UNIVERSITATEA TEHNICĂ CLUJ-NAPOCA

DEPARTAMENTUL ELECTROTEHNICĂ ŞI MĂSURĂRI

Cursul 12 ASOCIEREA SUITEI TCP/IP ALĂTURI DE ALTE PROTOCOALE

Introducere curs	În acest curs sunt prezentate suita TCP/IP i alte protocoale.
Obiective curs	• Nivele specifice rețelelor locale. • TCP/IP în rețele de date. • TCP/IP şi alte protocoale. • Nivele specifice rețelelor locale. • NetBIOS şi TCP/IP. • XNS şi TCP/IP. • ARCnet şi TCP/IP. • Rețele FDDI. • X.25 şi IP. • ISDN şi TCP/IP. • SMDS (Switched Multi-Megabit Data Services) şi IP. • ATM (Asynchronous Transfer Mode) şi BISDN
Durată medie de studiu individual	Durata medie de studiu individual: 100 minute. Acest interval de timp presupune parcurgerea continutului cursului şi rezolvarea testelor de autoevaluare

Cuprins:

TCP/IP în rețele de date.

Datorită modelului cu nivele, suita TCP/IP (care ocupă nivelele OSI 3 şi 4) se poate folosi, într-o rețea, împreună cu alte protocoale specifice celorlalte nivele. Aceste situaţii sunt destul de des întâlnite într-o rețea complexă în care este nevoie să se "profite", după caz, de avantajele diferitelor protocoale şi este important să se înțeleagă acest lucru.

TCP/IP şi alte protocoale.

TCP/IP nu este singurul protocol utilizat în rețelele de transfer de date, ci se găseşte în asociere cu altele, aflate la nivele superioare sau inferioare, cu care interacționează. Pentru a înțelege modul de interacțiune, se va analiza un exemplu de rețea locală (**LAN**), iar apoi se va extinde analiza asupra unui grup de rețele locale (intranet).

Nivelele ocupate de **TCP/IP**, în conformitate cu modelul **OSI**, au fost concepute să fie independente unele de altele, ceea ce permite combinarea diferitelor protocoale de transport şi de rețea. Când se trimite un mesaj de-a lungul unei rețele, fiecare protocol, specific unui nivel, introduce în antetul datagramei corespunzătoare informațiile necesare pentru procesarea acesteia.

Datele suferă un proces de încapsulare succesivă prin care fiecare protocol îşi anunță perechea de la celălalt capăt despre conținutul datagramelor şi tipul protocolului de nivel superior folosit. După înlăturarea antetului şi interpretarea informațiilor conținute de acesta, fiecare nivel îşi procesează datagramele după specificul protocolului utilizat [1].

Înlocuirea unui protocol cu altul este posibilă dacă protocoalele adiacente pot să opereze unele cu altele.

Pentru a examina cum operează nivelele între ele şi cum se poate adăuga, sau înlocui, un nivel ne vom folosi de exemplul prezentat în **figura 12.1**. Aceasta este o rețea care foloseşte Ethernet ca tehnologie (protocol) a legăturii de date (nivel **OSI 2**), **IP** pentru rețea (nivel 3) şi **TCP** pentru transport (nivel 4).

Figura 12.1 prezintă modul de încapsulare a datelor de la un nivel la altul şi transmiterea lor de-a lungul rețelei, într-o analiză comparată între modelul de referință **OSI** şi **TCP/IP**.

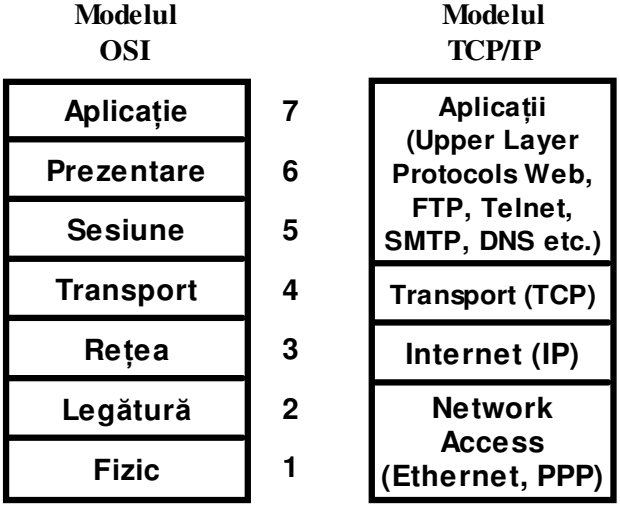

Fig. 12.1. Încapsularea succesivă, comparație între modelul **OSI** şi **TCP/IP**.

După cum s-a putut vedea mai înainte, procesul de transmisie în rețea începe cu un mesaj provenit de la un nivel superior (**ULP** - *Upper Layer Protocol*), care la rândul lui îl preia de la o aplicație, sau direct de la o aplicație.

Mesajul ajuns la nivelul transport este preluat de componenta **TCP**, este segmentat şi i se adaugă un antet care conține informațiile de transport necesare. Segmentul astfel pregătit este pasat apoi nivelului **IP** (de rețea) care face ceva asemănător, adăugând un antet cu informații proprii şi trimite pachetul astfel obținut nivelului legăturii de date unde este preluat de Ethernet care îl încapsulează într-un cadru şi îl trimite, prin rețea, spre destinație.

Acest model simplu are doar valoare didactică, deoarece în practică nivelul **IP** nu interacționează direct cu Ethernet, ci din motive legate de calitatea transferului de date, se adaugă un nivel suplimentar pentru izolarea eventualelor întreruperi sau blocaje de sistem.

Nivele specifice rețelelor locale.

Pentru a clarifica afirmațiile prezentate mai sus, în continuare se vor analiza în detaliu componentele de bază ale unei rețele locale.

În **figura 12.2** se prezintă, în detaliu, aceste nivele corespunzătoare unei tehnologii (Ethernet) care foloseşte **CSMA/CD** (*Carrier Sense, Multiple Access (CSMA) and Collision Detect*).

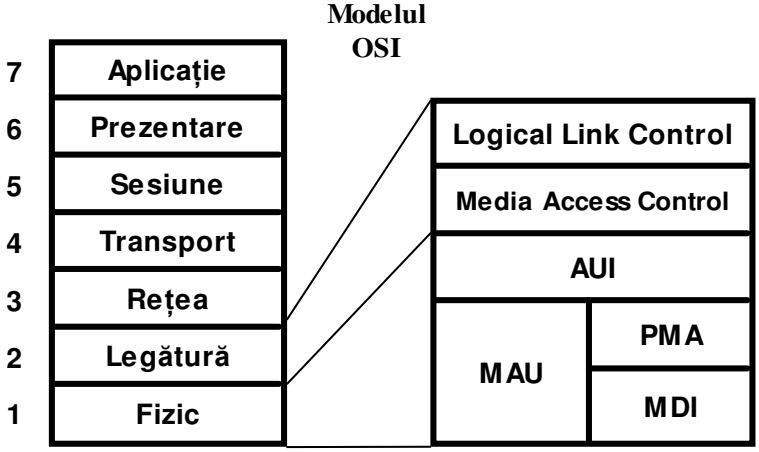

Fig. 12.2. Modelul unei rețele locale, cu detalierea nivelelor inferioare.

În acest exemplu sunt implicate câteva nivele suplimentare, numite subnivele.

1. Subnivelul **LLC** (*Logical Link Control* - controlul legăturii logice) este o interfață între nivelul **IP** şi cel de sub el (al legăturii de date - după modelul **OSI**, sau rețea după cel **TCP/IP**). Aşa cum s-a putut vedea într-un capitol anterior, există mai multe tipuri de **LLC**, dar la această etapă este suficientă înțelegerea rolului de tampon de date, al acestuia. Acest subnivel asigură un serviciu de transfer simplu, cu sau fără conexiune, în funcție de versiunea utilizată. **LLC** este utilizat de obicei împreună cu **HDLC** (*High-Level Data Link Control*).

În cazul unui serviciu fără conexiune, se foloseşte un cadru care conține un mesaj de tip **UI** (*Unnumbered Information*), iar pentru un seviciu bazat pe conexiune un cadru cu un mesaj de tip **ABM** (*Asynchronous Balanced Mode*), ambele asigurate de către **HDLC**. În aceste condiții, este foarte importantă configurarea **LLC** în conformitate cu cerințele impuse de **TCP/IP**.

2. Subnivelul **MAC** (*Media Access Control*), prezentat într-un capitol anterior, gestionează adresarea interfețelor şi unele elemente de control a traficului în rețea, cum ar fi detectarea coliziunilor şi sincronizarea transmisiilor. În mecanismul acestui control, **MAC** foloseşte funcțiuni de temporizare şi de retransmisie, fiind independent de mediul de propagare, dar este dependent de protocoalele utilizate în rețea.

Nivelul fizic este compus din câteva subnivele ale unor servicii specifice.

- Subnivelul **AUI** (*Attachment Unit Interface*) asigură legătura dintre componenta nivelului fizic al maşinii care face parte dintr-o rețea şi mediul fizic de propagare. Cu alte cuvinte, **AUI** este locul în care este localizat conectorul cablului, sau fibrei optice.
- Subnivelul **MAU** (*Medium Attachment Unit*) este compus din două părți PMA (*Physical Medium Attachment*) şi **MDI** (*Medium Dependent Interface*), fiecare putând fi considerate componente separate. **MAU** asigură conectarea maşinii la mediul de propagare, verificând integritatea datelor şi monitorizarea mediului de propagare. **MAU** este prevăzut cu funcțiuni care permit verificarea calității semnalului transmis şi rutine de testare a operării corecte a mediului.

Prin adăugarea în arhitectura rețelei a acestor nivele suplimentare, nivelul IP este separat de nivelul Ethernet, aşa cum se poate vedea în **figura 12.3.** Această configurație este mai des întâlnită decât cea prezentată în **figura 12.1.** Se observă, din reprezentarea schematică, cum fiecare dintre aceste nivele operează încapsulări succesive înainte de a trimite unitățile lor specifice de date nivelelor inferioare.

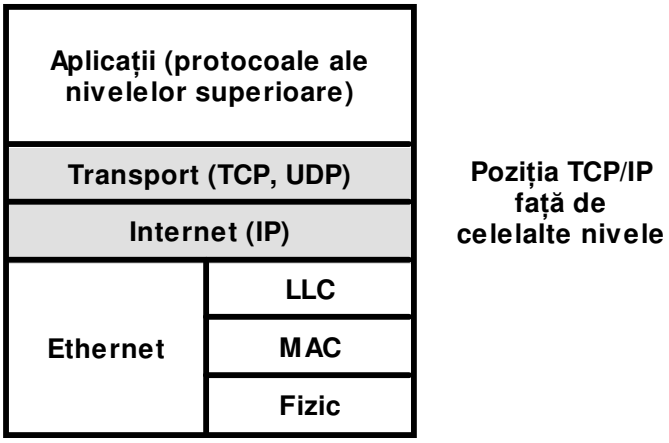

Fig. 12.3. Poziția TCP/IP alături de celelalte nivele.

Acest tip de rețele locale (numite şi **IP/802**, datorită faptului că procesele la nivelul legăturilor de date sunt reglementate de standardele **IEEE 802.2** pentru **LLC** şi **802.3** pentru **Ethernet**) pot utiliza un protocol **LLC** de tipul 1, fără conexiune, care transmite cadre **UI** (*Unnumbered Information*), datorită componentei **TCP** care este un protocol bazat pe conexiune, funcțiunile de verificare şi confirmare a datelor fiind asigurate de acesta. **LLC** şi **MAC** asigură separarea **IP** de nivelul fizic, dar mesajelor utile li se adaugă un număr suplimentar de anteturi (acest lucru nu este neapărat un inconvenient).

Antetul **LLC** conține ambele tipuri de adrese **SAP** (*Service Access Points*) necesare identificării protocoalelor nivelului superior.

În cazul utilizării **UDP** ca protocol de transport, acesta neavând mecanisme de confirmare şi verificare a datelor la fel de complexe ca **TCP**, va trebui utilizat un protocol **LLC** de tipul **2**. Aceste este prevăzut cu mecanisme specifice de verificarea integrității datelor, asemănătoare cu cele ale **TCP**, dar funcționând la nivelul legăturilor de date.

Dezavantajul unei astfel de soluții este că aceste funcțiuni sunt localizate sub nivelul **IP** şi nu deasupra lui. Într-o rețea complexă, cu multe porți de acces înlănțuite, unele pachete se pot pierde, iar **LLC** nu este capabil să gestioneze situații provocate de componente aflate la nivele superioare lui. În acest caz, aplicațiile care operează la nivelul cel mai înalt trebuie să rezolve acest gen de probleme.

Diferențele dintre tandemul "**TCP - LLC de tipul 1**" şi "**UDP - LLC de tipul 2**" sunt complexe şi variantele de aplicare trebuie bine alese. Combinația "**TCP - LLC de tipul 1**" oferă o siguranță şi integritate mai bună a datelor, iar "**UDP - LLC de tipul 2**", o rată de transfer mai ridicată.

NetBIOS şi TCP/IP.

NetBIOS (*Network Basic Input Output Sistem*) este o componentă a sistemelor de operare de rețea, dezvoltată pentru familia calculatoarelor personale. Această componentă permite aplicațiilor de la nivelul superior să interacționeze prin mesaje şi să-şi aloce reciproc resurse. NetBIOS operează deasupra nivelelor ocupate de **TCP** (**UDP**) şi **IP** şi interacționează bine cu acestea. În **figura 12.4** se poate vedea un exemplu de rețea care utilizează componente **NetBIOS**, încapsulate în **TCP/IP**.

NetBIOS este de fapt un serviciu pentru care sunt alocate trei numere de porturi. Portul **137** este dedicat serviciului de nume (specific **NetBIOS** şi nu are nici o legătură cu numele simbolic utilizat de **DNS**), portul **138** folosit de serviciul de transfer de datagrame (specifice informațiilor transmise de **NetBIOS**) şi portul **139** utilizat de nivelul sesiune (nivelul **OSI 5**). Se pot face asocieri şi conversii între numele furnizat de serviciul specializat al protocolului de internet (**DNS**) şi cel definit de **NetBIOS** (**NBNS** - *NetBIOS Name Server*).

NBNS se utilizează pentru identificarea unui **PC** care operează într-o arie de interacțiune

NetBIOS şi la interfaţarea dintre acesta şi **IP** poate fi folosit pentru asocierea reciprocă a celor două tipuri de nume.

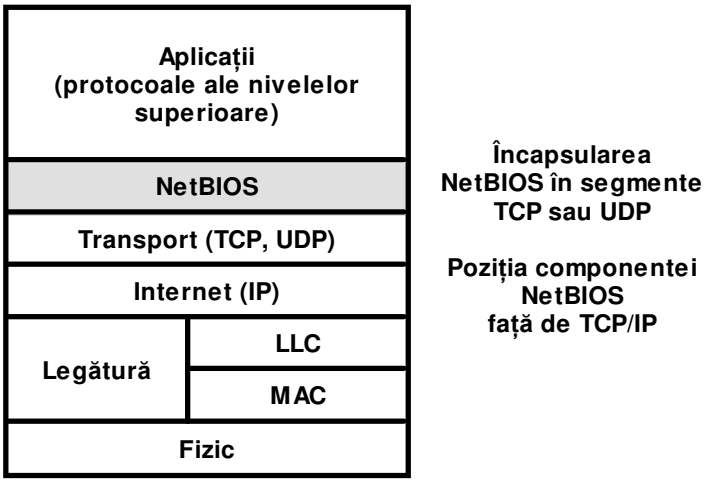

Fig. 12.4. Încapsularea componentelor **NetBIOS** în **TCP/IP**.

IP poate să fie configurat să opereze deasupra **NetBIOS** (încapsulare în **NetBIOS**), eliminând componentele **TCP** sau **UDP**. În această situaţie NetBIOS va lua locul acestora şi va asigura un serviciu fără conexiune, ceea ce obligă aplicaţiile să asigure funcţiuni de segmentare, verificarea integrităţii şi controlul fluxului datelor transmise. Aceasta se poate urmări în **figura 12.5** unde **NetBIOS** încapsulează datagramele (pachetele) **IP**.

Asocierea corectă a numelor (**IP** şi **NetBIOS**) este absolut necesară deoarece adresele pachetelor **NetBIOS** trebuie să corespundă adreselor **IP**. Pentru aceasta **NetBIOS** codifică numele în formatul adreselor **IP**, *xxx.xxx.xxx.xxx*.

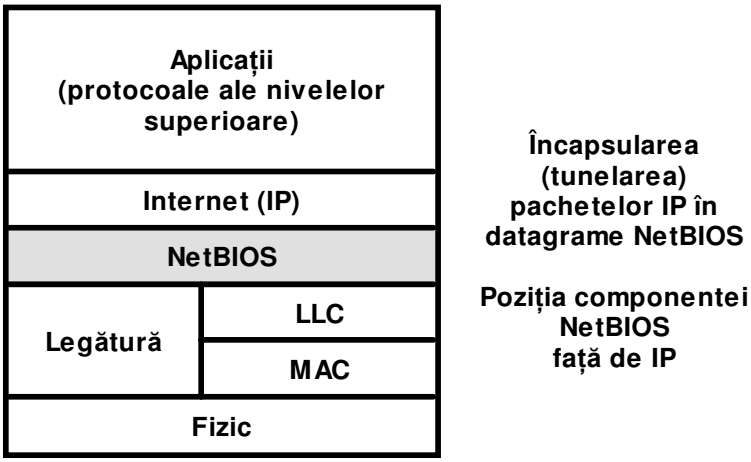

Fig. 12.5. Operarea componentei IP deasupra nivelului NetBIOS.

Acest tip de reţea are avantajul unei arhitecturi simple (de tip *Workgroup*), dar presupune ca nivelul superior (**ULP**), în acest caz aplicaţia, să suplinească funcţiunile protocolului de transport **TCP**, bazat pe conexiune. Proiectarea unor astfel de aplicaţii este însă mai dificilă şi necesită un consum suplimentar de resurse de sistem.

XNS şi TCP/IP.

Sistemul de reţea propus de firma Xerox (**XNX** - *Xerox Network System*) a fost, la un moment dat, larg răspândit sub forma unor pachete software comerciale. Succesul său avea la bază faptul că firma Xerox a distribuit în domeniul public codul sursă.

Protocoalele **XNS** au fost proiectate să opereze împreună cu versiunea proprie a standardului

Ethernet (varianta inițială a acestui standard a fost propusă pentru analiză forurilor **IEEE** şi este cunoscută ca **Novell Ethernet**).

XNS poate utiliza **IP** ca protocol de rețea şi **SPP** (*Sequenced Packet Protocol*), care asigură o parte din funcțiunile de transport utilizate de **TCP**, aşa cum se poate vedea în **figura 12.6**.

Ca protocol de nivel superior se foloseşte Courier, care asigură serviciile corespunzătoare nivelelor de sesiune şi prezentare (**OSI 5** şi **6**).

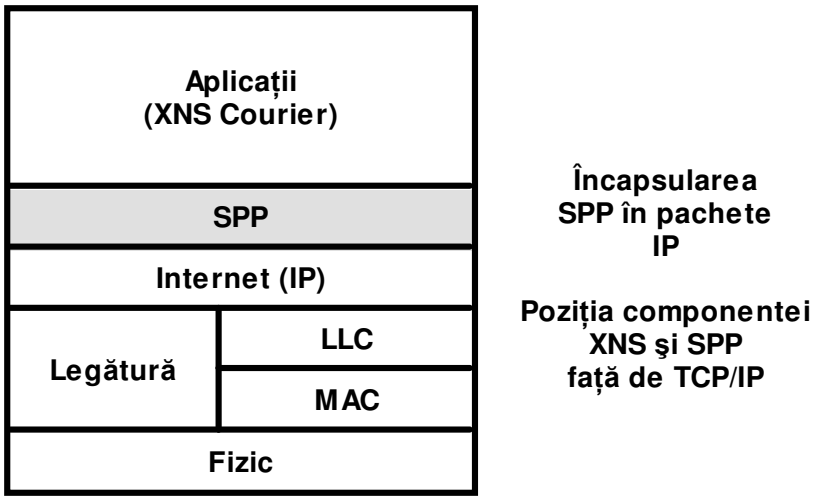

Fig. 12.6. Utilizarea protocolului Internet (**IP**) în rețele **XNS**.

XNS foloseşte termenul de **ITP** (*Internet Transport Protocols*) când se referă la setul de protocoale utilizate. Printre acestea se află **IP**, **RIP** (*Routing Information Protocol*) şi un protocol asemănător cu **ICMP** (*Internet Control Message Protocol*) care are acelaşi rol de verificare a conexiunilor pe baza unui set de mesaje de eroare.

IPX şi UDP.

Sistemele de operare de rețea **NetWare**, produse de firma Novell, utilizează un protocol de rețea (de nivel **OSI 3**, rutabil) asemănător cu **IP** numit **IPX** (*Internetworking Packet Exchange*), bazat pe principiile dezvoltate de Xerox la **XNS**.

Arhitectura **IPX** utilizează frecvent **UDP**, ca protocol de transport fără controlul transmisiei, dar se poate utiliza şi **TCP** în combinație cu **LLC** de **tipul 1**.

Sistemele de operare **NetWare** folosesc ca protocol de transport, cu controlul transmisiei, **SPX** *(Sequenced Packet Exchange),* ceea ce permite utilizarea **UDP**, protocol fără control, pentru încapsularea **IPX**. Eventualele pierderi, sau degradări ale datelor, vor fi corectate de **SPX**. Acest tip de arhitectură se poate vedea în **figura 12.7**.

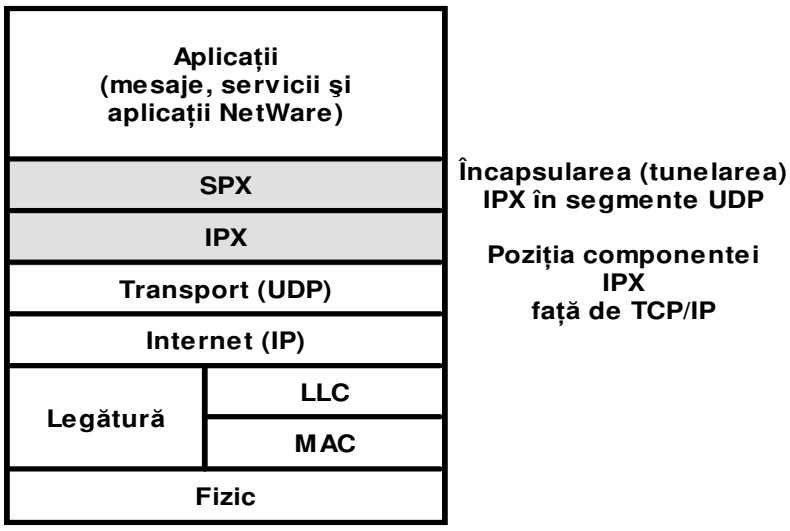

Fig. 12.7. Încapsularea IPX în segmente UDP.

Aşezarea nivelului **IPX** deasupra celui **UDP** asigură integritatea antetului **UDP** şi **IP**, în timpul transferului prin reţea, dar cu informaţiile necesare pentru **IPX**, încapsulate ca parte a mesajului util. Deoarece ambele protocoale operează cu adrese ale staţiilor din reţea, acestea trebuie bine corelate (tabele de echivalare a adreselor).

Spre deosebire de **IP** care foloseşte adresarea logică atât pentru staţie cât şi pentru reţea, **IPX** foloseşte o combinaţie a adresei logice (de reţea) cu cea hardware (adresa **MAC**).

Adresa unei staţii dintr-o reţea **IPX** se compune din 4 octeţi în câmpul adresei de reţea plus 6, corespunzători adresei **MAC** a interfeţei de reţea. Acest mod asigură unicitatea adresării **IPX**, fără să existe riscul alocării acesteia la mai multe dispozitive în aceeaşi reţea. Adresa este convertită în adresă **IP** atunci când datagrama este trimisă nivelului **UDP**.

Se poate configura reţeaua să se folosească **TCP** şi **IP** încapsulate în **IPX** şi **LLC** de tipul **1**.

Această soluţie este folosită în cazul transferării (tunelării) unor servicii **TCP/IP** în reţele bazate pe **IPX**. Arhitectura unei astfel de reţele se poate vedea în **figura 12.8**. Într-o astfel de reţea, asocierea adreselor **IP** se poate face utilizând **ARP**.

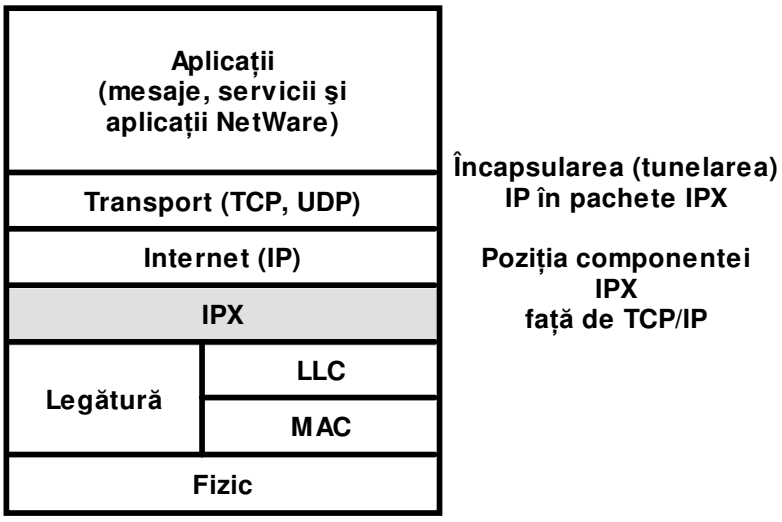

Fig. 12.8. Încapsularea **TCP/IP** în **IPX** (tunelarea **TCP/IP** în **IPX**).

ARCnet şi TCP/IP.

ARCnet este o arhitectură des utilizată la construirea reţelelor locale şi are variante care utilizează **IP**, fiind similară cu cea care utilizează **IPX**. **ARCnet** înlocuieşte **IPX** cu **IP**, aşa cum se

poate vedea în **figura 12.9**. Datagramele (pachetele) **IP** sunt încapsulate într-o datagramă **ARCnet**, care este transmisă, la rândul ei, nivelelor inferioare.

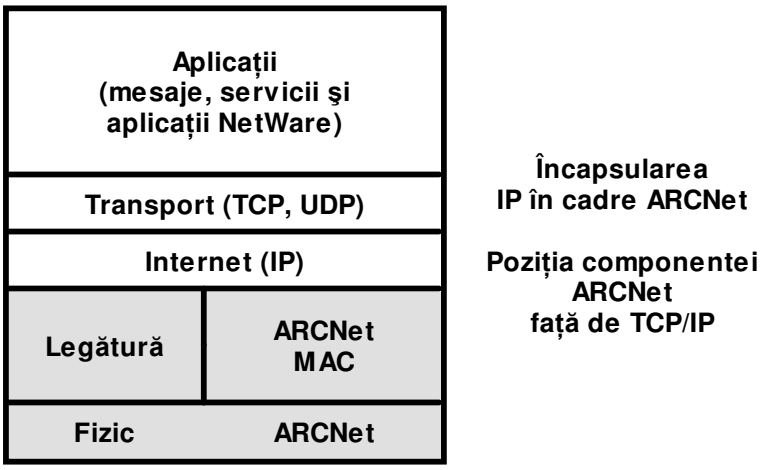

Fig. 12.9. Utilizarea **TCP/IP** în rețelele **ARCNet**.

Aşezarea datagramelor **IP** în spatele antetului **ARCnet**, asigură menținerea compatibilității pachetelor **IP** chiar şi în cazul în care acestea părăsesc rețeaua **ARCnet**. Asocierea adreselor **IP** şi **ARCnet** se face cu ajutorul componentei **ARP**, care permite şi funcția inversă **RARP**.

Rețele FDDI.

FDDI (*Fiber Distributed Data Interface*) este o tehnologie utilizată din ce în ce mai mult în ultimul timp care utilizează fibră optică ca mediu de propagare. Popularitatea în continuă creştere se datorează ratei mari de transfer ce o caracterizează. Utilizarea **TCP/IP** într-o astfel de rețea este asemănătoare cu cele prezentate la alte tipuri de rețele (arhitectură organizată pe nivele), diferența față de celelalte fiind legată de faptul că utilizează două subnivele pentru nivelul fizic.

Schema de adresare **FDDI** este asemănătoare cu tehnologiile Ethernet, necesitând asocierea adresei de la nivelul legăturii de date cu cea de la nivelul **IP** făcându-se cu ajutorul componentei **ARP**. **IP** se foloseşte alături de un serviciu fără conexiune, bazat pe **LLC** de **tipul 1**.

Dimensiunea cadrului **FDDI** este fixată la 4.500 octeți, incluzând aici antetul şi alte informații necesare operării acestuia. Scăzând pe acestea din urmă, mai rămân disponibili, pentru datele utile, 4.470 octeți. Documentele **RFC** corespunzătoare definesc 4.096 octeți de date şi 256 pentru antetul care defineşte nivelele superioare celui corespunzător la **MAC**.

Dimensiunea mare a datagramei poate genera probleme la nivelul unor porți de acces, de acea rutarea acestor datagrame trebuie făcută cu multă atenție, pentru a preveni trunchierea sau degradarea. Dacă rutarea ridică probleme se recomandă diminuarea dimensiunii datagramelor **FDDI** (se recomandă o valoare de 576 octeți de date de la care se poate apoi creşte până la valori care nu ridică probleme).

X.25 şi IP.

Rețelele **X.25** sunt caracterizate de o arhitectură care utilizează un nivel propriu de transport (**TP4**) deasupra **IP** şi un nivel de încapsulare **PLP** (*Packet Layer Procedures*) sub acesta, aşa cum se poate vedea în **figura 12.10**.

TP4 este asemănător cu **TCP**, dar nu utilizează porturi pentru identificarea serviciilor.

Câmpul de identificare a sursei şi a destinației sunt puncte de acces la serviciile de transport (**TSAP** - *Transport Service Access Points*). **TP4** este mai complex decât **TCP**, dar acest lucru nu este întotdeauna un avantaj, datorită faptului că terminalele au nevoie de o componentă suplimentară pentru încapsulare / decapsulare.

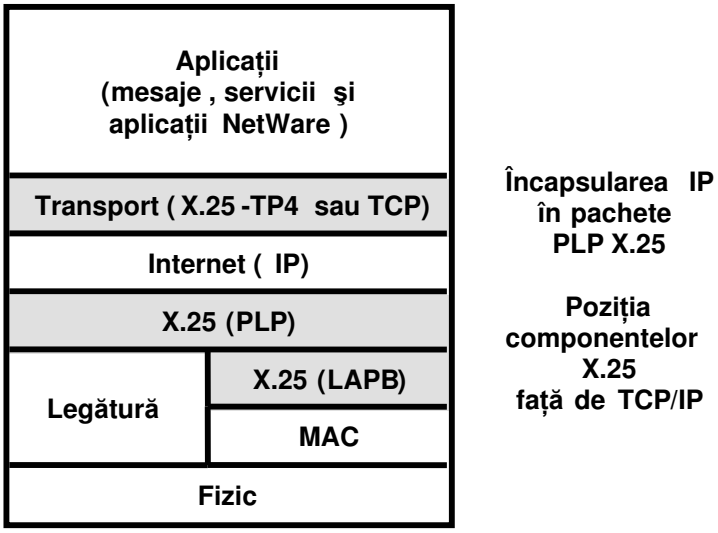

Fig. 12.10. Utilizarea IP în rețelele X.25.

Protocolul **X.25** nu se foloseşte pentru rețele locale, dar este des întâlnită în rețelele cu schimb de pachete (circuite virtuale). Documentele RFC 1356 şi RFC 1613 stabilesc regulile de utilizare ale protocoalelor **X.25** alături de **TCP/IP** şi definesc parametrii de interfațare ale acestora.

ISDN şi TCP/IP.

ISDN (*Integrated Services Digital Network*) este o tehnologie care foloseşte circuite comutate, asemănătoare celor utilizate în telefonia fixă, permițând construirea de rețele cu schimb de pachete. Poate încapsula diferite protocoale de nivel superior (**Rețea** şi **Transport OSI 3,4**), inclusiv **TCP/IP**. **IP** nu apare în mod explicit în modelul de reprezentare pe nivele deoarece este inclus în **CLNP**. **TCP** şi **IP** pot fi utilizate într-o rețea **ISDN**, în locul protocoalelor **TP4** şi **CLNP**, dar versiunile de sisteme **ISDN** au fost optimizate să le utilizeze pe acestea din urmă.

ISDN utilizează o arhitectură mai complexă decât cele mai multe dintre rețelele actuale, înlocuind porțile de acces şi ruterele cu adaptoare de terminal (**TA** - *Terminal Adapter*) şi noduri **ISDN**. Acestea realizează aceleaşi funcții, dar au o arhitectură internă mai complexă. Pentru detalii suplimentare se poate consulta capitolul dedicat acestei tehnologii.

SMDS (*Switched Multi-Megabit Data Services*) şi IP.

SMDS (*Switched Multi-Megabit Data Services*) este un sistem care asigură un serviciu de rețea cu schimb de pachete, fără conexiune, dar cu rată mare de transfer şi o dimensiune a pachetelor de până la 9188 octeți de date. Acest sistem utilizează un mecanism propriu de control al fluxului dintre abonat şi rețea, operând cu **IP**, prin intermediul unui subnivel controlat de **LLC**.

SMDS care utilizează **IP** permite definirea mai multor subrețele logice **IP**, care pot fi gestionate separat, dar care sunt tratate ca o singură unitate. Arhitectura unei rețele **SMDS** este destul de complexă şi utilizează protocolul **LLC** de tipul **1**.

ATM (*Asynchronous Transfer Mode*) şi BISDN.

ATM este un protocol conceput pentru legături de mare viteză, folosit alături de **BISDN** (*Broadband ISDN* - **ISDN** de bandă largă). Arhitectura sa este asemănătoare cu cea **TCP/IP**, dar la care s-au adăugat nivele suplimentare pentru a înlesni transferul unor servicii speciale, cum ar fi transmisia de imagine şi sunet.

Aceste performanțe au impus utilizarea de dispozitive speciale (**TA** - *Terminal Adapter*, asemănător cu cel folosit la **ISDN**) pentru accesare şi rutare, care de multe ori sunt diferite în funcție de serviciile furnizate. De la adaptorul de terminal **TA**, traficul este transferat serviciului **ATM** care asigură comutarea şi multiplexarea serviciilor [1].

TESTE DE AUTOEVALUARE

I. Alegeți varianta de răspuns corectă:

1. Într-o rețea bazată pe TCP/IP, componenta care asigură comunicația între aplicațiile NetBIOS, se află:

   a) Între nivelul IP şi cel TCP, sau UDP;
   b) Între nivelul legătură şi rețea;
   c) Deasupra nivelului transport;
   d) Deasupra nivelului TCP, sau UDP;
   e) Nu se utilizează.

2. Tunelarea protocolului IPX, în rețele bazate pe TCP/IP, necesită:
   a) încapsularea pachetelor IPX în datagrame UDP;
   b) încapsularea pachetelor IPX în datagrame TCP;
   c) încapsularea pachetelor IPX în pachete IP;
   d) încapsularea pachetelor IP în datagrame SPX;
   e) IPX nu se foloseşte simultan cu TCP/IP.

3. Într-o rețea X.25, pachetele IP se pot transfera prin:
   a) încapsulare în X.25 TCP (Transmission Control Protocol);
   b) încapsulare în X.25 TP4 (Transport Protocol Layer 4);
   c) încapsulare în X.25 LAPB (Lynk Access Procedure Balanced);
   d) încapsulare în X.25 PLP (Packet Layer Protocol);
   e) Protocolul IP nu poate fi transferat prin tehnologii care utilizează X.25

II. Alegeți răspunsul corect:

1. Protocolul IPX poate fi transferat prin tunelare în UDP/IP şi protocolul IP poate fi transferat prin încapsulat în IPX.

   □ adevărat □ fals

2. Puntru a asigura comunicația dintre aplicațiile bazate pe NetBIOS, această componentă poate fi încapsulată atât deasupra nivelului IP cât şi sub acesta.

   □ adevărat □ fals

3. Deoarece SPX este un protocol bazat pe conexiune, suita IPX/SPX se transferă prin tunelare prin UDP/IP.

   □ adevărat □ fals

RĂSPUNSURI

I. Varianta de răspuns corectă:

1. c, d
2. a
3. d

II. Alege□i răspunsul corect:
1. adevărat
2. fals
3. adevărat

Bibliografie

1. **Parker, T**., *Teach Yourself TCP/IP in 14 Days - Second Edition*, Sams Publishing, 1996.
2. **RFC 1356**, *Multiprotocol Interconnect on X.25 and ISDN in the Packet Mode*