Lectia 3. NIVELUL LEGĂTURĂ DE DATE

Tema prezentă rolul şi funcţiile nivelului legătură de date într-o arhitectură de reţea şi descrie unele protocoale specifice acestui nivel. Sunt evidenţiate necesitatea şi importanţa formatării fluxurilor de biţi în cadre bine definite, recunoscute şi prelucrate de echipamentele din nodurile de reţea, pe baza unor protocoale de nivel doi, pentru a asigura servicii nivelului superior.

După parcurgerea şi însuşirea acestei teme, studentul va cunoaşte:

- ***Care sunt rolul şi importanţa nivelului legătură de date într-o reţea de comunicaţii şi calculatoare***
- ***Divizarea ascestui nivel în două subnivele (subnivelul de control al accesului la mediul de comunicaţie şi subnivelul de control a legăturii logice) specifice reţelelor cu medii de comunicaţie partajate de mai mulţi utilizatori***
- ***Care sunt cele mai cunoscute tehnici de detecţie şi corecţie a erorilor***
- ***Care sunt cele mai cunoscute tehnici şi protocoale de control al fluxului***
- ***Descrierea şi funcţionarea unor protocoale de nivel doi larg utilizate în reţele (LAPB, HDLC, PPP, Ethernet, CSMA-CD, POP 3)***
- ***Protocoale de nivel 2 în reţele fără fir (protocoalele IEEE 802.11, 802.15, 802.16)***
- ***Segmentarea unei reţele prin folosirea punţilor şi a comutatoarelor***
- ***Proiectarea şi realizarea unei reţele locale la nivel 2 pe bază de switch-uri şi hub-uri***
- ***Realizarea de LAN-uri virtuale(VLAN) şi reţele virtuale private (VPN) bazate pe diverse tehnici (tunelare, MPLS)***

Lucrările de laborator vor viza studiul echipamentelor de reţea de nivel 2 (plăci şi carduri de reţea, switch-uri şi punţi), proiectarea şi simularea funcţionării de reţele locale bazate pe comutatoare şi realizarea de LAN-uri private (VPN).

Timpul minim necesar studierii temei este 10 ore.

Cuvinte cheie:
Ethernet, cadru de date, adresa MAC, LAPB, LAN, VLAN, IEEE 802.3, IEEE 802.11, IEEE 802.16, BlueTooth, CSMA, CSMA/CD, HDLC, PPP, MPLS, LLC, LD, CRC, control erori, switch, FHSS, DSSS,

Cuprins

3.1 Locul şi rolul nivelului LD

Nivelul legătură de date este situat deasupra nivelului fizic şi asigură servicii pentru nivelul rețea. **Rolul său de bază este transmiterea corectă a blocurilor de date între două noduri vecine din rețea.**

Funcțiile specifice pe care trebuie să le realizeze sunt:

- ***furnizarea unei interfețe bine definite cu nivelul rețea;***
- ***tratarea erorilor de transmisie apărut în mediul fizic;***
- ***reglarea fluxului de date pentru a nu bloca receptorul;***
- ***controlul accesului la mediul fizic***.

Pentru aceasta, pachetele de date care vin de la nivelul rețea sunt încapsulate în **cadre** în vederea transmiterii pe mediul fizic. Generic, un cadru de nivel LD are un antet (început de cadru), câmpul de **informație utilă** şi o **încheiere** (sfârşit de cadru).

Nivelul LD este în mod obişnuit împărțit în două subnivele:
- subnivelul de **control al legăturii logice** (**LLC – Logical Link Control**)
- subnivelul de **control al accesului la mediu** (**MAC- Medium Access Control**).

Primul se ocupă de **formarea cadrelor, controlul erorilor, servicii de confirmare** dacă este cazul, **interfața cu nivelul superior** etc. indiferent cum este partajat mediul de transmisie. El crează o interfață uniformă între nivelele superioare şi subnivelul MAC.

Al doilea subnivel are două roluri majore: **stabilirea şi respectarea regulilor de acces la mediu** comun de transmisie a mai multor utilizatori şi **adaptarea la mediul fizic**, astfel încât, să ascundă diferențele legate de diferite medii de transmitere, forme de semnal, coduri de linie etc.

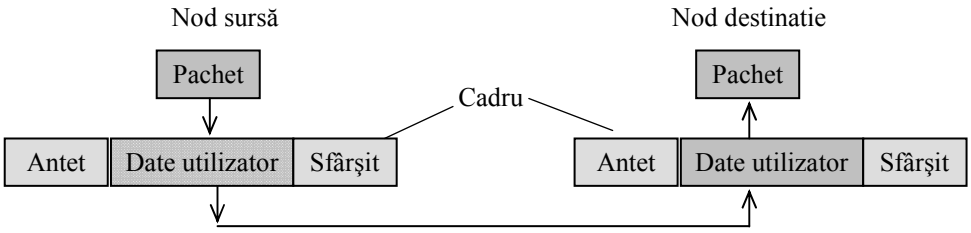


Fig. 3.1 Împachetarea PDU-urilor în cadre

3.2 Protocoale de nivel LD

Formatul cadrelor diferă de la un protocol la altul, dar o formă generală este cea din fig. 3.2.

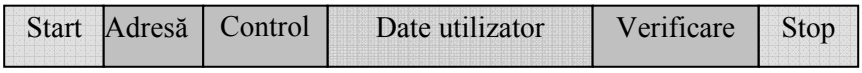


Fig. 3.2 Formatul general al unui cadru LD

Câmpurile **Start** şi **Stop** au structură fixă şi reprezintă delimitatori de cadru.

Câmpul **Adresă** conține adresele de nivel fizic (numite în Internet adrese MAC) ale sursei şi ale destinației.

Câmpul **Control** are rolul de a permite controlul transmisiei în funcție de timpul de recepție, inclusiv prelucrare şi retransmisie în caz de erori.

Blocul de **verificare** este destinat monitorizării erorilor de transmisie. Cea mai simplă metodă de control a erorilor este **bitul de paritate**. O altă metodă mai elaborată este **suma de control**. Ea se efectuează la emisie, se înscrie în câmpul de control şi se verifică la recepție. Dacă valorile sunt diferite, rezultă că în timpul transmisiei au apărut erori şi se iau decizii în consecință. Verificarea erorilor se poate face pentru tot blocul de date (tot cadrul) sau numai pentru antet.

Controlul recepției cadrelor se face în mod uzual prin proceduri de **confirmare pozitivă** (**positive acknowledgment**, abreviat **ack**) sau **confirmare negativă** (**negative acknowledgment, nak**) trimise pe o cale de reacție de la receptor la transmițător. Fiecare confirmare pozitivă arată un cadru recepționat corect, fiecare confirmare negativă arată o eroare şi presupune retransmiterea cadrului. Dacă după un timp prestabilit nu soseşte nici ack nici nak, cadrul este retransmis automat.

Există trei moduri de realizare a funcțiilor ack/nak:

1. Protocolul stop and wait. Se transmite un cadru şi se aşteaptă ack sau nak. Dacă nu apare nici o confirmare, cadrul se retransmite.

2. **Transmisia go back to N.** Cadrele se transmit continuu dacă există, fără a aştepta confirmarea. Când apare primul nak sau după un timp prestabilit se retransmit cadrul în cauză şi toate de după el.

3. Protocolul repetării selective. Se retransmite numai cadrul nevalidat.

Monitorizarea şi (sau) **detecţia** şi **corecţia erorilor**:

1. **bitul de paritate**.
2. **codurilor detectoare / corectoare de erori**
3. **verificarea ciclică a redundanţei** (**CRC – Cyclic Redundancy Check**).

Bitul de paritate.

Acesta este un bit plasat într-un câmp special în antet şi care este 0 sau 1, ales astfel încât suma tuturor biţilor din cadru (sau numai din unele câmpuri din cadru) să aibă o valoare prestabilită, pară sau impară. Această sumă se verifică la recepţie şi dacă nu se confirmă valoarea aşteptată, rezultă că există erori de transmisie. Metoda este foarte simplă şi uşor de aplicat. Marele neajuns este că nu poate sesiza decât existenţa unui număr impar de biţi eronaţi şi nu poate preciza câţi anume.

Codurile detectoare / corectoare de erori sunt coduri speciale destinate detectării/crectării erorilor. O noţiune de bază în teoria acestor coduri este **distanţa Hamming**.

Distanţa Hamming reprezintă numărul de poziţii prin care diferă între ele oricare două cuvinte de cod. Pentru a **detecta *d*** erori, distanţa Hamming trebuie să fie ***d*+1** iar pentru a **corecta *d* erori**, distanţa trebuie să fie **2*d*+1**.

Cele mai folosite coduri detectoare de erori sunt codurile polinomiale, iar metoda de detecţie se numeşte **verificarea ciclică a redundanţei** (**CRC – Cyclic Redundancy Check**).

Aceste coduri au la bază un polinom generator G(x) asupra căruia cad de acord şi transmiţătorul şi receptorul. Mesajul de transmis M(x) este împărţit la G(x) iar restul obţinut se adaugă la M(x) ca informaţie redundantă. La recepţie face din nou împărţirea mesajului recepţionat la G(x). Dacă restul împărţirii este 0, rezultă că transmisia s-a făcut fără erori. Dacă restul împărţirii este diferit de zero, înseamnă că au fost erori de transmisie şi se trece la corecţia lor. Metodele de corecţie sunt mai complicate şi pot fi studiate din literatura de specialitate.

Exemple de protocoale LD

La nivel legătură de date sunt standardizate mai multe protocoale elaborate de diferite organisme de standardizare:

ISI : **HDLC, ISO 3309, ISO 4305**
CCITT : **LAPB, LAPD**
IBM : **SDLC, BSC**
DEC : **DDCMP**
ANSI : **ADCCP** (Avanced Data Communication Control Protocol)
Internet : **PPP**

Protocolul HDLC (High-level Data Link Control)

HDLC este un protocol clasic orientat pe bit, larg folosit de decenii în multe aplicații. El derivă din mai vechiul standard **SDLC** (**Synchronous Data Link Control**) folosit de IBM la interconectaerea calculatoarelor mari. A devenit standard ANSI (**ADCCP**), apoi standard ISO. CCITT a aoptat şi modificat HDLC rezultând **LAP** (**Link Access Procedure**) care a făcut parte din standardul **X.25**. LAP a fost ulterior adaptat cu o versiune mai nouă a HDLC rezultând **LAPB** (**Link Access Procedure, Balanced**).

Toate aceste protocoale sunt bazate pe aceleaşi principii, sunt orientate pe bit şi folosesc o structură de cadru de tipul celei din figura 3.3.

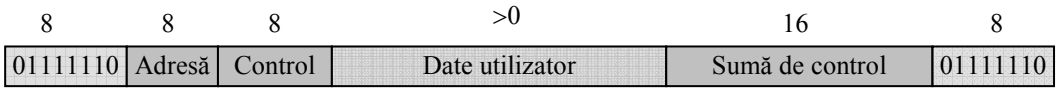


Fig. 3.3 Formatul unui cadru HDLC

Câmpul ***Adresă*** conține adresa de nivel fizic. Este folosită de echipamentele de nivel 2 (switchuri) pentru a trimite cadrele direct la destinație.

Câmpul ***Control*** este folosit pentru numere de secvență, confirmări şi alte scopuri.

Câmpul ***Date*** conține datele provenite de la nivelul superior; poate avea lungime arbitrară.

Câmpul ***Sumă de control*** este pentru CRC.

Cadrul este delimitat de flag-uri (**start, stop**) cu structură fixă.

Există trei tipuri de cadre în protocolul HDLC folosite pentru scopuri diferite:

I (**informațional** pentru cadre ce conțin informație de la utilizatori), **S** (**supraveghere**, pentru controlul erorilor) şi **U** (**unnumbered** pentru stabilirea legăturii).

Conținutul câmpului *Control* este specific fiecăruia dintre aceste tipuri.

Tipul de cadru se identifică prin primul bit (0 la tipul I) sau primii doi biți (10 la tipul S, respectiv 11 la tipul U).

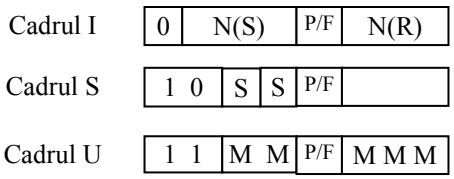


Fig. 3.4. Câmpul de control la cele trei tipuri de cadre

Cei doi biți S din pozițiile 3 şi 4 arată patru cadre S posibile, dar sunt folosite doar trei, după cum urmează.

00 Gata de recepție (RR)	*N(R) validează toate cadrele recepționate până la N(R)-1 inclusiv*
10 Nu este gata de rec (RNR)	*Controlează transmiterea prin blocare temporară. Validează recepția până la N(R)-1*
Reject (REJ)	*Rejectează toate cadrele de la N(R), dar le validează până a N(R)-1*

Câmpul N(S) din cadrul I arată ordinea cadrului. Fiecare cadru succesiv creşte secvenţa N(S) cu 1. Având trei poziţii, înseamnă că se pot transmite 8 cadre succesive după care transmisia se opreşte aşteptând confirmarea.

Cei 5 biţi M din cadrul U arată 32 de cadre de stabilirea legăturii posibile de transmis. În protocolul HDLC sunt definite **4 moduri de operare**:

1. **Modul cu răspuns normal (NRM)** folosit în mediul cu control centralizat. Este potrivit în lucrul multipunct, în care o staţie primară comunică cu mai multe staţii secundare. Staţiile secundare pot iniţia o comunicare numai cu permisiunea staţiei centrale care a iniţiat comunicarea.
2. **Modul cu răspuns asincron (ARM)** este similar NRM cu excepţia faptului că staţia secundară nu necesită permisiunea staţiei primare pentru a iniţia o comunicare.
3. **Modul asincron echilibrat (ABM)** este pentru transmisia punct la punct între parteneri egali. Este folosită în X.25.

Câmpul P/F de un bit (Poll/Final – Test/Final) este folosit când un calculator sau un concentrator interoghează un grup de terminale. Când este setat pe P, calculatorul invită terminalul să transmită date. Toate cadrele transmise de terminal au câmpul setat pe P, cu excepţia cadrului final (când nu mai are date de transmis) care are valoarea setată pe F. Prin urmare, HDLC poate implementa un mecanism de comandă folosind bitul P/F şi câmpul de adresă.

3.3 Nivelul LD în Internet

Protocolul punct la punct (PPP)

Este definit de RFC 1661 şi dezvoltat în alte RFC (1662, 1663**).**
PPP face detecţia erorilor, suportă mai multe protocoale, permite negocierea adreselor IP în momentul conectării, autentificarea şi alte funcţii.

PPP furnizează trei lucruri:
1. **o metodă de împărţire în cadre,** format care permite detecţia erorilor;
2**. un protocol al legăturii** pentru a **obţine liniile, a le testa şi a negocia opţiunile** iar la terminarea transmisiei **eliberarea** lor. Acest protocol se numeşte **LCP** (**Link Control Procedure**). El suportă comunicaţii sincrone şi asincrone;
3. **un mod de a negocia opţiunile nivelului reţea** printr-un protocol de control al reţelei (**NCP – Network Control Protocol**).

Un scenariu tipic de folosire a PPP este următorul. Un calculator apelează de la domiciliu un furnizor de servicii Internet, conecându-se la ruterul acestuia printr-un modem. După stabilirea legăturii telefonice, calculatorul trimite o serie de pachete LCP în câmpul de informaţie al unuia sau mai multor cadre PPP. Aceste pachete şi răspunsurile lor selectează parametrii PPP care vor fi utilizaţi. După ce s-

au pus de acord asupra acestor parametrii, se transmit mai multe pachete NCP pentru a configura nivelul rețea.

Formatul cadrului PPP este asemănător cu cel al cadrului HDLC, doar că primul este orientat pe caracter şi nu pe bit. Toate cadrele PPP trebuie să aibă un număr întreg de octeți. Cadrele PPP pot fi transmise pe linii comutate, linii închiriate, linii SDH/SONET, etc.

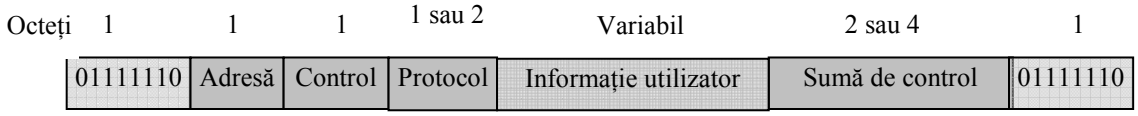


Fig. 3.5 Formatul cadrului PPP pentru operare nenumerotat

Indicatoarele de început şi de sfârşit au acelaşi format ca la HDLC. *Adresa* este setată inițial la 11111111 determinând toate stațiile să accepte cadrul. *Controlul* are valoarea implicită 00000011 indicând cadru nenumerotat. Câmpul *Protocol* indică ce tip de pachet este în câmpul de informație utilă: LCP, NCP, IP, IPX, Apple Talk şi altele. Protocoalele care încep cu 0 sunt de nivel rețea (IP, IPX, XNS, OSI CLNP). Cele care încep cu 1 sunt folosite pentru a negocia alte protocoale. Câmpul *Informație utilizator* are lungimea implicită 1500 octeți, dar poate fi negociat folosind LCP.

Prin urmare, PPP este un mecanism de încadrare multiprotocol potrivit pentru linii cu modem, linii seriale orientate pe bit (HDLC, SDH) etc.

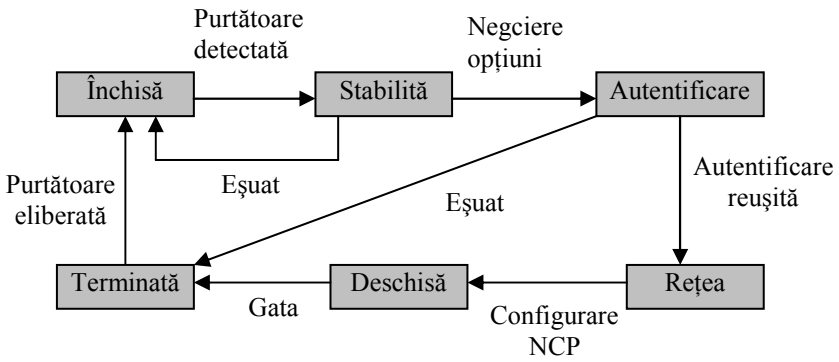


Fig. 3.6 Diagrama de faze la stabilirea şi eliberarea unei linii

PPP nu este un simplu protocol de transfer de date între două noduri din rețea. El permite deschiderea legăturii sau refuzul acesteia, negocierea unor opțiuni, recunoaşterea reciprocă a gazdelor corespondente etc. Prin urmare, o linie de legătură dintre două noduri vecine trece prin mai multe stări care pot fi evidențiate pe diagrama de faze din fig. 3.6.

În repaus linia este închisă. Protocolul se inițializează cu această stare, semnificând că nu există purtătoare la nivel fizic şi nici o conexiune fizică. După stabilirea legăturii, linia trece în starea *Stabilită* şi începe negocierea opțională LCP, care dacă reuşeşte conduce la *Autentificarea* reciprocă a corespondenților. Apoi se intră în faza *Rețea* când este apelat protocolul NCP pentru a configura nivelul rețea. Dacă configurarea reuşeşte, se trece în starea *Deschisă* şi poate începe transferul datelor. La

terminarea transferului datelor, linia trece în starea *Terminată* când nu se mai transmit date, dar există încă legătură fizică (purtătoare). De aici se trece în faza *Închisă* când este întreruptă şi purtătoarea.

3.4 Subnivelul controlul accesului la mediu (MAC)

Problema controlului accesului la mediu se pune atunci când un număr oarecare de utilizatori trebuie să folosească în comun (să partajeze) acelaşi mediu de transmisie. Mediul de transmisie poate fi considerat în acest caz ca un **canal de difuzare** sau un **canal multiacces** sau un **canal cu acces aleator**. Protocolul care rezolvă problema accesului simultan a utilizatorilor la acelaşi mediu fizic de transmisie aparține unui subnivel al legăturii de date, subnivelul MAC. El este foarte important în LAN-uri.

O posibilă rezolvare, dar greu de acceptat din diverse motive, este **alocarea statică** prin diviziune în timp (TDM) sau în frecvență (FDM) sau în cod (CDM). Fiecărui utilizator i se alocă un spațiu de timp sau de frecvență sau un cod, pe care le poate folosi când are nevoie. Alocarea este ineficientă în cazul în care un număr foarte mare de utilizatori folosesc puțin şi aleator mediul de transmisie.

Alocarea dinamică permite accesul abonaților la mediu după anumite reguli care pot asigura utilizarea eficientă a acestuia.

3.4.1 Protocoale MAC cu detecție de purtătoare

CSMA cu detecția coliziunii (CSMA/CD). Când două stații găsesc canalul liber şi încep emisia simultan, vor detecta imediat şi coliziunea şi opresc imediat transmisia cadrelor care oricum se pierd. Astfel se gâştigă oarece timp în care canalul este ocupat. Protocolul CSMA/CD este larg folosit în LAN-urile Ethernet. Există şi alte variante de protocoale de acces cu detecție de purtătoare (CSMA/CA, etc.)

3.4.2 Protocoale MAC cu jeton

O altă posibilitate de a evita coliziunile constă în folosirea unui jeton (un cadru special de control) care circulă pe mediul fizic. O stație care dorește să transmită date captează jetonul şi astfel nici o altă stație nu mai poate transmite. După ce a terminat transmisia, stația care deținea jetonul îl eliberează pentru a putea fi folosit de o altă stație. În funcție de topologia rețelei, există protocoale cu jeton pe magistrală (IEEE 802.4) sau pe inel (IEEE 802.5).

Seria de standarde IEEE 802 cuprinde:
802.1 – Principiile generale şi arhitectura LAN-urilor
802.2 - LLC (Logical Link Control)
802.3 – Ehternet (CSMA-CD)
802.3u – Ethernet rapid

802.4 – Token bus
802.5 – Token ring
802.6 – DQDB (Dual Queue Dual Bus), standard de MAN
802.9 – LAN-uri izocrone pentru aplicații în timp real
802.10 – LAN-uri virtuale şi securitate
802.11 – LAN-uri fără fir
802.14 – Modemuri de cabluri
802.15 – Rețele personale (Bluetooth)
802.16 – WAN de bandă largă fără fir

3.4.3 Standardul 802.3 Ethernet

În general un LAN conține un număr oarecare de calculatoare (utilizatori) conectați împreună la un mediu de transmisie comun, pe care îl folosesc în mod partajat. Datele trimise pe mediul de comunicație sunt distribuite la toți utilizatorii, dar recepția se face doar de către cel căruia îi sunt adresate prin specificația de adresă. Un astfel de LAN formează ceeace se numeşte un "**domeniu de coliziune**". La un moment dat pe un mediu comun de transmisie nu pot exita date decât de la un singur transmițător, altfel semnalele se amestecă şi se perturbă între ele. Pentru a evita coliziunile, standardul Ethernet foloseşte tehnica **CSMA CD (Carrier Sense Multiple Access with Collision Detection**). Când o stație doreşte să transmită date, ascultă mediul. Dacă este ocupat aşteaptă un timp aleator, după care încearcă o nouă transmisie. Dacă este liber transmite imediat.

Structura cadrului Ethernet

Din punct de vedere al cadrului Ethernet, protocolul oferă trei tipuri de informații: **identificarea entităților sursă şi destinație de nivel fizic** ce comunică între ele, precizarea **protocolului de nivel superior** şi o **sumă de control** pentru verificarea integrității datelor.

Structura cadrului Ethernet este aproape identică, indiferent de varianta de Ethernet folosită, şi conține următoarele câmpuri:

- Preambul
- Început de cadru 1 octet
- Adresa destinație - 6 octeți
- Adresa sursă - 6 octeți
- Lungime/Tip (Type field) - 2 octeți
- Date - 46 ÷ 1500 octeți
- FCS - 4 octeți

Preambul (7 octeți) pentru sincronizarea ceasului receptorului este de forma 1010
Început de cadru (un octet) de forma 10101011

Adresa sursă şi *Adresa destinaţie* sunt adresele fizice ale echipamentelor (adrese MAC).

Câmpul *Lungime/Tip* are doi octeţi şi arată lungimea câmpului de date. El poate fi interpretat în două feluri: dacă valoarea acestuia este mai mică de 1536 (0x600 în hexazecimal) atunci el reprezintă lungimea. Dacă este mai mare de 1536, el reprezintă protocolul de nivel superior folosit.

Câmpul de ***date*** trebuie să fie mai mare de 46 de octeţi. Dacă cumva datele sunt de lungime mai mică, atunci i se adaugă o "umplutură" numită padding pentru a ajunge la dimensiunea de 46 octeţi. Acest câmp nu are voie să depăşească valoarea MTU - Maximum Transmission Unit - care pentru Ethernet este 1500 octeţi, ceea ce înseamnă că un cadru Ethernet nu are voie să fie mai mic de 64 şi mai mare de 1518 octeţi .

Câmpul de control **FCS** este adăugat în cadru pentru a determina dacă nu cumva au apărut eroari în timpul transmisiei.

Câmpul de completare (***pad***) de 0...46 octeţi este folosit atunci când câmpul de date are mai puţin de 64 octeţi şi pot apărea probleme de detecţie a coliziunilor. Explicaţia este următoarea: o staţie găseşte linia liberă şi începe să emită. Înainte ca şirul de biţi să ajungă le cea mai îndepărtată staţie, aceasta găsind linia liberă, emite şi ea şi, ca urmare, apare o coliziune. Pentru a detecta o coliziune, durata unei transmisii trebuie să dureze mai mult decât o valoare minimă care depinde de distanţa dintre staţiile cele mai îndepărtate. Pentru un LAN de 10 Mbps, cu lungimea cablului de 2500 m şi 4 repetoare, cadrul minim trebuie să dureze 51,2 μs. Aceasta cuprinde minimum 64 octeţi, deci pentru date minimum 46 octeţi.

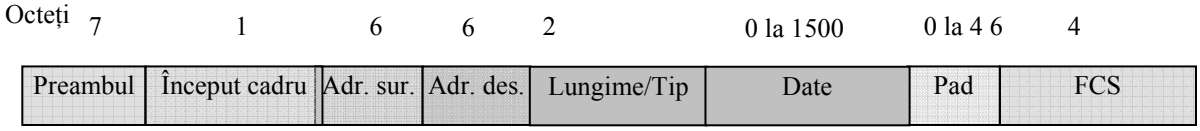


Fig. 3.8 Formatul de cadru Ethernet

3.4.4 Ethernet comutat

O soluţie de evitarea coliziunilor este **Ethernetul comutat,** bazat pe comutator. Comutatorul este capabil să selecteze cadrele după adresă şi să le trimită direct spre destinaţie fără a mai inunda toată reţeaua şi a pune în funcţiune mecanismul CSMA – CD.

Observaţie: Comutatorul distribuie cadrele doar în interiorul unui LAN. El nu poate trimite cadre înter alte reţele.

Principalele funcţii ale unui comutator sunt: **învăţarea adreselor fizice** (crearea şi completarea tabelei de comutare, munită uneori şi tabelă MAC) şi **direcţionarea cadrelor** de pe o interfaţă de intrare spre una de ieşire.

O tabelă de comutare conţine în principal două câmpuri: **adresa MAC destinaţie** şi **interfaţa de ieşire** prin care se poate ajunge la acea destinaţie. Ea se păstrează în memoria RAM a comutatorului şi se pierde la închiderea acestuia.

Host	Adresa MAC destinație	Interfață
A1	00.00.53.40.9.01.12	E0
A2	00.00.44.20.58.22.91	E0
A3	00.48.33.60.90.04.4A	E1

Suplimentar

Pentru a înțelege cum se construieşte tabela de comutare, cum învață comutatoarele să-şi construiască tabela MAC, să analizăm figura de mai jos.

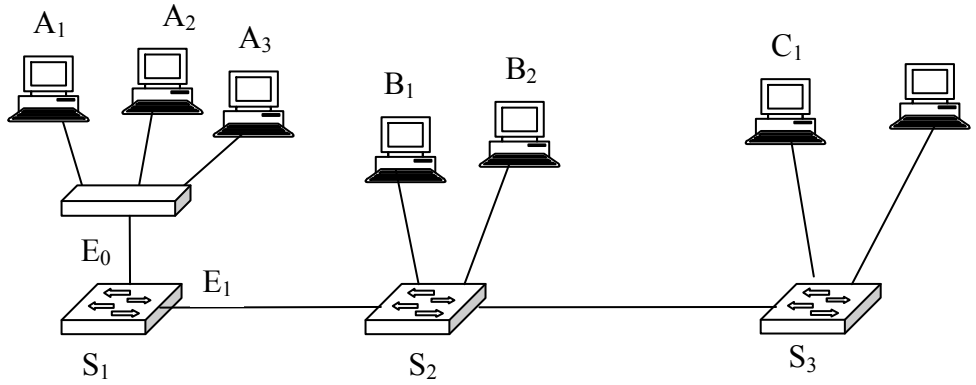


Fig.3.9 Segmentarea unui LAN folosind comutatoare

Să presupunem că se porneşte comutatorul S1 şi că staţia A1 vrea să comunice cu staţia B1. Ea ascultă mediul şi când este liber emite un cadru cu adresa destinaţie a lui B1 şi îl trimite comutatorului S1 la care este conectat. S1 caută în tabela sa de comutare şi deoarece nu găseşte această înregistrare, trimite cadrul pe toate interfeţele sale, mai puţin de unde a venit (face inundare). În acelaşi timp verifică dacă adresa sursă de unde a venit cadrul se găseşte în tabelă. Dacă nu o găseşte (şi aceasta este situaţia deoarece S1 abia a fost deschis), o înregistrează împreună cu interfaţa E0 de pe care a venit cadrul, "stiind" de acum că segmentul A al reţelei poate fi atins prin acea interfaţă. Cadrul ajunge în comutatorul S2 unde este consultată tabela de comutare a acestuia. Dacă în tabelă se găseşte înregistrarea cu adresa şi interfaţa lui B1, atunci cadrul este trimis acolo. Dacă nu, se repetă procedura inundării şi de către S2 şi cadrul va ajunge oricum la destinaţie. Pentru ca şi înregistrarea lui B1 să apară în tabela lui S2, este necesar ca B1 să emită un cadru spre oricare destinaţie. Deoarece la nivel LD ne se foloseşte o schemă de comutare ierarhică cum este cazul la nivel reţea, tabelele de comutare trebuie să conţină înregistrări despre toate gazdele din reţea, nu numai ale celor din segmentul dat. Asta face ca dimensiunile tabelelor să fie mari.

Dacă tabelele de comutare sunt mari şi neordonate, căutarea în acestea poate deveni o problemă grea, consumatoare de timp. De aceea înregistrările din tabelă pot fi însoţite de un contor de timp care se resetează la fiecare folosire a înregistrării. Rolul său este de a şterge acele înregistrări care nu sunt folosite un anumit interval de timp, simplificând astfel dimensiunea tabelelor.

Care este rolul comutatorului în segmentarea unei rețele? Urmarind fig. 3.9 să presupunem că A1 vrea să comunice cu A2. El trimite un pachet pe hub care se va distribui tuturor echipamentelor conectate la acesta, inclusiv la comutatorul S1. A2 va recepționa pachetul care îi este destinat, iar toate celelalte calculatoare de pe segmentul A îl vor ignora. Comutatorul S1 văzând că el este destinat segmentului A, nu îl va trimite spre alte segmente, deci el va rămâne localizat în segmentul A. Dacă în locul lui S1 ar fi fost un hub, acesta ar fi difuzat pachetul şi spre alte segmente întrucât hub-ul nu face selecție pe bază de adrese MAC.

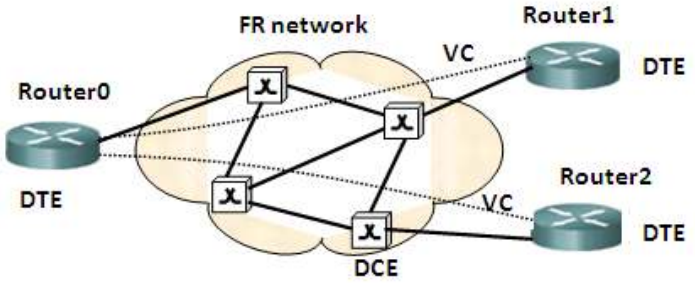
Cum funcționează comutatorul S2 pentru segmentul B? Dacă B1 vrea să comunice cu B2, el trimite un pachet cu adresa destinație la comutatorul S2. Acesta analizaeză antetul pachetului, citeşte adresa destinație şi pe baza tabelului de comutare trimite pachetul direct spre B2. În acelaşi timp un alt calculator din segmentul B poate trimite pachete spre alte destinații fără a fi influențat de comunicația dintre B1 şi B2.

Comutatorul izolează comunicația unicast între stații aflate în acelaşi segment la nivelul segmentului. Consecințele acestu fapt sunt deosebit de importante. În primul rând comutatorul limitează domeniile de coliziune. Totodată, el oferă mai mai multă bandă disponibilă deoarece comunicația din interiorul unui segment nu consumă din banda disponibilă întregii rețele.

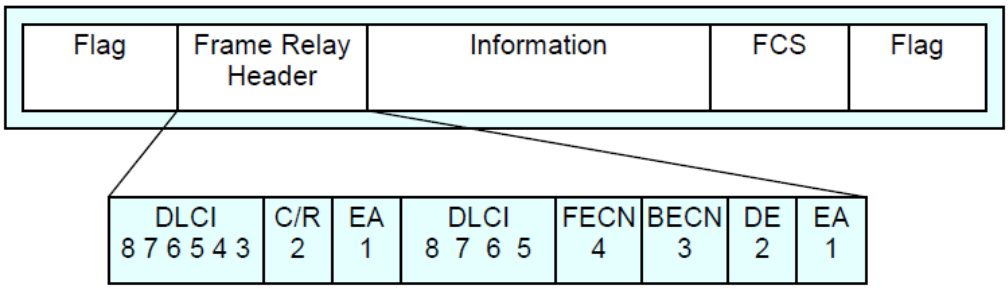
O altă consecință o reprezintă minimizarea riscurilor de securitate legate de atacurile din interiorul rețelei locale. Unul din cele mai populare atacuri este ascultarea liniei (sniffing attack) prin care se forțează nivelul legătură de date de pe una din stațiile conectate la mediul distribuit să trimită spre nivelele superioare toate cadrele, inclusiv cele care nu sunt desztinate acestei stații. În felul acesta se păoate monitoriza tot traficul ce traversează un segment de rețea. Folosireea comutatoarelor poate izola de restul rețelei acele stații susceptibile de ascultare.

3.4.5 Serviciul Frame Rrelay

Frame Relay este o tehnologie de comunicație la nivel legătură de date, orientată pe conexiune care folosește un format specific de cadre de date numite **frame relay**. Într-o rețea Frame Relay se stabilește o **conexiune virtuală** (VC) între fiecare pereche de echipamente terminale de date (DTE), conexiunea fiind specificată printr-un identificator de conexiune (**data-link connection identifier - DLCI**). Pe o cale fizică dintre două echipamente de date pot fi multiplexate simultan mai multe circuite virtuale.



Elemente constitutive într-o rețea FR



Cadrul FR

Cadrul FR are o structură asemănătoare cu protocolul LAPD şi se vede în figura următoare. Antetul cadrului are următoarele câmpuri:

DLCI de lungime 10 biți, reprezentând identificatorul (adresa) circuitului virtual permanent.

C/R specifică faprul că un cadru este o cerere sau un răspuns

EA adresa extinsă specifică faptul că o adresă FR poate fi extinsă pe un număr mai mare de biți.

FECN (Forward Explicit Congestion Notification) este un flag de notificare spre destinație a apariției congestiei.

BECN (Aackward Explicit Congestion Notification) este un flag de notificare spre sursă a apariției congestiei. Cei doi biți sunt folosiți în mecanismul de control al congestiei prin reducerea ratei de transmitere a cadrelor.

DE (Discard Eligibility) este un bit de control care arată că un cadru poate fi descărcat în cazul apariției congestiei.

Information se referă la faptul că un cadru FR poate încapsula alte cadre de la alte protocoale, de exemplu X.25, IP, SDLC etc.

Un **circuit virtual permanent (PVC)** dintr-o rețea FR este o legătură logică ale cărei puncte finale şi clasă de servicii au fost definite de managementul de rețea. Un PVC constă din adresa elementului de rețea de origine, DLCI-ul de origine, adresa elementului de rețea destinație şi DLCI-ul destinație. Termenul "origine" se referă la interfața de acces unde este inițiat PVC, iar "destinație" se referă la interfața unde PVC se termină. Este de reținut că FR oferă legături punct la punct, aşa cum solicită mulți clienți din rețea. În interiorul rețelei, comutarea cadrelor se face de către comutatoare specific (**FR switches**) numite DCE (**Data Communications Equipment)** care folosesc identificatorul de circuit ca adresă de comutare.

LMI - **Local Management Interface** este un protocol standard de semnalizare folosit între un ruter (DTE) şi primul switch FR (DCE) responsabil de crearea şi menținerea conexiunilor şi statutului conexiuniilor virtuale permanante. El asigură

- Un mechanism keep-alive care verifică dacă se transmit date
- Stabileşte conexiuni unicast si alocă DLCI-uri
- Indică starea tuturor circuitelor virtual cunoscute pe switch

În acest scop, echipamentele transmit mesaje LMI de tipul Hello, Status Request şi Status Report la interval de timp prestabilite sau configurate explicit.
Mesajele de stare a interfețelor locale de management (LMI - **Local Management Interface)** a circuitelor virtuale asigură comunicarea şi sincronizarea dintre dispozitivele FR DTE şi DCE. Aceste mesaje sunt folosite pentru a raporta periodic starea PVC-urilor şi a preveni livrarea datelor spre "găuri negre", adică acolo unde nu mai sunt PVC.

Se poate folosi protocolul Frame Relay ARP invers pentru a construi rute dinamice în rețele FR care rulează IP. ARP invers permite serverului de comunicații să descopere adresa de protocol a unui dispozitiv asociat unui circuit virtual. ARP invers este utilizat în locul comenzii frame relay de mapare care permite stabilirea corespondenței (maparea) între un protocol specific, adresa şi un DLCI specific. ARP invers nu este necesar pentru interfețe punct la punct deoarece există o singură destinație şi nu este necesară descoperirea ei.

FR nu are mecanisme de refacere (corecție) a erorilor, ci doar un mechanism CRC de detecție a acestora. În schimb, FR are mecanisme de control al congestiei prin controlul ratei de transmisie, inclusive de aruncare a unor cadre în caz de congestie.

Rețeaua FR asigură conexiuni non-broadcast multiacces, adică este o rețea NBMA, deosebire majoră față de Ethernet, care este o rețea broadcast multiacces.

Termeni Frame Relay

Termen	Descriere
Virtual Circuit (VC)	Logical path that connects routers
Permanent Virtual Circuit (PVC)	A predefined VC (equated to leased line)
Switched Virtual Circuit (SVC)	Dial connection in concept
Data Terminal Equipment	Devices connected to Frame Relay Service

(DTE)	
Data Communications Equipment (DCE)	Frame Relay switches, typically in service provider's network.
Access Link	Leased line between DTE and DCE
Access Rate (AR)	Speed at which access link is clocked.
Data-link Connection Identifier (DLCI)	Frame Relay address used in headers to identify the VC
Nonbroadcast Multiaccess (NBMA)	Broadcasts not supported, but more than 2 devices can be connected
Local Management Interface	Protocol used between DCE and DTE, manages the connection (signaling messages, keepalive messages).

Frame Relay Standards

What specification defines	ITU Document	ANSI Document
Data-link specifications (LAPF header/trailer)	Q.922-A	T1.618
PVC Management, LMI	Q.933-A	T1.617-D
SVC Signaling	Q.933	T1.617
Multiprotocol encapsulation	Q.933-E	T1.617-F

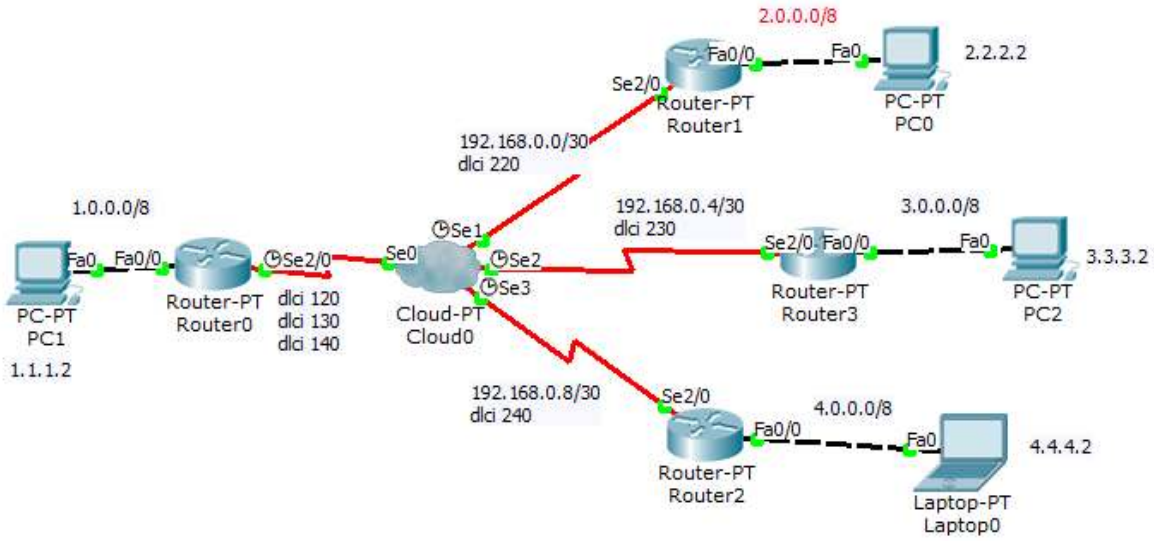
Exemplu de rețea FR configurată pe rutere Cisco

Interfața S2/0 a ruterului R0 este configurată cu trei subinterfețe în scopul creerii a trei conexiuni virtuale din rețeaua 10.0.0.0/24 spre rețelele 2.0.0.0/24, 3.0.0.0/24 şi 4.0.0.0/24. Conexiunile virtuale sunt stabilite prin configurarea tabelei de comutare FR din cloud, care este un simulator de switch FR.

FR switching map

From Port	Sublink	To Port	Sublink
Serial0	aa	Serial1	aaa
Serial0	bb	Serial2	bbb
Serial0	cc	Serial3	ccc

Topologia rețelei FR şi un exemplu de configurare a ruterelor R0 şi R1 se văd în figura de mai jos.



R0#Show running

interface FastEthernet0/0
ip address 1.1.1.1 255.0.0.0
duplex auto
speed auto
interface Serial2/0
noip address
encapsulation frame-relay
clock rate 56000
!
interface Serial2/0.1 point-to-point
ip address 192.168.0.1 255.255.255.252
frame-relay interface-dlci 120
!
interface Serial2/0.2 point-to-point
ip address 192.168.0.5 255.255.255.252
frame-relay interface-dlci 130
interface Serial2/0.3 point-to-point
ip address 192.168.0.9 255.255.255.252
frame-relay interface-dlci 140
ip route 2.0.0.0 255.0.0.0 192.168.0.2
ip route 3.0.0.0 255.0.0.0 192.168.0.6
ip route 4.0.0.0 255.0.0.0 192.168.0.10

R1#show running

interface FastEthernet0/0
ip address 2.2.2.1 255.0.0.0
duplex auto
speed auto
!
interface Serial2/0
ip address 192.168.0.2 255.255.255.252
encapsulation frame-relay
frame-relay interface-dlci 220
R2#show run
interface FastEthernet0/0
ip address 3.3.3.1 255.0.0.0
duplex auto
speed auto
!
interface Serial2/0
ip address 192.168.0.6 255.255.255.252
encapsulation frame-relay
frame-relay interface-dlci 230
!
ip route 1.0.0.0 255.0.0.0 192.168.0.5

3.5 LAN- uri fără fir

3.5.1 Stiva de protocoale 802.11

Nivelul fizic este aproape acelaşi ca la nivelul fizic OSI, dar la nivelul LD sunt diferențiate clar subnivelele MAC şi LLC în scopul ascunderii față de nivelul rețea a diferențelor dintre variantele 802.x.

Elaborat în 1997, standardul 802.11 specifică la nivelul fizic trei tehnici de transmisie:

- **infraroşu (IR);**
- **radio pe 2,4 GHz** folosind tehnica **saltului de frecvență FHSS sau DSSS,** cu o rată de transmisie a datelor de 1÷2Mbps;
- **radio de bandă largă tot în banda 2,4 GHz tot cu salt de frecvență în bandă largă (OFDM sau HR-DSSS)** asigurând viteze de transmitere a datelor de **11 Mbps** sau **54 Mbps.**

Tehnica IR foloseşte lungimile de undă din fereastra I-a (850 nm) sau fereastra a II-a (1300nm) a sticlei de cuarț cu propagare în spațiul liber (**FSO - Free Space Optics**) cu difuzare prin reflexii multiple pe obiectele din mediu.

Tehnicile radio folosesc saltul de frecvență sub diferite moduri.

FHSS (**Frequency Hopping Spread Spectrum** – spectru împrăştiat cu salt de frecvență) foloseşte un număr de canale radio plasate în partea inferioară a benzii de 2,4 GHz în care emițătorul sare aleator de pe un canal pe altul. Salturile de frecvență sunt comandate de un generator de numere pseudoaleatoare. Acelaşi tip de generator trebuie să comande şi salturile de frecvență de la recepție. În plus tehnicile cu salt de frecvență necesită o sincronizare foarte bună între emițător şi receptor.

Metoda **DSSS** (**Direct Sequence Spread Spectrum** – spectru împrăştat cu secvență directă) este asemănătoare cu **CDMA** (**Code Division Multiple Access** – acces multiplu cu diviziune în cod). Fiecare bit este transmis ca o o secvență de 11 fragmente generate pe baza unui cod aleator.

Metoda **OFDM** (**Orthogonal Frequencies Division Multiplexing** – multiplexare cu diviziune în frecvențe ortogonale) foloseşte un set de 52 de frecvențe ortogonele (48 pentru date şi 4 pentru sincronizare) şi permite rate de până la 54 Mbps. Este tot o formă de împrăştiere a spectrului pe frecvențe ortogonale, adică frecvențe care nu se suprapun ca valoare în nici un moment al transmisiei. Frecvențele sunt modulate diferit în funcție de rata transmisiei: PSK la viteze mici sau QAM la viteze mari.

HR-DSSS (**High Rate – DSSS** - secvență directă de mare viteză) este o altă tehnică de spectru larg care foloseşte 11 milioane de fragmente pe secundă pentru a obține rate de 11 Mbps în banda 2,4 GHz.

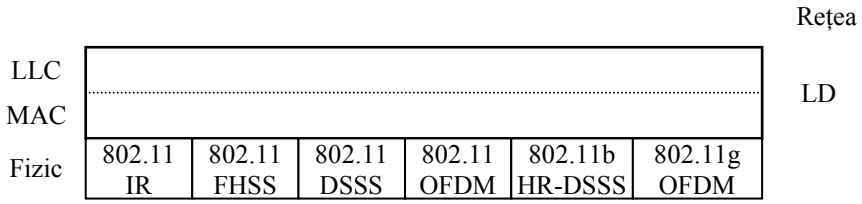


Fig. 3.11 Partea fizică a stivei 802.11

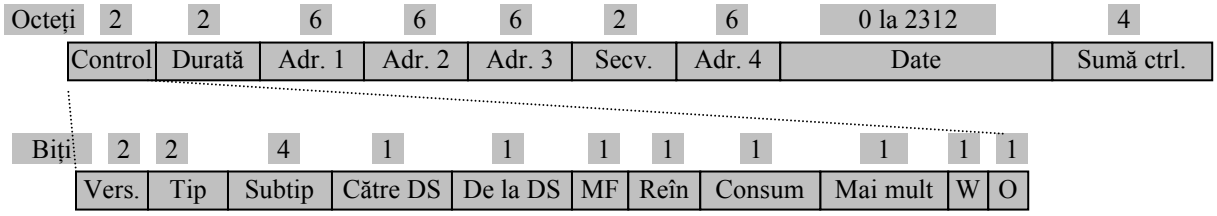


Fig. 3.12 Cadrul 802.11

Formatul cadrului 802.11 este prezentat în fig. 3.12

Vers. – arată versiunea de protocol
Subtip – subtipul de cadru. RTS- Request for Transmission, CTS- Confirm For Transmission
Către DS, De la DS – arată sensul de transmitere (către distribuție, de la distribuție)
MF – More Fragments arată că vor urma mai multe fragmente
Reîn (cercare) – arată o retransmisie a cadrului anterior
W (wired equivalent privacy) se referă la confidențialitate.

3.5.2. Servicii asigurate de standardul 802.11

Fiecărei stații locale fără fir trebuie să i se asigure 9 servicii, 5 legate de distribuție şi 4 pentru stații. Serviciile legate de distribuție se referă la gestiunea apartenenței la celulă şi interacțiunea cu stațiile din sfera celulei. Ele sunt:

1 **Asociere**a – conectarea stației mobile la bază. Când o stație mobilă intră în raza de acțiune a unei stații de bază ea îşi anunță identitatea şi capacitățile (viteze suportate, cereri de servicii PCF(Point Coordination Functions)etc. Cererea de asociere poate fi acceptată sau nu.

2 **Dezasocierea** – se poate iniția de stația mobilă sau de stația de bază. Operația trebuie făcută înainte de închiderea stației sau de ieşirea ei din raza de acțiune.

3 **Reasocierea** - revenirea în zona stației de bază înainte de a fi dezasociată

4 **Distribuția**

5 **Integrarea** – adaptarea cadrului la formatul cadrului intern ai 802.11

Serviciile în interiorul celulei sunt:

1 **Autentificarea** – numai stațiile autorizate şi autentificate se pot conecta în celulă la LAN.

2 **Deautentificarea** – când o stație dorește să părăsească rețeaua ea este scoasă din evidență Reinserarea se poate face numai prin autentificare.

3 **Confidențialitatea** – este asigurată prin serviciul de criptare. Algoritmul de criptare folosit este RC4 (inventat de R. Rivest).

4. **Livrarea datelor** – este funcția principală a standardului. Ca şi la Ethernet, livrarea nu este sigură 100%, nivelurile superioare având sarcina de a rezolva problemele.

3.5.3 Rețele fără fir de bandă largă (IEEE 802.16) Suplimentar

*În acest sens a fost elaborat standardul 802.16 început în 1999 şi finalizat în 2002, numit **wireless MAN** sau **wireless local loop**.*

El se deosebeşte esențial de 802.11 şi rezolvă probleme diferite. Standardul 802.16 asigură legături MAN între locații fixe (clădiri), pe când 802.11 asigură conectarea abonaților mobili în LAN. Banda de trecere a acestei rețele este mult mai mare deoarece şi traficul dintre clădiri sau alte locații fixe este mare.

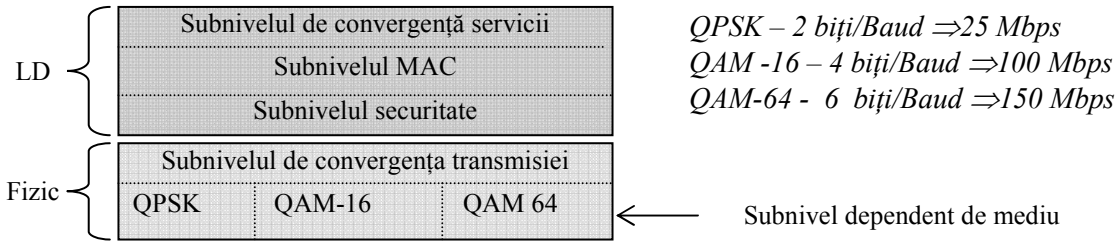


Fig. 3.13 Structura protocoalelor 802.16

Se foloseşte banda de frecvențe de peste 10 GHz care este mai puțin aglomerată şi poate ajunge până la 66 GHz.

Aici particularitățile propagării undelor milimetrice fac posibile legături punct la punct mai uşoare decât difuzarea. 802.11 este o interețea mobilă, pe când 802.16 este o rețea staționară, ca o rețea TV pe cablu. Nivelul fizic foloseşte unde milimetrice în banda 10 ÷66 GHz cu propagare rectilinie, aproape ca lumina, cu posibilitatea montării mai multor antene directive pe acelaşi catarg.

Nivelul fizic** este împărțit în două subnivele: **subnivelul dependent de mediul fizic** şi **subnivelul de convergență a transmisiei.

*Subnivelul convergența transmisiei are rolul de a ascunde diferitele tehnologii de transmisie folosite pe mediul fizic. Nivelul LD are 3 subnivele. Primul de jos rezolvă **probleme de securitate**: criptare, gestiune chei etc. Acest lucru este necesar deoarece standardul 802.16 foloseşte transmisia în mediu deschis şi posibilitatea intercepției nedorite a comunicației este mare. Următorul rezolvă problema **accesului la mediu**. Modelul presupune că stația de bază controlează sistemul pentru accesul abonaților. **Subnivelul convergență servicii** asigură legătura cu celelalte protocoale 802 (interfațarea cu nivelul rețea). El poate lucra direct cu PPP, IP, Ethernet, ATM, cu protocoale*

orientate pe conexiune sau neorientate pe conexiune. Pentru a rezolva problema legăturilor bilaterale (duplex) şi de regulă nesimetrice(recepţia mai mare decât emisia), se folosesc două tehnici: FDD (Frequency Division Duplexing) şi TDD (Time Division Duplexing.

Toate ***serviciile standardului 802.16 sunt orientate pe conexiune****. Fiecare conexiune este stabilită la configurare şi asigură următoarele servicii:*

- *serviciu cu viteză constantă la transmisie;*
- *serviciu pentru aplicaţii de transfer de date în timp real;*
- *servicii care nu necesită transfer în timp real;*
- *servicii de tipul cea mai bună încercare (best effort).*

Arhitectura este diferită de 802.11 şi de Ethernet care nu prezintă conexiuni la nivel MAC. Serviciul cu viteză constantă este folosit când se face transfer de voce necomprimată, la fel ca pe canalele E_1/T_1. Acest serviciu are nevoie de a transmite o cantitate predeterminată de date într-un timp stabilit apriori. Fiecărei conexiuni de acest fel i se alocă un număr predeterminat de intervale de timp (alocare fixă de bandă). Serviciul cu aplicaţii în timp real este destinat aplicaţiilor media compresate în care banda alocată poate varia. Alocarea se face dinamic, funcţie de nevoile de moment ale transmiţătorului.

3.4.4 Bluetooth (IEEE 802.15) Suplimentar

Unitatea de bază a unei asemenea reţele este o picoreţea formată dintr-un nod master şi până la 7 staţii slave, toate situate într-o regiune cu diametru până la 10 m. O colecţie interconectată de asemenea piconeturi este denumită scatternet (reţea dispersată). Un piconet este un sistem TDM centralizat în care sclavii fac doar ceea ce spune stăpânul.

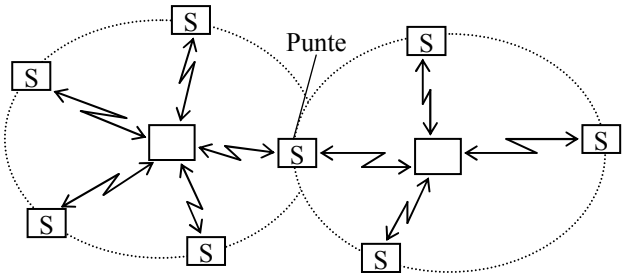


Fig. 3.12 Structură de reţea Bluetooth

Stiva de protocoale Bluetooth nu respectă nici modelul OSI, nici TCP/IP, nici 802 sau altele. Este o suită ad-hoc de protocoale ierarhizată aproximativ pe 4 nivele.

Nivelul radio funcţionează în banda 2,4 GHz. Banda este divizată în 79 de canale de câte 1 MHz fiecare, cu o acoperire de 10 m. Modularea cu un bit pe hertz asigură o rată de transfer de 1Mbps. Se foloseşte tehnica FHSS cu 1600 de salturi/s. Rolul nivelului radio este de a transmite biţi de la stăpân la sclav şi invers.

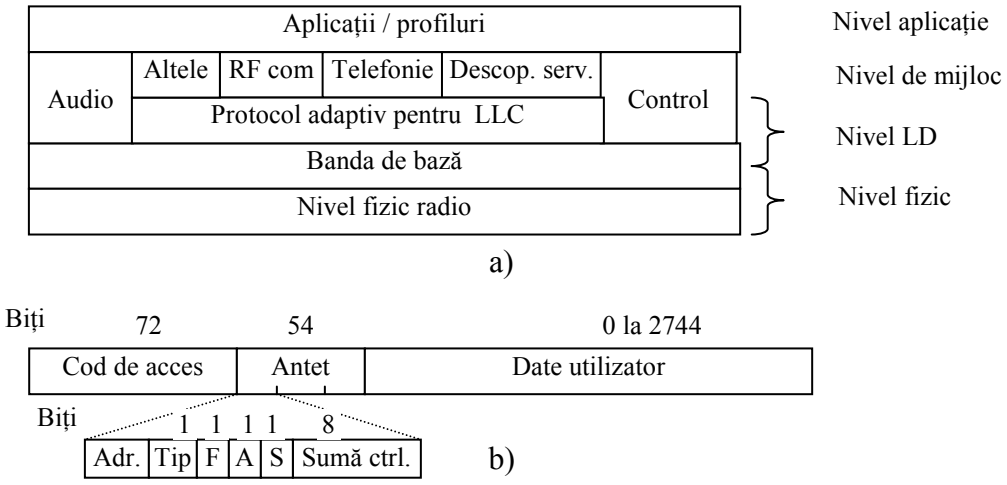


Fig.3.15 Standardul Bluetooth a) arhitectura b) formatul de cadru

Nivelul bandă de bază rezolvă unele probleme lgate de controlul accesului la mediu. Stăpânul dintr-un piconet defineşte o serie de cuante de timp de 625 μs. În cuantele pare transmite stăpânul, în cele impare sclavii. Stăpânul are la dispoziție jumătate din timp, iar sclavii împart cealaltă jumătate.

Nivelul L2CAP (Logical Link Control Adaptation Protocol) are trei funcții majore. Prima este de a accepta la transmisie pachete până la 64 kB de la nivelurile superioare şi a le sparge în cadre, iar la recepție să facă operațiunea inversă. A doua funcție este de a multiplexa şi demultiplexa pachete provenite de la diferite surse. A treia funcție este de a garanta calitatea serviciilor.

Nivelul aplicație/profiluri defineşte 13 aplicații Bluetooth tipice:

1. *Acces generic - proceduri pentru întreținerea legăturii*
2. *Descoperire servicii – protocol pentru descoperirea serviciilor oferite*
3. *Port serial – înlocuitor de cablu pentru legătură pe port serial;*
4. *Interschimbare obiecte – defineşte relația client / server pentru schimbare de obiecte*
5. *Acces la rețeaua locală – protocol între calculator portabil şi rețeaua locală fixă*
6. *Rețea pe linie telefonică – Apelarea unui notebook de la telefon*
7. *Fax – permite unui fax mobil să comunice cu un telefon mobil*
8. *Telefon fără fir –*
9. *Em / Rec portabil – radiotelefon portabil*
10. *Căşti de telefonie cu transmițător*
11. *Transfer de fişiere*
12. *Sincronizare – permite unui PDA să se sincronizeze cu un calculator.*

3.6 Punți între LAN-uri

3.6.1. Locul şi rolul punților

În prezent multe organizații au mai multe LAN-uri, unele chiar diferite, pe care doresc şi trebuie să le interconecteze. Acest lucru se poate face prin dispozitive numite **punți** (bridges) care operează la nivel legătură de date. Punțile examinează adresele la nivel LD pentru a face rutarea (adresa de cadru). Punțile nu examinaează câmpurile de informație utilă din cadru, informație care poate conține pachete IP, ATM, IPX, OSI etc. Spre deosebire de punți, ruterele examinează adresele din pachete şi fac rutarea pe baza lor. Necesitatea interconectării LAN-urilor apare din mai multe motive.

1. O organizație mare, cu mai multe departamente, va avea LAN în fiecare departament, dar va trebui să comunice şi interdepartamental.
2. Localizarea fizică la distanță a departamentelor şi în consecință a LAN-urilor nu permite utilizarea unei singure rețele dacă distanțele sunt prea mari (de exemplu peste 2,5 km la Ethernet) sau dacă sunt prea mulți utilizatori.
3. Separarea logică şi chiar fizică pe categorii a utilizatorilor, de exemplu într-o universitate, separarea studenților de cadre universitare şi de cerectători ştiințifici..
4. Fiabilitatea unui LAN poate fi serios afectată dacă un nod se defectează şi trimite un şir de date eronate Plasarea unei punți într-un loc bine ales poate proteja utilizatorii de defectele unui nod.

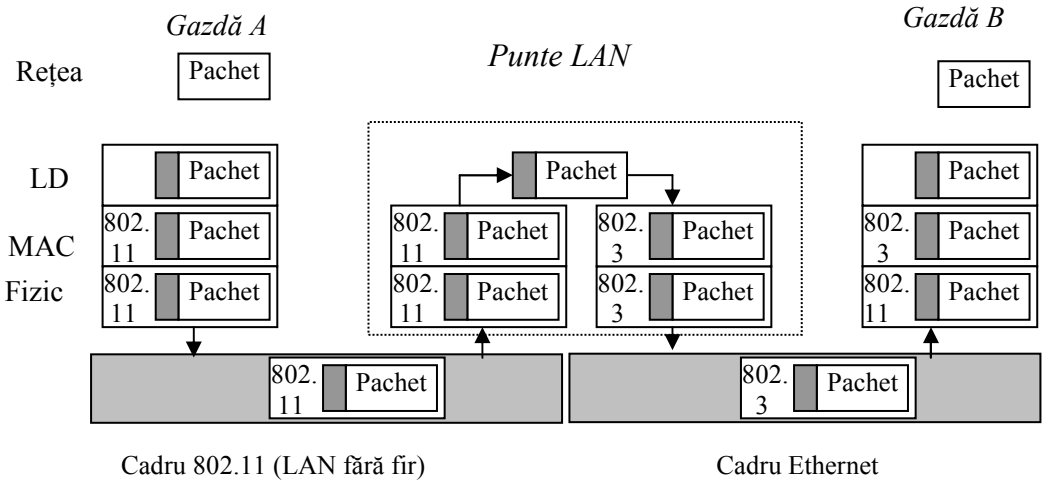


Fig. 3.16 Funcționarea unei punți de la 802.11 la 802.3

5. Restricționarea accesului unor categorii de utilizatori poate fi iarăşi un motiv de funcționare sigură şi de securitate a rețelei şi a protecției datelor
6. În mod normal un LAN are un mod transparent de lucru, în care toți abonații pot primi toate datele, nu numai cele adresate lor. Punțile pot separa părți din rețea, astfel încât, să nu ajungă informațiile sensibile la îndemâna cui nu trebuie.

Problemele generale ale interconectării LAN-urilor sunt:

- formatul diferit al cadrelor;

- lungimea diferită a datelor utilizator;
- viteze diferite pentru date;
- nivele diferite de prioritate.

Un exemplu de punte între un LAN fără fir (802.11) şi un LAN Ethernet este în fig. 3.16. Puntea desface antetul specific unui LAN şi îl adaugă pe cel al celuilalt LAN unde va trimite pachetele. Acest proces se face la nivelul MAC.

Dacă o punte conectează *k* LAN-uri, atunci ea va avea *k* subnivele MAC, câte unul pentru fiecare tip de LAN.

Problema cea mai dificilă la interconectarea a două LAN-uri este lungimea diferită a cadrului, când un cadru mai lung nu poate fi transferat într-o rețea care are cadre mai scurte. La acest nivel problema împărțirii cadrului în părți mai scurte nu se pune. Toate protocoalele de nivel LD presupun recepția totală a cadrului sau respingerea sa. Nu există posibilitatea spargerii şi reasamblării de cadre. Teoretic, o asemenea posibilitate ar putea exista şi au fost făcute unele încercări şi propuneri, dar în final nu au fost acceptate. Prin urmare, cadrele prea lungi trebuie eliminate pentru a accepta transparența.

Calitatea serviciilor este şi ea diferită în funcție de tipul de LAN. Ultimele standarde de LAN asigură un anumit nivel al calității serviciilor (de exemplu rată de transfer constantă la 802.16), ceea ce Ethernetul nu poate asigura.

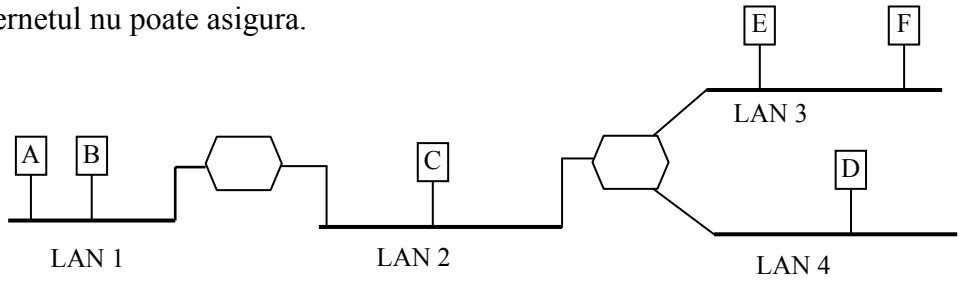


Fig. 3.17 Configurație de 4 LAN-uri şi 2 punți

Ratele de transfer diferite din LAN-uri necesită memorii tampon mari şi chiar în aceste condiții pot apărea congestii. Aşadar, punțile dintre LAN-uri au de rezolvat suficient de multe şi de complicate probleme. Ideal ar fi ca să se poată cumpăra punți proiectate după standarde IEEE şi ele să funcționeze perfect, fără modificări şi adaptări soft sau hard.Totuşi în prezent s-a reuşit ca în mare măsură punțile să funcționeze transparent. O punte transparentă, care funcționează în mod transparent, admite orice cadru transmis de pe oricare din LAN-rile la care este conectată.

În configurația din fig. 3.17 puntea B1 este conectată între LAN 1 şi LAN 2, iar B2 este între LAN 2, LAN 3 şi LAN 4. Un cadru din LAN 1 destinat lui A (din acelaşi LAN) şi care ajunge şi în puntea B1 este eliminat imediat. Un cadru din LAN 1 pentru a ajunge în C sau F trebuie transmis de B1. Deci primul lucru pe care îl face o punte este să decidă dacă un cadru trebuie transmis sau eliminat. Dacă trebuie transmis atunci este examinată tabela de adrese de dispersie menținută în interiorul punții. De exemplu tabelul lui B2 ar include pe A ca aparținând lui LAN 2 deoarece să trimită acest pachet prin LAN 2.

La prima conectare a punților tabelele sunt vide. Nici una dintre punți nu ştie unde se află destinațiile. În această fază se foloseşte algoritmul de inundare. Orice cadru care vine pentru o

destinație necunoscută este trimis către toate LAN-urile la care este conectată puntea. În timp, punțile învață unde se găsesc destinațiile şi încep să fie completate tabelele de dispersie. Algoritmul de completare se numeşte **învățare regresivă** (backward learning). Ideea este simplă. Dacă o punte vede un cadru venind de la C, atunci el ştie că tot pe unde a venit va fi trimis şi cel destinat lui C. Prin urmare, toate cadrele destinate lui C (fig 3.17) vor fi trimise prin ieşirea LAN 2 a punții. În felul acesta se completează tabelul de dispersie pe măsură ce sosesc pachete în rețea.

Topologia se poate schimba şi calculatoarele şi punțile pot fi sau în funcțiune sau nu. Pentru a trata topologiile dinamice, ori de câte ori se crează o intrare în tabelă, se notează şi timpul de sosire a cadrului. Astfel timpul asociat fiecărei intrări arată ultimul moment în care a fost primit cadrul de la calculator. Periodic, un proces din punte scanează tabela de dispersie şi curăță toate înregistrările mai vechi de câteva minute. În felul acesta, dacă un calculator este scos din locul său din LAN şi reinstalat în altă parte, în câteva minute el se va găsi în tabela de dispersie. De asemenea, este de reținut că la un calculator nou instalat în rețea se va putea ajunge numai prin inundare, inainte ca el să fi expediat primul cadru.

Procedura de dirijare prin punți este următoarea:

1. Dacă LAN-ul sursă este acelaşi cu LAN-ul destinație, elimină cadrul.
2. Dacă LAN-ul sursă diferă de cel destinație, trimite cadrul pe portul rezultat din tabela de dispersie.
3. Dacă LAN-ul destinație este necunoscut, foloseşte inundarea.

Căutarea şi actualizarea în tabelele de dispersie se fac astăzi cu circuite VLSI specializate în câteva microsecunde.

3.7 LAN-uri virtuale

Din diverse motive (administrative, topologice, fizice etc.) administratorii de rețele doresc să grupeze utilizatorii în LAN-uri şi să controleze accesul dintr-un LAN în altul. Pe de altă parte, o placă de rețea defectă poate să înceapă să inunde rețeaua cu cadre de difuzare şi să producă astfel congestie şi blocare.

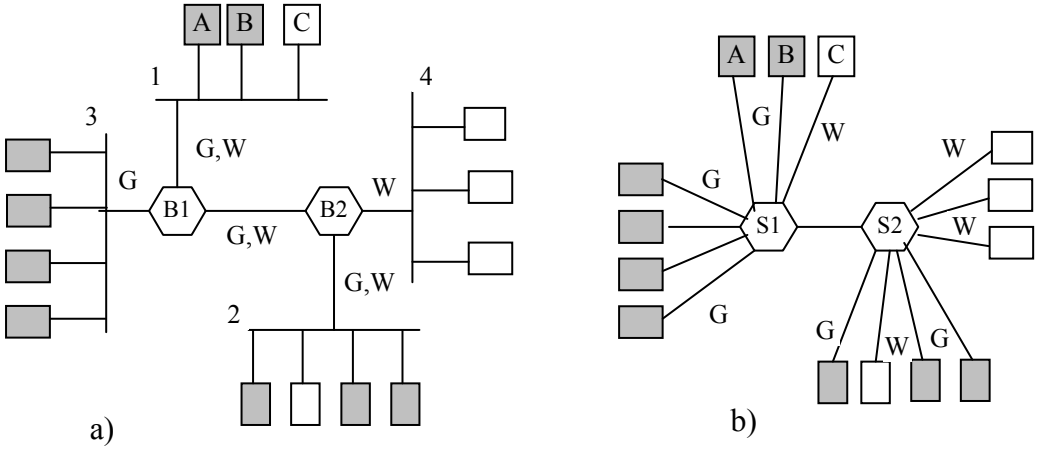


Fig. 3.20 a) Patru LAN-uri interconectate prin 2 punți b) Aceeaşi rețea organizată ca 2 VLAN-uri

Ca răspuns la problemele de mai sus şi la nevoia de flexibilitate sporită cerută de utilizartori prin care să se reconfigureze soft o rețea realizată pe o cablare fixă, au apărut **rețelele locale virtuale, VLAN**. Ele au la bază comutatoare dedicate. În fig. 3.20 se prezintă 4 rețele fizice organizate în 2 VLAN-uri folosind punți sau comutatoare.

Se obişnuieşte a se nota VLAN-urile prin culori diferite, în cazul prezentat G (gri) şi W (alb). Pentru a asigura funcționarea corectă a VLAN-urilor, trebuie create tabele de configuare în punți sau comutatoare. Aceste tabele stabilesc care VLAN este accesibil din fiecare dintre porturi (linii).

De exemplu un cadru recepționat de la VLAN-ul gri (G) trebuie trimis pe toate porturile marcate G. Un port poate fi marcat cu mai multe culori. Presupunem că maşina A difuzează un cadru. Puntea B1 va recepționa cadrul, vede că este de la VLAN-ul gri şi îl va înainta spre toate porturile notate G. Puntea B1 având 2 porturi notate G sau WG (în afara celui de pe care a venit cadrul), va trimite acest cadru pe ambele porturi. Ajungând în puntea B2, cadrul venit de la A prin B1 va fi difuzat pe portul de ieşire GW, dar nu va fi trimis şi pe portul W. În felul acesta, cadrul de la A va fi difuzat la toate maşinile gri şi numai la ele.

Problema care se pune este cum ştiu punțile sau comutatoarele care este "culoarea" unui cadru? Există trei metode, toate folosind un **indicator (identificator) de VLAN**:

1. fiecărui port îi este asociată o culoare (identificator) de VLAN
2. fiecărei adrese MAC îi este asociată o culoare VLAN
3. fiecare protocol de nivel 3 (sau adrese IP) îi este asociată o culoare de VLAN.

Pentru utilizarea identificatorului de VLAN a fost creat un **standard nou, 802.1Q** şi un nou format de cadru. Acesta conține două câmpuri în plus față de 802.3: identificator de protocol VLAN şi marcator. Plăcile Ethernet care suportă VLAN construiesc direct cadre 802.1Q.

3.7.1 Rețele virtuale private

O rețea virtuală privată (***VPN***) este o rețea a unei societăți implementată pe o infrastructură comună, folosind aceleaşi politici de securitate, management şi performanță care se aplică de obicei într-o rețea privată.

VPN-ul oferă în plus o multitudine de posibilități de conectare:

- conectarea utilizatorilor mobili;
- realizarea de intranet între diferite locații aflate la distanță;
- realizarea unor legături extranet cu partenerii de afaceri.

Tehnologiile VPN oferă o cale de a folosi infrastructurile rețelelor publice cum ar fi *Internetul* pentru a asigura acces securizat şi privat la aplicații şi resurse ale companiei pentru angajații din birourile aflate la distanță sau pentru cei care lucrează de acasă, pentru partenerii de afaceri şi chiar pentru clienți. Un VPN poate fi realizat pe diverse rețele de transport deja existente: Internetul public, rețeaua furnizorului de servicii IP, rețele Frame Relay şi ATM.

Astăzi, tot mai multe VPN-uri sunt bazate pe rețele IP. Tehnologia VPN folosește o combinație de **tunneling, criptare, autentificare şi mecanisme şi servicii de control al accesului,** pentru a transporta traficul pe Internet, pe o rețea IP administrată, sau pe o rețea a unui furnizor de servicii de transport de date.

Cum funcționează VPN ?

Când un dispozitiv VPN primeşte o instrucțiune de transmitere a unui pachet prin Internet, negociază o schemă de criptare cu un dispozitiv VPN similar din rețeaua destinație. Datele în format IPX/PPP sunt trecute în format IP pentru a putea fi transportate prin rețeaua publică. Al doilea obstacol este datorat faptului că Internetul nu asigură confidențialitatea datelor. În consecință, oricine poate „vedea" traficul poate să şi citească datele conținute în pachete. Aceasta este cu adevărat o problemă în cazul firmelor care vor să comunice informații confidențiale şi, în acelaşi timp, să folosească Internetul.

Soluția pentru aceste probleme a fost denumită **tunelare** (tunneling) şi a permis apariția VPN. În loc de pachete lansate într-un mediu care nu oferă protecție, datele sunt mai întâi criptate, apoi încapsulate în pachete de tip IP şi trimise printr-un „tunel" virtual prin Internet. Acum, indiferent de protocolul în care au fost transmise, datele pot călători prin Internet. La destinație, terminatorul de tunel primeşte pachetul, înlătură informația de IP şi decriptează datele în concordanță cu schema stabilită inițial. După decriptare, datele sunt transmise la server sau router, care le plasează în rețeaua locală.

Rezumat

Nivelul Legătură de date organizează fluxurile de biți în blocuri de date numite cadre, recunoscute de echipamentele de rețea de nivel 2, care le prelucrează astfel încât pe un link ale rețelei să se asigure o transmitere corectă, fără erori. Principalele sarcini ale nivelului legătură de date sunt: detecția şi corecția erorilor de transmisie, controlul fluxului, controlul accesului la mediu şi comutarea datelor la nivel fizic. Echipamentele de nivel legătură de date se găsesc la fiecare capăt al unui link şi ele rulează protocoale de nivel 2.

Controlul erorilor se poate face prin tehnica bitului de paritate, tehnica CRC sau folosirea unor coduri de linie speciale, detectoare –corectoare de erori. Mecanismul cu fereastră glisantă este foarte folosit pentru a integra controlul fluxului cu controlul erorilor într-un mod convenabil.

Multe rețele folosesc la nivel legătură de date unul dintre protocoalele orientate pe biți: SDLC, HDLC, LAPB iar Internetul foloseşte PPP ca principal protocol pe liniile punct la punct.

Multe rețele folosesc un singur canal pentru toate comunicațiile, necesitând astfel diverse scheme şi algoritmi de alocare a canalului. Cele mai simple scheme sunt cele bazate pe diviziunea în frecvență (FDM) şi pe diviziunea în timp (TDM). Acestea sunt alocări statice şi au eficiență bună dacă traficul este cunoscut şi invariabil în timp. Dacă numărul stațiilor este variabil, iar traficul în rafală, sunt mai utile protocoalele de alocare dinamică: CSMA/CD, CSMA/CA, CDMA, tehnicile cu salt de frecvență (FHSS, DSSS).

Ethernetul este forma cea mai răspândită pentru rețelele locale. LAN-urile diferite sunt interconectate prin punți şi comutatoare. O nouă dezvoltare în domeniul interconectării rețelelor

locale este VLAN, care separă topologia logică a LAN-urilor de cea fizică. Ea prmite realizarea unor rețele virtuale de tip LAN peste Internet.

Întrebări de control

1. Care sunt locul şi rolul nivelului LD şi ce servicii oferă nivelului superior (rețea)?
2. Care sunt considerentele împărțirii nivelului LD în subnivele? Ce importanță practică are acest lucru?
3. Care este lungimea tipică a unui cadru Ethenet? Care sunt considerentele avute în vedere la stabilirea lungimii unui cadru?
4. Care este structura generică a unui cadru LD şi care este rolul câmpurilor?
5. Care sunt deosebirile dintre controlul fluxului şi controlul erorilor?
6. Ce este distanța Hamming şi ce rol are în detecția/corecția erorilor?
7. Care sunt principalele cauze ale erorilor de transmisie şi cum se pot reduce?
8. Care sunt principalele tehnici de control al accesului la mediu? Enumerați avantajele şi dezavantajele lor.
9. Un octet cu valoarea hexa 4C trebuie codificat astfel ca să permita detecția erorilor pe baza bitului de paritate folosind regula parității pare. Care va fi forma binară a cuvântului de cod?
10. Descrieți locul şi rolul punților în LAN-uri.Cum se pot realiza LAN-uri virtuale. Descrieți asemănările şi deosebirile dintre comutatoare, punți, repetoare, hub-uri, rutere, porți.
11. Ce este o rețea virtuală privată şi cum se poate realiza?
12. De ce specificațiile 1000Base-SX precizează că frecvența ceasului în linie trebuie să fie 1250 MHz, deşi gigabitEthernetul are rata 1000 Mbps?