IV.4 COMUTATOARE DE REȚEA (SWITCH)

Dezavantajul hub-urilor de partajare este acela că nu elimină restricția ca numai un singur nod al rețelei să transmită la un moment dat, aplicând o anumită metodă de acces la mediul fizic. De aceea, producătorii de echipamente pentru rețelele de calculatoare au introdus matricile de comutație specifice centralelor telefonice (PBX - *Public Branch eXchange*) în comunicațiile de date, pentru realizarea în paralel a mai multor legături punct-la-punct simultane și evitarea

congestiilor. Astfel s-au obținut hub-urile cu matrice de comutare (*Switched Hubs*) sau **comutatoarele pentru LAN** (*LAN Switch*).

Conexiunile paralele, simultane dintre mai mulți utilizatori ai rețelei de calculatoare sunt create asemenea legăturilor virtuale telefonice folosind matrici de comutare.

Echipamentele care realizează comutarea cadrelor sunt denumite simplu **comutatoare de rețea** (*switch*) și sunt utilizate în rețele LAN cu diverse arhitecturi (Ethernet, Token-Ring, FDDI, Fast Ethernet), dar și pentru transmisiile în sisteme ATM (*Asynchronous Transfer Mode*) pentru comutarea semnalelor digitale de tip voce, audio sau video, la viteze foarte mari (de ordinul Gbps). În WAN, se utilizează comutatoare de mare viteză, cu capacități superioare celor pentru LAN.

Avantajele utilizării unui switch sunt evidente:

1. Prin intermediul switch-ului, se poate extinde rețeaua, structurată relativ simplu, fizic sau logic (rețele locale virtuale VLAN - *Virtual LAN*).

2. Reduce încărcarea rețelei prin filtrarea traficului.

3. Poate interconecta segmente de LAN cu medii fizice și viteze de transmisie diferite (10BaseT, 10BaseF, 100BaseT).

4. Permite utilizarea sistemelor de priorități pentru transmisie, prin introducerea în cadru a unui factor de calitate (QoS - *Quality of Service*).

În funcție de complexitatea operațiilor efectuate de switch, acesta poate lucra:

- pe nivelul OSI 2 al legăturii de date, mai precis pe subnivelul MAC sau pe LLC;
- pe nivelul 3 de rețea;
- pe nivelul 4 de transport.

Un **switch de subnivel MAC** (*Cut-through switch*) citește adresa MAC a destinației unui cadru și pe baza unui tabel de adrese (memorat pe durata procesului de "învățare" - *learning*), realizează legătura punct-la-punct dintre portul de intrare și cel de ieșire și expediază pachetul (*forwarding*). Decizia de comutare se poate lua și pentru fragmente foarte mici de pachete (sub 64B). Evident transferul este foarte rapid, dar este posibil ca acel cadru să fie afectat de erori și nodul-destinație să solicite retransmisia lui. Astfel rețeaua este folosită ineficient prin transmisia unui cadru eronat precum și a cererii de retransmisie.

Acest tip de switch este indicat în transmisiile în care se impun întârzieri mici de transmisie, fără un control strict al erorilor.

Un **switch de subnivel LLC** (*Store-and-forward switch*) citește cadrul primit, îl memorează și testează secvența FCS pentru detecția eventualelor erori. Dacă nu au apărut erori, cadrul este transferat către portul corespunzător destinației (Fig. IV.8) Acest switch realizează mai lent transferul decât unul de subnivel MAC, dar nu încarcă inutil rețeaua. Acest switch lucrează pe

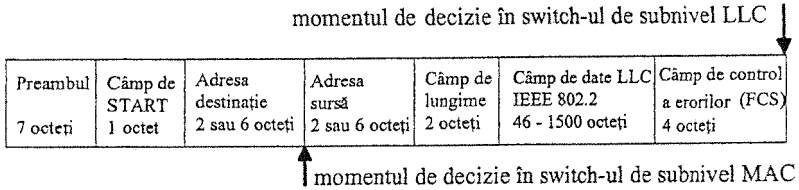


Fig. IV.8 Momentele la care se ia decizia de comutare

același principiu cu 'punțile' de rețea (*bridge*), folosite pentru interconectarea mai multor rețele locale.

Pentru creșterea vitezei de funcționare a **switch**-ului **de nivel 2**, s-a propus o soluție de compromis (*Error-free cut-through switch*), un switch care în mod normal lucrează rapid, pe subnivelul MAC și numai dacă pe o anumită cale se sesizează apariția unor erori, atunci portul de ieșire respectiv este reconfigurat să funcționeze pe subnivelul LLC pe un interval limitat de timp. Acest switch nu ia decizii de comutare înainte de a recepționa primii 64 de octeți.

Switch-ul de nivel 2 asigură conexiuni **transparente** față de nivelele OSI superioare, întrucât lucrează numai pe baza adreselor MAC și nu depinde de protocolul de rețea folosit. Viteza de comutare a pachetelor în switch-ul de nivel 2 este mare.

Interconectarea unor segmente de rețea cu viteze diferite (de exemplu, 10 Mbps și 100 Mbps), poate crea la nivelul switch-ului **erori de depășire** a capacității de memorie (*buffer overflow*), urmate de pierderea unor cadre de date.

Producătorii de echipamente au propus diferite soluții pentru această problemă.

Prima constă în utilizarea unor memorii suplimentare dar determină creșterea costului echipamentului.

A doua soluție aplică procedeul de 'alarmă falsă', ca o reacție negativă, și nodul-sursă primește mesajul fals de apariție a unei coliziuni fiind forțat (*backpressure*) să oprească transmisia pe o durată aleatoare. Astfel se permite descărcarea memoriei până la transmisia de noi date dinspre nodul de mare viteză.

Un switch de nivel 2 poate fi utilizat în diferite rețele (Ethernet, Token Ring, FDDI, Fast Ethernet, ATM), cu diverse medii fizice de transmisie. Numărul porturilor din switch și cel al adreselor MAC admise pe fiecare port pot varia de la un echipament la altul. Unele porturi pot lucra în regim duplex cu condiția ca și placa de rețea (NIC) a echipamentului conectat la acel port să admită transmisia duplex a datelor.

Supravegherea funcționării unui switch este mai complicată decât a unui hub, întrucât trebuie urmărite mai multe legături punct-la-punct.

Există trei variante pentru realizarea managementului unui switch:

1. pe **principiul simplu al "oglinzii"** (*port mirroring*), se copie informația dintr-un port al switch-ului într-un analizor de LAN; numai un singur port poate fi monitorizat la un anumit moment;

2. pe **principiul "oglinzilor multiple"** (*multiple port mirroring*) se creează un sistem de monitorizare la distanță (RMON - *Remote Monitoring*), în mod aleator, la intervale regulate de timp, a unor grupuri de porturi din switch, dar tot numai câte unul la un anumit moment;

3. prin **sistemul RMON simultan** (*Simultaneous RMON View*) permite supravegherea simultană a traficului din mai multe porturi folosind un procesor (CPU - *Central Processing Unit*) separat doar pentru management și memorii suplimentare pentru a nu reduce performanțele switch-ului. RMON MIB este cea mai utilizată metodă pentru managementul switch-ului. Apar probleme în ce privește utilizarea simultană a RMON MIB și SNMP.

Există switch-uri de nivel 2 care admit utilizarea algoritmului de deducere a 'drumului minim' într-un graf (*Spanning Tree Algorithm*), în baza standardului IEEE 802.1d, asemenea routerelor.

Switch-urile **de nivel 3** (*L3 Switch*) combină avantajul vitezei mari de comutație a switch-ului de nivel 2 cu cele ale ruterelor (controlul traficului, deducerea rutei optime etc). Un switch de nivel 3 depinde de protocoalele de rețea utilizate.

Un astfel de switch realizează automat procesul de "învățare" a adreselor (*learning*) și construcție a tabelelor de comutare și rutare. Legăturile între diferite subrețele se realizează direct la nivelul de rețea. Nu se mai folosesc procesoarele RISC (*Reduced Instruction Set Computing*), ci cele ASIC. Funcțiile de rutare se realizează în baza anumitor protocoale de rețea, de exemplu, RIP (*Routing Information Protocol*); RIP II; OSPF (*Open Shortest Path First*); DVMRP (*Distance Vector Multicast Routing Protocol*). Aceste switch-uri lucrează ca routere rapide realizând rutarea la nivelul porturilor.

Switch-urile **de nivel 4** (*L4 Switch*) iau decizii de rutare evaluând informațiile de pe nivelul OSI 4 de transport, cum ar fi numerele porturilor logice (23 - port Telnet; 80 - port WWW etc), specificate de protocoalele de transport (de exemplu, TCP, UDP, SPX).

Observații:

1. Lățimea benzii oferite de un switch pe porturile active în paralel, devine suficient de mare prin folosirea standardelor de transmisie duplex și GbE (*Gigabit Ethernet*).
2. Întârzierile determinate de switch în procesul de transmisie a datelor devin importante în transmisiile de date în timp real (voce, audio, video).

VI

INTERCONECTAREA REȚELELOR LOCALE

Creșterea volumului de date vehiculate în rețelele de arie largă, în particular în Internet și WWW, impune utilizarea unei lățimi de bandă tot mai mari și a unor sisteme de operare mai rapide (Windows, Unix, Mac), care admit efectuarea simultană a mai multor sarcini (*multitasking*), deci și a tranzacțiilor multiple, simultane cu rețeaua.

Creșterea lățimii de bandă disponibile pentru utilizatorii unei rețele locale, este posibilă prin **segmentarea LAN** în mai multe domenii de coliziune, folosind echipamente de tip switch, bridge și/sau ruter, interconectate prin intermediul unei magistrale de date (*backbone*) la nivelul căreia se definește un alt domeniu de coliziune, distinct de cele asociate segmentelor de rețea formate.

VI.1 PUNȚI DE REȚEA (BRIDGE)

BRIDGE-ul sau **puntea** dintr-o rețea de calculatoare este un dispozitiv care lucrează pe subnivelul MAC al modelului OSI fiind denumit și **releu de nivel 2** (*Layer 2 Relay*). Acesta interconectează mai multe segmente de LAN pentru a realiza o rețea locală extinsă (*Extended LAN*), cu mai multe noduri decât numărul maxim prevăzut de standardele de rețea, respectiv la distanțe mai mari decât cele impuse prin limitările cauzate de caracteristicile fiecărui mediu fizic de transmisie (lungime maximă a segmentului de cablu; număr maxim de segmente interconectate prin repetoare sau hub-uri conform regulii Ethernet 5-4-3 etc).

Bridge-ul lucrează pe nivelul legăturii de date cu cadre de date (*data frame*), deci în mod transparent față de protocoalele definite pe nivelele OSI superioare și independent de protocoalele de rețea aplicate.

Accesul la mediul fizic de transmisie se realizează în baza standardului de rețea utilizat deci este posibil să apară întârzieri în transferul cadrelor prin punte fiind necesară stocarea lor. Puntea citește câmpurile de adresă MAC ale sursei și destinației și retransmite fiecare cadru către rețeaua în care se găsește destinația (*store-and-forward*). Este posibilă filtrarea inteligentă a cadrelor pe baza adreselor MAC ceea ce permite reducerea încărcării rețelelor, creșterea lățimii de bandă disponibile, controlul accesului și securizarea transmisiei la nivelul punții.

O punte poate interconecta segmente de LAN având medii fizice de transmisie diferite (UTP, cablu coaxial, fibră optică) dar lucrând pe baza aceluiași protocol de nivel 2 (de exemplu Ethernet: 10 BASE T; 10 BASE 2; 10 BASE 5 etc).

O punte este prevăzută cu diferite porturi fizice care pot asigura fiecare accesul multiplu la nivelul lor, dacă se configurează în mod adecvat cu mai multe interfețe logice (*ppp; fr*).

Dacă puntea dispune de un port pentru legătură în WAN, atunci ea poate fi utilizată pentru realizarea unui LAN extins din mai multe rețele locale din WAN, separate geografic, și configurată 'de la distanță' (*remote bridge*).

În figura VI.1 este reprezentată o rețea locală extinsă cu punți. Fiecare punte permite intrarea sau transferul cadrelor din rețeaua centrală în cea locală numai dacă destinația aparține acesteia. În caz contrar cadrul nu este trecut prin bridge. De asemenea, un cadru trimis din LAN-ul propriu este transferat de punte în rețeaua de legătură, pe magistrala de date de mare viteză (*backbone*), numai dacă destinația nu se găsește în același LAN cu sursa.

De exemplu, un mesaj transmis de stația A1 pentru stația C2 va fi transferat prin puntea B1 în rețeaua de legătură, preluat de puntea B2 și retransmis stației C2.

Mesajul nu trece prin puntea B3. Dacă se face o transmisie între două terminale din interiorul aceluiași LAN, atunci cadrul nu este transferat de puntea proprie în rețeaua centrală.

Puntea memorează adresele nodurilor din rețeaua locală proprie într-un tabel de adrese.

Tabelul punții conține numele interfețelor și adresele fizice ale echipamentelor direct conectate la fiecare dintre acestea.

Dacă adresa destinației nu este cunoscută, atunci mesajul respectiv este transmis prin broadcast către toate stațiile.

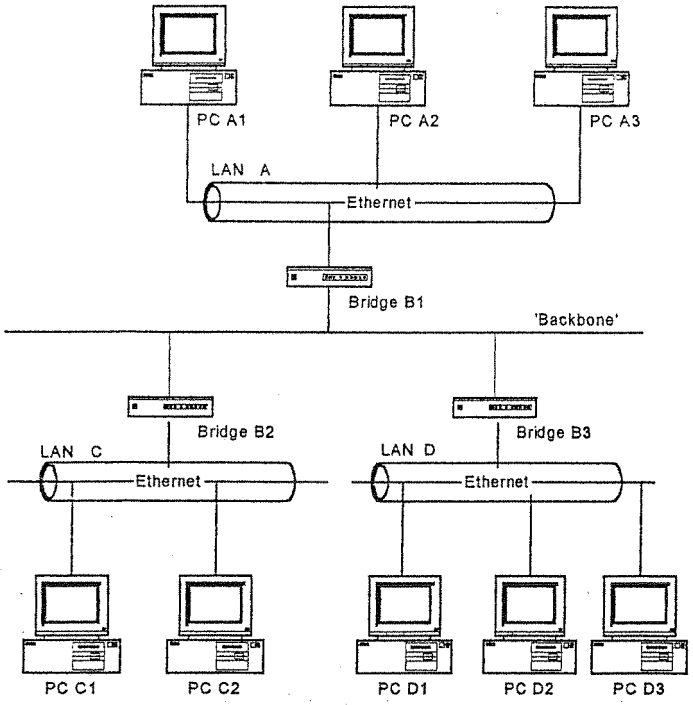


Fig. VI.1 Exemplu de LAN extins cu punți

În situația în care adresa destinației este inexistentă și există bucle în topologia rețelei, mesajul se poate propaga la infinit, producând așa-numitul fenomen de 'furtună de difuzare' (*broadcast storm*). Acest fenomen este mai puternic dacă un mesaj este destinat unui nod care nu aparține rețelei proprii și este trecut prin mai multe punți către așa-zisa destinație. Broadcast-ul se realizează atunci la nivelul fiecărei punți și fenomenul ia amploare. Deducem că punțile sunt ineficiente și chiar neindicate în rețelele cu topologie redundantă.

În rețelele de arie largă cu topologie fizică de tip 'plasă' (*mesh*), unele punți permit utilizarea căilor multiple (redundante) de transmisie și alegerea căii optime dintre sursă și destinație aplicând algoritmul de deducere a drumului minim dintr-un graf (*STA Spanning-Tree Algorithm*). De asemenea, pentru WAN, se pot defini la nivelul punții ierarhii de priorități pentru reducerea întârzierilor de transmisie a anumitor cadre.

Comutarea de pachete prin intermediul punților de transmisie se realizează prin algoritmi software, ceea ce determină apariția unor întârzieri de transmisie cauzate de procesele logice de decizie. Segmentarea rețelelor locale cu punți determină o creștere a timpului de transmisie de până la 30 %. Avantajoasă este posibilitatea definirii filtrelor de trafic la nivelul punții.

Spre deosebire de punțile de rețea, comutarea de pachete prin switch este un proces relativ rapid care se realizează prin intermediul unei structuri hardware (matricea de comutație) la care calculatoarele sunt direct conectate. Ca dezavantaje ale utilizării switch-urilor se observă formarea mai multor domenii de coliziune dar menținerea unui singur domeniu de braodcast și imposibilitatea limitării vitezei de trafic prin switch. Ca avantaje trebuie remarcate viteza mare de comutare și posibilitatea definirii rețelelor locale virtuale (VLAN - *Virtual LAN*).

Procesul de comunicație prin punte (*bridging process*) este complex și se realizează în două etape:

1. **procesul de învățare** (*learning process*) se realizează în mod adaptiv și constă în 'învățarea' adreselor MAC ale tuturor stațiilor dintr-un LAN extins. La primirea unui cadru, puntea caută adresa MAC a sursei în harta stațiilor (*station map*) și dacă nu o găsește, atunci o include în aceasta. Se inițializează contorul pentru măsurarea duratei intervalului de timp în care puntea cunoaște această adresă (*aging timer*). Contorul este reinițializat de fiecare dată când se recepționează o adresă cunoscută. La expirarea acestui timp, adresa stației respective este ștearsă din harta stațiilor. Orice cadru recepționat care are adresa de destinație cunoscută (inclusă în harta stațiilor) este transmis pe portul corespunzător stației respective.

2. **procesul de transferare** (*forwarding process*). Orice cadru recepționat este preluat de punte cu condiția ca adresa destinației să aparțină LAN-ului respectiv și numai dacă portul pe care a fost primit este în starea activă (*forwarding state*). Dacă adresa destinației apare în harta stațiilor atunci cadrul este transferat pe portul respectiv. În cazul în care adresa destinației nu este inclusă în harta stațiilor, cadrul este retransmis pe toate porturile punții (*flooding*) cu excepția celui de pe care a fost recepționat. Cadrul este transferat de un port numai dacă acesta este activ. În caz contrar, cadrul este descărcat din memoria punții și datele se pierd. Procesul de transfer a cadrelor prin punte poate fi controlat prin filtrare. Rata de transfer a cadrelor la nivelul punții poate avea valori cuprinse între 700 și 30.000 pachete pe secundă.

Porturile unei punți, definite ca tip și număr, pot să se găsească în una din următoarele cinci stări:

1. **starea inactivă** (*disabled*) - nu se face nici o operație la nivelul portului;
2. **starea de 'ascultare'** (*listening*) - se pot recepționa cadre;
3. **starea de 'învățare'** (*learning*) - se recepționează cadrele și se realizează harta stațiilor;
4. **starea activă** (*forwarding*) - se recepționează și se transferă cadre prin portul respectiv iar algoritmul *'spanning tree'* este activat;

5. **starea de blocare** (*blocking*) - transferul de cadre prin port este inactiv dar algoritmul '*spanning tree*' este activ pentru operare la nivelul portului.

Există punți care permit 'la cerere' (*on-demand bridge*) realizarea transmisiilor de tip '*broadcast*' sau '*multicast*'. Acest fapt poate conduce la încărcarea excesivă a rețelelor ceea ce impune configurarea adecvată a echipamentelor pentru filtrarea severă a traficului. În acest caz nu se aplică algoritmul '*spanning tree*'.

Urmărirea funcționării unei punți se face cu protocoale de management de rețea (SNMP) folosind baze de date separate (MIB).

Clasificarea punților se poate face pe mai multe criterii.

În funcție de arhitectura LAN utilizată, punțile se împart în:

1. **punți transparente** (*transparent bridges*) care interconectează segmente de LAN cu același protocol la nivelul legăturii de date;

2. **punți de translare** (*translating bridge* sau *multiprotocol bridge*) care realizează conversia formatului cadrului de date dintr-un standard în altul (de exemplu, Ethernet și Token-Ring) și sunt prevăzute cu mai multe plăci de rețea.

3. **punți de încapsulare** (*encapsulating bridge*) pentru interconectarea unui LAN Ethernet cu unul FDDI.

În funcție de localizarea lor, punțile pot fi:

1. **punți locale** (*local bridge*) care interconectează două LAN-uri direct printr-un anumit mediu de transmisie. Acestea conțin mai multe plăci de rețea și pot face conversia de la un mediu la altul.

2. **punți 'la distanță'** (*remote bridge*) conțin plăci de rețea pentru conectarea la diverse LAN-uri precum și porturi de acces 'la distanță' în WAN prin modemuri și un port serial (RS-232). Ele realizează compresia datelor pentru reducerea lățimii de bandă ocupate, sunt monitorizate prin SNMP și suportă Telnet pentru configurarea lor 'de la distanță'.

În rețelele WAN 'fără fir' (*wireless*) se utilizează perechi de **punți de transmisie 'fără fir'** (*wireless bridge*) pentru legături la distanțe mari (de peste 5 km), care suportă STA, filtrare bazată pe adrese MAC, SNMP, criptare de date și protecție contra fenomenului '*broadcast storm*' .

Performanțele unei punți se apreciază prin următorii parametri:

1. **rata de transfer fără erori;**

2. **rata de pierdere a pachetelor;**

3. **întârzierea de transmisie** (se minimizează prin folosirea unui procesor rapid de comunicație în punte).

Configurarea prin soft a unei punți include:

1. definirea porturilor, fizice, respectiv logice (de exemplu: *eth0; eth1; ppp0; ppp1; ppp2*) ;

2. definirea protocoalelor pentru care se aplică procesul de '*bridging*' (*ARP; Novell; AppleTalk* ș.a.), eventual activarea algoritmului '*spanning tree*';

3. definirea grupurilor de utilizatori;

4. definirea filtrelor de includere a utilizatorilor autorizați sau de excludere a anumitor cadre (de exemplu, încapsulate conform anumitor standarde sau de dimensiuni prea mari). Rata de filtrare a unei punți variază de la 7000 la 60.000 de cadre pe secundă.

Se utilizează diverse comenzi de configurare a punților, cu sintaxa definită de firma producătoare a echipamentelor:

- de activare a punții (enable bridge);
- de activare a algoritmului de deducere a drumului minim prin graf (enable bridge spanning);
- de definire a interfețelor logice și fizice (create; add);
- de definire a protocoalelor recunoscute de punte (add bridge protocol), tipul protocolului fiind specificat printr-un număr de patru cifre din sistemul hexazecimal.
- de introducere a unot filtre de transmisie (add bridge filter);
- de vizualizare a modului de configurare (show).

Observație

Fișierele de configurare pot fi încărcate în memoria echipamentelor folosind TFTP ca protocol de transfer.

VI.2 ECHIPAMENTE DE DIRIJARE (ROUTER)

Echipamentul de dirijare (*router*) este un echipament de comunicație de nivel rețea (*layer 3 device*) care utilizează algoritmi specifici de deducere a căii optime de transfer a datelor într-o rețea de arie largă având căi redundante, pe baza informațiilor pe care le deține referitor la topologia rețelei.

Rutarea este operația de dirijare a datelor între două noduri prin stabilirea 'drumului minim' din graful asociat topologiei fizice sau celei logice a unei rețele. Astfel routerul maximizează ratele de transfer și de filtrare a pachetelor.

Orice LAN poate comunica într-un WAN dacă este conectat la aceasta printr-un router.

Baza de date în care sunt incluse informațiile despre topologia rețelei poate fi configurată **static**, de către administratorul de rețea, sau **dinamic**, prin intermediul protocoalelor de rutare.

Rutarea statică nu permite reactualizarea la timp a tabelelor de rutare și este practic ineficientă în cazul utilizării protocoalelor de adresare dinamică.

Un router poate transfera date între LAN-uri diferite ca standard de transmisie (Ethernet, FDDI, ATM) fiind prevăzut cu diverse interfețe având adrese individuale. Routerele pot face conversiile necesare ale formatului pachetelor în cazul interconectării unor segmente de rețea cu standarde și protocoale diferite.

Observație

Routerele sunt prevăzute atât cu interfețe fizice, cât și cu interfețe logice, de exemplu, interfețe *ppp* definite prin protocolul PPP *(Point-to-Point Protocol)* în cazul transmisiilor TDM, având alocate adrese de nivel rețea proprii (de exemplu, adrese IP) pe baza cărora se realizează rutarea pachetelor. PPP, ca protocol de nivel OSI 2, încapsulează în mod transparent datagramele transmise pe legături seriale lucrând ca multiplexor/demultiplexor pe aceste linii. PPP (RFC 1717) este responsabil de aplicarea protocoalelor de autentificare PAP (*Password Authentication Protocol*) și CHAP (*Challenge Handshake Authentication Protocol*). PPP negociază cu utilizatorii numele și parolele dar există riscul interceptării lor întrucât nu sunt transmise criptat. Între routerele aflate la 'distanță' se pot aplica procedee de criptografiere a acestor informații. Este indicată schimbarea periodică a parolelor.

Rutarea pachetelor, mai precis transferul pachetelor în interiorul ruterului către un anumit port de ieșire din router se face pe baza **tabelului de rutare,** care asociază adresele de rețea ale rețelelor de destinație posibile cu interfețele de ieșire din router. Routerul realizează deci operația de comutare a pachetelor (*switching*) pe interfața corespunzătoare. Pentru adrese de destinație neincluse explicit în tabelul de rutare, se definește o rută implicită (*default route*).

Exemplu:

În figura VI.2, LAN A transmite date către LAN B.

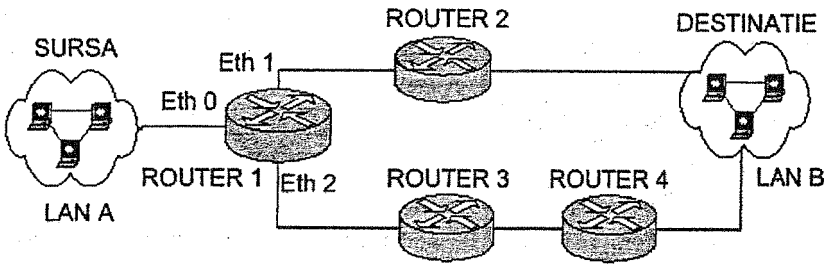


Fig.VI.2 Exemplu de LAN-uri interconectate cu routere în WAN

LAN A este conectat la interfața *Eth 0* a ruterului 1.

Pentru LAN B ca destinație, în tabelul de rutare al ruterului 1, se includ două căi, prin interfața *Eth1*, respectiv prin *Eth2*, cu precizarea căii optime (Tabel VI.1).

Tabel VI.1

Intrări în tabelul de rutare definit pentru routerul 1

LAN destinație	Interfață de ieșire	Optim
LAN B	*Eth1*	+
LAN B	*Eth2*	-

Se observă că în graful rețelei de comunicații (cu routere) nu apar bucle. Routerul transmite pachetul pe ruta optimă, cea de rezervă urmând a fi utilizată în cazul întreruperii traficului pe prima rută.

Din cadrul recepționat se extrage pachetul și se citește adresa de nivel OSI 3 a stației de destinație. Aplicându-se acesteia masca de rețea se deduce adresa rețelei de destinație, urmând să se ia decizia de comutare pe o anumită interfață a ruterului prin deducerea rutei optime.

Se folosește o anumită metrică pentru stabilirea 'drumului minim' dintre două noduri din graful rețelei (număr de routere sau 'hopuri' prin care se face transferul, întârziere de transmisie, risc minim de coliziune etc). La nivelul interfeței de ieșire, pachetul este reîncapsulat într-un cadru, conform standardului de nivel OSI 2 aplicat pe acea interfață. În rețelele WAN mixte (de exemplu, Ethernet și Token-Ring) se poate folosi același protocol de nivel-rețea (de exemplu, IP) și același mod de adresare de nivel OSI 3, dar formate diferite pentru cadrele definite pe nivelul OSI 2.

De fiecare dată când topologia rețelei se modifică (prin dezvoltarea sau reconfigurarea rețelei ori cauzat de coliziunile din trafic), este necesară reactualizarea tabelelor de rutare (*reconvergence*). Timpul de reconversie a tabelelor depinde de protocolul de rutare aplicat. Dacă routerele din WAN nu dispun toate de aceleași informații topologice, atunci este posibil să se ia decizii de rutare incorecte sau inaplicabile. Dacă un router nu poate expedia un pachet (*destination unreachable*), atunci se transmite către sursă un mesaj de eroare (de exemplu, prin intermediul ICMP).

Protocoalele care utilizează modul de adresare ierarhizat definit pe nivelul OSI 3 se numesc **protocoale rutabile.**

De exemplu, IP, FTP, IPX, AFP (AppleTalk) sunt protocoale rutabile.

Orice protocol care nu utilizează adrese definite pe nivelul de rețea este considerat **protocol nerutabil.** De exemplu, protocolul NetBeui utilizat pentru managementul unui LAN este nerutabil și pachetele transmise de acesta vor fi transferate de router prin procedeul de bridging.

Dacă într-o rețea un anumit protocol (de exemplu, IP) este definit ca protocol rutabil, atunci cadrele transmise de un router IP definite cu un protocol nerutabil (cadrele non-IP) vor fi retransmise de acesta prin procesul de '*bridging*'.

Un router definit pe un singur protocol de rețea are avantajul că știe exact unde se găsește în pachet adresa destinației și procesează rapid datele. În plus, prin citirea tipului protocolului de rețea în cadrul de date (de exemplu, în cadrul Ethernet), routerul poate transfera datele numai în rețeaua care lucrează cu acel protocol. Astfel se reduce încărcarea rețelei și se pot defini priorități de transmisie.

Routerele multiprotocol lucrează cu structuri diferite de pachete, cu diverse formate ale adresei de destinație, ceea ce îngreuiază procesul de rutare și determină întârzieri de transmisie mai mari (30% - 40%). De aceea, în multe cazuri, se preferă interconectarea LAN-urilor cu switch-uri de nivel 3 sau 4.

Observații:

1. Un router, deși este un echipament de comunicație de nivel 3, poate fi configurat să lucreze și ca bridge (*BR - BRouter*).

2. Un router poate lucra ca 'zid de protecție' (*firewall*) între două LAN-uri interconectate pentru eliminarea transmisiilor broadcast nedorite și a fenomenului de saturare a rețelelor (*flooding*), pentru securizarea traficului de pachete și asigurarea transparenței legăturii.

3. Segmentarea rețelelor cu routere este mai avantajoasă decât cea realizată cu bridge-uri sau switch-uri, deoarece se lucrează cu adrese de rețea, respectiv cu o schemă de adresare ierarhizată, pe domenii de coliziune mai mici, aplicând un algoritm de deducere a rutei optime ceea ce asigură fluența traficului și minimizează riscul de coliziune, dar determină unele întârzieri de transmisie.

4. Routerele nu transmit cadre prin broadcast pe baza adreselor fizice (de exemplu, ARP), ceea ce reduce încărcarea rețelelor. Astfel routerele delimitează domeniile de broadcast.

5. Routerele pot fi configurate software, prin comenzi specifice, definite de firma producătoare.

VI.3 PROTOCOALE DE RUTARE

Protocoalele de rutare stabilesc mecanismul prin care routerele obțin informațiile referitoare la topologia rețelei (de exemplu, RIP - *Routing Information Protocol;* IGRP - *Internal Gateway Routing Protocol;* EGRP - *Enhanced IGRP*; OSPF - *Open Shortest Path First* etc).

Aceste protocoale permit actualizarea tabelului de rutare al fiecărui router și transmisia informațiilor referitoare la modificările survenite în acesta către routerele învecinate.

Clasificarea protocoalelor de rutare se poate face pe baza criteriului de deducere a rutei optime:

1. **vectori de distanță** (ex. RIP; IGRP);

2. **starea legăturii** (OSPF);

3. **combinații între vectorii de distanță și starea legăturii** (protocoale hibride, de exemplu EGRP).

O altă clasificare a protocoalelor de rutare se face în funcție de aria de acoperire a acestora.

Dacă rețeaua WAN este divizată în mai multe sisteme autonome (AS - *Autonomous System*), atunci comunicația dintre routerele din interiorul acestora se face cu **protocoale de rutare interne** (de exemplu, RIP, IGRP) iar între routerele care asigură comunicația dintre sistemele autonome se utiizează **protocoale de rutare externe** (ex: EGP - *External Gateway Protocol*; BGP - *Border Gateway Protocol*) (Fig.VI.3).

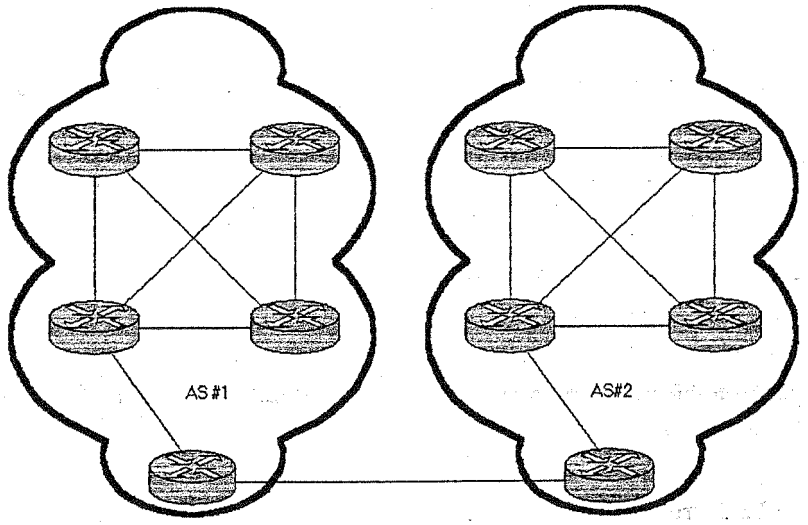


Fig.VI.3 Interconectarea unor sisteme autonome

VI.3.1 Protocoale de rutare cu vectori de distanță

Protocoalele de rutare cu vectori de distanță impun transmisia periodică către toate routerele învecinate a informațiilor de rutare utilizate de un router. Astfel se reactualizează bazele de date care conțin informațiile referitoare la topologia rețelei.

Fiind un proces de tip "pas-cu-pas", rutarea cu vectori de distanță nu asigură o cunoaștere exactă a topologiei rețelei iar reactualizarea tabelelor de rutare se face relativ lent.

Un router **RIPv1** (*Routing Information Protocol version 1*) transmite prin broadcast, la fiecare 30 secunde, un mesaj de înștiințare (*hello*) către toate routerele adiacente din WAN, specificând pentru fiecare rețea de destinație, distanța până la aceasta ca număr de hopuri (de exemplu, maxim 15). Astfel tabelele de rutare sunt reactualizate. Protocolul nu lucrează la nivel de subrețele. Pachetele IP transmise își decrementează timpul de viață la trecerea printr-un router urmând să fie distruse atunci când timpul pentru transfer expiră. RIPv1 este considerat protocol de rutare statică.

Protocolul **RIPv2** (RFC 1723), permite aplicarea măștilor de subrețea și includerea subrețelelor în tabelul de rutare. Acest protocol dinamic poate fi utilizat și în interiorul LAN-ului pentru interconectarea subrețelelor folosind un router intern deci este de tip IGRP (*Internal Gateway Routing Protocol*).

Protocolul **DVMRP** (*Distance Vector Multicast Routing Protocol*) este orientat pe ariile de acoperire ale ruterelor ceea ce presupune că modificările intervenite în tabelele de rutare sunt comunicate prin multicast numai ruterelor din aria respectivă. După expirarea timpului de viață, anumite linii din tabelul de rutare sunt eliminate. Protocolul poate fi aplicat pe subrețele. Fiind un protocol bazat pe vectori de distanțe, nu evită blocajele de trafic. Vectorii de distanță sunt calculați pe diferite grafuri de rețea, cu metrici diverse (întârziere de transmisie, siguranță, costuri etc) ceea ce permite deducerea rutei optime în funcție de opțiunile exprimate în pachetele de date.

Uneori volumul informațiilor de rutare poate fi relativ mare și este eficientă gruparea rutelor corespunzătoare diferitelor adrese de destinație în entități mai mari, prin procedeul CIDR (*Classless Interdomain Routing*).

VI.3.2 Protocoale de rutare bazate pe starea legăturii

Protocoalele de rutare care utilizează starea legăturii mențin la nivelul fiecărui router o bază de date complexă, cu informații despre toate routerele din rețea, nu numai despre cele învecinate. Pe baza grafului rețelei, se aplică algoritmul de deducere a căii minime și se stabilește ruta optimă pentru fiecare rețea de destinație. În cazul schimbării topologiei rețelei, actualizarea tabelelor de rutare se face relativ rapid.

Protocolul de rutare dinamică **OSPF** (*Open Shortest Path First*) se aplică în rețelele mari ca număr de noduri, inclusiv pe subrețele, cu autentificarea datelor, iar rutarea și rerutarea pachetelor se face mai rapid decât prin RIP, definindu-se arii de acoperire pentru fiecare router. Acest protocol este de tip IGRP și a fost special proiectat pentru rutare în rețelele care utilizează TCP/IP. Fiecare router intern din sistemul autonom (AS - *Autonomous System*) deține o bază de date proprie în care sunt incluse informații privind starea interfețelor ruterului, routerele vecine și altele. Routerele vecine se informează reciproc prin *flooding* numai dacă apar modificări în tabelele proprii de rutare, în care se precizează pentru fiecare rută, suplimentar față de RIP, costul și lățimea de bandă disponibilă. Interconectarea ariilor de acoperire din sistemele autonome, se face prin intermediul unor routere AS desemnate (*boundary router*) iar între AS-uri se utilizează **routere externe** (*external router*) care permit transferul unor pachete la distanțe mari în WAN. Deducerea rutei optime se face pe baza unor arbori de acoperire a AS, în care nu apar bucle iar routerele externe sunt noduri terminale în 'arbore'.

Calea spre destinație poate fi de tip:

1. INTRA - în interiorul unei singure arii din AS;

2. INTER - traversează mai multe arii din același AS fără a traversa un router de la granița AS;

3. EXT1 - calea trece printr-un router din AS și rămâne în interiorul AS. Se utilizează două metrici, metrica OSPF internă și cea a routerului AS, pentru a deduce ruta optimă.

4. EXT2 - calea trece dintr-un AS în altul printr-un router extern, deci se combină metrica OSPF internă cu cea a routerului EGP (*External Gateway Protocol*) pentru găsirea rutei optime.

Protocoalele RIP sunt orientate pe vectori de distanță și utilizează numai informațiile furnizate de routerele adiacente, în timp ce OSPF este orientat pe starea legăturii dintre noduri (LST - *Link State Technology*) și permite optimizarea transferului pe baza informațiilor deținute de toate routerele din WAN. Routerele OSPF admit importul și exportul de informații din și spre un router RIP.

VI.3.3 Rutarea IP

Un router definit pentru IP este numit **router IP** sau **gateway** (' poartă' de transmisie). În prezent, un gateway poate lucra și la nivelele superioare celui de rețea din modelul OSI, termenul fiind utilizat într-un sens mult mai larg decât cel de router IP.

Switch

La prima vedere un switch seamăna foarte bine cu un hub, dar după cum vedeți, simbolul său arată un flux informațional bidirecțional.

Menirea acestui dispozitiv este de a concentra conectivitatea garantînd în acelaşi timp lățimea de bandă. Switch-ul este un dispozitiv ce combină conectivitatea unui hub cu posibilitatea regularizării traficului pentru fiecare port(acțiune realizată cu ajutorul bridge-ului). Ca manieră de lucru, el comută pachetele de pe porturile transmițătoare către cele destinatare, asigurînd fiecărui port lățimea de bandă maximă a rețelei.

Această comutare a pachetelor se face pe baza adresei MAC, ceea ce face din switch un dispozitiv de nivel 2 (gîndiți-vă la fiecare port al unui switch ca la un mini-bridge).

Router-ul

Simbolul routerului descrie foarte bine cele două funcții ale sale: selecția căii de transmitere a informațiilor şi comutarea pachetelor către cea mai bună rută.

Fizic, routerele se prezintă sub o mulțime de forme, în funcție de model şi de producător. Componentele principale ale routerului sînt interfețele prin care rețeaua proprietară se conectează la alte segmente de rețea. Din acest motiv el este considerat un dispozitiv inter-rețele.

Scopul routerului este să examineze pachetele recepționate, să aleagă cea mai bună cale de transmitere a acestora şi în final să le transfere către portul corespunzător. Pentru rețelele mari, el reprezintă cel mai important dispozitiv prin care se reglează traficul rețelei. Deciziile routerului în ceea ce priveşte selectarea căii de rutare se iau pe baza informațiilor de la nivelul 3 (adresele de rețea), motiv pentru care sînt considerate echipamente de nivel 3. De asemenea, ele asigură conectivitate pentru diferitele tehnologii ale nivelului2: Ethernet, Token Ring, FDDI.

Dacă lucrurile nu sînt prea clare încă, încercați să citiți şi materialele de la următoarele adrese: http://www.whatis.com/encapsul.htm, http://www.jyu.fi/~eerwall/packet.htm, http://www.cs.mun.ca/~donald/bsc/node13.html,http://www.erg.abdn.ac.uk/users/gorry/course/intro-pages/encapsulation.html.

Capitolul 3: Nivelul legătură date

Pînă în acest moment am discutat mai mult despre ce se întîmplă la nivel fizic într-o rețea: medii de transmisie, bitii care traversează aceste medii, componente care transmit semnale electrice şi topologii. Nivelul 1 joacă un rol important în comunicația ce apare între calculatoare, dar efortul său singular nu este de ajuns. Fiecare din funcțiile nivelului 1 are propriile limitări, dar acestea sînt eliminate prin ceea ce se întîmplă la nivelul 2:

The Institute of Electrical and Electronic Engineers (IEEE)[3] este organizația profesională care a definit standardele aplicabile în domeniul rețelelor de calculatoare:

- 802.1- modul de interconectare în retea;
- 802.2- controlul legăturii logice (LLC);
- 802.3- rețele LAN cu acces multiplu şi cu detectarea purtătoarei şi a coliziunilor CSMA / CD, sau **rețelele Ethernet**[4];
- 802.4- rețele LAN cu transfer de jeton pe magistrală (Token Bus);
- 802.5- rețele LAN cu transfer de jeton în inel (Token Ring);
- 802.6- rețele metropolitane (MAN);
- 802.11- rețele fără fir;
- 802.12-rețele LAN cu prioritate la cerere.

Conform standardului Ethernet, o rețea locală este compusă din noduri şi medii de interconectare. Nodurile pot fi împărțite în două categorii:

- **Data terminal equipment (DTE)** – sînt echipamentele care funcționează ca sursă sau destinație a cadrelor transmise prin rețea. Cel mai adesea în această categorie intră PC-urile.

- **Data communication equipment (DCE)** – sînt dispozitive intermediare care recepționează şi transmit cadrele prin rețea. Se includ în această categorie hub-urile, switch-urile, router-ele, NICi-urile sau modemurile.

În timp ce modelul OSI reprezintă teoria care a stat la baza dezvoltării rețelelor, standardele IEEE au apărut în momentul în care rețelele au devenit realitate, cînd problemele practice trebuiau rezolvate. Chiar dacă modelul OSI este folosit în continuare, cînd se vorbeşte de nivelul 2 se au în vedere şi cele două noi componente apărute în timp: LLC şi MAC:

- **Media Access Control** (MAC) – realizează tranziția în jos, către mediul fizic de transmisie
- **Logical Link Control** (LLC)[5] - realizează tranziția în sus, către nivelul rețea.

Subnivelul LLC este independent de tehnologia folosită, în timp ce MAC este dependent de tehnologia folosită.

3.1 Funcțiile MAC

[3] http://standards.ieee.org
[4] Pe larg la adresa http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ethernet.htm
[5] Definit prin IEEE 802.2

Subnivelul LLC a fost introdus de către IEEE din nevoia de a asigura independența tehnologică a unora din funcțiile nivelului legătură date. Oarecum inconsistent în serviciile pe care le oferă protocoalelor de la nivelul rețea, subnivelul LLC comunică cu tehnologiile specifice nivelurilor dinaintea sa.

LLC preia datele protocolului rețea şi le adaugă mai multe informații de control pentru a transmite pachetele IP către destinație. Pachetul IP astfel reîmpachetat este transmis subnivelului MAC unde urmează a fi încapsulat.

Subnivelul LLC răspunde de gestionarea comunicațiilor între echipamentele de pe o singură linie/legătură a rețelei. LLC este definit prin specificațiile IEEE 802.2, specificații care se referă atît la serviciile orientate conexiune cît şi la cele fără conexiune, servicii folosite de protocoalele superioare.

Subnivelul MAC se ocupă de protocoalele pe care un calculator le foloseşte pentru a accesa mediul fizic de transmisie a datelor. Adresa MAC are o lungime de 48 de biti, şi este exprimată în hexazecimal (12 cifre). Primele 6 care formează OUI (Organizational Unique Identifer), sînt administrate de către IEEE, identificînd producătorul sau vînzătorul produsului. Celelalte 6, descriu numărul interfeței (Serial Number Interface) sau o altă valoare administrată de fiecare producător sau vînzător.

Adresa MAC este "scrisă" în memoria ROM a cartelei de rețea, de unde este apoi copiată în RAM la inițializarea cartelei. Prin urmare, dacă o cartelă este înlocuită, se va schimba şi adresa fizică a calculatorului.

Cînd un dispozitiv din cadrul unei rețele Ethernet încearcă să transmită date către alt dispozitiv, va căută să deschidă un canal de comunicație cu acesta, folosind adresa MAC: datele transmise vor transporta şi adresa MAC a destinației. Pe măsură ce datele traversează mediul fizic de transmisie, NIC-ul fiecărui calculator din rețea verifică dacă adresa sa MAC corespunde adresei destinație inclusă în pachet. Dacă adresele nu sînt identice, NIC ignoră datele din pachet, date ce continuă să circule către următoare destinație. Dacă adresele sînt identice, NIC face o copie a pachetului cu date şi plasează această copie în calculator, la nivelul legătură de date. Pachetul original va continua să circule prin rețea, către alte destinații, unde se va verifica corespondența dintre adresele MAC.

Dezavanatajul major al adresării MAC constă în faptul că aceste adrese nu au o structură strict definită: vînzătorii au OUI-uri diferite. Altfel spus, adresarea MAC nu este o adresare ierarhică, după cum se va vedea că este adresarea IP. Pe măsură ce rețeaua "creşte", acest dezavantaj devine o problemă majoră.

3.2 Încadrarea (Framing)

Framing-ul sau *încadrarea* este un mecanism prin care se obțin informații complexe, operație ce nu poate fi realizată prin simpla transmisie a biților prin mediul fizic al rețelei. Care sînt calculatoarele ce doresc să comunice între ele? Cînd începe comunicarea între două calculatoare şi cînd se termină? Cînd îi vine rîndul unui calculator să comunice?

Spuneam că nivelul fizic al unui calculator se ocupă doar de biti. În timp ce încearcă să transmită aceşti biti către destinație, nivelul fizic nu garantează că nu există şi erori. Aici intervine nivelul legătură date. Prin încadrare, biti transmişi de nivelul fizic sînt încapsulați la nivelul 2 în unități de date ale protocolului de nivel 2 (PDU de nivel 2) sau cadre (cadruri).

Există mai multe tipuri de cadru-uri în funcție de standardele folosite la descrierea lor. În mod generic, un cadru este împărțit în secțiuni numite cîmpuri, fiecare cîmp fiind alcătuit din bytes:

Orice calculator conectat la o rețea trebuie să dețină un mecanism prin care să poată atrage atenția celorlalte calculatoare din rețea cu privire la transmiterea unui cadru. Acest lucru este posibil prin intermediul cîmpului *start* din formatul cadru-ului.

Orice cadru conține informații cu privire la numele calculatorului sursă (sub forma adresei MAC) şi numele calculatorului destinație (tot adresa MAC). Un cadru are însă şi cîmpuri specalizate: lungimea exactă a cadrului sau tipul său pentru a specifica protocolul de nivel 3 ce face posibilă transmiterea sa prin rețea.

Datele transmise prin rețea sînt împărțite în două componente: datele propriu zise şi un set de bytes încapsulați, denumiți *padding bytes*, sau bytes de umplere. Aceşti bytes sînt adăugați cadrului pentru ca acesta să aibă o lungime minimă şi să poată respecta intervalul de timp în care este transmis.

Informațiile conținute de un cadru sînt susceptibile de a suporta erori ce pot să aibă surse diferite. Cadrele care conțin erori sînt retransmise. Acest lucru este realizat cu ajutorul cîmpului secvență/cifră de control a cadrului. Această cifră este un număr obținut pe baza datelor din cîmpul de date al cadrului. Acesta este citit de calculatorul destinație pentru a verifica dacă cadrul recepționat este corect sau este alterat de zgomotele rețelei.

Calculatorul sursă calculează o cifra de control pe care o adaugă cadrului. La destinație, se calculează o nouă cifră de control pe baza datelor conținute de cadrul recepționat, cifră care este comparată cu cea calculată de sursa mesajului. Dacă cele două cifre de control sînt identice, datele din cadru vor fi acceptate. Dacă cifrele de control nu sînt identice, sursa va fi atenționată că trebuie să retransmită datele. Pentru ca transmisia să se termine în condiții optime, sursa mesajului trebuie să atragă atenția celorlalte calculatoare asupra momentului în care cadrul se termină.

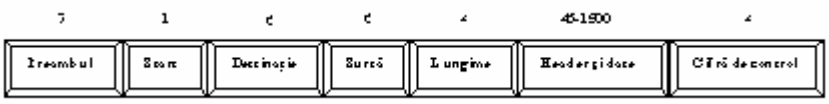
3.2.1 Standardul Ethernet

Standardul Ethernet este definit de IEEE (Institute for Electrical and Electronic Engineers) ca IEEE 802.3. Acest standard defineşte regulile pentru configurarea unei rețele Ethernet precum şi modul de interacțiune între diferitele elemente ale unei astfel de rețele (există 18 variante ale acestui standard!).

Cadrul Ethernet

Fiecare calculator echipat cu o placă de rețea Ethernet, funcționează independent de toate celelalte stații din retea: nu există un control centralizat. Toate stațiile ataşate la rețea sunt conectate la acelaşi sistem de transport pentru semnal, denumit mediu de comunicație. Informația este transmisă serial, bit cu bit prin linia de comunicație către toate stațiile ataşate acesteia**.** Figura următoare ilustrează formatul unui cadru Ethernet aşa cum este el prezentat în specificațiile IEEE 802.3[6] (cifrele reprezintă lungimea cîmpurilor în bytes)

[6] http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ethernet.htm#xtocid8



Conform acestui standard, cîmpurile care alcătuiesc un cadru Ethernet sînt:

- *Preambul*

Această secvență de 56 biti este folosită pentru sincronizarea transmisiei. Aceşti biti permit componentelor unei rețele să detecteze prezența unui semnal şi să înceapă citirea acestui semnal înainte de sosirea datelor conținute în cadrul respectiv. Prin intermediul acestor biti stația destinatară este avertizată cu privire la sosirea unui cadru.

- *Start cadru(SOF)*

Conform specificațiilor IEEE 802.3, byte-ul care delimitează începutul cadru-ului de restul conținutului său se termină cu doi biti consecutivi cu valoarea 1 (10101011). Aceşti biti servesc la sincronizarea recepției cadru-ului de către toate stațiile.

- *Adresă destinație şi adresă sursă*.

Primii 3 bytes ai acestui cîmp sînt precizati de către IEEE în funcție de cerințele producătorilor de echipamente pentru rețele. Următorii 3, sînt descrişi chiar de producători (parcă am mai vorbit de asta nu?). Adresa sursă este o adresă unicast (single node). Adresa destinație poate fi unicast, multicast sau broadcast.

- *Lungime/tip*

Acest cîmp indică numărul de bytes de date care urmează în cadru după acest cîmp sau tipul cadrului dacă acesta este asamblat folosind un format opțional

- *Date*

După ce procesările de la nivelurile fizic şi legătură date s-au terminat, datele conținute în cadru sînt transmise către un protocol de nivel superior care trebuie definit în cadrul acestui cîmp. Dacă datele din cadru nu ocupă cel puțin 46 bytes, vor fi inserați bytes de umplere pînă la atingerea acestei valori.

- *Cifră de control*

Acest cîmp conține o cifră de verificare pe 4 bytes, cifră ce este calculată de către dispozitivul care transmite datele, urmînd a fi recalculată de către receptor şi comparată cu originalul în scopul identificării eventualelor diferente.

Dispozitivele Ethernet trebuie să permită un interval minim de timp între două cadre care se transmit pe un mediu. Acest interval se numeşte *intercadru gap (IFG)* sau *interpacket gap (IPG)* şi foloseşte pentru pregătirea recepționării următorului cadru transmis de o stație. Acest interval este de 9,6 microsecunde pentru rețelele pe 10 Mbps, 960 nanosecunde pentru 100 Mbps şi 96 nanosecunde pentru 1 Gbps.

În continuare vom prezenta cele două protocoale prin care se controlează accesul la mediul de transmisie într-o rețea Ethernet: *half-duplex* şi *full-duplex*.

Half-Duplex Ethernet[7] (CSMA/CD Access Protocol)

[7] Comunicație semi-duplex

Half Duplexul reprezintă forma tradiţională de control în Ethernet, bazată pe protocolul CSMA/CD – Carrier Sense Multiple Access/Collision Detection (acces multiplu cu detecţia purtătoarei şi coliziunii).

Pe baza acestui protocol, staţiile care partajează acelaşi mediu şi care doresc să iniţieze o transmisie, trebuie să asculte canalul pentru a vedea dacă nu cumva transmite altcineva în acel moment. În cazul în care canalul este ocupat, staţia aşteaptă pînă la eliberarea acestuia. Atunci cînd canalul este liber, staţia transmite un cadru către toate celelalte staţii (operaţie care se numeşte *broadcast* sau *difuzare).* Există însă probabilitatea ca, imediat ce această staţie începe să transmită, o altă staţie să fie pregătită de transmisie şi să asculte canalul. Dacă cadru-ul difuzat în reţea nu a ajuns încă la cea de a doua staţie, aceasta din urmă va detecta canalul ca fiind liber şi va iniţia la rîndul său o transmisie, rezultînd o coliziune.

Coliziunile pot fi detectate urmărind puterea sau lăţimea impulsului semnalului recepţionat şi comparîndu-le cu semnalul transmis. În acest caz, staţia care a iniţiat transmisia lansează în reţea o secvenţă *jam* (de blocare) de 32 biti prin care se asigură că toate celelalte staţii din reţea au fost informate cu privire la eşuarea transmisiei. Apoi staţi asursă îşi abandonează transmisia, aşteaptă o perioadă de timp şi încearcă iar dacă nici o altă staţie nu a început să transmită între timp. Acest proces se repetă pînă cînd cadrul este transmis cu succes la destinaţie.

În sinteză, principalele etape în transmiterea unui cadru sînt:

1. staţia care doreşte să transmită ascultă reţeaua cu scopul detectării prezenţei unei staţii care transmite (carrier sense – detecţia purtătoarei)
2. dacă este detectată o purtătoare activă, transmisia este amînată. Staţia continuă să monitorizeze reţeaua pînă în momentul dispariţiei purtătoarei
3. dacă nu este detectată o purtătoare activă, staţia sursă iniţiază transmiterea cadrelor
4. odată cu transmiterea cadrului, staţia sursă supraveghează mediul în vederea detectării coliziunilor.
5. dacă este detectată o coliziune, staţia sursă opreşte transmisia cadrelor şi lansează o secvenţă de blocare pentru a se asigura că toate celelalte staţii iau cunoştinţă de existenţa coliziunii.
6. după ce a transmis secvenţa de blocare, staţia sursă aşteaptă o perioadă de timp înainte de a recîncepe transmisia (de la punctul 1). Acest proces se numeşte *backoff algorithm*[8] (algoritm de regresie): se reduce probabilitatea de apariţie a coliziunilor prin adaptarea dinamică a numărului staţiilor care încearcă să transmită (interval de întîrziere generat aleatoriu)
7. dacă totuşi reapar coliziuni, intervalul de generare aleatorie creşte exponenţial. Algoritmul asigură o întîrziere minimă cînd se ciocnesc numai cîteva staţii, dar garantează că ciocnirea este rezolvată într-un interval rezonabil cînd este vorba de mai multe staţii.
8. procesul se repetă pînă cînd o staţie transmite un cadru fără coliziuni.

Un parametru important al operării în modul half duplex este *slot time* (mărimea cuantei). Acest parametru a fost definit ca avînd 512 intervale de bit (51,2 microsecunde) pentru reţelele Ethernet care operează la viteze de 10 şi 100 Mbps, respectiv 4096 intervale de bit pentru reţelele Gigabit. Mărimea cuantei se referă la intervalul de timp pe care un dispozitiv îl aşteaptă înainte de a retransmite după apariţia unei coliziuni.

Pe măsură ce traversează reţeaua, semnalele transmise suferă întîrzieri. Aceste întîrzieri reprezintă timpul necesar unui semnal să tranziteze prin componentele electronice ale reţelei. Cu cît lungimea segmentelor şi numărul de repetoare(huburi) se apropie de maximul

[8] binary exponential backoff algorithm (algoritm de regresie binară exponenţială)

admis de standardele Ethernet (2500 metri şi 4 repetoare) cu atît se măreşte şi intervalul de timp necesar unui semnal pentru a traversa reţeaua de la un capăt la altul. Acest interval de timp se numeşte *întîrziere la propagare.*

Suma dintre întîrzierea dus-întors la propagare (maximă) şi timpul necesar pentru a transmite o secvenţă de blocare sînt componentele care definesc mărimea cuantei în Ethernet.

O cuantă cu mărimea de 512 intervale de bit stabileşte mărimea minimă a unui cadru Ethernet la 64 bytes (în cazul Gigabyte, cele 4096 intervale de bit impun adăugarea unui cîmp de extensie la cadru pentru a se atinge mărimea minimă de 512 bytes). Orice cadru a cărui dimensiune este mai mică de 64 bytes este considerat *fragment de coliziune* şi este distrus în mod automat de staţia care îl recepţionează.

Mărimea cuantei impune o limită maximă în ceeea ce priveşte dimensiunea unei reţele: lungimea segementelor de cablu şi numărul repetoarelor pe o singură cale. Dacă reţeaua este dezvoltată dincolo de aceste limite apare fenomenul de *coliziune întîrziată*. Acestea sînt coliziunile care apar prea tîrziu în timpul transmiterii unui cadru pentru a mai putea fi gestionate prin funcţia de control al accesului. Cadrele afectate vor fi distruse fiind necesară reiniţierea transmisiei.

Mărimea cuantei este cea care asigură că dacă este posibil să apară o coliziune, aceasta va fi identificată în primii 512 biti transmisi sub formă de cadre (4096 pentru Gigabyte).

Revenim acum la agoritmul de regresie pentru a explica mai în detaliu ce se întîmplă. Prin intermediul acestui algoritm staţia care a iniţiat transmisia determină intervalul de timp care trebuie să treacă după apariţia unei coliziuni, înainte ca un cadru să fie retransmis. De ce este nevoie de aşa ceva? Dacă toate staţiile ar aştepta acelşi interval de timp , atunci în mod sigur va apărea o nouă coliziune. Acest lucru este evitat prin algoritmul amintit: fiecare staţie generează aleator un număr care va determina timpul cît trebuie să aştepte înainte de a trece la identificarea purtătoarei. Acest interval de timp se numeşte *întîrziere de regresie.*

După apariţia primei coliziuni, fiecare staţie aşteaptă 0 sau 1 cuante înainte de a încerca o nouă transmisie. Dacă apare o nouă coliziune intervalul de aşteptare va fi între 0 şi 3 cuante, pentru o a treia coliziune între 0 şi 7 (2^3-1). În general, după *i* coliziuni se aşteaptă între 0 şi 2^i-1 cuante. Dacă se ajunge la un număr de 10 coliziuni, intervalul de aşteptare este îngheţat la 1023 cuante. După 16 coliziuni, funcţia MAC raportează eşecul calculatorului (**excessive collision error**) iar cadrul care trebuia transmis este distrus, aplicaţia care îl folosea fiind nevoită să iniţieze o nouă transmisie.

De ce atîtea vorbe despre acest algoritm? Pentru că erorile care apar ca urmare a coliziunilor în exces dintr-o reţea reprezintă cel mai bun indiciu că reţeaua nu mai este eficientă.

Timpul necesar transmiterii unui cadru este invers proporţional cu rata de transmisie. Pentru o reţea cu o lăţime de bandă de 100Mbps, un cadru cu o dimensiune minimă este transmis într-un timp egal cu 1/10 din mărimea cuantei. Prin urmare o coliziune care apare în timpul acestei transmisii nu va putea fi detectată de staţiile care emit semnal. Este moticul pentru care diametrul maxim al unei reţele pe 10 Mbps nu poate fi utilizat în cazul reţelelor pe 100Mbps (Fast Ethernet). Soluţia în acest caz a fost reducerea diametrului reţei.

Parametru	**10 Mbps**	**100 Mbps**	**1000 Mbps**
Mărimea minimă a unui cadruMinimum	**64 bytes**	**64 bytes**	**520 bytes**

cadru size			
Diametrul maxim al domeniului de coliziune	**100 metri UTP**	**100 metri UTP** **412 metri fibră**	**100 metri UTP** **316 metri fibră**
Dimetrul maxim al domeniului de coliziune cînd se folosesc repetoare	**2500 metri**	**205 metri**	**200 metri**
Numărul maxim de repetoare pe o rută LAN	**5**	**2**	**1**

Full-Duplex Ethernet[9]

Acest al doilea mod de operare al rețelelor Ethernet depăşeşte limitările impuse prin protocolul CSMA/CD: o stație, la un moment dat, poate fie să transmită date, fie să recepționeze. Niciodată nu se întîmplă acest lucru simultan.

În cazul full-duplex, două stații pot să schimbe simultan informații dacă există o legătură care să permită acest lucru. În acest caz, *throughput-ul* agregat al rețelei se dublează!

Operarea în modul full-duplex este restricționată de respectarea mai multor criterii. În primul rînd, mediul fizic de transmisie trebuie să suporte transmiterea şi recepționarea simultană de informații, fără a exista interferențe. Mediile a căror specificații *respectă* aceste cerințe sînt: 10-Base-T, 10Base-FL, 100Base-TX, 100Base-FX, 100Base-T2, 1000Base-CX, 1000Base-SX, 1000Base-LS, and 1000Base-T (vom reveni cu detalii). Următoarele specificații *nu* suportă modul full-duplex: 10Base5, 10Base2, 10Base-FP, 10Base-FB, and 100Base-T4.

În al doilea rînd, pentru a opera în acest mod, legăturile trebuie să fie point-to-point (punct-la-punct) sau altfel spus legătura trebuie să fie direct între două stații. Atît timp cît nu există conflicte ca în cazul mediilor partajate, nu vor apărea coliziuni şi prin urmare nici protocolul CSMA/CD nu mai este necesar. Ambele stații trebuie să suporte şi să fie configurate pentru a opera în modul full-duplex.

Deşi mai sînt destule de spus, ne oprim aici cu descrierea Ethernetului nu înainte de a mai aminti despre *agregarea legături* sau *trunking-ul* disponibil în modul full-duplex. Acest lucru înseamnă că mai multe legături fizice de tip point-to-point pot fi agregate pentru a funcționa ca o singură legătură logică.

3.5.3 Cablarea IEEE 802.3

Chiar dacă despre cabluri am mai discutat în cadrul nivelului 1, ne îndreptăm din nou atenția asupra lor, dar de astă dată prin prisma standardelor IEEE 802.3. În mod obişnuit Ethernetul foloseşete doar cîteva din standardele existente în materie de cabluri: 10Base5,

[9] duplex integral

10Base2, 10BaseT, 10 BaseF, 100BaseF. Notația anterioară înseamnă că rețeaua folosește o anunmită lățime de bandă, utilizează semnalizarea în bandă de bază și poate suporta segmente de diferite lungimi pe diferite medii de transmisie. Vom face o prezentare sintetizată a acestor standarde.

Standard	Mediul fizic	Lățime de bandă	Lungime segment	Topologie fizică	Topologie logică
10Base2	Coaxial subțire	10Mbps	185 metri	Bus	Bus
10BaseT	UTP categoria 5	10Mbps	100 metri	Star/Extended star	Bus
10BaseFL	Fibră optică multimod	10Mbps	2000 metri	Star	Bus
100BaseTX	UPT categoria 5	100Mbps	100 metri	Star	Bus
100BaseFX	Fibră optică multimod	100Mbps	2000 metri	Star	Bus
1000BaseT	UTP categoria 5	1000Mbps	100 metri	Star	bus

3.4 FDDI

Comitetul de standardizare ANSI X3T9.5 este primul autor al standardului **Fiber Distributed Data Interface (FDDI)**. După completarea tutuor specificațiilor ANSI a transmis standardul FDDI Organizației Internaționale pentru Standardizare (ISO) care a realizat o versiune internațională a standardului FDDI, versiune perfect compatibilă cu versiunea ANSI.

Chiar dacă astăzi rețelele FDDI nu sînt atît de comune precum cele Ethernet sau Token-Ring, pe măsură ce costurile de implementare se vor reduce, ele vor deveni accesbile pe o scară mai mare.

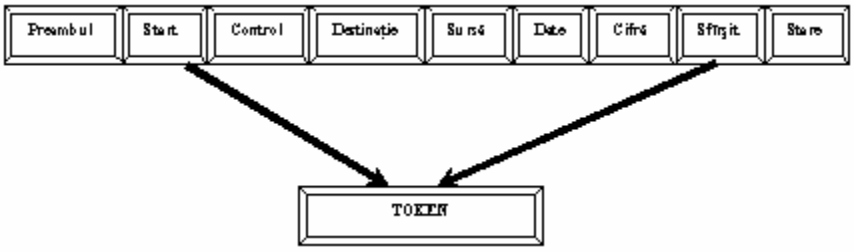
FDDI prezintă 4 specificații:

Media Access Control (MAC)- definește modul în care se realizează accesul la mediul fizic de transmisie, incluzînd: formatul cadru-ului, ddresarea, manipularea jetonului, algoritmul prin care se calculează CRC (verificarea redundanței ciclice) și mecanismele pentru refacerea stării inițiale ca urmare a apariției unei erori

Physical Layer Protocol – protocolul nivelului fizic definește procedurile pentru codificarea/decodificarea datelor, incluzînd: cerințele ceasului (frecvența), încadrarea și alte funcții.

Physical Layer Medium – mediul nivelului fizic definește caracteristicile mediului de transmisie, incluzînd:conexiunile fibrei optice, ratele de eroare la nivel de bit, componentele optice.

Station Management- definește configurația stațiilor într-o rețea FDDI, incluzînd: configurația inelului, adăugarea și eliminarea stațiilor, inițializarea, izolarea căderilor, statistici.



După cum se vede şi din poza de mai sus, cîmpurile ce alcătuiesc un cadru FDDI sînt:

- *Preambul*- pregăteşte fiecare staţie pentru a putea recepţiona cadru-ul
- *Delimitator de start*- indică începutul unui cadru
- *Control*- indică mărimea cîmpurilor adresă şi conţine informaţii de control (de exemplu dacă datele sînt asincrone sau sincrone)
- *Adresă destinaţie*- conţine o singură adresă (unicast), un grup de adrese (multicast) sau adresele tuturor staţiilor (broadcast). Adresele au 6 bytes.
- *Adresă sursă*- identifică staţia care trimite cadru-ul (are 6 bytes)
- *Date*- conţine informaţii de control sau informaţii destinate unui protocol de nivel superior.
- *Cifră de control*- este completată de staţia sursă care calculează o CRC. Această valoare depinde de conţinutul cadru-ului. Staţia destinaţie recalculează această valoare pentru a determina dacă cadru-ul a fost modificat în timpul tranzitării prin reţea.
- *Delimitator de sfîrşit*- indică sfîrşitul cadru-ului
- *Stare*- permite staţiei sursă să determine apariţia erorilor şi dacă la destinaţie cadru-ul a fost recepţionat şi copiat de respectiva staţie.

Strategia folosită în reţelele FDDI pentru transmiterea jetonului este similară cu cea din reţelele token-ring. FDDI permite alocarea lăţimii de bandă în timp real, fapt ce le face ideale pentru o mare varietate de aplicaţii. Acest lucru este posibil prin cele două tipuri de trafic ce pot fi implementate: sincron şi asincron.

Traficul sincron poate consuma doar o porţiune din totalul lăţimii de bandă a unei reţele (să zicem 100Mbps), în timp ce traficul asincron consumă restul. Lăţimea de bandă pentru traficul sincron este alocată staţiilor care necesită transmiterea continuă a datelor (de exemplu, voce sau video). Specificaţiile FDDI SMT definesc o schemă distribuită prin care se alocă lăţimea de bandă.

În traficul asincron, lăţimea de bandă este alocată folosind o schemă de priorităţi pe 8 niveluri. Fiecare staţie are atribuit un nivel de prioritate asincron. Fiecare staţie poate folosi la un moment dat toată lăţimea de bandă asincronă. Mecanismul de prioritate poate bloca staţiile care nu folosesc lăţimea de bandă sau care au un nivel de prioritate prea mic.

Specificaţiile FDDI definesc două tipuri de fibră: single mod (sau mono-mod) şi multi mod. Aceste moduri se referă la fascicolul de lumină care intră în fibra optică sub un anumit unghi.

Mono-modul, după cum îi spune şi numele, permite unui singur tip de fascicol să se propage prin fibră, în timp ce multi-modul suportă mai multe tipuri de fascicole. Deoarece în multi-mod lumina care se propagă prin fibră poate parcurge distanţe diferite (în funcţie de unghiul de incidenţă) iar semnale să ajungă la destinaţie la intervale diferite de timp, mono-modul oferă lăţime de bandă mai mare. Acesta este şi motivul pentru care fibra

mono-mod este folosită mai ales la cablările între clădiri în timp ce fibra multi-mod se foloseşte pentru cablările intra-clădiri.

Dispozitivivele prin care se generează lumină sînt LED-urile pentru fibra multi-mod şi laserul pentru fibra mono mod.

Conform specificațiilor FDDI, pentru realizarea conexiunilor fizice se foloseşte un inel (ring) dublu. Prin fiecare din aceste inele, traficul se desfăşoară în sensuri opuse. Fizic, inelele sînt alcătuite din două sau mai multe conexiuni punct-la-punct între stațiile adiacente. Unul din cele două inele se numeşte inel principal şi este folosit pentru transmiterea datelor. Cel de al doilea inel se numeşte secundar şi este folosit în general pentru back-up.

În FDDI se întîlnesc două categoii de stații:

Single Attachement Stations (SAS) sau stații din clasa B, ataşate inelului principal prin intermediul unui concentrator care oferă conectivitate pentru mai multe astfel de stații. Concentratorul este cel care oferă continuitate rețelei în cazul întreruperilor de tensiune sau „căderilor" oricăreia dintre stații.

Dual Attachement Stations (DAS) sau stații din clasa A ataşate ambelor inele. Fiecare din aceste stații are două porturi (A şi B) prin care se conectează la ambele inele ale FDDI.