui pachet. Același mecanism poate fi folosit de un sistem pentru a testa dacă un alt sistem este accesibil, adică dacă există o rută în funcționare normală până la acel sistem și dacă sistemul este capabil să recepționeze pachete. Acest mecanism este reprezentat de protocolul ICMP (Internet Control Message Protocol). Protocolul ICMP permite ruterilor să transmită altor ruteri sau sistemelor mesaje de eroare sau de control. Fiecare mesaj ICMP este inclus în câmpul de date al unui pachet IP (fig. 5.7) care, la rândul său, este inclus în câmpul de date al unui cadru. Pachetele care poartă mesaje ICMP sunt rutate la fel ca și cele care transportă datele utilizatorului doar că, dacă apar erori în transmiterea acestor pachete, ele nu generează alte mesaje ICMP. Există mai multe tipuri de mesaje ICMP, fiecare având formatul său propriu. Indiferent însă de tipul mesajului, fiecare format începe cu aceleași trei câmpuri:

- tipul mesajului (8 biți);
- cod (8 biți), furnizând informații suplimentare despre tipul mesajului;
- secvența de verificare (16 biți), folosind același algoritm ca și IP dar verificând

numai mesajul ICMP.

Două dintre mesajele ICMP, foarte utilizate de administratori de rețele și de către utilizatori pentru a verifica existența unei rute funcționale spre o anumită destinație, sunt mesajele de “cerere ecou” (echo request) și “răspuns ecou” (echo reply). Un sistem de extremitate sau un ruter poate transmite un mesaj "cerere ecou" către o anumită destinație. Sistemul sau ruterul de destinație, care recepționează acest mesaj, răspunde prin mesajul "răspuns ecou" transmis către sursă. Cererea conține un câmp de date opționale. Răspunsul va conține o copie a acestor date. În felul acesta se poate

verifica dacă o anumită destinație este accesibilă și răspunde. Totodată este verificată și o parte din rețea.

Un alt tip de mesaj ICMP, numit “destinație inaccesibilă” (destination unreachable) este transmis de un ruter către sursă atunci când acesta nu poate trece mai departe un pachet, spre un alt ruter sau direct spre sistemul de destinație.

Alte mesaje ICMP semnalează situațiile de congestie (suprasolicitarea unui ruter), de redirectionare, de rutare ciclică (în buclă, la nesfârșit) etc.

- Protocolul ARP -

Adresa fizică corespunzătoare adresei IP a unui sistem din aceeași rețea fizică se obține utilizând protocolul ARP (Address Resolution Protocol). Dacă un sistem A trebuie să afle adresa fizică a unui alt sistem B aflat în aceeași rețea fizică, a cărui adresă IP o cunoaște, el va transmite un pachet ARP cerere, în care se specifică adresa IP a sistemului B, pachet inclus într-un cadru de difuziune. Acest cadru este recepționat de toate celelalte sisteme din rețeaua fizică respectivă, iar sistemul care-și recunoaște adresa IP (sistemul B în cazul de față) va transmite un pachet ARP răspuns, care va conține adresele sale fizică și IP, pachet inclus într-un cadru adresat sistemului A.

- Protocolul RARP -

De obicei adresa IP a unui sistem este memorată în memoria sa secundară, unde sistemul de operare o găsește atunci când utilizează protocoalele TCP/IP. Sistemele care nu dispun de memorie secundară își pot afla propria adresă IP, prin intermediul protocolului RARP (Reverse Address Resolution Protocol), de la un server RARP. Un astfel de sistem va emite un mesaj RARP cerere, inclus într-un cadru de difuzie. Toate sistemele din rețea vor primi acest cadru cerere, dar numai serverele RARP vor răspunde, transmițând mesajul RARP răspuns, conținând adresa IP solicitată, către sistemul solicitant.

- Proxy ARP -

Este o tehnică utilizată pentru a atribui același identificator de rețea pentru două rețele fizice distincte (Fig. 5.8). Să presupunem că un anumit identificator de rețea a fost atribuit, în etapa inițială, primei rețele. Ulterior se mai adaugă o rețea, cea de a doua, legată de prima rețea printr-un ruter și i se atribuie și ei același identificator.

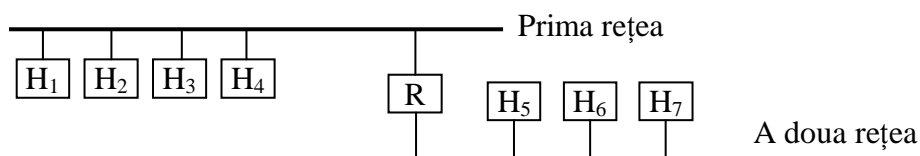


Figura 5.8 Ruter Proxy ARP

Ruterul care interconectează cele două rețele fizice cunoaște ce sistem este în fiecare rețea și utilizează ARP pentru a menține iluzia că există o singură rețea. Spre exemplu, când sistemul H_1 trebuie să comunice cu sistemul H_5 , folosește mai întâi ARP pentru a afla adresa fizică a lui H_4 , cunoscând adresa IP a acestuia. Ruterul R, pentru că folosește Proxy ARP, va capta cadrul de difuzie ARP de la sistemul H_1 , stabilește că sistemul H_5 este în cealaltă rețea și răspunde sistemului H_1 trimițând propria adresă fizică. Când ruterul va primi pachetul IP destinat sistemului H_5 , într-un cadru adresat lui, îl va lansa în rețeaua a doua (rețeaua ascunsă), într-un cadru adresat sistemului H_5 . La fel va proceda ruterul și pentru cereile ARP emise de sisteme din rețeaua a doua, referitoare la sisteme din prima rețea.

Avantajul acestei tehnici constă în faptul că, prin simpla adăugare de software Proxy ARP unui singur ruter, se mai introduce o rețea fără a modifica tabelele de rutare ale celorlalți ruteri.

5.1.4 Nivelul transport

Protocoalele nivelului transport furnizează proceselor de aplicații servicii de transfer de date cap la cap. Sunt definite două protocoale la acest nivel: UDP (User Datagram Protocol) și TCP (Transmission Control Protocol).

- Protocolul UDP -

Este un protocol simplu care, folosind IP pentru transportul pachetelor, permite identificarea nu numai a sistemelor sursă și destinație, prin adresele lor de rețea, ci și a programelor de aplicație între care se realizează transferul de informație. Sistemele de operare ale calculatoarelor permit executarea simultană a mai multor programe de aplicație așa încât, în fapt, destinatarul final pentru un mesaj transmis prin rețea este un anumit proces (program de aplicație) dintre toate cele care se execută simultan pe un sistem de calcul.

Pentru a se face distincție între multiplele programe ce se execută pe un același sistem, UDP utilizează un set de puncte abstracte asociate acestora, numite porturi de protocol, fiecare port fiind identificat printr-un număr.

Serviciul furnizat de UDP este un serviciu fără conexiune, nefiabil, ceea ce înseamnă că pot avea loc pierderi de mesaje, duplicări, livrarea mesajelor la destinație se poate face într-o ordine diferită de cea în care au fost emise.

Fiecare mesaj UDP este numit pachet de utilizator (user datagram), pentru a-l distinge de pachetul IP (IP datagram). Formatul mesajului UDP este prezentat în figura 5.9. Mesajul UDP se compune dintr-un antet relativ redus (8 octeți) și câmpul de date. Antetul precizează porturile de protocol ale sursei și destinației între care se face transferul mesajului, lungimea totală a mesajului UDP (inclusiv antetul) măsurată în octeți.

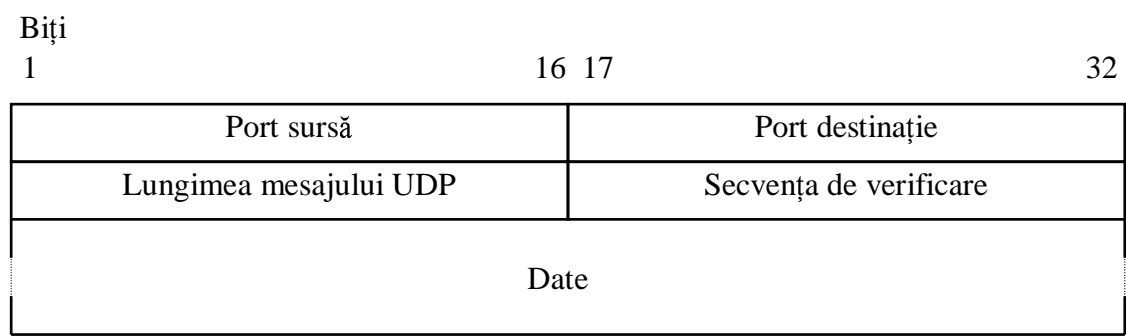


Figura 5.9 Formatul mesajului UDP

Specificarea portului sursă este opțională. Dacă nu se specifică acest port câmpul respectiv din antet se completează cu biți 0. Este opțională, de asemenea, și utilizarea secvenței de verificare care, în caz că se folosește, ia în considerare nu numai antetul (ca la IP) ci și câmpul de date.

De fapt secvența de verificare se calculează pe un câmp mai mare decât cel ce corespunde mesajului UDP. Pentru a crea posibilitatea de a verifica la recepție că mesajul UDP a ajuns la destinația corectă, secvența de verificare se calculează pentru un ansamblu format din mesajul UDP, precedat de un pseudoantet care conține adresele de rețea ale sursei și destinației. Acest pseudoantet nu se transmite, dar la recepție protocolul UDP calculează secvența de verificare pe baza mesajului UDP recepționat și a adreselor sursă și destinație, disponibile în antetul pachetului IP care a transportat mesajul respectiv. Dacă secvența astfel calculată coincide cu cea din mesajul UDP

rezultă că mesajul a ajuns la destinația (sistem și port) desemnată de sursă. Figura 5.10 prezintă poziția mesajului UDP în pachetul IP.

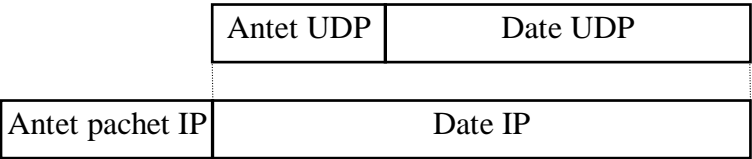


Figura 5.10 Poziția mesajului UDP în pachetul IP

- Protocolul TCP -

Protocolul TCP, operând la nivelul transport, asigură un serviciu cu conexiune fiabil, cu livrarea mesajelor la recepție în ordinea în care au fost emise. Înainte de a începe transferul datelor, între cele două procese de utilizator (programe de aplicație) se stabilește, prin intermediul rețelei, o conexiune logică numită circuit virtual. În acest scop programele de aplicație transmițător și receptor interacționează cu sistemele de operare în rețea din sistemele respective. Un program aplicație realizează un apel, care trebuie să fie acceptat de către celălalt program aplicație. Cele două sisteme de operare, prin modulele destinate protocolului de comunicație, își transmit mesaje prin rețea pentru a verifica dacă transferul este autorizat (acceptat) și dacă ambele părți sunt gata pentru acest transfer. Conexiunea fiind stabilită, cele două programe de aplicație sunt informate că transferul datelor poate să înceapă. Programul de aplicație transmițător transferă datele spre nivelul transport sub forma unui flux de biți, împărțit în octeți. Același flux, în aceeași ordine a octeților, este primit de programul de aplicație în sistemul de destinație.

La nivelul transport fluxul octeților primiți de la programe de aplicație este împărțit în segmente, care sunt apoi transmise în rețea spre destinație. Fiecare segment, format dintr-un număr oarecare de octeți, este transportat în rețea de un pachet IP. Conexiunile asigurate de TCP/IP la acest nivel sunt conexiuni duplex, ceea ce înseamnă că cele două procese își pot transmite date simultan unul către celălalt. Un avantaj al acestei conexiuni duplex constă în faptul că se poate transmite informația de control (al erorii, al fluxului), înapoi către sursă, în pachete ce transferă datele în sens opus, reducându-se astfel traficul în rețea.

Livrarea la destinație a fluxului de octeți în ordinea în care aceștia au fost emiși, fără pierderi și fără duplicate, se asigură prin folosirea unei tehnici de confirmare

pozitivă cu retransmitere, combinată cu fereastră glisantă. Mecanismul ferestrei glisante utilizat de TCP, operând la nivelul octeților și nu al segmentelor, permite atât o transmisiune eficientă, cât și un control al fluxului.

Octeții din fluxul datelor primite de la programul aplicație sunt numerotați în ordine. Transmițătorul, să-l notăm A, emite continuu segmente, formate cu acești octeți, către celălalt capăt al conexiunii, să-l notăm B, urmărind în același timp confirmările venite în sens invers în chiar segmentele de date transmise de B către A. O confirmare venită de la capătul B specifică numărul de ordine (de secvență) al primului octet din segmentul pe care acesta (capătul B) îl așteaptă, ceea ce înseamnă, implicit, o confirmare pentru recepția tuturor octeților anteriori transmiși de A. Numerele de ordine ale octeților pe care îi poate emite transmițătorul fără a avea confirmarea de recepție a lor sunt specificate de fereastra glisantă (fig. 5.10).

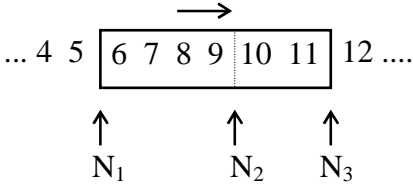


Fig. 5.10 Fereastră glisantă

Pentru o conexiune transmițătorul alocă trei numărătoare (N_1 , N_2 , N_3) care vor preciza în orice moment poziția ferestrei glisante. Numărătorul N_1 marchează începutul ferestrei glisante (limita inferioară), separând octeții emiși și pentru care s-au primit confirmările de recepție de cei pentru care nu s-au primit confirmări. Numărătorul N_3 indică sfârșitul ferestrei (limita superioară), adică numărul de ordine al ultimului octet ce poate fi inclus într-un segment ce urmează a fi transmis fără să mai vină vreo confirmare de recepție. Numărătorul N_2 marchează, în interiorul ferestrei, limita ce separă octeții deja transmiși de cei încă netransmiși.

Și receptorul va folosi o fereastră asemănătoare pentru a reconstitui fluxul octeților emiși. În același timp, având în vedere că protocolul TCP stabilește conexiuni duplex și că pe fiecare sens de transmisiune se utilizează câte o fereastră de emisie și una de recepție, rezultă că în fiecare capăt al conexiunii vor exista două ferestre, una glisând pe fluxul datelor ce se emit, iar cealaltă pe fluxul datelor ce se recepționează.

Protocolul TCP permite modificarea dimensiunii ferestrei glisante pentru a reliza un control al fluxului. Fiecare confirmare, pe lângă specificarea numărului de octeți recepționați (în ordine), conține și o indicație privind numărul de octeți pe care

receptorul îi poate accepta, dependent de mărimea spațiului liber din memoria tampon a acestuia. Transmițătorul își va modifica dimensiunea ferestrei de emisie corespunzător acestei indicații a receptorului, ceea ce va conduce și la creșterea eficienței transmisiei prin reducerea simțitoare a numărului pachetelor pierdute, rejectate de receptor și, în consecință, reducerea și a numărului retransmiterilor.

Deoarece protocolul TCP oferă un serviciu cu conexiune, conexiunea ce se stabilește pentru transferul datelor este identificată printr-o pereche de puncte de capăt (porturi de protocol). În felul acesta același port de protocol poate fi simultan capăt al mai multor conexiuni. Spre exemplu, un sistem poate permite accesul concurențial la serviciul său de poștă electronică, acceptând pe un același port de protocol mesajele transmise simultan de la mai multe calculatoare, cu fiecare dintre acestea având stabilită o altă conexiune, identificată distinct de celelalte.

- Formatul segmentului TCP -

Mesajele transferate la nivelul transport, prin protocolul TCP, între două sisteme, se numesc segmente. Formatul unui segment este prezentat în figura 5.11.

Fiecare segment se compune dintr-un antet, urmat de date. Antetul conține informație de identificare și informație de control. Primele două câmpuri, port sursă și port destinație, conțin numerele porturilor TCP care identifică cele două programe de aplicație de la capetele conexiunii.

Biți	1	4	10	16	17	32
	Port sursă				Port destinație	
	Număr de secvență					
	Număr confirmat					
	L.antet	Rezervat	U A P R S F			Fereastră
	Secvența de verificare				Pointer urgent	
	Opțiuni					Biți de completare
	Date					

Fig. 5.11 Formatul unui segment TCP

Numărul de secvență reprezintă numărul de ordine, în secvență, al primului octet din câmpul de date. *Numărul confirmat* reprezintă numărul de secvență al octetului de date ce se așteaptă a fi recepționat. Trebuie remarcat că numărul de secvență se referă la

fluxul datelor ce se transmit în același sens cu segmentul respectiv, iar numărul confirmat se referă la fluxul datelor transmise în sens invers.

Lungimea antetului se exprimă printr-un întreg care reprezintă numărul cuvintelor de 32 biți din care este constituit antetul. Este necesar să se indice lungimea antetului deoarece lungimea câmpului rezervat pentru specificarea opțiunilor este variabilă.

Există mai multe tipuri de segmente, funcție de scopul în care sunt folosite: transfer date, stabilire conexiune, eliberare conexiune, numai pentru confirmări (fără transfer date), transfer date în regim de urgență etc. Specificarea tipului de segment se face prin biții notați U, A, P, R, S și F.

Câmpul *pointer urgent* indică poziția datelor care se transmit în regim de urgență în fluxul general al datelor.

În câmpul *fereastră* se specifică numărul de octeți, începând cu cel menționat în câmpul de confirmare, pe care transmițătorul îi poate accepta (pe sensul invers de transmisiune).

Secvența de verificare este folosită pentru a verifica integritatea întregului segment (antet și date) dar, ca și în cazul protocolului UDP, pentru a da posibilitatea receptorului să verifice că segmentul a ajuns la adresa de destinație corectă, se utilizează și un pseudoantet având formatul din figura 5.12. Pseudoantetul nu se transmite, nu face deci parte din segment, dar se atașează segmentului numai pentru calculul secvenței de verificare. El conține adresele de rețea (IP) ale sursei și destinației, identificatorul protocolului și lungimea totală a segmentului TCP, inclusiv antetul TCP. Identificatorul protocolului este reprezentat de valoarea trecută în câmpul rezervat tipului de protocol din formatul utilizat de nivelul imediat inferior. Pentru pachetele IP care transportă segmente TCP această valoare este 6.

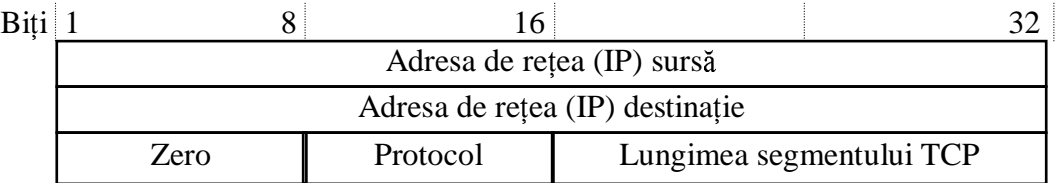


Fig. 5.12 Formatul pseudoantetului

Protocolul TCP folosește câmpul *opțiuni* pentru negocieri între cele două capete ale conexiunii. Printre altele, prin aceste negocieri se permite receptorului să specifice dimensiunea maximă a segmentelor pe care el o poate suporta, aspect foarte important,

spre exemplu, atunci când un mic calculator personal, cu o capacitate mică a memoriei tampon, este conectat la un supercalculator.

În ceea ce privește dimensiunea segmentelor, teoretic valoarea optimă a acesteia este determinată de dimensiunea maximă admisă de rețea pentru pachetele IP, pe calea de la sursă la destinație, așa încât să nu fie necesară fragmentarea segmentelor. Fragmentarea segmentelor conduce la formarea de pachete IP ce corespund aceluiași segment, dar care sunt în mod independent tratate de rețea. Toate fragmentele trebuie să ajungă la destinație, altfel trebuie să se retransmită întreg segmentul. Deoarece probabilitatea de pierdere (și rejectare) a unui fragment (pachet IP) nu este zero, creșterea dimensiunii segmentului peste pragul de fragmentare conduce la multiplicarea situațiilor în care este necesară retransmiterea segmentelor. Desigur, segmentele retransmise pot avea dimensiuni diferite în raport cu cele inițiale, acesta fiind un motiv suplimentar pentru care în TCP confirmarea se face nu la nivel de segment ci la nivel de octet.

Timpul de așteptare a confirmărilor pentru octeții conținuți într-un segment emis este limitat. Când acest timp expiră, fără a se primi confirmarea de recepție, se presupune că segmentul a fost eronat sau pierdut și se retransmite. Este evident că timpul de așteptare trebuie să depindă de timpul necesar unui pachet să ajungă la destinație și de timpul necesar pentru întoarcerea confirmării. Acești timpi depind de legăturile de date parcurse (debit), de întârzierea cu care sunt prelucrate pachetele în fiecare ruter, deci și de trafic și, prin urmare, sunt variabili, pentru o aceeași conexiune, de la un moment la altul. Pentru a se adapta la aceste întârzieri variabile introduse de rețea, protocolul TCP folosește un algoritm de retransmitere adaptiv prin care se reglează permanent limita timpului de așteptare a confirmărilor.

5.1.5 Nivelul aplicație

Protocoalele de la nivelul aplicație asigură o serie de servicii utilizatorilor rețelei. Aceste servicii permit utilizatorilor și programelor să interacționeze cu servicii automatizate de pe calculatoare distante și cu utilizatori aflați la distanță. Dintre protocoalele de nivel aplicație incluse în grupul TCP/IP pot fi menționate:

- Remote login (Telnet, Rlogin) - procedură prin care un utilizator se identifică într-un sistem distant, beneficiind apoi de resursele acestuia;

- FTP (File Transfer Protocol - transfer de fișiere) - procedură ce permite unui utilizator să transfere datele în ambele sensuri între un sistem local și unul distant;

- SMTP (Simple Mail Transfer Protocol - poștă electronică) - procedură de tranfer al mesajelor, permițând unui utilizator să transmită mesaje și fișiere către un alt utilizator conectat la o rețea de tip TCP/IP sau de alt tip, având însă o conexiune cu rețeaua TCP/IP;

- DNS (Domain Name System - sistemul numelor pentru domenii) - serviciu director care menține corespondența și face traducerea între numele date de utilizatori sistemelor lor conectate la rețea și adresele de rețea (IP) ale acestora;

- SNMP (Simple Network Management Protocol) - serviciu care permite realizarea unor funcțiuni de administrare a rețelei;

- PING (Packet InterNet Groper) - serviciu care poate fi utilizat pentru a testa conectivitatea între două sisteme;

- WWW (World Wide Web) - serviciu care permite accesul la diferite baze de date.

În cele ce urmează vor fi prezentate succint serviciile DNS, Remote login, FTP și SMTP.

5.1.5.1 Serviciul DNS (Domain Name System)

Fiecare sistem conectat la rețeaua Internet se identifică prin adresa sa de rețea, formată din 32 biți. Deși acest format de adresă este foarte convenabil pentru rutarea pachetelor, utilizatorii preferă să atribuie sistemelor nume care pot fi ușor reținute. Numele unui sistem, constând dintr-o secvență de caractere dintr-un alfabet finit, reprezintă de asemenea un identificator. Aceste nume sunt utile numai dacă există un sistem eficient care să țină corespondența între ele și adresele de rețea.

Ținând seama de numărul foarte mare al sistemelor conectate la rețeaua Internet, atribuirea numelor trebuie să se facă în așa fel încât să se evite coincidențele, să nu fie necesar un centru care să le administreze în totalitate și să permită realizarea unui sistem simplu și eficient de traducere a lor în adrese de rețea.

În acest scop, pentru alcătuirea numelor se folosește o structură ierarhizată realizată prin intermediul unui mecanism, numit sistemul numelor pentru domenii (DNS). Acest mecanism se referă, pe de o parte, la sintaxa numelor și regulile pentru

delegarea autorităților responsabile cu atribuirea lor și, pe de altă parte, la realizarea unui sistem de calcul distribuit care face trecerea de la nume la adrese.

Numele pentru domenii constau dintr-o secvență de subnume despărțite prin puncte, secvență ce corespunde structurii organizațiilor care au responsabilitatea atribuirii acestor subnume. Nivelul cel mai înalt este autoritatea Internet și este împărțit în următoarele domenii:

Numele domeniului	Semnificație
COM	Organizații comerciale
EDU	Instituții de învățământ
GOV	Instituții guvernamentale
MIL	Grupuri militare
NET	Centre de administrare a rețelelor mari
ORG	Alte organizații
ARPA	Domeniu temporar ARPANET
INT	Organizații internaționale
Codul țării	Fiecare țară (identificatorul standard internațional format din două litere)

Nivelul cel mai de jos este și el un domeniu, specificat prin întreaga secvență de nume. Spre exemplu, să considerăm următorul nume format din trei etichete: **comm.pub.ro**. Domeniul cel mai de jos este **comm. pub. ro** și este numele unui domeniu pentru Catedra de Telecomunicații a Universității Politehnica din București, România. La nivelul imediat superior este domeniul **pub.ro** (numele domeniului pentru Universitatea Politehnica din București, România) iar nivelul cel mai înalt este **ro** (numele domeniului pentru România).

Așa cum se vede din exemplul dat, numele domeniului se scrie începând cu eticheta locală și sfârșind cu eticheta domeniului celui mai înalt. Domeniul **comm.pub.ro** poate fi împărțit la rândul său în alte subdomenii (numite tot domenii) și în acest caz va mai apare o etichetă. Precizarea calculatorului conectat la rețeaua Internet se face tot printr-o etichetă, cu care va începe numele domeniului pentru respectivul calculator.

Sistemul care are rolul să facă trecerea de la nume la adrese este constituit din mai multe servere, distribuite în rețeaua Internet, care pot comunica între ele așa cum arată schema din figura 5.13. Legăturile între serverele figurate în desen nu trebuie considerate ca fiind conexiuni fizice.

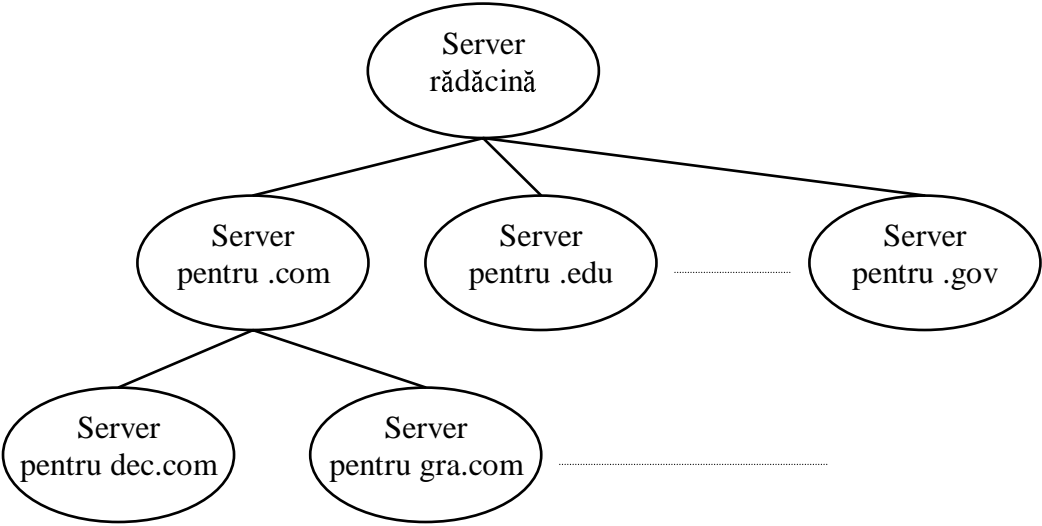


Fig. 5.13 Organizarea serverelor pentru DNS

În fiecare sistem conectat la Internet funcționează un proces de rezolvare a problemei translătării numelui în adresă IP. Un utilizator care solicită un program de aplicație specifică numele sistemului cu care aplicația trebuie să comunice. Înainte de a folosi protocolul TCP sau UDP pentru a comunica cu sistemul respectiv, programul aplicație trebuie să găsească adresa IP a acestuia. Pentru aceasta solicită procesului de translatare a numelui adresa IP, specificând numele. Este posibil ca procesul de translatare să furnizeze adresa cerută pe baza informațiilor memorate la soluționarea cererilor anterioare. În caz contrar va transmite un mesaj de solicitare către un server de nume. Desigur, procesul de translatare trebuie să cunoască cel puțin adresa unui server de nume. Dacă serverul solicitat nu poate furniza adresa din baza sa de date el va contacta un server ierarhic superior.

Protocolul DNS include facilități care au rolul să crească eficiența operațiilor de translatare a numelui.

5.1.5.2 Remote login (Telnet)

Protocolul Telnet permite accesul unui utilizator la toate comenzile disponibile pe un calculator distant, oferind trei servicii de bază. Primul dintre ele definește un

terminal virtual care furnizează o interfață standard spre sistemul distant, datorită căreia programele de utilizator (client) nu trebuie să țină seama de detaliile specifice acestui sistem distant. Un al doilea serviciu constă în posibilitatea oferită atât clientului cât și serverului (sistemul distant) de a negocia între un set de opțiuni standard. Spre exemplu, se poate negocia lungimea codului pentru reprezentarea caracterelor: 7 sau 8 biți. În sfârșit, în al treilea rând, Telnet tratează ambele capete ale conexiunii în mod simetric. Astfel, un program de aplicație de pe calculatorul utilizatorului devine client, stabilește o conexiune TCP cu serverul (program ce oferă un serviciu aflat pe un calculator distant), primește caracterele transmise de la terminalul utilizatorului și le transmite către server, în timp ce, în sens invers, acceptă caracterele pe care serverul le transmite înapoi și le afișează la terminalul utilizatorului.

Pentru a putea funcționa într-o rețea cu o mare diversitate de calculatoare și sisteme de operare protocolul Telnet definește un terminal virtual, specificând formatul în care se transmit datele și comenzile în rețea (fig. 5.14).

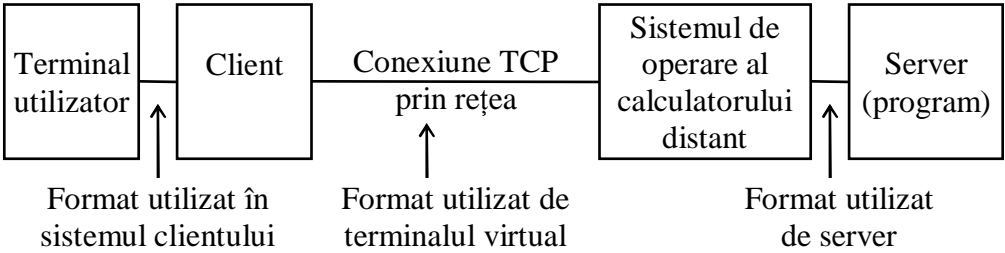


Fig. 5.14 Utilizarea terminalului virtual de către Telnet

Terminalul virtual reprezintă un format intermediar al datelor și comenzilor în trecerea lor prin rețea de la terminalul utilizatorului la server și invers.

Așa cum s-a arătat, una din opțiunile ce pot fi negociate este lungimea caracterelor. Dacă, prin negociere, s-a convenit asupra reprezentării caracterelor care se tipăresc (litere, cifre, semne de punctuație etc) prin combinații de 7 biți (codul ASCII), comenzile vor fi transmise utilizând o parte din caracterele de control ale codului ASCII. Alfabetul terminalului virtual are caracterele de control prezentate în figura 5.15.

Caracter ASCII	Valoare zecimală	Semnificația atribuită pentru terminalul virtual
BEL	7	Semnal sonor sau video
BS	8	Mută cursorul cu o poziție spre stânga
HT	9	Mută cursorul în următoarea celulă spre dreapta (tabel)
LF	10	Mută cursorul în jos (vertical) la rândul următor
VT	11	Mută cursorul în următoarea celulă
FF	12	Mută cursorul la începutul paginii următoare
CR	13	Mută cursorul la marginea din stânga a rândului curent

Fig. 5.15 Interpretarea caracterelor de control ASCII

În afara acestor caractere de control se mai folosește o secvență de două caractere de control din ASCII (CR - LF) pentru comanda ENTER (sau RETURN - sfârșitul rândului). La comanda ENTER dată de la terminalul utilizatorului, programul client (Telnet) va transmite în linie secvența CR - LF. În serverul Telnet această secvență este translatată în caracterul care are semnificația de sfârșit de rând în calculatorul distant.

Pentru a asigura o mai mare flexibilitate protocolului Telnet este prevăzută posibilitatea de a defini funcțiunile de control separat de caracterele ASCII. În felul acesta, fără a rezerva unele caractere pentru control, între client și server se pot transfera orice secvențe de caractere ASCII. Orice funcțiune de control este specificată prin doi octeți, dintre care primul este același pentru toate funcțiunile, este notat IAC (interpret as command) și reprezintă în binar numărul zecimal 255. În această variantă toate caracterele ASCII vor fi reprezentate prin 8 biți.

5.1.5.3 Transferul de fișiere (FTP)

Protocolul pentru transferul de fișiere (FTP - File Transfer Protocol) permite unul dintre cele mai utilizate servicii oferite de aplicațiile TCP/IP. Prin acest protocol se poate face un transfer de fișiere de la un sistem la altul, indiferent de deosebirile ce există între ele privind modul în care sunt memorate, accesate sau protejate fișierele. Dată fiind această diversitate privind fișierele, o cerere de transfer de fișier trebuie însoțită de specificarea următoarelor atribute: tipul datelor, tipul fișierului și modul de transmisiune.

FTP poate fi utilizat atât pentru a transmite informația codată în caractere cât și date binare. Utilizatorul trebuie să specifice forma în care datele urmează a fi memorate

în sistemul de destinație. Datele pot fi caractere ASCII de 7 biți, reprezentate însă prin octeți (formatul terminalului virtual), caractere EBCDIC de 8 biți sau secvență continuă de simboluri binare.

Tipurile de fișiere definite de FTP sunt: (1) structură fișier, întregul fișier constând dintr-un șir de octeți terminat printr-un marker de sfârșit al fișierului; (2) secvență de înregistrări cu marcarea, în cursul transferării fișierului, a sfârșitului fiecărei înregistrări; (3) structură de pagină, utilizată la începuturile rețelei ARPANET, foarte puțin folosită în prezent.

Modurile de transmisiune posibile sunt: flux continuu, bloc sau comprimat. În modul flux continuu, folosit pentru transferul oricărui tip de fișier, datele sunt transmise fără a fi prelucrate (fără a crea blocuri speciale și fără compresie). Fișierul se transmite așa cum este.

În modul bloc un fișier este transmis sub forma unor blocuri individuale. Fiecărui bloc i se atașează un prefix prin care se specifică lungimea și se încheie cu un marker de sfârșit. Atât sursa cât și destinația țin evidența blocurilor transferate și în caz de întrerupere transferul este reluat de la ultimul bloc recepționat corect.

În modul comprimat secvențele continue cu același caracter (octet) sunt înlocuite, înainte de transmisiune, printr-un singur caracter, cel din secvență și numărul care indică lungimea secvenței. Procesul FTP de la recepție va reconstitui secvența originală.

- Funcționarea protocolului FTP -

Procesul FTP din sistemul care face cererea pentru transferul de fișier se numește client FTP iar procesul FTP din sistemul care primește cererea se numește server FTP. Utilizatorul solicită serviciul FTP specificând clientului FTP numele sistemului ce urmează a primi cererea. Clientul FTP stabilește o conexiune TCP cu serverul FTP folosind pentru destinație numărul portului de protocol stabilit prin standard pentru servere FTP (21). Această conexiune, numită conexiune de control, este folosită pentru transmiterea informației de control, reprezentată de comenzi și răspunsuri.

Clientul FTP transmite comenzi către serverul FTP specificând contul și parola utilizatorului. Serverul FTP permite sistemului pe care este instalat să realizeze autentificările necesare privind dreptul de acces al utilizatorului și trimite spre clientul FTP rezultatul acestor verificări. Dacă utilizatorul este acceptat clientul FTP va trimite

comenzi indicând numele fișierului, tipul datelor, tipul fișierului și modul de transmisiune ce urmează a fi utilizate pentru transfer, precizând dacă va transmite un fișier către server sau va primi de la acesta o copie a unui fișier. Serverul răspunde dacă opțiunile de transfer sunt acceptate sau nu.

Dacă opțiunile de transfer sunt acceptate serverul FTP stabilește o altă conexiune TCP cu clientul FTP, pentru transferul datelor, folosind pentru destinație un port de protocol al cărui număr a fost în prealabil specificat de clientul FTP.

Transferul fișierului se face, conform opțiunilor convenite, pe conexiunea de transfer al datelor, beneficiind de procedurile TCP (controlul fluxului, controlul erorii, retransmitere) pentru a fi complet și corect.

FTP definește și formatele utilizate pentru comenzile și răspunsurile transmise pe conexiunea de control. O comandă constă dintr-un șir de patru octeți reprezentând caractere din alfabetul terminalului virtual, iar un răspuns constă dintr-un cod numeric de trei digiți urmat de un șir text opțional.

Grupul de protocoale TCP/IP conține și un alt protocol mai simplu pentru transferul de fișiere în situațiile care nu necesită interacțiuni complexe între client și server. Numit TFTP (Trivial File Transfer Protocol), el nu implică operațiile de autentificare și folosește protocolul de transport UDP. Un fișier este transmis în blocuri de mărime fixă, 512 octeți, pentru fiecare bloc așteptându-se confirmarea de recepție un interval de timp limitat.

5.1.5.4 Poșta electronică (SMTP)

Protocolul SMTP (Simple Mail Transfer Protocol) specifică modul în care mesajele de poșta electronică sunt transferate între procese SMTP aflate pe sisteme diferite. Procesul SMTP care are de transmis mesaj este numit client SMTP, iar procesul SMTP care primește mesajul este serverul SMTP. Protocolul nu se referă la modul în care mesajul care trebuie transmis este trecut de la utilizator către clientul SMTP sau cum mesajul recepționat de serverul SMTP este livrat utilizatorului destinatar și nici cum este memorat mesajul sau de câte ori clientul SMTP încearcă să transmită mesajul.

Utilizatorul specifică printr-o pereche de identificatori numele sistemului de destinație și adresa unei cutii poștale pe acest sistem. De obicei adresa cutiei poștale este chiar identificatorul login al utilizatorului destinatar, iar numele sistemului este același

cu numele domeniului pentru sistemul respectiv. Iată, spre exemplu, o adresă de poștă electronică: **barbu@pns.comm.pub.ro**.

Formatul mesajului cuprinde două părți, antetul și corpul, separate printr-un rând liber. Standardul specifică formatul antetului, lăsând corpul la latitudinea transmițătorului.

O linie din antet specifică destinația. Ea începe cu **To:** și conține adresa de poștă electronică a destinatarului. O altă linie începe cu **From:** și conține adresa de poștă electronică a transmițătorului.

Operația de transmitere a unui mesaj implică parcurgerea a trei etape: stabilirea unei conexiuni între SMTP client și SMTP server, transferul mesajului pe această conexiune și eliberarea conexiunii. Când există un mesaj de transmis, SMTP client stabilește o conexiune TCP cu SMTP server din sistemul de destinație utilizând un număr al portului de destinație asociat cu SMTP, așteaptă răspunsul serverului (220 READY FOR MAIL), după care transmite comanda HELO (prescurtare pentru “hello”) conținând numele utilizatorului transmițător. Serverul transmite un răspuns prin care se identifică și indică disponibilitatea de a recepționa mesajul.

Faza de transfer al mesajului începe cu comanda MAIL, conținând numele utilizatorului care transmite mesajul, urmată de una sau, după caz, mai multe comenzi RCPT indicând destinatarii mesajului. Transferul efectiv al mesajului se face în cadrul comenzii DATA, care este urmată de datele ce reprezintă textul mesajului. La fiecare comandă serverul SMTP trimite un răspuns adecvat. Utilizându-se o conexiune TCP pentru transferul mesajelor de poștă electronică se asigură, prin detecția erorilor și retransmitere, livrarea corectă a lor la sistemul de destinație (server). Totuși, protocolul SMTP nu definește o procedură care să garanteze că mesajul a fost livrat corect utilizatorului destinatar de pe acel sistem.

După ce serverul a recepționat corect și complet mesajul pentru un anumit utilizator destinatar, SMTP client va șterge numele acestuia de pe lista destinatarilor mesajului respectiv. Dacă mesajul este adresat mai multor destinatari el va fi eliminat, împreună cu lista destinatarilor, din coada mesajelor pentru emisie, după ce s-au trimis copii către toți destinatarii.

În momentul în care faza de transfer pentru un anumit mesaj s-a încheiat, conexiunea TCP poate fi utilizată pentru transferul altui mesaj în același sens, sau în

sens invers, sau poate fi eliberată. Eliberarea conexiunii TCP se face prin comanda QUIT generată de SMTP client.

Formatul comenzilor SMTP include codul comenzii, alcătuit din patru octeți reprezentând caractere din alfabetul terminalului virtual, urmat, la unele comenzi, de un argument. Iată câteva comenzi: HELO, MAIL (from:), RCPT (to:), DATA, SEND (from:), TURN, QUIT. Răspunsurile au același format ca și în FTP: cod numeric de trei digiți urmat de un șir text.

5.2 Protocoalele Novell NetWare

Produsele NetWare, elaborate de compania Novell, sunt utilizate în rețelele locale de calculatoare personale. Multe dintre componentele familiei NetWare sunt folosite pentru a realiza un mediu de calcul bazat pe server, în care sistemele de utilizator, în calitate de clienți, solicită serviciile de rețea oferite de servere dedicate. Serverele NetWare sunt frecvent servere de fișiere, de imprimantă sau de poștă electronică. Sistemele client și server comunică între ele printr-o legătură de date LAN sau printr-o rețea extinsă.

5.2.1 Arhitectura NetWare

În figura 5.16 este prezentată, comparativ cu modelul OSI, arhitectura susținută de familia produselor NetWare. După cum se poate observa, celor două nivele inferioare din modelul OSI, fizic și legătură de date, le corespunde nivelul numit “mediul de transmisiune”. Rețelele NetWare permit o gamă largă de tehnologii LAN pentru acest nivel: Ethernet, Token Ring, ARCnet etc.

La nivelul rețea, numit interrețea (internet) în terminologia NetWare, se utilizează protocoalele IPX și RIP. Protocolul IPX (Internet Packet Exchange) asigură serviciul de transmisiune fără conexiune și servicii de rutare în cazul unei rețele extinse, obținute prin interconectarea mai multor rețele. Protocolul RIP (Routing Information Protocol) este folosit pentru comunicația sistemelor de extremitate cu ruteri și între ruteri cu scopul de a determina rutele pe care trebuie dirijat traficul de utilizator în rețea.

5.2.2 Mecanismul de adresare la nivelul rețea

Mecanismul de adresare permite identificarea unică a oricărui sistem dintr-o rețea NetWare. Fiecare sistem are o adresă de rețea compusă din două părți (fig. 5.17).

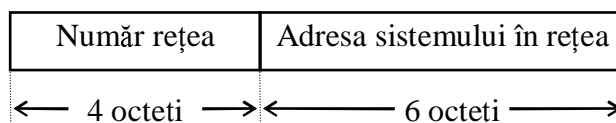


Fig. 5.17 Structura adresei de rețea

Prima parte, constituită din patru octeți, identifică subrețeaua la care este conectat sistemul, administratorul rețelei atribuind un număr unic de rețea fiecărei subrețele. Fiecare punct de conexiune la o subrețea este identificat printr-o adresă de șase octeți care, de obicei, este adresa NIC (Network Interface Card) administrată global, conform IEEE. Deși atribuirea numărului de rețea este la latitudinea administratorului rețelei, firma Novell asigură serviciul de alocare unică a numerelor de rețea oricărei organizații care solicită acest lucru, evitând astfel apariția conflictelor de adresă.

Procese de aplicație comunică între ele folosind structuri de date numite “socket”. Un anumit proces ce se execută pe un sistem este identificat printr-un număr format din doi octeți, inclus, împreună cu adresa de rețea a sistemului, în formatul de adresă al fiecărui socket.

5.2.3 Nivelul rețea

Acest nivel furnizează un serviciu fără conexiune pentru transferul pachetelor de date de la un sistem la altul. Protocoalele utilizate la acest nivel specifică modul în care se transferă pachetele de date (IPX) și cum se transmit informațiile de rutare (RIP).

- Protocolul IPX -

Protocolul IPX este un utilitar care permite realizarea legăturilor punct la punct folosind ca bază protocolul XNS (Xerox Network System) și asigurându-i acestuia capacitatea de interconectare a rețelelor. Formatul pachetelor IPX este prezentat în figura 5.18. Câmpul sumei de verificare, constând din patru octeți, nu este utilizat în IPX. El este inclus numai pentru compatibilitate cu specificările protocolului XNS. Lungimea pachetului include atât antetul cât și datele de utilizator. Câmpul pentru controlul transportului este utilizat în cursul rutării în rețea pentru a indica numărul de

subrețele traversate. Tipul pachetului identifică tipul datelor din câmpul de date. Acestea pot fi date de protocol RIP, NCP (NetWare Core Protocol) sau SPX. Numărul rețelei de destinație identifică subrețeaua la care este conectat sistemul. Numărul socketului de destinație identifică procesul particular din sistemul destinatar către care trebuie livrat pachetul pentru prelucrare. Câmpuri similare sunt prevăzute pentru a identifica sursa pachetului.

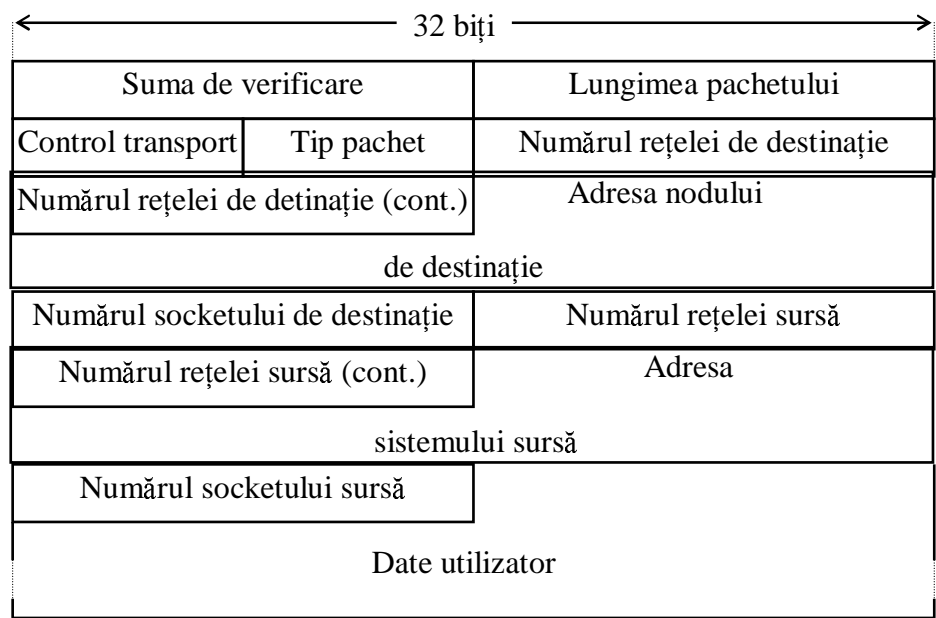


Fig. 5.18 Formatul pachetelor IPX

- Rutarea în rețea -

Prin examinarea adresei de rețea a sistemului destinatar un sistem sursă poate determina dacă acesta este conectat la aceeași legătură de date LAN sau la o altă subrețea. În cazul în care sistemul de destinație este conectat în aceeași (sub)rețea LAN, având același număr de rețea ca și sistemul sursă, acesta (sistemul sursă) va folosi serviciile nivelului “mediul de transmisiune” pentru a transmite pachetul direct sistemului de destinație. În caz contrar sistemul sursă va transmite pachetul către un ruter conectat la propria rețea LAN.

Modul în care se transmite informația de rutare între ruteri și între ruteri și sistemele de extremitate, precum și modul în care un ruter obține și păstrează această informație sunt specificate de protocolul RIP. Prin intermediul acestui protocol se pot realiza următoarele funcțiuni:

- un sistem de extremitate poate solicita informație de rutare de la alți ruteri;

- un ruter poate solicita informație de rutare de la alți ruteri;
- un ruter poate răspunde la o solicitare a unui sistem de extremitate sau a altui ruter;
- un ruter poate transmite către alți ruteri informație de rutare fără ca aceasta să fie solicitată.

Fiecare ruter păstrează un tabel cu informație de rutare, tabel ce va fi utilizat pentru a determina unde să transmită fiecare pachet primit de la un sistem conectat la aceeași rețea LAN. Pentru fiecare subrețea tabelul conține următoarele date: numărul de rețea, numărul de ruteri intermediari până la subrețeaua respectivă, o măsură a timpului necesar unui pachet să ajungă de la ruter la subrețea, un identificator al plăcii de interfață cu rețeaua (NIC) pe care ruterul ar trebui s-o utilizeze pentru a transmite un pachet către această subrețea, adresa de rețea a primului ruter către care ar trebui dirijate pachetele, un numărător de timp (timer) prin care se cronometrează intervalul de timp scurs de la ultima recepție a unei informații privind ruta spre subrețeaua respectivă (dacă acest interval de timp depășește o anumită limită subrețeaua este eliminată din tabel).

Timpul necesar unui pachet să ajungă de la un ruter la o subrețea depinde de numărul de legături de date ce trebuie traversate și de caracteristicile acestora. Acest timp, înscris în tabelul de rutare, servește pentru selectarea celei mai rapide rute.

- **Pachetele RIP** -

Informația de rutare se transmite prin intermediul pachetelor RIP al căror format este prezentat în figura 5.19.

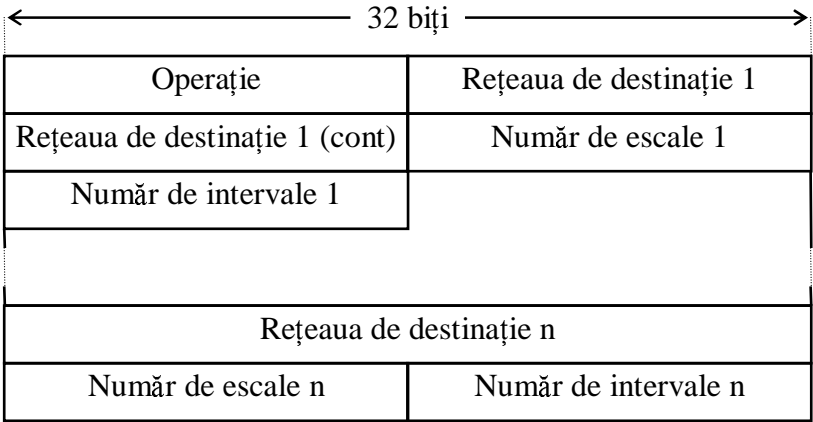


Fig. 5.19 Formatul pachetului RIP

Fiecare pachet conține un câmp *operație* și unul sau mai multe seturi cu următoarele câmpuri: *rețeaua de destinație*, *număr de escale* (hops) și *număr de intervale de timp* (ticks). Câmpul *operație* arată dacă pachetul este o cerere sau un răspuns. Câmpul *rețeaua de destinație* conține numărul rețelei de destinație. *Numărul de escale* reprezintă numărul de ruteri prin care pachetul a trecut. Fiecare ruter incrementează acest număr cu o unitate și dacă se ajunge la numărul 16 pachetul este eliminat. *Numărul de intervale de timp* reprezintă o estimare a timpului necesar pachetului să ajungă de la sursa care l-a generat la ruterul care l-a primit. Fiecare ruter adaugă la această valoare o mărime care depinde de caracteristicile următoarei legături de date pe care ruterul va dirija pachetul.

- Localizarea unui ruter -

Pentru a localiza un ruter conectat la propria rețea LAN, un sistem de extremitate difuzează pe rețeaua sa LAN un pachet RIP-cerere conținând numărul rețelei de destinație către care urmează să transmită un pachet de date. Toți ruterii conectați la rețeaua LAN proprie primesc acest pachet-cerere. Ruterul cu cea mai scurtă cale către rețeaua de destinație transmite înapoi un pachet RIP-răspuns prin care indică sistemului sursă adresa sa. Sistemul sursă va transmite astfel pachetul de date către acest ruter.

- Inițializarea tabelului cu informație de rutare -

Ruterii utilizează pachetele RIP pentru a schimba între ei informații de rutare, așa încât fiecare ruter are în permanență tabelul cu informația de rutare complet și actualizat. În momentul în care un ruter este activat, tabelul de rutare va conține informația de rutare privind subrețelele la care este conectat direct. Această informație este difuzată apoi de ruter, prin intermediul pachetelor RIP-răspuns, către aceste subrețele. Pentru a limita traficul reprezentat de informația de rutare, pachetele RIP cerere și răspuns difuzate într-o subrețea nu sunt trecute de către ruterii care le recepționează în subrețelele adiacente. După aceasta ruterul va difuza un pachet RIP-cerere, prin care solicită altor ruteri furnizarea informațiilor de rutare pe care aceștia le dețin. Ruterii care au recepționat pachetul cerere vor emite un pachet RIP-răspuns cu informație din tabelele lor de rutare.

Pentru selectarea informației de rutare ce va fi inclusă în pachetul RIP-răspuns se folosește algoritmul celei mai bune informații. Corespunzător acestui algoritm, spre exemplu, pachetul RIP-răspuns emis într-o subrețea nu va conține informație pe care ruterul a recepționat-o chiar din acea subrețea.

5.2.4 Nivelul transport

În rețelele NetWare nivelul transport asigură comunicația cap la cap între un sistem client și un sistem server. Principalele protocoale utilizate la acest nivel sunt: SPX (Sequenced Packet Exchange) și SAP (Service Advertising Protocol).

- Protocolul SPX -

Protocolul SPX furnizează un serviciu de transport cu conexiune, utilizând serviciul fără conexiune oferit de protocolul IPX de la nivelul rețea. Pentru schimbul datelor între doi utilizatori ai serviciului SPX se stabilește în prealabil o conexiune între aceștia. Pachetele SPX, transportate în pachetele IPX, vor fi numerotate în secvență și receptorul va utiliza numerele de secvență pentru a controla recepționarea pachetelor în ordinea în care acestea au fost emise. Prin pachetele transmise în sens invers se realizează totodată și confirmările de recepție, specificându-se numărul de secvență al următorului pachet așteptat la recepție. De asemenea, prin specificarea numărului de memorii tampon (listen buffers) disponibile la recepție, se realizează și un control al fluxului. Formatul pachetului SPX este prezentat în figura 5.20.

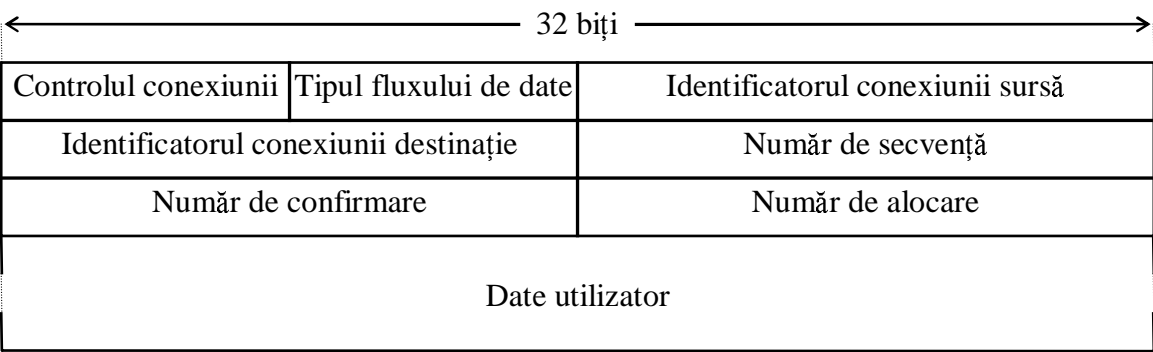


Fig. 5.20 Formatul pachetului SPX

Câmpul *controlul conexiunii* este utilizat pentru a cere o confirmare sau pentru a identifica un pachet care este prelucrat de SPX și care nu este trecut către un nivel superior. Câmpul *tipul fluxului de date* este folosit pentru a cere sau pentru a confirma terminarea unei conexiuni. *Identificatorul conexiunii sursă* specifică numărul alocat conexiunii la socketul sursă. În mod similar *identificatorul conexiunii destinație* specifică numărul alocat conexiunii la socketul destinație. În câmpul *număr de secvență* se trece numărul de secvență alocat pachetului emis. *Numărul de confirmare* reprezintă numărul de secvență al următorului pachet ce se așteaptă a fi recepționat, prin aceasta

confirmându-se recepția tuturor pachetelor având un număr de secvență mai mic. *Numărul de alocare* specifică numărul memoriilor tampon disponibile pentru pachetele recepționate la acest capăt al conexiunii.

- Protocolul SAP -

Protocolul SAP permite serverelor să facă cunoscute în rețea serviciile lor. Când un server este activat pentru prima dată el va difuza, în subrețeaua din care face parte, un pachet SAP conținând numele său, informația de rutare și tipul serviciului pe care-l oferă. În continuare, periodic, aceste date vor fi redifuzate de către server în subrețeaua sa. Ruterii vor folosi aceste date pentru actualizarea tabelor cu informații de rutare, iar prin schimburile realizate între ruteri, cu informații de rutare, tabelele lor vor conține informații despre toate serverele din rețea.

Când un sistem client are nevoie de un anumit tip de serviciu el va emite un pachet SAP-cerere către oricare server sau ruter din subrețeaua sa. Serverul sau ruterul va emite un pachet răspuns conținând numele și adresa unuia sau ale mai multor servere de tipul specificat.

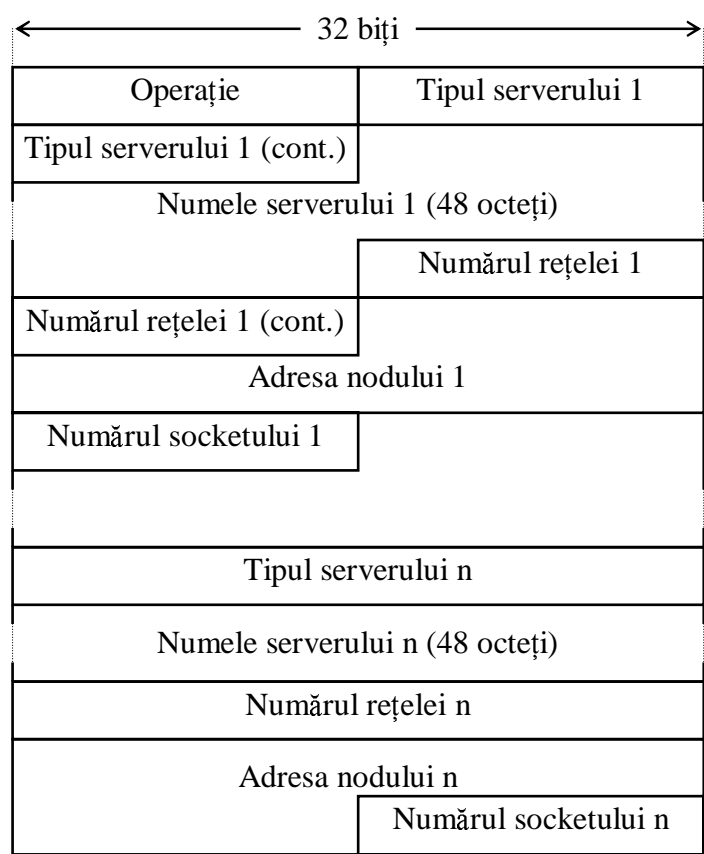


Fig. 5.21 Formatul pachetului SAP

Formatul pachetelor SAP este prezentat în figura 5.21. Câmpul *operație* identifică unul din următoarele patru tipuri de pachete:

- cererea unui sistem pentru numele și adresa celui mai apropiat server de un anumit tip;
- răspunsul privind cel mai apropiat server solicitat;
- cerere pentru numele și adresa tuturor serverelor de un anumit tip;
- răspunsul privind toate serverele de tipul solicitat.

Celelalte câmpuri, în continuare, specifică tipul serverului, numele său, adresa sa de rețea și numărul socketului corespunzător.

5.2.5 Servicii de aplicații

Rețelele NetWare integrează o serie de componente care permit funcțiuni bine determinate și care constituie resurse partajabile ale rețelei. Cele mai importante dintre ele sunt serverul de rețea și perifericele partajabile.

Un server realizează trei funcțiuni principale:

- gestionarea partajării fișierelor ținând seama de parametrii sistemului de securitate al rețelei;
- coordonarea comunicațiilor între sistemele conectate în rețea;
- controlul utilizării imprimantelor și discurilor din rețea, atașate lui.

Într-o rețea pot fi mai multe servere. Fiecare server își controlează propriile activități, menționate mai sus și le coordonează cu cele ale altor servere.

- Partajarea fișierelor -

Printr-un sistem de administrare a fișierului (NFS - NetWare File System) un server NetWare gestionează accesul la fișiere aflate pe discuri rigide interne sau externe. Fiecare disc, dintre cele 32 pe care le poate administra un server, este organizat, ierarhic, în volume, directori, subdirectori și fișiere. Fiecare disc este divizat în mai multe unități fizice, numite volume. Fiecare volum poate fi divizat în unități logice numite directori. Fiecare director poate conține, la rândul său, subdirectori, conform unei structuri de tip arbore.

Utilizatorii au acces la anumiți directori identificabili, fiecare, prin câte o literă. Accesul la un director este acordat fie pentru întregul director, fie pentru unele fișiere

din el. Sistemul de securitate al rețelei se bazează pe un anumit număr de drepturi care determină mai multe nivele de securitate.

Dreptul de acces la rețea este controlat prin numele și parola utilizatorului. Pentru a avea acces la rețea numele unui utilizator trebuie să fie înscris de administratorul rețelei în lista de utilizatori autorizați. În ceea ce privește parola, ea este în general opțională și rămâne sub controlul direct al utilizatorului.

Drepturile de utilizator, acordate de administratorul rețelei, controlează accesul la directori și, implicit, la fișiere. Pot fi acordate opt tipuri de drepturi pentru un utilizator sau pentru un grup de utilizatori. Acestea sunt:

- citirea unui fișier deja deschis;
- scrierea (modificarea) într-un fișier deja deschis;
- deschiderea unui fișier;
- ștergerea unui fișier;
- crearea, schimbarea numelui sau distrugerea unui subdirector;
- vizualizarea listei fișierelor unui director;
- modificarea atributelor fișierelor unui director, schimbarea numelui și modificări în fișierele acestui director.

Când solicită accesul la un director utilizatorul specifică tipul de acces solicitat și serverul îi acordă drepturile de acces stabilite pentru el. Prin atributele alocate directorilor și fișierelor, care au prioritate față de drepturile utilizatorilor, se asigură un control al posibilităților de modificare a acestora. Astfel, spre exemplu, dacă un fișier are atributul “ștergere inhibată” (delete inhibit) utilizatorul nu poate șterge acest fișier chiar dacă el are dreptul de a șterge.

- Partajarea imprimantei -

Acest serviciu permite utilizarea partajată a imprimantelor atașate la un server sau la un sistem în rețea. Sarcinile de imprimare sunt aranjate într-o coadă de așteptare și realizate pe măsură ce imprimanta devine disponibilă pentru fiecare dintre ele. Serviciul include facilități de administrare a cozilor de așteptare, așa încât pot fi alocate mai multe cozi de așteptare pentru o aceeași imprimantă sau mai multe imprimante pot partaja aceeași coadă de așteptare. Sunt asigurate și alte facilități precum: reordonarea cozilor, redirecționarea unei cozi către o altă imprimantă, etc.

- Poșta electronică -

Acest serviciu, performant și ușor de realizat, permite transmiterea unui mesaj de la un utilizator către un alt utilizator sau către un grup de utilizatori. Mesajul transmis este conservat într-o “cutie” de scrisori electronice, rezidentă pe discul serverului, într-o zonă accesibilă utilizatorului destinatar. Utilizatorul poate astfel citi în orice moment conținutul cutiei sale.

Fiecare utilizator posedă un spațiu pe discul serverului, rezervat cutiei sale de scrisori. Un utilizator nu are dreptul de acces la cutia de scrisori a altui utilizator sau, cel puțin, nu i se acordă un astfel de drept.

Protocolul NCP (NetWare Core Protocol) gestionează toate cererile clienților pentru serviciile unui server utilizând protocolul IPX și realizând, prin mecanisme proprii, controlul conexiunii și numerotarea în secvență pentru a asigura un serviciu de transfer de date fiabil.

Arhitectura NetWare permite extensii, pentru a oferi noi facilități clienților, prin intermediul unor module software (NLM - NetWare Loadable Modules, anterior numite procese cu valoare adăugată, VAP - Value Added Processes) care se adaugă la software-ul de bază ce se execută într-un server NetWare.

Gama programelor de aplicații care pot avea acces la serviciile rețelelor NetWare poate fi mult extinsă prin utilizarea interfețelor de programare a aplicațiilor (API - Application Programming Interface). Setul API oferit de NetWare permite fie solicitarea directă a serviciilor de transport IPX și SPX, fie solicitarea serviciilor de aplicații NetWare.

5.3 Protocoalele ISO/ITU-T

Deși protocoalele ISO/ITU-T referitoare la interconectarea sistemelor deschise (OSI) nu sunt încă acceptate pe scară mare, principiile lor dau coerență problematicii vaste a rețelelor, structurarea arhitecturii rețelelor în șapte nivele servind ca bază de comparație pentru alte grupuri de protocoale.

5.3.1 Nivelul rețea

Conform grupului de protocoale elaborate de ISO și ITU-T pentru modelul OSI, nivelul rețea oferă două tipuri de servicii: fără conexiune și cu conexiune. Serviciul cu

conexiune (Recomandarea ITU-T X.25) va fi prezentat în capitolul privind rețelele publice de date.

- Serviciul fără conexiune -

Serviciul fără conexiune al nivelului rețea se realizează conform protocolului CLNP (Connectionless Network Protocol - ISO 8473), echivalent protocolului IP din grupul TCP/IP și el permite transmiterea pachetelor de date între doi utilizatori ai rețelei, fiecare pachet fiind tratat de rețea în mod independent de celelalte.

Realizarea transferului datelor prin traversarea mai multor subrețele ridică probleme în ceea ce privește alegerea caracteristicilor serviciului oferit utilizatorilor. Spre exemplu, fiecare subrețea definește o dimensiune maximă a mesajelor. Ar fi inefficient ca pachetele emise de utilizatori să fie limitate la cea mai mică valoare a dimensiunilor maxime admise de subrețelele din care este alcătuită rețeaua. De aceea, dimensiunea pachetelor emise de un utilizator este independentă de subrețelele utilizate. În fiecare comutator situat pe ruta ce o străbate mesajul spre destinatar se face, dacă este necesar, o fragmentare a mesajului corespunzător dimensiunii admise de subrețeaua ce urmează pe acea rută (fig. 5.21). De reținut că reasamblarea mesajelor fragmentate nu se face în comutatoare ci la destinație.

Formatul pachetului este o secvență de octeți și arată ca în figura 5.23. Primul octet specifică protocolul de rețea utilizat. Protocolul CLNP este precizat prin codul hexazecimal 81.

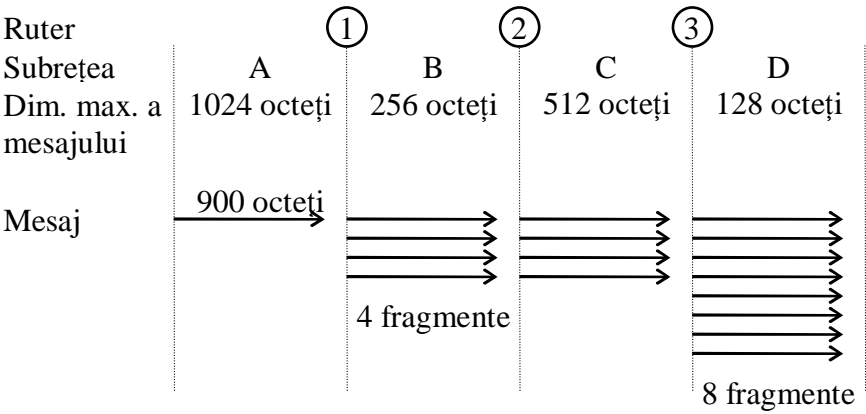


Figura 5.22 Fragmentarea mesajelor în comutatoare

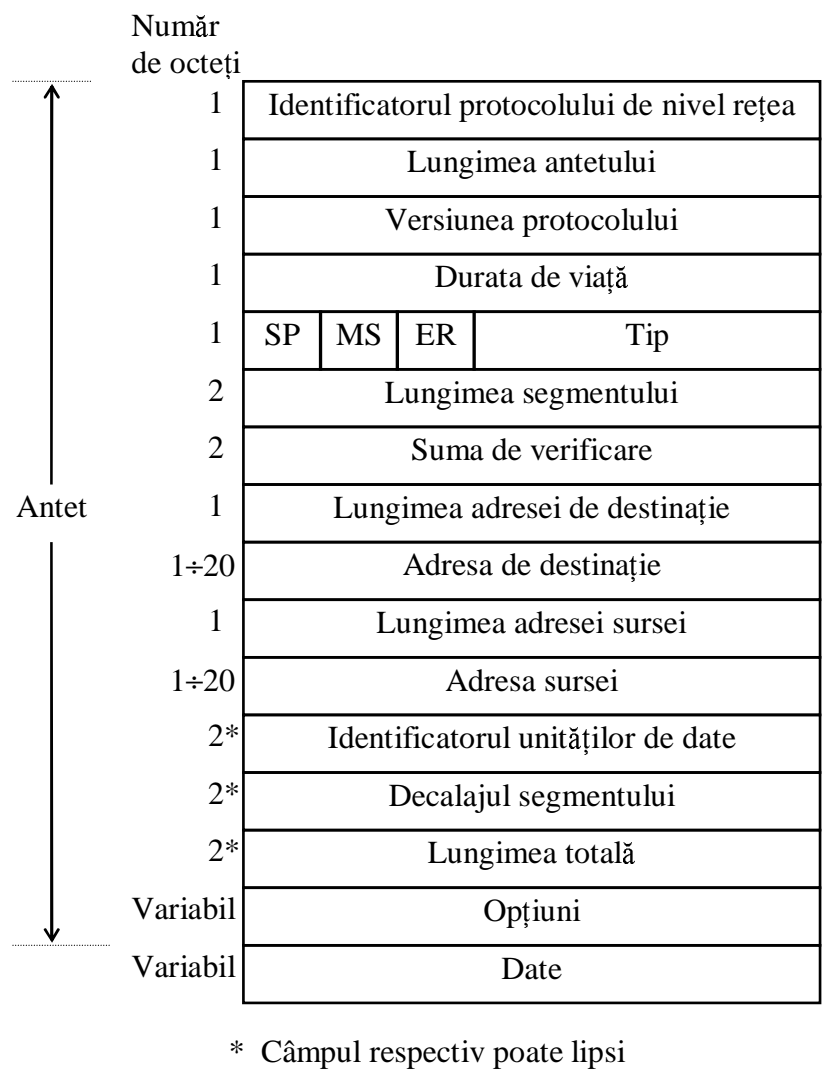


Figura 5.23 Formatul pachetului de date

Dacă acest octet este egal cu zero înseamnă că nu există nivelul rețea, caz în care formatul pachetului se reduce la acest octet, urmat de partea de date, iar pachetul este furnizat, fără alt control, nivelului inferior sau, corespunzător sensului de transmisiune, nivelului superior. Acest format permite nivelului transport să accedă la nivelul legătură cu un cost minim (și reciproc, de la nivelul legătură la nivelul transport) în cazul în care, spre exemplu, mesajele se transmit între sisteme conectate la aceeași rețea.

Lungimea antetului indică numărul de octeți din care este constituit antetul. Lungimea maximă este de 254 octeți, valoarea 255 fiind rezervată pentru eventuale extensii ale formatului. Având în vedere posibilitatea de apariție a unor noi versiuni ale protocolului un octet este rezervat pentru a preciza versiunea utilizată.

Durata de viață a pachetului este exprimată în unități de timp egale cu 0,5 secunde. Inițial câmpul ce marchează durata de viață este fixat de către sursă la o anumită valoare și fiecare ruter (comutator) va decrementa acest câmp cu o mărime ce reprezintă o supraestimare a timpului necesar pentru transferul mesajului la următorul ruter, ținându-se seama și de timpul de așteptare pentru prelucrare. Astfel, dacă transferul va dura mai puțin de 0,5 secunde se va face decrementarea cu o unitate, iar dacă transferul va dura 1,2 s (legătură prin satelit), decrementarea va fi de trei unități. Când acest câmp ajunge la zero pachetul va fi eliminat. Existența acestui câmp permite, printre altele, eliminarea pachetelor care circulă în buclă atunci când informațiile de rutare sunt contradictorii sau nu sunt complete.

Dacă un pachet este fragmentat durata de viață este copiată în câmpul respectiv al fiecărui fragment. Dacă un fragment este eliminat într-un ruter oarecare din cauză că durata sa de viață s-a epuizat, pachetul nu va mai putea fi reconstituit. Bitul ER pus la valoarea 1 de către sursă arată că aceasta dorește să fie avertizată dacă pachetul nu poate fi livrat la destinație. În acest caz ruterul care a eliminat pachetul sau un fragment al lui trebuie să transmită către sursă un pachet de avertizare.

Sursa poate interzice fragmentarea unui pachet punând bitul SP=0. Dacă într-un ruter oarecare un astfel de pachet nu poate fi transmis mai departe fără a fi fragmentat el va fi eliminat și, în funcție de valoarea bitului ER, ruterul va transmite sau nu un pachet de avertizare înapoi către sursă. Bitul MS=0 semnalează că fragmentul respectiv conține ultimii octeți ai pachetului inițial.

Câmpul “tip” indică fie un pachet de date, fie un pachet de avertizare transmis către sursă. Câmpul “lungimea segmentului” dă lungimea totală, adică inclusiv antetul, a fragmentului sau pachetului din care face parte antetul.

Câmpurile “identificatorul unităților de date”, “decalajul segmentului” și “lungimea totală” apar numai dacă este permisă fragmentarea și sunt necesare pentru a facilita reasamblarea corectă a pachetului la destinație. Toate fragmentele unui pachet conțin același identificator al unităților de date. Toate pachetele având aceleași adrese sursă și destinație, care pot fi fragmentate și coexistă simultan în rețea, trebuie să aibă identificatori diferiți.

Câmpul “decalajul segmentului” indică poziția fragmentului în pachetul din care aparține, specificând numărul de octeți cu care fragmentul este decalat față de începutul pachetului de date.

Câmpul “lungimea totală” indică lungimea totală (antet și date) a pachetului original și permite destinației să știe, în cazul în care primește un fragment de pachet, care trebuie să fie dimensiunea memoriei tampon rezervate reasamblării.

Așa cum s-a mai arătat, adresele de rețea ISO au o lungime variabilă, până la 20 octeți și, după cum se poate observa, în formatul pachetului sunt prevăzute câmpuri de câte un octet pentru a specifica lungimea fiecărei adrese.

Câmpul “suma de verificare” conține doi octeți prin intermediul cărora se verifică antetul. Utilizarea acestei sume de verificare este opțională, la latitudinea utilizatorului. Dacă în acest câmp se pune valoarea zero înseamnă că nu se face o verificare a antetului, ceea ce va conduce la reducerea timpului de prelucrare în ruteri.

Trebuie remarcat că, deoarece ruterii modifică cel puțin câmpul duratei de viață a pachetului (în cazul unei fragmentări se fac mai multe modificări), pe lângă verificarea acestei sume la recepția unui pachet ei trebuie să o recalculeze după modificările efectuate în antet pentru a reexpedia pachetul (fragmentul).

Primul octet al acestei sume de verificare trebuie să satisfacă relația:

$$\sum_{i=1}^L a_i = 0 \text{ (modulo 255)}$$

în care L este lungimea iar a_i este valoarea octetului din poziția i . Cel de al doilea octet al sumei de verificare trebuie să satisfacă relația:

$$\sum_{i=1}^L (L-i+1)a_i = 0 \text{ (modulo 255)}$$

Dacă în urma efectuării calculelor pentru determinarea celor doi octeți, în vederea expedierii sau reexpedierii pachetului (fragmentului), rezultă valoarea zero pentru unul dintre ei sau pentru ambii, în câmpul sumei de verificare se va trece valoarea 255 pentru octetul respectiv.

Câmpul “opțiuni” permite includerea unor opțiuni ale utilizatorului privind serviciul furnizat de nivelul rețea. Formatul general al unei opțiuni este arătat în figura 5.24. Opțiunile pot fi introduse într-o ordine oarecare, dar fiecare opțiune nu poate apărea decât o singură dată. Dintre opțiuni menționăm:

- funcția de completare (padding), utilizată pentru a lungi antetul la o mărime convenabilă;
- funcția de rutare prin sursă, prin care i se permite sursei să specifice în totalitate sau parțial ruterii prin care trebuie să treacă pachetul;

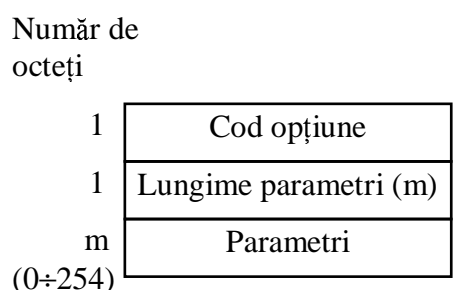


Figura 5.24 Formatul unei opțiuni

- funcția de înregistrare a rutei, permițând destinatarului să cunoască ruta străbătută de pachetul recepționat;
- calitatea serviciului (QOS - quality of service maintenance), permițând sursei să specifice importanța relativă a criteriilor de calitate pentru utilizator (prioritatea timpului de transfer în raport cu costul, a procentului de erori în raport cu timpul de transfer etc), ceea ce va constitui pentru ruteri un criteriu de alegere a rutei;
- proritaea, opțiune prin care se clasifică pachetele după importanța lor urmând ca ruterii să acorde întâietate pachetelor prioritare.

Se poate observa că în serviciul fără conexiune sursa și destinația sunt cuplate foarte slab. Nu există pachete de gestionare a schimburilor de informații, exceptând pachetul de avertizare (ER - Error Report) care este emis de receptor sau de un ruter atunci când a intervenit o situație ce conduce la rejectarea pachetului și numai dacă sursa a cerut, prin bitul ER=1, avertizarea sa pentru astfel de situații.

- Protocoale de rutare -

Fiecare ruter are nevoie, pentru realizarea funcției de rutare, de anumite informații, pe care le obține de la ruterii vecini și de la sistemele de extremitate aflate pe aceeași legătură de date. În același timp fiecare sistem de extremitate aflat într-o rețea LAN trebuie să cunoască adresa fizică (nivel legătură de date) a cel puțin unui ruter pentru a putea dirija, prin el, pachetele către sisteme din afara LAN-ului.

Pentru a permite fiecărui sistem de extremitate și fiecărui sistem intermediar să obțină informațiile de rutare locală, corespunzătoare unei subrețele, în grupul de protocoale ISO există protocolul cunoscut sub denumirea prescurtată ES - IS (end system - to - intermediate system), definit de standardul ISO 9542. Un alt protocol,

utilizat pentru rutarea între sisteme intermediare (ruteri), cunoscut sub denumirea IS - IS (intermediate system - to - intermediate system), este definit în standardul ISO 10589.

Principalul rol al protocolului ES - IS este, pe de o parte, să permită unui sistem de extremitate să cunoască adresa fizică a unui ruter conectat la aceeași subrețea iar, pe de altă parte, să permită ruterilor cunoașterea adreselor fizice și de rețea ale sistemelor de extremitate din subrețelele la care ei sunt conectați. În acest scop protocolul definește trei tipuri de mesaje: ESH (End System Hello) - emis de sistemele de extremitate, ISH (Intermediate System Hello) și RD (Redirect) - emise de ruteri.

Fiecare dintre aceste mesaje (pachete) are un antet, asemănător cu cel corespunzător protocolului CLNP (serviciul rețea fără conexiune), cu o parte identică pentru toate cele trei tipuri și un câmp de opțiuni (fig. 5.25).

Toate câmpurile din antet au aceeași semnificație ca și la pachetele CLNP, exceptând câmpul “timp de menținere”, care înlocuiește câmpul “lungimea segmentului” și care specifică receptorului timpul maxim de reținere a informației de adresă (rutare) conținute în respectivul pachet. Acest lucru este necesar deoarece informația de adrese este periodic actualizată prin intermediul acestor pachete. Dacă, la un moment dat, un sistem de extremitate este deconectat, fizic sau prin întreruperea alimentării electrice, în baza de date cu informații de rutare din fiecare ruter va fi eliminată în mod automat rubrica corespunzătoare acestui sistem.

În standardele ISO nu se utilizează termenii “adresă de rețea” (nivel rețea) și “adresă fizică” (nivel legătură de date) pentru identificarea unui sistem de extremitate sau intermediar. Sunt utilizate două concepte, unul sub denumirea de “punct de acces la serviciul rețea” (NSAP - Network Service Acces Point) și altul sub denumirea “titlul entității rețea” (NET - Network Entity Title). Ele se justifică prin faptul că nivelul rețea furnizează un serviciu și un utilizator al serviciului rețea are acces la nivelul rețea prin intermediul unui punct NSAP. Un sistem de extremitate poate avea mai multe puncte NSAP dacă există mai mulți utilizatori ai nivelului rețea. Dar nivelul rețea, în concepția ISO, nu poate fi, el însuși, utilizator al nivelului rețea și deci nu este autorizat să aibă un NSAP.

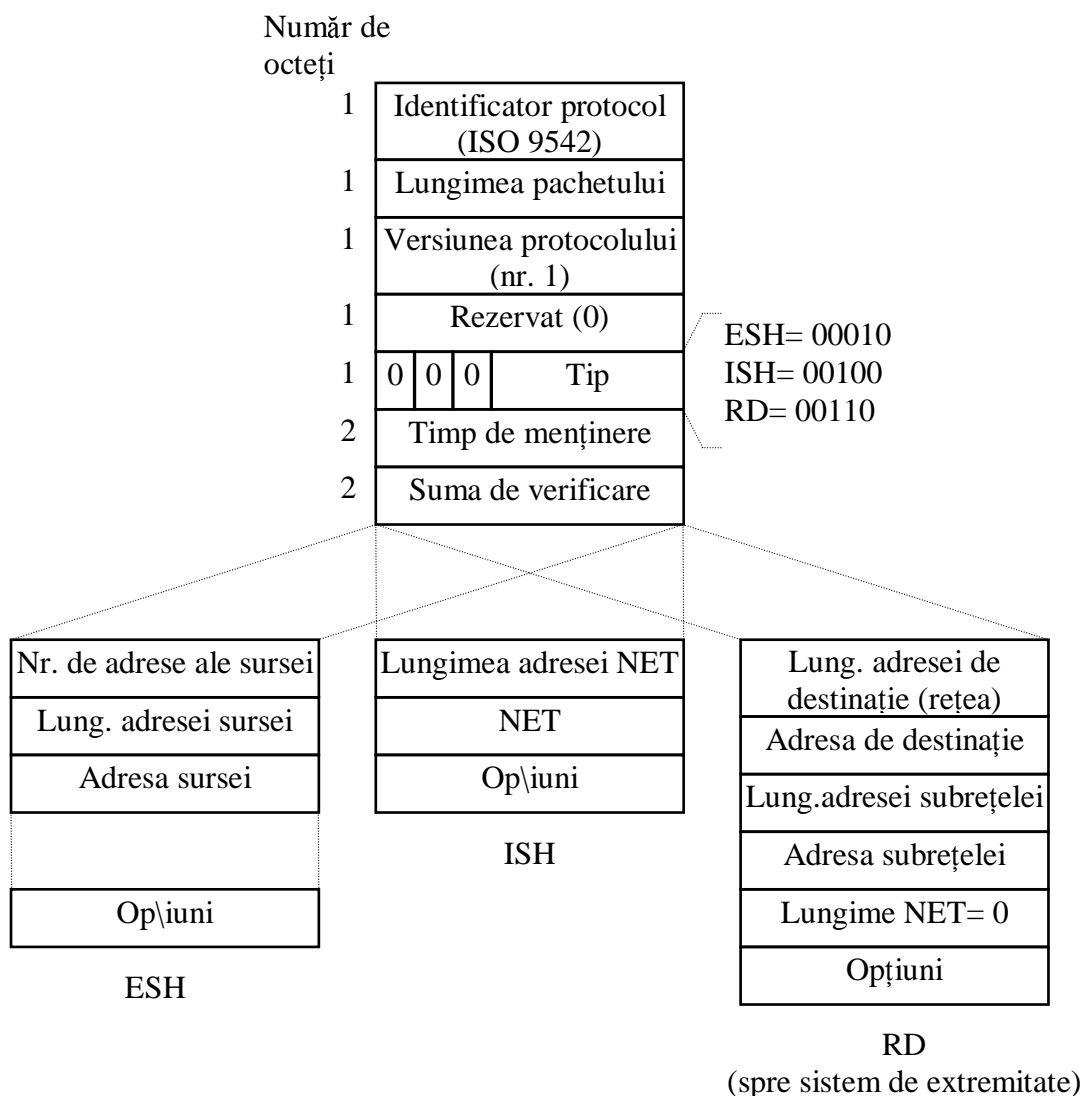


Figura 5.25 Formatul pachetelor ES - IS

Pentru pachetele de protocol, care nu transportă date, emise de nivelul rețea, nu se specifică un NSAP, ci un “titlu al entității rețea” (NET). Din această cauză se utilizează termenii de adresă NSAP și adresă NET.

Adresa fizică, corespunzând unui punct de conexiune a sistemului la subrețea, este notată SNPA (subnetwork point of attachment). Ea identifică sistemul în subrețeaua la care este conectat, dar pentru identificarea într-o rețea globală este nevoie și de precizarea subrețelei. Un sistem intermediar va avea mai multe adrese SNPA, câte una pentru fiecare dintre subrețelele la care este conectat.

Adresa NSAP are un câmp care precizează subrețeaua în care se află conectat sistemul (ES sau IS) și un alt câmp care identifică sistemul în subrețea. Primul câmp

este numit partea domeniului inițial (IDP - Initial Domain Part) și identifică subrețeaua la care este conectat sistemul, iar al doilea câmp este numit partea specifică a domeniului (DSP - Domain Specific Part). Ultimul octet al DSP este un octet de selecție. Lungimea DSP este variabilă, dar pentru sistemele conectate la rețelele locale este convenabil ca DSP să fie reprezentată chiar de adresa de nivel legătură de date (adresa fizică, șase octeți) a sistemului plus octetul de selecție. În felul acesta un sistem de extremitate se poate autoconfigura atunci când este conectat într-o rețea ISO care utilizează un câmp DSP de șapte octeți și protocoalele ES - IS și IS - IS. Cu protocolul ES - IS el poate descoperi adresa de rețea (NET) a unui ruter adiacent și poate copia câmpul IDP al acestuia pentru a obține propria adresă de rețea.

Pachetele ESH, emise de un sistem de extremitate, informează ruterii conectați la aceeași subrețea (rețea locală) care sunt adresele NSAP și SNPA ale acestui sistem. Pachetele ISH, emise de un ruter, informează toate sistemele de extremitate din fiecare subrețea la care este conectat care este perechea de adrese NET și SNPA.

Pachetele de redirecționare (RD) sunt utilizate de un ruter pentru a informa un sistem de extremitate, dintr-o subrețea la care și el este conectat, despre o adresă NSAP locală sau a unui ruter mai adecvat pentru a ruta pachetul spre destinația menționată într-un pachet de date recepționat de el anterior.

Emiterea periodică a pachetelor ESH și ISH permite actualizarea bazelor de date cu informații de rutare (RIB - Routing Information Base) ale sistemelor de extremitate și intermediare. Într-un sistem de extremitate RIB conține tabele cu perechile de adrese NET - SNPA ale tuturor sistemelor intermediare locale (conectate la aceeași subrețea). Într-un sistem intermediar RIB conține tabele cu perechile de adrese NSAP - SNPA ale sistemelor de extremitate din subrețelele la care el este conectat, obținute prin protocolul ES - IS, dar și tabele cu informații privind rutarea între sisteme intermediare, obținute prin protocolul IS - IS.

Când un sistem intermediar recepționează un pachet de date el îl va dirija direct spre sistemul de extremitate destinatar, dacă acesta este conectat la una din subrețelele sale locale sau către un sistem intermediar vecin, dacă pachetul trebuie rutat către o subrețea distantă. Două sisteme intermediare sunt considerate vecine dacă sunt conectate la aceeași subrețea. În baza de date cu informații de rutare a fiecărui sistem intermediar trebuie introduse, prin operațiile de administrare a rețelei, o listă a

subrețelelor la care este atașat împreună cu costul asociat utilizării fiecăreia dintre ele și o listă a sistemelor intermediare vecine cuprinzând adresele lor NET și SNPA.

În afară de pachetele care sunt transmise în cadrul protocolului ES - IS sistemele intermediare vecine schimbă între ele pachete cu informații de rutare în cadrul protocolului IS - IS. Fiecare pachet IS - IS conține o listă a subrețelelor la care este conectat sistemul intermediar ce a emis pachetul, care sunt deci utilizabile prin intermediul acestui sistem, împreună cu costurile asociate fiecăreia dintre ele (starea legăturilor). Pentru fiecare subrețea (legătură de date) sunt mai multe costuri asociate, câte unul pentru fiecare indicator (metrică) luat în considerare. Acești indicatori sunt: debit permis, întârzierea în transmiterea pe legătura respectivă, preț de cost, probabilitate de eroare.

Un sistem intermediar care recepționează un astfel de pachet înregistrează informația conținută în el și-l retransmite către vecinii săi, exceptându-l pe cel de la care a primit pachetul. În felul acesta toate sistemele intermediare din rețeaua globală vor realiza o aceeași matrice de conexiuni (graf) a rețelei, nodurile fiind reprezentate de sistemele intermediare iar legăturile dintre noduri reprezentând subrețelele (legături de date), fiecare cu costul asociat. Cu aceste date, folosind un algoritm de rutare cunoscut sub denumirea “algoritmul celei mai scurte căi” (shortest path first algorithm), se determină cea mai scurtă rută (cu costul global cel mai mic) de la un nod sursă (sistem intermediar) către fiecare dintre celelalte sisteme intermediare, deci către fiecare subrețea din rețea.

Un sistem de extremitate (sursă) transmite fiecare pachet de date către unul din sistemele intermediare (ruteri) locale folosind adresa sa SNPA obținută din RIB. Sistemul intermediar receptor determină identificatorul subrețelei din adresa NSAP de destinație conținută în pachet și consultă baza sa de date pentru a decide unde va transmite acest pachet. Dacă este o subrețea la care el este conectat, îl va trimite direct la sistemul de extremitate destinatar, folosind adresa SNAP a acestuia. Dacă este o subrețea distantă pachetul va fi transmis ruterului vecin aflat pe ruta cea mai scurtă către destinație.

5.3.2 Nivelul transport

În modelul de referință OSI nivelul 4 (transport) furnizează nivelului superior (sesiune) un serviciu de transmisiuni de date cap la cap, pentru care topologia rețelei este total transparentă iar fiabilitatea datelor recepționate este foarte bună.

Calitatea serviciului unei conexiuni de transport poate fi selectată de utilizatori și se exprimă prin mai mulți parametri, negociabili sau configurabili:

- întârzierea cu care se stabilește o conexiune de transport;
- probabilitatea de eșec la stabilirea unei conexiuni;
- întârzierea la deconectare;
- debitul permis;
- probabilitatea de întrerupere a unei conexiuni;
- întârzierea în transferul datelor;
- procentul erorilor reziduale;
- protecția conexiunii (securitatea datelor față de observatori indezirabili);
- prioritatea conexiunilor (importanța relativă a diferitelor conexiuni deschise de un utilizator influențează deciziile ce se iau în cazul unei degradări a serviciului).

Obținerea calității cerute implică o operație complexă de gestionare a resurselor. În figura 5.26 se prezintă un exemplu în care, pentru a mări debitul pe conexiunile transport sau pentru a îmbunătăți fiabilitatea lor (prin redundanță), se utilizează mai multe conexiuni rețea pentru o singură conexiune transport. În mod asemănător mai multe conexiuni transport pot fi multiplexate pe o singură conexiune rețea.

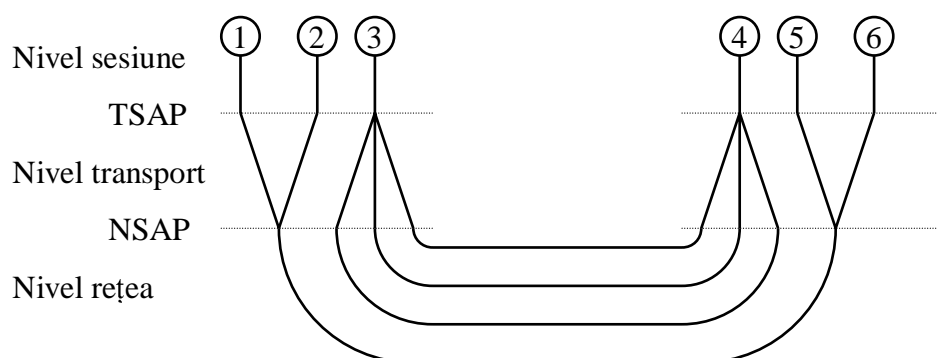


Figura 5.26 Conexiuni transport

Alegerea unei anumite calități a serviciului transport este dictată atât de necesitățile aplicației cât și de calitatea serviciului pe care-l oferă rețeaua. Calitatea

serviciului oferit de rețea este determinată de procentul erorilor reziduale în transmisiunea de la nivelul rețea. Se iau în considerare două feluri de erori: semnalate și nesemnalate de serviciul rețea. O eroare semnalată corespunde spre exemplu unei deconectări inopinate datorită unei defecțiuni, unei reinițializări etc. O eroare nesemnalată corespunde cazului în care serviciul rețea furnizează o entitate de informație eronată pentru protocolul transport, dar corectă pentru serviciul rețea. Spre exemplu, duplicarea entității de informație furnizate nivelului transport este o eroare nesemnalată.

Serviciile de rețea sunt clasificate după calitate, în funcție de procentul erorilor reziduale, în trei tipuri, caracterizate după cum urmează.

- Tip A: procent scăzut de erori de ambele tipuri, semnalate și nesemnalate, deci un serviciu fiabil.

- Tip B: procent scăzut de erori nesemnalate, dar un procent inacceptabil, pentru necesitățile aplicației, de erori semnalate. Este necesar un mecanism, la nivelul transport, care să asigure reluarea în cazul erorilor semnalate pentru a le face invizibile pentru utilizator.

- Tip C: procent inacceptabil de erori de ambele tipuri. Aceasta implică dotarea serviciului transport cu mijloace de detecție a erorilor și de reluare pentru a oferi un serviciu fiabil.

Ținând seama de calitatea serviciului rețea, de care beneficiază nivelul transport, se definesc cinci clase ale serviciului transport.

- Clasa 0 (clasă simplă) - Este cea mai simplă clasă, nu furnizează mijloace de recuperare când apar erori și nici mijloace de multiplexare a mai multor conexiuni transport pe o singură conexiune rețea. Această clasă a fost concepută pentru rețelele de tip A.

- Clasa 1 (clasă de recuperare a erorilor fundamentale) - Are o capacitate redusă de detecție a erorilor și de reluare. Erorile pot fi: întreruperea inopinată a conexiunii de rețea, recepția unei entități de date care nu aparține unei conexiuni transport cunoscute etc. Această clasă a fost concepută pentru rețelele de tip B.

- Clasa 2 (clasă de multiplexare) - Oferă posibilitatea de multiplexare a mai multor conexiuni de transport pe o singură conexiune de rețea și un mecanism de control al fluxului. Neoferind mijloace de detecție a erorilor este destinată rețelelor de tip A.

- Clasa 3 (clasă de multiplexare și de recuperare a erorilor) - Această clasă combină proprietățile claselor 1 și 2 și este destinată rețelelor de tip B.

- Clasa 4 (clasă de detectare și de recuperare a erorilor) - Această clasă este cea mai completă. Efectuează multiplexarea, reluarea la erori semnalate, detectarea erorilor și retransmiterea, controlul fluxului. Este destinată pentru rețelele de tip C.

Toate cele cinci clase presupun funcționarea în modul cu conexiune, ceea ce înseamnă parcurgerea a trei etape pentru un transfer de date folosind serviciul nivelului transport: stabilirea conexiunii la nivelul transport, transferul datelor și eliberarea conexiunii. Acesta este modul de lucru preferat în cele mai multe aplicații, dar el necesită totuși un protocol complex, incluzând fazele de stabilire și de eliberare a conexiunii. În unele aplicații, în care este important să se utilizeze un protocol mai simplu, se poate folosi un serviciu mult mai eficient, dar mai puțin fiabil, bazat pe un mod de lucru fără conexiune, care nu necesită cele două faze menționate. În continuare va fi descris serviciul transport clasa 4, fiind principalul serviciu oferit în rețelele locale.

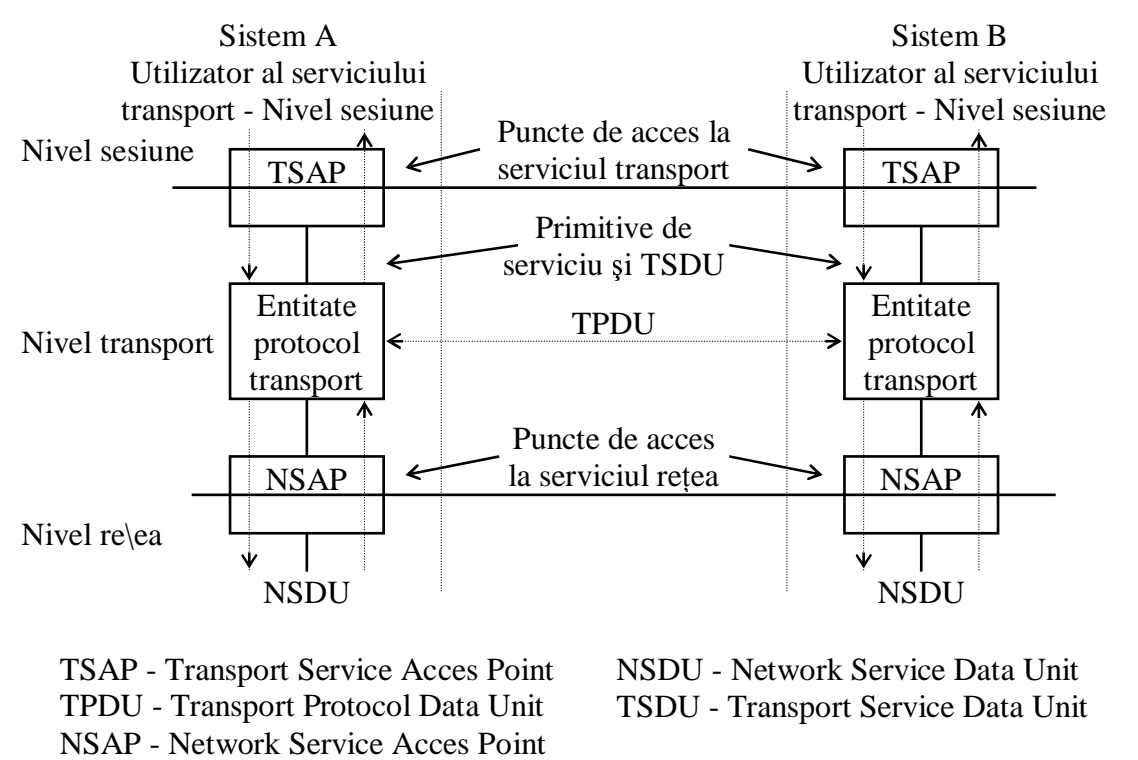


Figura 5.27 Interacțiunile nivelului transport cu nivelele vecine

Interacțiunile nivelului transport cu nivelele vecine sunt conforme cu modelul de referință OSI și sunt prezentate în figura 5.27. Utilizatorul furnizează mesajele sale și le

primește sub formă de unități de date ale serviciului transport (TSDU). Serviciul transport schimbă între entitățile sale unități de date de protocol (TPDU) care includ datele de utilizator (TSDU), fragmentate sau nu. Nivelul transport beneficiază de serviciul rețea, transmițând nivelului rețea și primind de la acesta unitățile de date NSDU. În tabelul 5.1 sunt prezentate primitivele de serviciu asociate nivelului transport, împreună cu parametrii lor, iar în figura 5.28 este prezentată o diagramă a succesiunii în timp a acestor primitive pentru realizarea serviciului transport.

- Funcționarea protocolului la nivelul transport -

Între entitățile de protocol transport din două sisteme, între care s-a stabilit sau urmează a se stabili o conexiune la nivelul transport, se schimbă unități de date de protocol (TPDU) care pot conține date de utilizator, asociate primitivelor de serviciu și informație de control al protocolului, adăugată de entitățile de protocol.

Tabelul 5.1 Primitivele sevciiului transport

Primitive	Parametri	Faza în care se utilizează
T.CONNECT.request .indication	Adresa chemătorului Adresa chematului Ipțiunea “date expres” Calitatea serviciului Date de utilizator (< 32 octeți)	Stabilirea conexiunii
T.CONNECT.response .confirm	Adresa care răspunde Calitatea serviciului Opțiunea “date expres” Date de utilizator	
T.DATA.request .indication	Date de utilizator	Transfer date
T.EXPEDITED-DATA .request .indication	Date “expres” (< 16 octeți)	
T.DISCONNECT.request .indication	Date de utilizator	Eliberarea conexiunii
T.UNIT-DATA.request	Adresa chemătorului	

.indication	Adresa chematului Calitatea serviciului Date de utilizator	Serviciul fără conexiune
-------------	--	-----------------------------

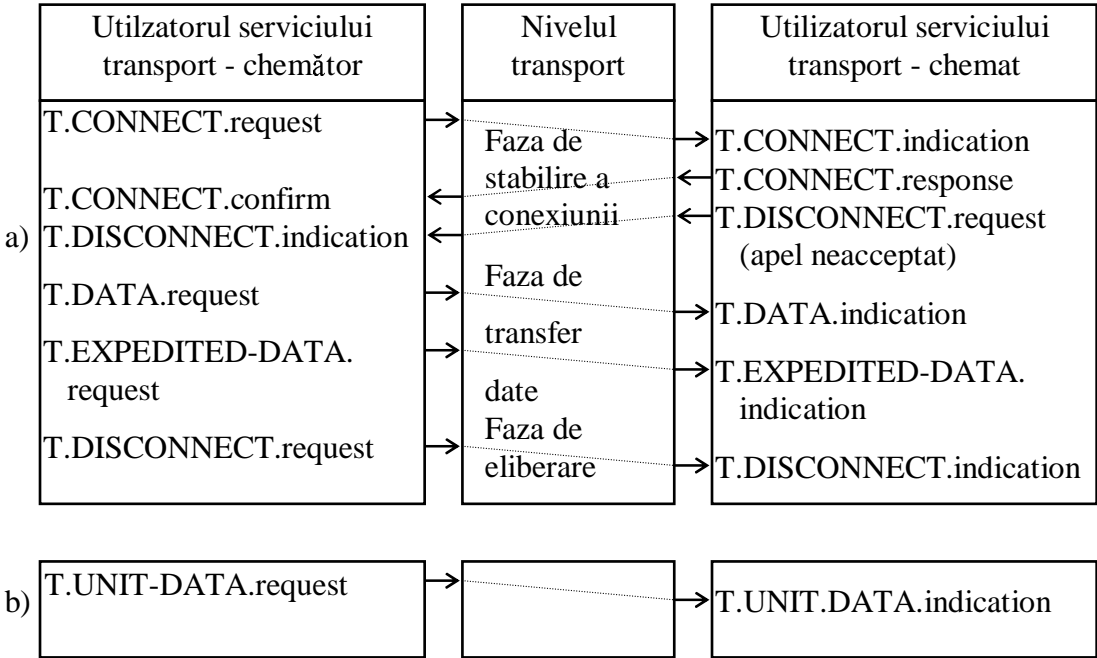


Figura 5.28 Diagrama de utilizare a primitivelor de serviciu pentru realizarea serviciului transport: cu conexiune (a) și fără conexiune (b)

Unitatea TPDU generată de o entitate de protocol este transferată entității corespondente folosind serviciile nivelului rețea.

Protocolul transport utilizează următoarele tipuri de TPDU:

Tip PDU	Notăție	Date transmise
Cerere conectare	CR (Connect request)	≤ 32 octeți
Confirmare conectare	CC (Connect confirm)	≤ 32 octeți
Cerere deconectare	DR (Disconnect request)	—
Confirmare deconectare	DC (Disconnect confirm)	≤ 64 octeți
Date	DT (Data)	Lungime negociată
Date expres	ED (Expedited data)	≤ 16 octeți

Confirmare recepție date	AK (Data acknowledge)	—
Confirmare recepție date expres	EA (Expedited acknowledge)	—
Rejectare	RJ (Reject)	—
Eroare	ER (Error)	—
Date (serviciul fără conexiune)	UD (Unit data)	

Formatul fiecărui tip de TPDU este prezentat în figura 5.29. Octetul LI (length indicator) indică lungimea antetului în octeți. Valoarea maximă este 254, 255 fiind rezervată pentru eventuale extensii. Primii patru biți ai următorului octet indică tipul TPDU, iar ceilalți patru biți arată mărimea creditului. Câmpurile “referință destinație” și “referință sursă” identifică conexiunea aleasă de sursă. Câmpul “clasă” specifică clasa protocolului ce urmează a fi utilizat (0 - 4) iar câmpul “opțiuni” specifică dacă vor fi utilizate câmpuri normale sau extinse pentru numerotarea TPDU și dacă, în clasa 2 numai, se va utiliza controlul fluxului sau nu.

Câmpurile menționate constituie partea fixă a antetului. Cele mai multe PDU mai conțin o parte variabilă a antetului și o parte cu date de utilizator. Partea variabilă constă într-un număr de câmpuri de câte un octet prin care se negociază parametrii conexiunii. Acești parametri sunt: identificatorul punctului de acces la serviciul transport - în TPDU de tip CR și CC, dimensiunea TPDU - CR și CC (128 octeți dacă nu se negociază sau, prin negociere: 128, 256, 512, 1024, 2048, 4096, 8192), numărul versiunii protocolului - CR și CC, clasa protocolului de rețiere - CR și CC, suma de verificare - numai pentru clasa 4 (pentru fiecare TPDU), opțiuni adiționale - CR și CC, debit - CR și CC, procentul erorilor reziduale - CR și CC, prioritatea conexiunii - CR și CC, timp de tranzit - CR și CC, încercări de reconectare - CR și CC, informație adițională definită de utilizator - DR, număr de confirmare - AK, confirmarea controlului fluxului - AK, TPDU anulat (nevalid) - ER.

Stabilirea unei conexiuni la nivelul transport începe prin generarea de către un utilizator al serviciului transport a unei primitive T.CONNECT.request, la care entitatea locală a protocolului transport crează o unitate de date de protocol tip CR (TPDU - CR) și o emite către entitatea corespondentă din sistemul chemat (fig. 5.28).

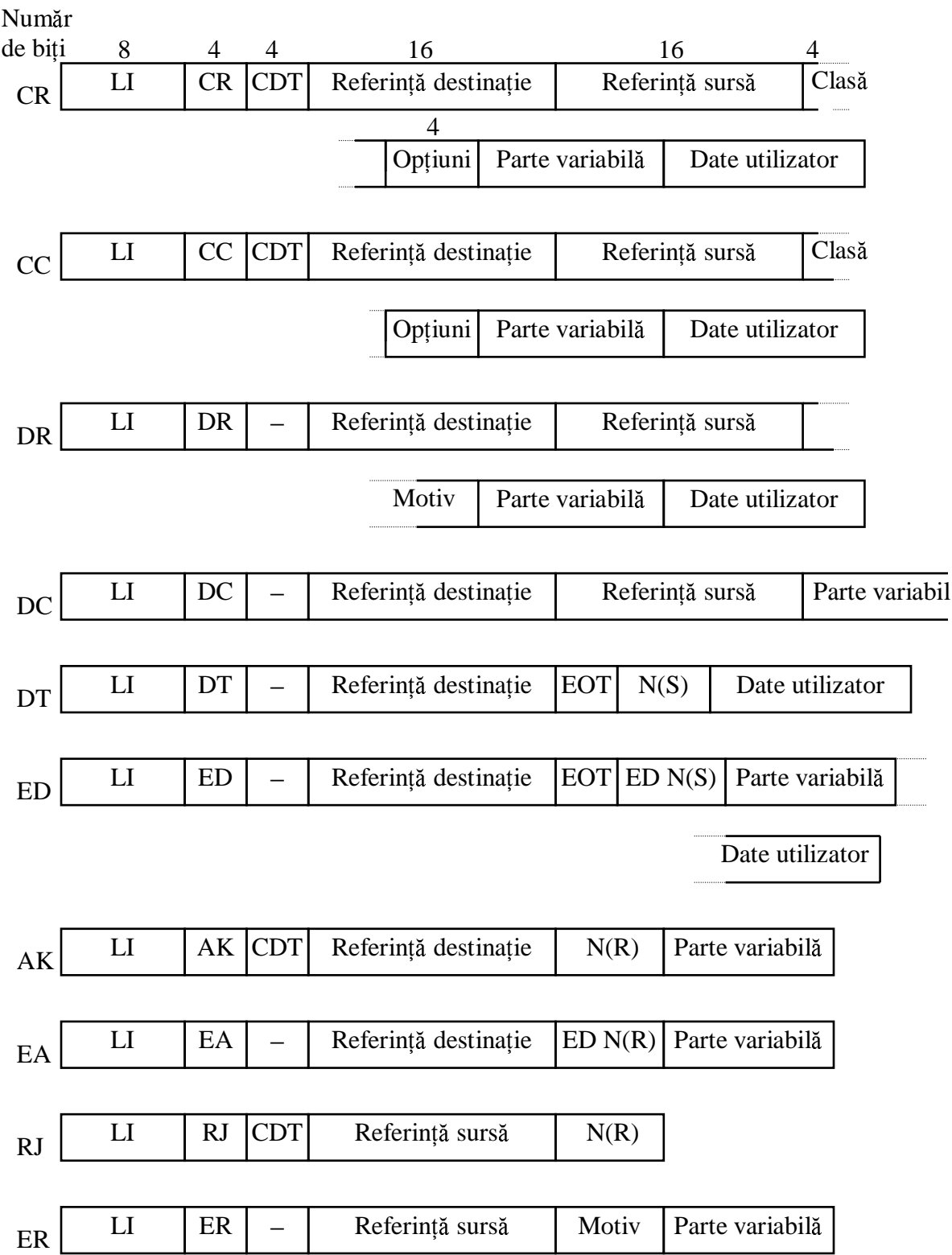


Figura 5.29 Formatele TPDU

Recepționând TPDU - CR entitatea corespondentă semnalează cererea de conexiune utilizatorului din propriul sistem printr-o primitivă T.CONNECT.indication.

Dacă acest utilizator acceptă apelul va răspunde cu o primitivă T.CONNECT.response. În caz contrar va răspunde cu primitiva T.DISCONNECT.request.

În funcție de primitiva de serviciu primită ca răspuns la T.CONNECT.indication entitatea de protocol transport din sistemul distant va emite o unitate TPDU - CC sau TPDU - DR. La primirea TPDU - CC sau DR entitatea de protocol din sistemul chemător va semnala utilizatorului stabilirea sau nu a conexiunii, printr-o primitivă T.CONNECT.confirm, respectiv T.DISCONNECT.indication, în acest ultim caz precizând, ca un parametru, motivul rejectării.

În cursul fazei de stabilire a conexiunii se negociază o serie de parametri, indicați în TPDU - CC și CR. După ce conexiunea transport a fost stabilită, entitățile de protocol transport pot accepta datele de utilizator pentru transferul lor în ambele sensuri. Transferul datelor este inițiat de un utilizator prin primitiva T.DATA.request. Entitatea de transport locală va transfera datele conținute în această primitivă (TSDU) în una sau mai multe unități de protocol TPDU - DT, în funcție de volumul datelor și de dimensiunea maximă a TPDU specificată pentru conexiunea respectivă. Fiecare TPDU - DT conține un bit EOT care, dacă este 1, arată că această unitate TPDU - DT este ultima dintr-o secvență ce constituie o unitate TSDU.

Toate unitățile TPDU - DT sunt numerotate în ordine. Câmpul de numerotare N(S) are un format lung (30 biți) sau un format scurt (6 biți), a cărui alegere se face, prin negociere, în fază de stabilire a conexiunii. Numărul de secvență servește atât pentru a indica ordinea TPDU într-o secvență cât și, împreună cu TPDU - AK, pentru confirmări și controlul fluxului. După ce au fost recepționate toate TPDU care alcătuiesc un mesaj TSDU, entitatea de protocol (recepție) reassemblează mesajul și-l trece utilizatorului prin primitiva T.DATA.indication (fig. 5.30).

Numărul de secvență la recepție N(R), plasat în TPDU de confirmare (AK), confirmă recepționarea în ordine a TPDU până la inclusiv TPDU având N(S) egal cu $N(R) - 1$. Dacă se recepționează o unitate TPDU având un număr N(S) diferit de cel așteptat, entitatea de protocol transport de la recepție va trimite înapoi o unitate TPDU - RJ cu N(R)

egal cu N(S) așteptat. Pentru a evita efectele pierderii unor unități TPDU - AK sau RJ sunt utilizate mecanisme de contorizare a timpului, prin intermediul cărora, dacă după un anumit interval de timp de la emiterea unei TPDU ce reclamă un anumit răspuns acesta nu sosește, TPDU se va retransmite.

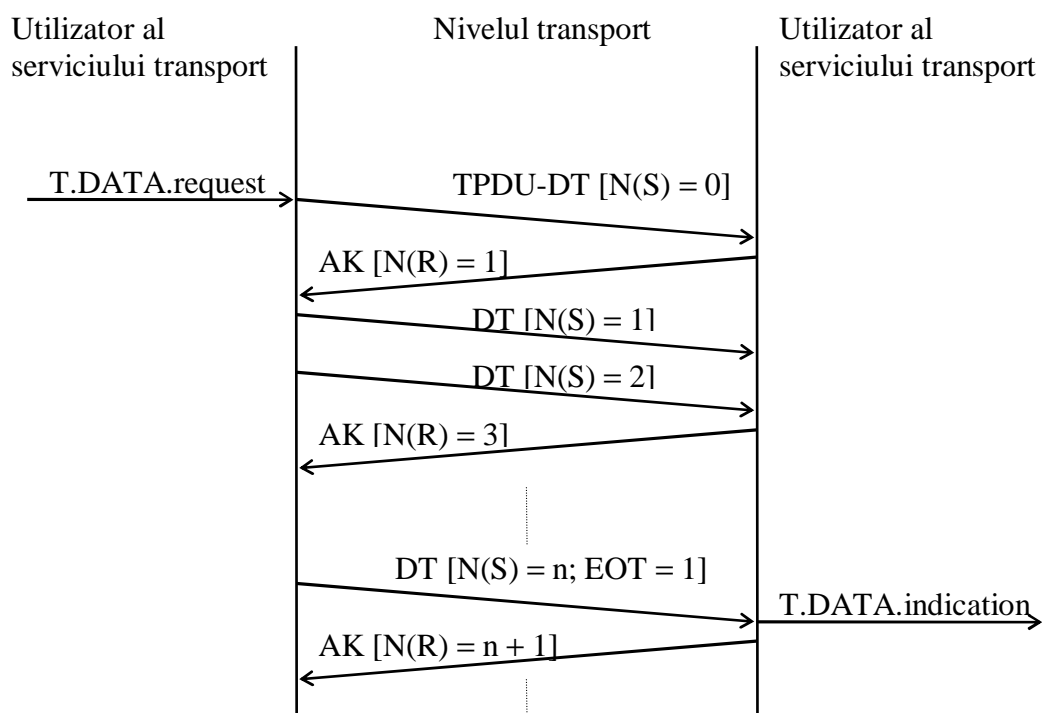


Figura 5.30 Transferul unui mesaj prin mai multe TPSDU

Detectarea erorilor la nivelul transport se face cu ajutorul unui câmp de 16 biți inclus în categoria “parametri” în care, la fiecare TPDU de tip CC, CR și DT se trece suma de verificare. Această sumă de verificare este alcătuită din doi octeți, determinați astfel încât să fie stisfăcute relațiile:

$$\sum_{i=1}^L a_i = 0 \quad (\text{modulo } 255)$$

$$\sum_{i=1}^L i a_i = 0 \quad (\text{modulo } 255)$$

unde i este poziția octetului în interiorul TPDU, a_i este valoarea octetului din poziția i iar L este lungimea TPDU în octeți. Dacă la recepție aceste relații nu se verifică unitatea TPDU va fi eliminată. Mecanismele de timp și de retransmitere vor asigura emiterea unei noi copii a acesteia.

Controlul fluxului se realizează cu ajutorul unui mecanism cu fereastră glisantă. Pentru fiecare sens de transmisiune este specificată o valoare de credit inițială (câmpul CDT - credit din TPDU - CR și CC), egală cu numărul unităților TPDU - DT pe care receptorul le poate primi. Numărul de secvență $N(S)$ este pus inițial la zero pentru fiecare sens de transmisiune, acest zero fiind și limita inferioară a ferestrei de emisie.

Limita superioară a ferestrei este determinată de valoarea de credit specificată de receptor. Limitele ferestrei de emisie sunt modificate în faza de transfer al datelor pe baza valorilor $N(R)$ și de credit recepționate de la entitatea de transport corespondentă (fig. 5.31).

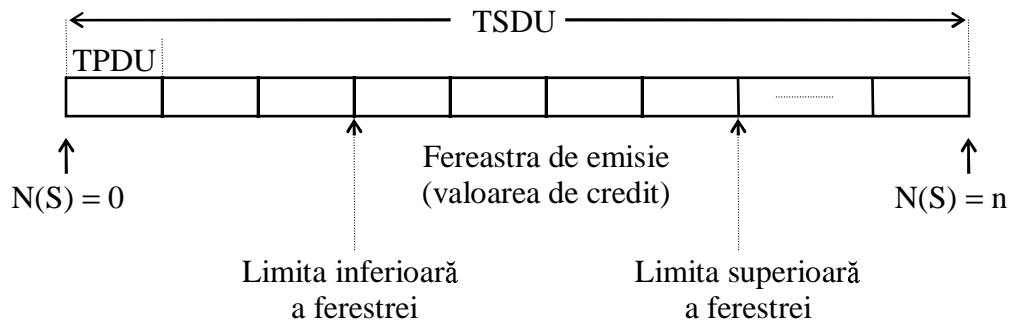


Figura 5.31 Mecanismul de control al fluxului

Când $N(S)$ devine egal cu limita superioară a ferestrei se oprește transferul datelor pe sensul respectiv. Fereastra de emisie este administrată de receptorul corespondent. Acesta indică numărul de unități TPDU pe care este gata să le recepționeze (valoarea de credit CDT) prin intermediul unităților TPDU - AK. Receptorul poate reduce sau crește creditul în funcție de resursele de care dispune la un moment dat, necesare pentru recepționarea unităților TPDU - DT. El poate chiar stopa transferul datelor trimițând un credit egal cu zero.

Unitățile TPDU - ED (expres) sunt tratate altfel decât TPDU normale. Datele expres sunt transmise prioritar, înaintea datelor normale. Nu se pot transmite mai multe TPDU - ED, una după alta, fără a avea confirmarea de recepție a fiecăreia dintre ele. Unitățile TPDU - ED sunt numerotate și fiecare TPDU - ED este confirmată printr-o unitate TPDU - EA cu același număr. Fiecare TPDU - EA recepționată deschide o fereastră de lărgime 1 pentru următoarea unitate TPDU - ED.

Transmiterea unei unități TPDU- ED este solicitată prin primitiva T.EXPEDITED-DATA.request. Receptorul confirmă imediat datele expres și le furnizează utilizatorului de date prin primitiva T.EXPEDITED-DATA.indication.

Eliberarea conexiunii poate fi inițiată, de oricare dintre utilizatorii serviciului transport, prin generarea unei primitive T.DISCONNECT.request către entitatea de transport locală, menționând motivul eliberării ca un parametru. Entitatea transport va transmite o unitate TPDU - DR, la recepția căreia entitatea de transport corespondentă

va trimite înapoi o unitate TPDU - DC și va genera o primitivă T.DISCONNECT.indication către utilizatorul local (fig. 5.28).

5.3.3 Protocoale suport pentru aplicații

Spre deosebire de grupul de protocoale TCP/IP, unde protocoalele de aplicații (sau procesele de aplicație) interacționează direct cu protocoalele nivelului transport (UDP și TCP), în modelul OSI ele interacționează prin entitățile de protocol asociate nivelelor intermediare sesiune și prezentare. Aceste nivele intermediare cooperează cu protocoalele nivelului aplicație pentru a asigura funcția suport pentru o aplicație particulară. Multe dintre primitivele de serviciu asociate nivelului aplicație fac translația direct la primitivele prezentare/sesiune echivalente.

- Nivelul sesiune -

Nivelul sesiune asigură unei entități de protocol aplicație, prin intermediul serviciilor oferite de nivelul prezentare, mijloacele pentru:

- stabilirea unei căi de comunicație logice (conexiune sesiune) cu o altă entitate aplicație în vederea schimbului de date (unități de dialog) și eliberarea normală a conexiunii;

- stabilirea unor puncte de sincronizare în interiorul dialogului și, în cazul erorilor (întreruperi), revenirea la starea anterioară unui punct de sincronizare, pentru a evita repetarea integrală a unității de dialog;

- întreruperea unui dialog și reluarea ulterioară a sa dintr-un punct prestabilit;

- negocierea utilizării de jetoane care permit emiterea datelor și eliberarea.

Jetoanele permit schimbarea sensului de transfer al datelor și crearea dialogurilor. Jetonul este un obiect logic purtător de drepturi și atribuții. Utilizatorul (unic) care posedă jetonul este singurul autorizat să folosească serviciile asociate jetonului. Sunt definite patru tipuri de jetoane: de date, de eliberare, pentru sincronizare minoră și pentru sincronizare majoră și gestionarea activității.

În conceperea serviciilor nivelului sesiune s-a avut în vedere că acest nivel va folosi serviciul cu conexiune punct la punct oferit de nivelul transport. Ca urmare nivelul sesiune presupune că transmisiunea datelor se face fără erori și fără duplicări pe o conexiune între un cuplu de utilizatori.

Un jeton poate fi disponibil sau indisponibil. Dacă este disponibil el este alocat unuia sau altuia dintre cei doi utilizatori și poate fi trecut dela unul la altul. Dacă jetonul este indisponibil cei doi utilizatori pot accede liber la serviciile asociate jetonului. Spre exemplu, dacă jetonul de date este disponibil, conexiunea sesiune este exploatată, pentru transferul datelor, în mod alternant (semiduplex), iar dacă este indisponibil conexiunea va fi exploatată în modul bidirecțional simultan.

Jetoanele de sincronizare sunt asociate procesului de sincronizare utilizat în cursul unei sesiuni. Dacă doi utilizatori ai serviciului sesiune au de schimbat un mare volum de date este recomandabil ca datele să fie structurate în unități identificabile pentru ca, în cazul în care în rețea survine o defecțiune, să fie afectată numai unitatea de date care este în curs de transferare. Această funcțiune se obține cu ajutorul punctelor de sincronizare înserate în fluxul de date, care permit identificarea unor momente precise, semnificative pentru aplicație. Punctele de sincronizare majore permit structurarea fluxului datelor ce trebuie transferate în cursul unei sesiuni în unități de date numite dialoguri. În interiorul unui dialog pot fi înserate puncte de sincronizare minore (fig. 5.32)

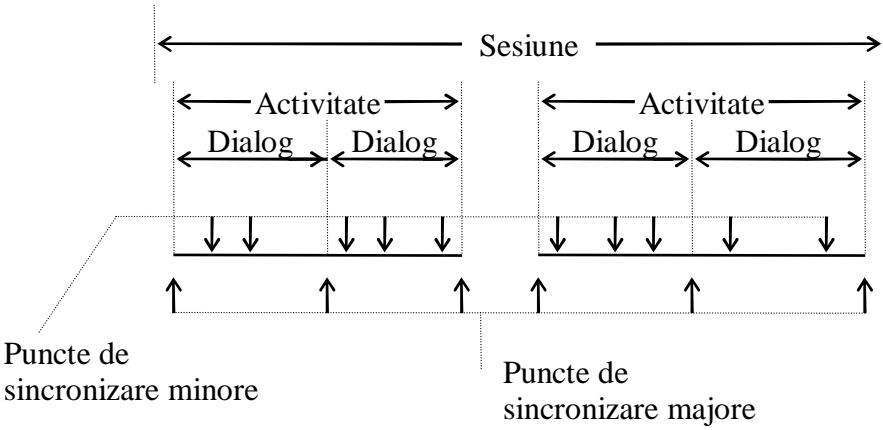


Figura 5.32 Structurarea sesiunii în activități și dialoguri

Un element de structurare care ține seama de natura logică a informației transmise este activitatea. O sesiune poate include una sau mai multe activități distincte, dar în orice moment este autorizată numai o activitate. Este posibil de asemenea ca o activitate să se desfășoare pe parcursul mai multor sesiuni. Fiecare activitate este constituită din mai multe dialoguri succesive. Spre exemplu, o activitate privind

transferul unui număr de fișiere poate fi structurată în dialoguri, câte unul pentru fiecare fișier.

O conexiune sesiune are, ca și conexiunile de la nivelele inferioare, trei faze: stabilire, transfer date, eliberare. În cadrul fiecărei faze sunt disponibile mai multe servicii. Deoarece pentru o anumită aplicație nu sunt necesare toate serviciile și pentru a permite utilizatorilor să negocieze serviciile necesare, acestea sunt grupate în unități funcționale care, la rândul lor, în diferite combinații, formează subseturi (profiluri) de servicii oferite utilizatorilor. Fiecare aplicație poate alege (negocia) profilul de care are nevoie.

Unitățile funcționale sunt:

- Nucleu (kernel) - asigură funcțiunile minimale pentru gestionarea conexiunii sesiune (stabilire, transfer date, eliberare);
- Semiduplex - permite schimbul datelor în modul alternant, controlând sensul transferului de date;
- Sincronizare - asigură (re)sincronizarea în cursul unei sesiuni;
- Gestionarea activității - asigură identificarea, începutul, sfârșitul, întreruperea și reluarea activităților;
- Eliberarea negociată;
- Raportarea excepției - asigură raportarea unei excepții în cursul unei sesiuni.

Subseturile alcătuite prin combinarea acestor unități funcționale sunt:

- subsetul de bază (BCS - Basic combined subset), incluzând nucleul și unitatea semiduplex;
- subsetul de sincronizare de bază (BSS - Basic synchronized subset), incluzând unitățile de sincronizare;
- subsetul activității de bază (BAS - Basic activity subset), incluzând unitățile pentru gestionarea activității și raportarea excepției.

Ca și în cazul serviciilor oferite de celelalte nivele și serviciul sesiune este solicitat și folosit prin intermediul unor primitive de serviciu, cu parametrii asociați, ca de exemplu: S.CONNECT, S.DAT, S.RELEASE, S.TOKEN-PLEASE etc. Celor mai multe dintre primitivele de serviciu le corespund tipuri diferite de unități de date de protocol sesiune (SPDU).

Structura unei unități SPDU este prezentată în figura 5.33.

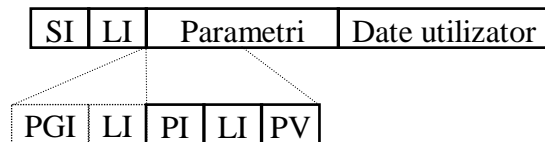


Figura 5.33 Formatul SPDU

Fiecare tip de SPDU este identificat printr-un octet care ocupă câmpul SI. Câmpul LI, format dintr-un octet sau din trei octeți, indică numărul de octeți care mai urmează până la sfârșitul SPDU. Dacă acest număr este cel mult 254, câmpul LI are un singur octet, iar dacă este mai mare de 254 are trei octeți, primul octet fiind totdeauna 255. Diferitele tipuri de SPDU au un număr diferit de câmpuri, reprezentând fiecare un parametru. Fiecărui parametru îi corespunde un identificator de parametru (PI), un identificator al lungimii parametrului (LI) și o valoare a parametrului (PV). În anumite situații parametrii sunt grupați, șirul lor fiind precedat de un identificator al grupului de parametri (PGI) și un identificator al lungimii grupului de parametri (LI).

Datele de utilizator asociate unei primitive de serviciu pot fi segmentate de entitatea de protocol sesiune într-un număr de SPDU pentru a fi transferate folosind o conexiune transport. Mai multe SPDU pot fi grupate într-o aceeași unitate TPDU. Deoarece serviciul transport garantează succesiunea unităților TPDU, unitățile SPDU vor fi furnizate destinatarului în ordinea în care ele au fost trecute, la emisie, către nivelul transport.

- Nivelul prezentare

Nivelul prezentare, definit de standardele ISO 8822 și ISO 8823, se ocupă de reprezentarea (sintaxa) datelor în mesajele asociate unei aplicații, pe durata transferului acestora între două procese de aplicație. Prin intermediul nivelului prezentare mesajele au același înțeles pentru procesele de aplicație între care ele se transferă. Fără acest nivel programele de aplicație ar trebui rescrise de fiecare dată când în rețea se introduce un nou sistem de operare.

Datele asociate unui limbaj de programare de nivel înalt nu au aceeași reprezentare în toate calculatoarele. Pentru ca ele să fie interpretate la fel, înaintea de transferarea lor între două procese, trebuie convertite din sintaxa locală (abstractă) într-o sintaxă de transfer (concretă), larg utilizată. În mod similar, la recepție, înainte de a fi prelucrate, datele vor fi convertite din sintaxa de transfer în sintaxa locală.

Pentru a nu se impune utilizarea unui anumit (mereu același) limbaj de programare pentru orice aplicație, deci pentru a lăsa la latitudinea utilizatorilor alegerea

limbajului de programare într-o anumită aplicație, ISO și ITU-T au definit o sintaxă abstractă generală, adecvată pentru definirea tipurilor de date asociate celor mai multe aplicații distribuite, numită ASN.1 (Abstract Syntax Notation 1). Datele asociate unei aplicații sunt definite mai întâi folosind ASN.1, după care aceste definiții sunt prelucrate de un compilator, adecvat limbajului de programare utilizat. Compilatorul va da definițiile tipurilor de date echivalente împreună cu un set de proceduri/funcțiuni de codare și de decodare pentru fiecare tip de date. Definițiile tipurilor de date sunt combinate (linked) și utilizate cu programul de aplicație corespunzător iar procedurile/funcțiunile de codare și de decodare sunt utilizate de entitatea prezentare pentru a realiza operațiile de codare (la emisie) și de decodare (la recepție) asociate cu fiecare tip de date.

În timp ce o sintaxă abstractă este definită prin reguli de specificare asociate datelor, independente de codul (mașină) utilizat pentru reprezentarea lor, o sintaxă de transfer definește concret modul de codare a datelor (câmpuri de biți sau octeți) pentru transferul lor. Operația care permite trecerea de la o sintaxă abstractă la o sintaxă de transfer este similară operației de compilare a unui program.

Deși sarcina principală a nivelului prezentare este conversia sintaxei datelor, deoarece la acest nivel se fac prelucrări ale datelor înainte și după transferul lor, tot aici este recomandabil să se realizeze, dacă sunt necesare, funcțiunile de criptare și/sau de compresie a datelor. Astfel, entitatea prezentare din sistemul sursă, după codarea datelor fiecărui mesaj din sintaxa abstractă locală în sintaxa de transfer corespunzătoare, criptează datele conform unui algoritm negociat cu sistemul receptor și apoi le comprimă folosind de asemenea un algoritm acceptat de receptor. La recepție, înainte de a decoda datele în sintaxa abstractă locală pentru a fi furnizate entității aplicație, vor fi efectuate operațiile inverse.

Asocierea unei sintaxe abstracte cu o sintaxă de transfer compatibilă constituie un context de prezentare. Una din funcțiunile asociate nivelului prezentare este de a negocia un context de prezentare adecvat utilizării pe o conexiune sesiune/prezentare. În plus, nivelul prezentare trebuie să faciliteze nivelului aplicație folosirea multiplelor servicii oferite de nivelul sesiune. Rezumând, funcțiunile nivelului prezentare sunt:

- negocierea unei sintaxe de transfer;
- transformarea datelor utilizatorului sursă în sintaxa de transfer și, reciproc, transformarea datelor recepționate din sintaxa de transfer în sintaxa abstractă locală;

- adaptarea cererilor de serviciu ale nivelului aplicație, pentru funcțiuni de control al dialogului și al sincronizării, în primitivele corespunzătoare ale serviciului sesiune.

5.3.4 Nivelul aplicație

Rețelele de comunicații permit realizarea unor aplicații care fac apel la date și resurse de calcul (software și hardware) situate în diferite locuri. Sistemul de comunicație stabilește legături între un ansamblu de sarcini care concură la executarea aplicației.

În modelul de referință OSI nivelul aplicație reprezintă interfața cu sistemul de comunicații, oferită utilizatorilor (procesele de aplicație), și specifică facilitățile oferite acestora, interacțiunile lor cu serviciul de comunicații.

Nivelul aplicație constă din mai multe entități de protocol (Fig. 5.34), fiecare numită element al serviciului aplicație (ASE - Application Service Element). Deoarece anumite funcțiuni sunt comune multor aplicații, acestea sunt realizate prin protocoale separate care vor fi conectate cu protocoale specifice de aplicație, adecvate pentru a satisface un anumit serviciu suport. Combinația de protocoale rezultată, numită entitate de aplicație, este oferită utilizatorului (procesul de aplicație).

Protocoalele comune mai multor aplicații sunt numite CASE (Common Application Service Element) iar celelalte, specifice câte unei aplicații, sunt numite SASE (Specific Application Service Element).

Comunicația între două procese de aplicație utilizatoare se realizează fie utilizând un canal de comunicație (logic) stabilit între cele două entități de aplicație înainte de a se transfera datele, fie utilizând un schimb simplu de mesaje cerere/răspuns. O conexiune logică între două entități de aplicație este numită asociere. Elementul ASE care inițiază stabilirea și eliberarea unei asocieri între două elemente ASE specifice (SASE) este numit element de serviciu pentru controlul asocierii (ACSE - Association Control Service Element).

Un număr redus de elemente ASE specifice funcționează utilizând mesaje scurte cerere/răspuns care nu implică un volum mare de informație adițională (de protocol). Elementul ASE definit pentru a permite acest tip de aplicație este numit ROSE (Remote Operations Service Element).

Multe aplicații distribuite implică situații în care mai multe procese de aplicație solicită accesul lor la o singură resursă partajată. Spre exemplu, un sistem de fișiere într-o aplicație bancară care conține conturile clienților este accesat concurențial de sistemele clienților pentru a realiza operații de creditare și debitare pe diferite conturi. Pentru buna funcționare a unui astfel de sistem este necesar un mecanism de control (concurențial). O problemă asemănătoare apare în cazul în care copii ale aceluiași fișier sunt păstrate în locații diferite. În acest caz este necesar ca la fiecare modificare a fișierului să se facă actualizarea în toate copiile sale.

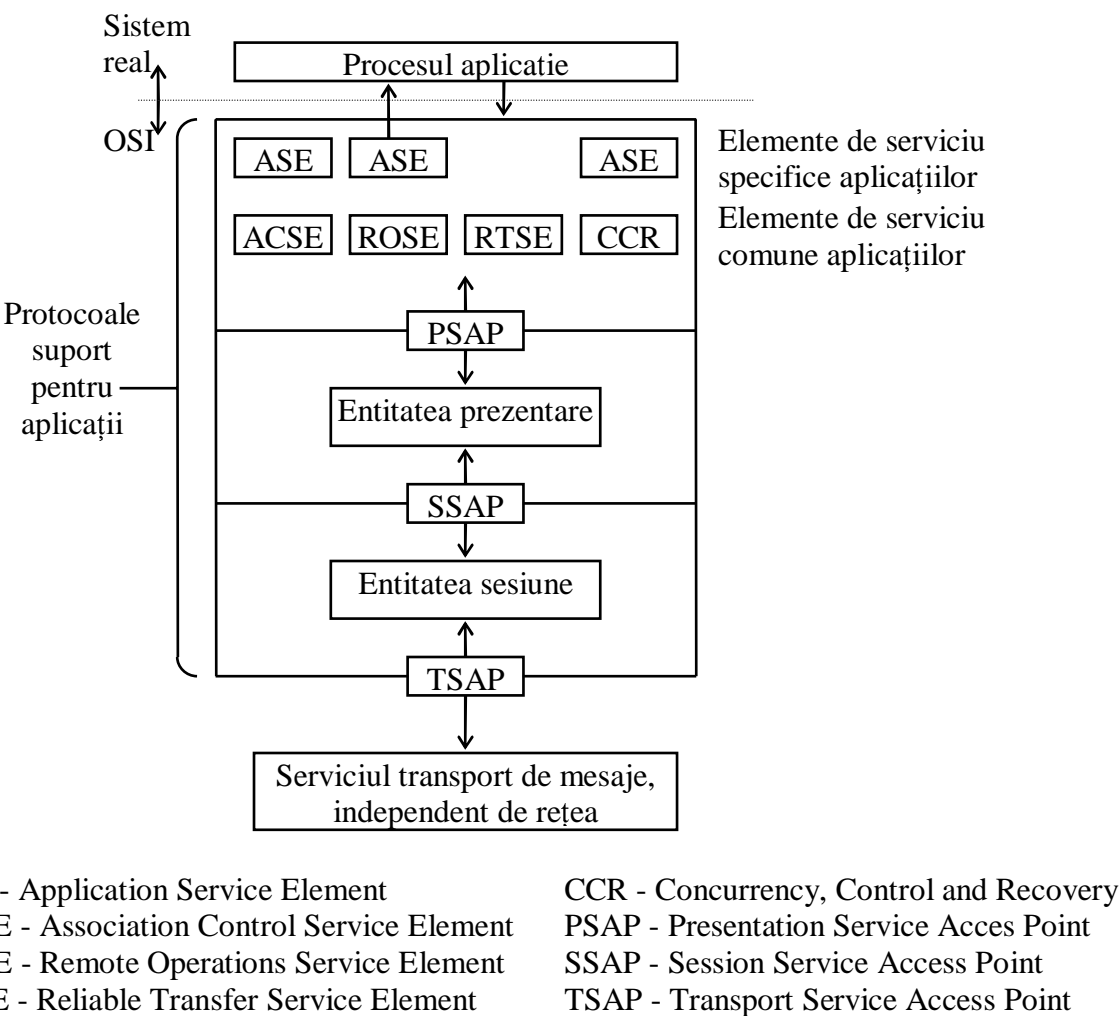


Figura 5.34 Protocoale suport pentru aplicații

Ambele probleme menționate mai sus sunt comune multor aplicații distribuite. Pentru controlul acestor operații a fost definit un element ASE numit CCR (Commitment, Concurrency and Recovery).

Unele aplicații folosesc adesea două sau trei elemente de serviciu de tipul celor prezentate (ACSE, ROSE și CCR) într-o singură entitate de aplicație.

Un alt element ASE, definit înainte de a fi complet specificat setul serviciilor prezentare, care utilizează o combinație de servicii ACSE și un mic subset al serviciilor nivelului sesiune, este numit RTSE (Reliable Transfer Service Element).

- Protocoale de aplicații OSI -

În afara protocoalelor suport pentru aplicații, amintite în paragrafele precedente, sunt definite sau în curs de definire o serie de protocoale (ASE) specifice unor aplicații. Unele dintre ele asigură servicii similare celor furnizate de protocoalele de aplicații TCP/IP. În continuare vor fi prezentate pe scurt o parte din protocoalele de aplicații ISO.

- Terminalul virtual -

Acest protocol furnizează servicii similare celor oferite de protocolul Telnet. El permite unui utilizator să interacționeze de la un terminal cu un proces de aplicație care se desfășoară (rulează) pe un calculator distant ca și cum terminalul ar fi conectat direct la acel calculator.

Există o mare varietate de terminale și de asemenea au fost elaborate multe programe de aplicații pentru a fi utilizate de aceste terminale. Scopul terminalului virtual este de a permite accesul la aceste aplicații de la multitudinea de terminale diferite. Pentru aceasta nu se definește un terminal virtual unic, cu caracteristici prestabilite. Caracteristicile terminalului virtual vor fi negociate în funcție de aplicația ce urmează a fi accesată.

- Transferul de fișiere (FTAM - File transfer, acces and management) -

Este similar protocolului FTP. El permite unor procese de aplicații distribuite să acceseze și să administreze un server de fișiere distant.

- Poșta electronică -

Acest sistem de transfer de mesaje este cunoscut, în titulatura ISO, ca MHS (Message Handling System) sau MOTIS (Message Oriented Text Interchange Standard). Este similar protocolului SMTP din grupul TCP/IP. Se bazează pe serviciul public de difuzare (operare) a mesajelor X.400 definit de ITU-T. Recomandările X.400 reprezintă un grup de protocoale, fiecare dintre ele realizând o anumită funcție specifică serviciului internațional de mesagerie electronică.

- Protocolul de administrare a rețelei -

Este similar protocolului SNMP din TCP/IP și este cunoscut sub denumirea CMISE (Common Management Information Service Element). El permite emiterea și recepționarea mesajelor utilizate pentru administrarea rețelei. CMISE reprezintă de fapt o componentă a unui ansamblu mai amplu de protocoale de administrare (SMAE - System Management Application Entity) care, printre altele, permite unui administrator de rețea să administreze de la distanță diferite obiecte asociate mediului OSI: protocoale, poduri, routere, comutatoare de pachete, etc.