VI.4 REȚELE LOCALE VIRTUALE (VLAN)

O rețea locală virtuală (VLAN - *Virtual Local Area Network*) reprezintă gruparea logică a componentelor unei rețele locale, fără a ține cont de gruparea lor fizică.

Segmentarea fizică a unui LAN cu echipamente de comunicație de tip hub, switch, sau bridge face posibilă segmentarea domeniului de coliziune inițial în mai multe domenii de coliziune, dar păstrează un singur domeniu de broadcast, ceea ce permite un control mai eficient al congestiilor din rețea dar nu reduce încărcarea rețelei prin transmisia mesajelor de broadcast.

Routerul este singurul echipament care delimitează un domeniu de broadcast, îndeplinind funcția de așa-numit "zid-de-foc" (*firewall*) (Fig. VI.5).

În multe cazuri este utilă gruparea calculatoarelor-gazdă în domenii de broadcast separate, pe diferite criterii independent de conexiunile fizice existente în rețea și de amplasarea lor în spațiul unei clădiri sau a unui campus.

Într-o clădire sau într-un grup de clădiri, se pot defini grupuri de utilizatori cu preocupări similare. De exemplu, departamentul comercial al unei societăți poate să includă calculatoare situate pe diferite nivele ale aceleiași clădiri sau în mai multe corpuri de clădire.

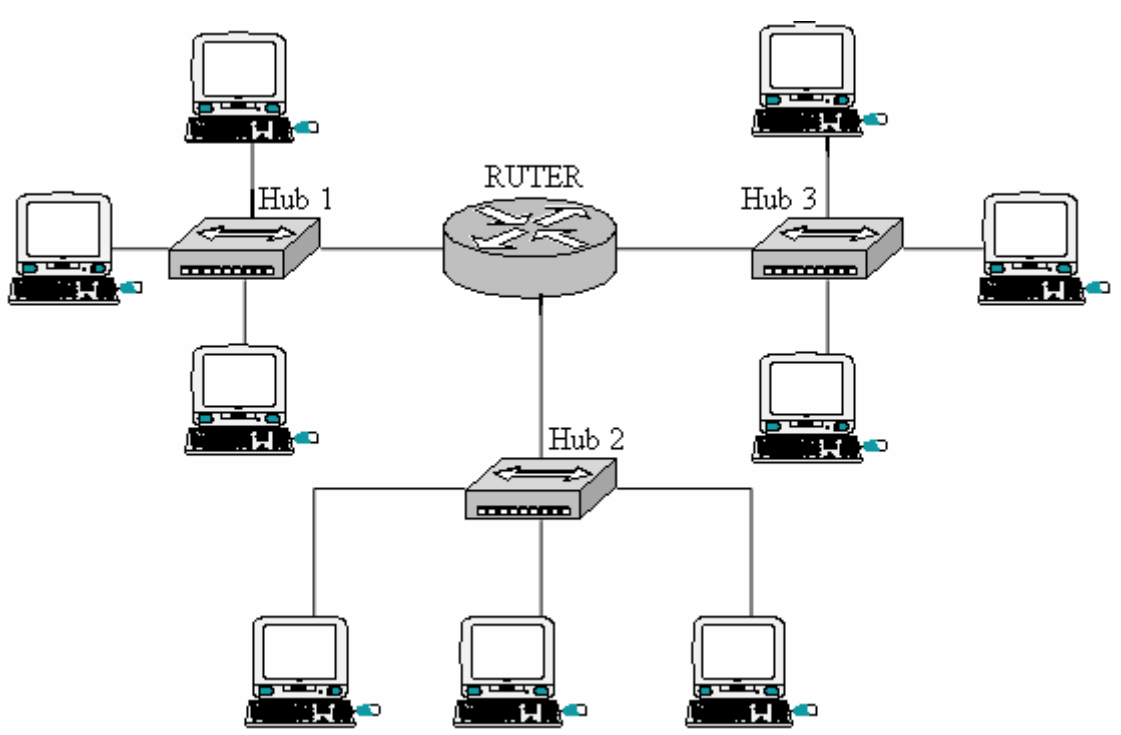

Fig. VI.5 Rețea locală segmentată cu un router

Acestea trebuie să acceseze o bază de date unică, cu informații specifice și în același timp trebuie creată posibilitatea difuzării unor mesaje prin broadcast, către toți utilizatorii din acel departament. Accesul din afara grupului respectiv trebuie restricționat. Similar se pot defini grupuri de utilizatori care lucrează în departamentul tehnic, în cel administrativ sau în cel financiar. Se obțin astfel mai multe grupuri de utilizatori și mai multe rețele locale virtuale, cu domenii de coliziune și de broadcast independente: VLAN 1, VLAN 2, VLAN 3 și VLAN 4 (Fig. VI.6).

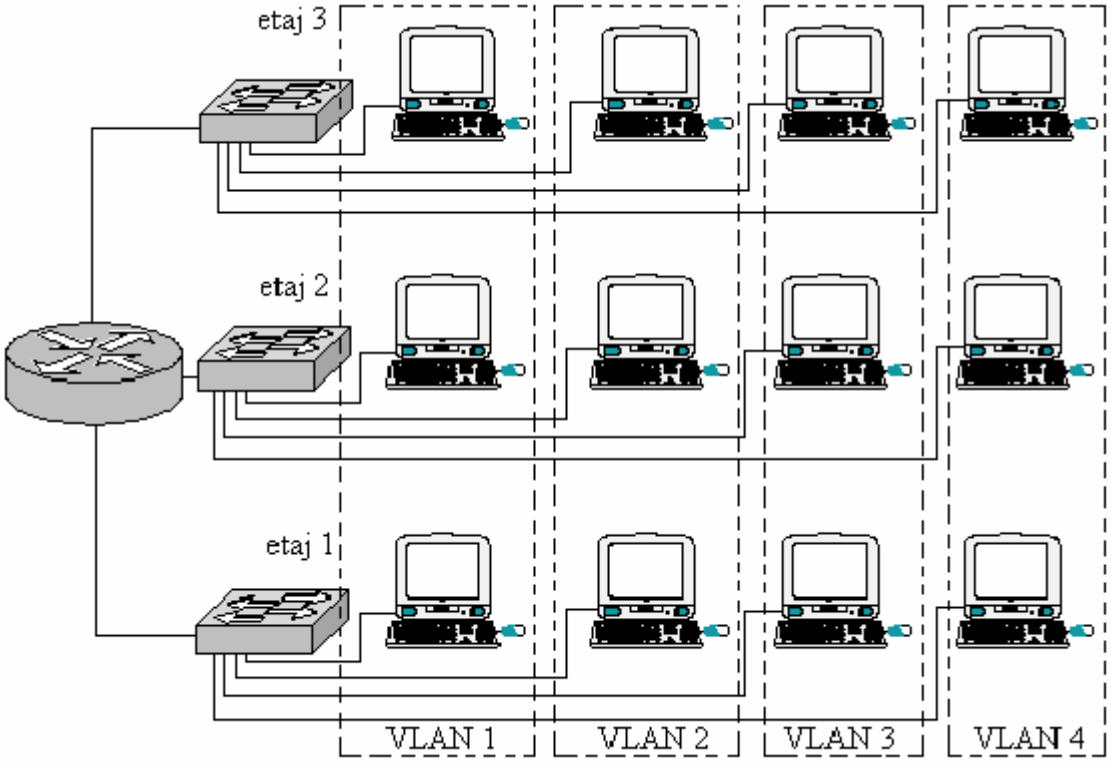

Fig. VI.6 LAN cu patru rețele locale virtuale

Definirea VLAN-urilor se poate face în funcție de diverși factori:

- numere de identificare (ID - *identifier*) a porturilor;
- adrese MAC;
- protocoale de rețea;
- porturi de aplicație.

Fiecare VLAN reprezintă un domeniu de broadcast independent, ceea ce permite reducerea încărcării rețelei prin difuzarea mesajelor către toți utilizatorii.

Se poate defini câte un VLAN pe fiecare port al switch-ului. Mai multe porturi din switch pot să aparțină aceluiași VLAN. La nivelul switch-ului, transmisiile prin broadcast se fac numai pe porturile asociate aceluiași VLAN.

VLAN-urile lucrează pe nivelele OSI 2 și 3. Comunicația între VLAN-uri se face prin rutare, deci pe nivelul de rețea, prin intermediul unui router sau al unui switch de nivel 3.

Includerea utilizatorilor în VLAN-uri se realizează prin soft, cu comenzi specifice incluse în fișierele de configurare a echipamentelor de comunicații din rețea.

Implementarea VLAN-urilor este avantajoasă întrucât schimbarea locației fizice a unui calculator care rămâne în același VLAN nu impune reconfigurarea routerelor și nici modificarea structurii cablate a rețelei. În plus, definirea rețelelor virtuale oferă o securitate mai mare a comunicațiilor din rețea, prin restricționarea accesului între VLAN-uri.

Principiile VLAN pot fi aplicate și în rețelele de arie largă (WAN), prin utilizarea unor magistrale de date de mare viteză (*backbone*) de exemplu, Fast Ethernet, FDDI, ATM.

Există două principii de definire a VLAN-urilor:

1. **Identificarea cadrelor** (*frame tagging*), conform standardului IEEE 802.1q.

La fiecare cadru de date care circulă pe această magistrală între diferite VLAN-uri, se poate atașa un identificator de VLAN pentru dirijarea traficului.

2. **Filtrarea cadrelor** între VLAN-uri (*frame filtering*), pe baza unui tabel de adrese.

În rețeaua prezentată pentru exemplificare în figura VI.7, switch-urile pot filtra cadrele între VLAN-uri pe baza unui tabel de adrese, permanent actualizat folosind informațiile furnizate de sistemul de management al rețelei. Cadrele sunt transferate în VLAN-ul corespunzător, în funcție de adresa MAC de destinație.

Tabel de adrese

Adrese MAC	VLAN
12-aa-54-9f-ee-d5	1
30-46-93-b3-f1-0c	1
25-5b-d3-2e-40-a3	2
d6-55-07-91-42-32	2
52-11-6a-de-2f-50	3
a2-14-fd-d8-10-72	3

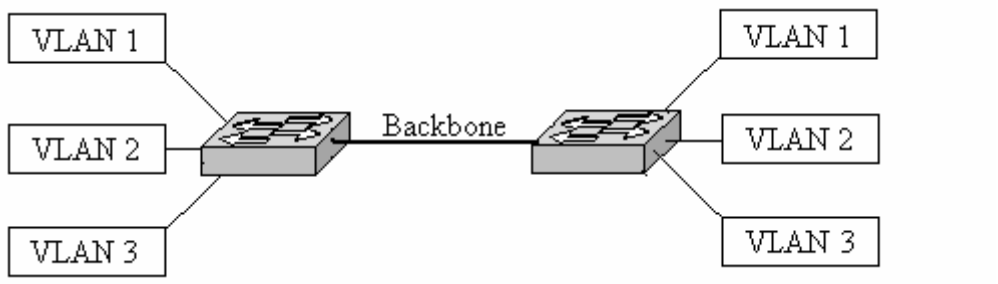

Fig. VI.7 VLAN-uri interconectate de o magistrală de date

Filtrarea cadrelor este o operație complexă și de durată relativ mare. Metoda de proiectare a VLAN-urilor prin identificarea cadrelor se realizează pe nivelul OSI 2 și este mai flexibilă decât cea prin filtrare. Identificatorul de VLAN se atașează în antetul cadrului la intrarea pe magistrala de date și este eliminat la ieșirea din aceasta. Acest identificator se folosește numai între switch-uri sau routere, în backbone, adică în zona de **cablare verticală**, în care se lucrează pe mai multe nivele OSI. Identificatorii de VLAN nu apar în zona de **cablare orizontală,** de comunicație la nivel fizic, între hub-uri și echipamentele terminale (Fig. VI.8).

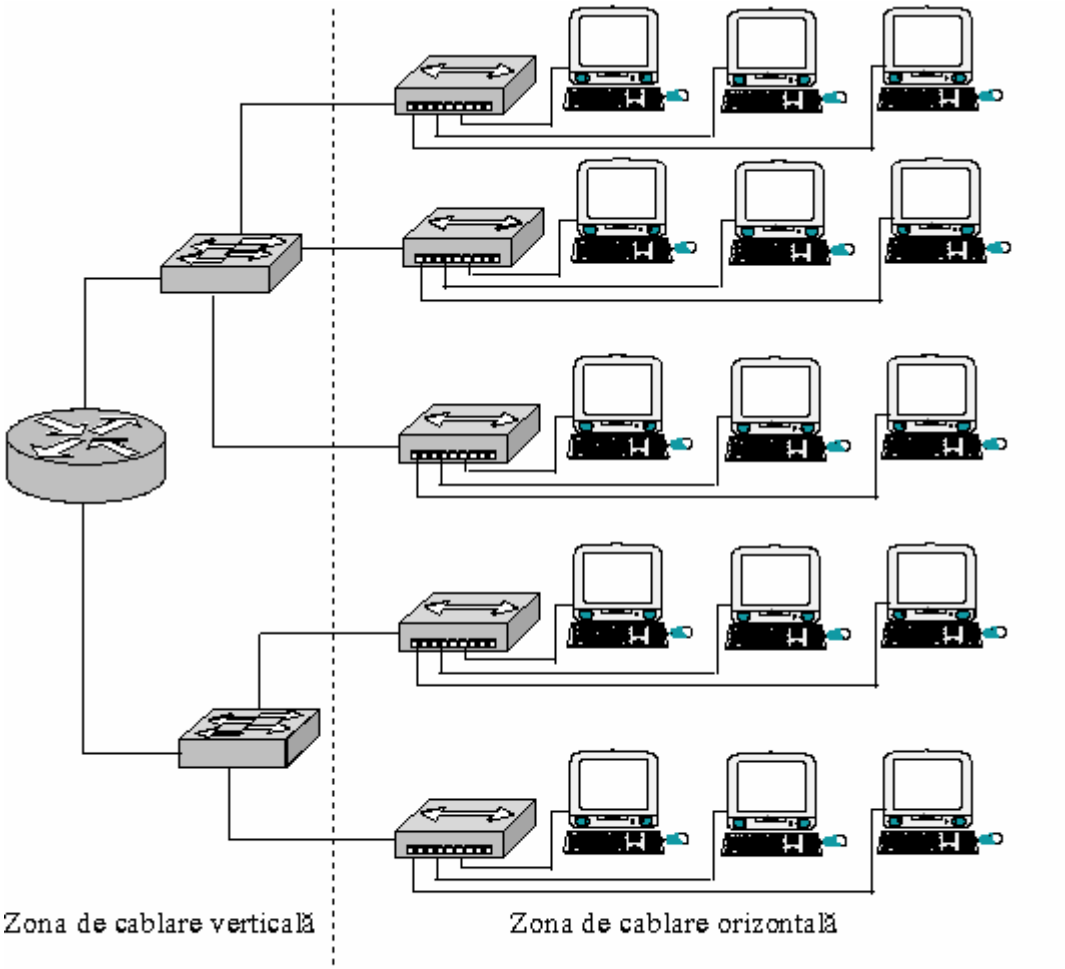

Fig. VI.8 Schemă de conexiuni fizice

Mecanismul de control implementat de switch analizează fiecare cadru și decide operația care trebuie efectuată:

- transfer spre o destinație unică (*forwarding*);
- filtrare (*filtering*);
- difuzare în VLAN-ul corespunzător (*broadcast*).

Analiza cadrului poate include:

- adresa MAC a sursei;
- adresa MAC de destinație;
- tipul protocolului de rețea.

Există trei **metode de implementare a VLAN-urilor**:

I. Metoda de implementare a VLAN-urilor pe baza porturilor fizice (*port-centric*) definește VLAN-urile direct, prin asociere cu anumite porturi din switch/router (vezi schema de conexiuni logice din figura VI.9, asociată schemei de conexiuni fizice din figura VI.8).

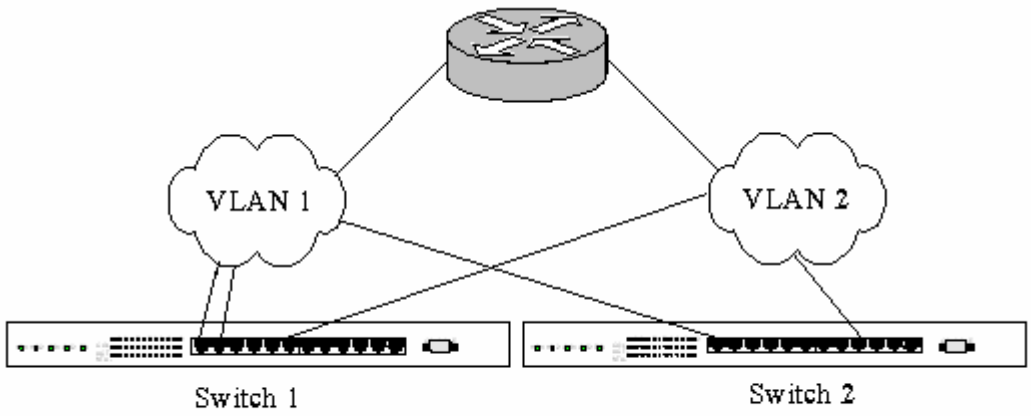

Fig. VI.9 Schema de conexiuni logice de definire a VLAN-urilor

Fiecărei rețele virtuale i se alocă o **adresă de rețea** (de exemplu, într-o rețea bazată pe suita TCP/IP se pot aloca adrese IP de clasă C: 194.125.48.0, 194.125.49.0). Aceste adrese sunt incluse în tabelul de rutare. Routerul interconectează VLAN-urile și dirijează pachetele spre VLAN-ul corespunzător, în interiorul aceluiași VLAN sau între VLAN-uri distincte.

Utilizatorii unui VLAN sunt conectați la porturile fizice din fiecare switch, asociate acelui VLAN.

Metoda este avantajoasă. Administrarea VLAN în acest caz, se face relativ simplu. Securitatea comunicației este crescută. Transmisiile prin broadcast dintr-un VLAN nu afectează celălalt VLAN și în general, pachetele destinate unui VLAN nu sunt transmise și în alte VLAN-uri.

Ca dezavantaj, se observă faptul că un nou utilizator al unui VLAN trebuie conectat fizic în mod obligatoriu la unul din porturile asociate acelui VLAN. Pot să apară deci unele limitări ale capacității rețelei virtuale, ceea ce ar impune modificarea topologiei fizice a rețelei și eventual achiziționarea unor noi echipamente (switch-uri sau huburi de partajare cu număr mai mare de porturi).

II. **Metoda statică** definește VLAN-urile prin asociere cu porturile din switch, gestionarea VLAN realizându-se la nivelul unei **stații de management** și nu la nivelul unui router (Fig. VI.10). Baza de date de management (MIB) a VLAN conține informațiile referitoare la modul de alocare a porturilor din switch-uri rețelelor virtuale.

Asocierea dintre porturi și VLAN-uri se face în mod static, pe baza tabelelor de adrese MAC utilizate de switch-uri. Orice schimbare în topologia rețelei impune intervenția administratorului de rețea pentru actualizarea MIB-ului. Configurarea VLAN-urilor statice este relativ simplă. Comunicația în aceste rețele are un grad mare de securitate.

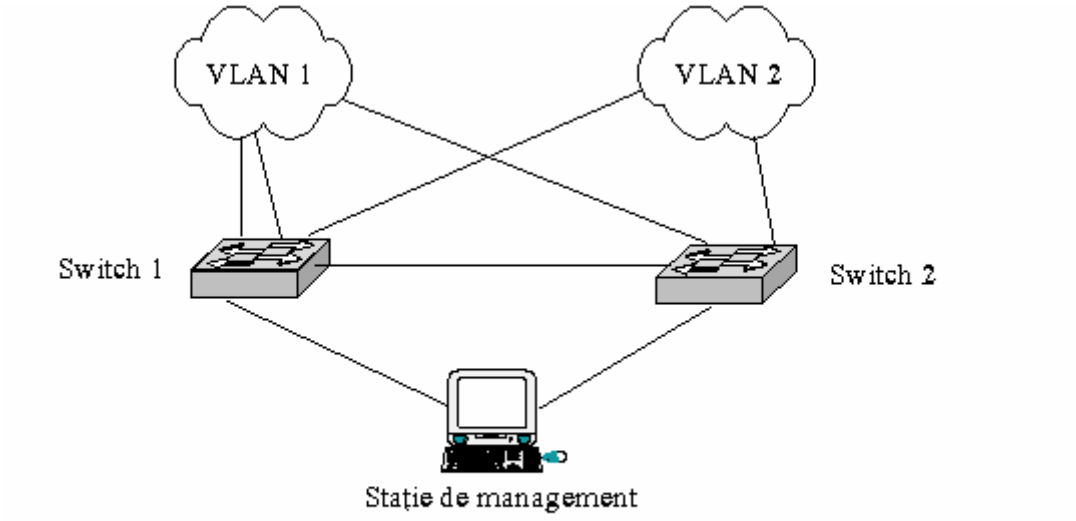

Fig. VI.10 Definirea rețelelor virtuale statice

III. **Metoda dinamică** descrie modul de implementare a VLAN-urilor dinamice, folosind baze de date, memorate și actualizate automat într-un **server de configurare a VLAN-urilor**, fără intervenția administratorului de rețea. Acesta răspunde doar de faza inițială de creare a structurii bazei de date.

Fiecare utilizator, identificat prin adresa sa MAC, poate fi inclus într-un anumit VLAN prin conectare fie la un port deja configurat ca fiind asociat unei rețele virtuale, fie la un port neconfigurat anterior.

Metoda dinamică de definire a VLAN-urilor admite asocierea aceluiași port fizic succesiv cu diferite VLAN-uri. Se păstrează însă restricția că portul nu poate fi asociat cu mai multe VLAN-uri simultan.

Informația de configurare a VLAN-urilor este stocată în baza de date a serverului pentru VLAN care comunică cu toate routerele din rețea pentru actualizarea informațiilor de rutare.

VLAN-urile dinamice se pot defini nu numai pe baza adreselor fizice, dar și a celor de rețea sau a protocoalelor de rețea utilizate.

În cazul conectării unui nou utilizator la un port neconfigurat anterior, se verifică adresa utilizatorului și se configurează dinamic portul respectiv folosind informațiile din baza de date pentru VLAN-uri.

Observații:

1. Un port utilizat inițial pentru un VLAN poate fi reconfigurat ulterior pentru alt VLAN, fără a fi necesară intervenția administratorului de rețea pentru reconfigurarea ruterelor.
2. VLAN-urile pot împărți același spațiu de adrese, de exemplu adrese IP de rețea sau de subrețea.

Definirea rețelelor locale virtuale are o serie de avantaje:

- În aplicațiile curente, topologiile fizice și/sau logice ale rețelelor sunt deseori modificate, ceea ce impune în multe cazuri schimbarea structurii cablate, achiziția de noi echipamente de comunicații (hub, switch etc), reconfigurarea echipamentelor de tip bridge sau router, modificarea bazelor de date de management. Definirea VLAN-urilor determină **reducerea costurilor și eforturilor dedicate schimbărilor din topologia rețelelor.**
- Transmisiile broadcast apar nu numai ca utilitate (de exemplu în aplicațiile de tip multimedia), dar și prin funcționarea defectuoasă a unor componente din rețea (viruși de rețea, furtuni de difuzare etc). Prin divizarea domeniului de broadcast fie la nivelul ruterelor (*firewall*), fie prin definirea VLAN-urilor, **se reduce substanțial încărcarea rețelei.**
- Rețelele locale de calculatoare nu sunt suficient securizate pentru accesul din interior al unui intrus și sunt relativ ușor de penetrat din exterior. Implementarea VLAN-urilor permite **creșterea gradului de securitate a rețelei**. Securizarea VLAN-urilor dedicate anumitor aplicații sau resurse se face prin prin restricționarea numărului de utilizatori din fiecare rețea, separarea domeniilor de broadcast, verificarea oricărui nou utilizator al rețelei. Este absolut necesar să se includă toate porturile switch-urilor neincluse în alte VLAN-uri într-un VLAN simbolic, nededicat.

Suplimentar, la nivelul ruterelor se pot defini **liste de control a accesului** (ACL - *Access Control List*) pe diferite criterii:

- adrese fizice;
- adrese de rețea;
- protocoale;
- tipul aplicației.

Din motive de securitate se poate recurge la restricționarea accesului în VLAN pe baza listelor de acces, eventual și în funcție de anumite intervale orare.

Observație:
Se pot implementa și rețele virtuale private (VPN - *Virtual Private Network*), similare VLAN-urilor, dar care spre deosebire de acestea, VPN-urile realizează criptarea informațiilor pentru o mai bună securizare a transmisiei.

VI.5 ECHIPAMENTE DE SECURIZARE (FIREWALL)

Internetul este o rețea cu foarte mulți utilizatori din întreaga lume și prin care se transferă cantități uriașe de informații.

Pentru aplicarea unei politici de securitate a rețelei, se utilizează echipamente de securizare de tip "zid de foc" (*firewall*) care aplică anumite reguli și constrângeri privind accesul pe diferite interfețe ale sale.

Un router poate fi configurat ca firewall. De asemenea, unele sisteme de operare (de exemplu, Windows XP) au opțiunea de activare a unui firewall intern.

Firewall-ul interconectează rețeaua publică și o rețea privată, asigurând securitatea datelor vehiculate intern în rețea și protecția rețelei private față de eventualele atacuri externe (Fig.VI.11).

Un firewall are minimum două interfețe:

- una pentru conexiunea dintre firewall și rețeaua publică (în particular, Internet-ul);
- cealaltă interconectează firewall-ul cu rețeaua internă privată (*intranet*), care necesită securizare.

Firewall-ul protejează rețeaua privată de unele atacuri externe și restricționează accesul din afară la resursele acesteia.

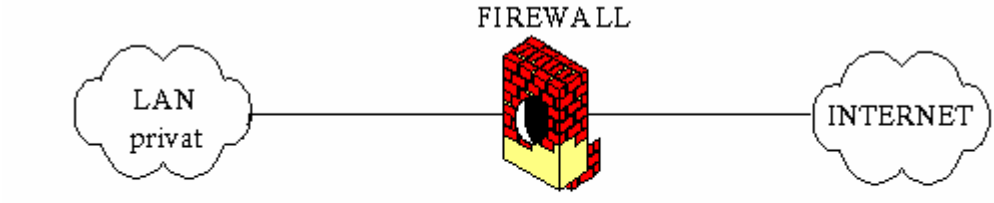

Fig. VI.11 Interconectarea unei rețele private cu una publică prin intermediul unui firewall

Întrucât firewall-ul reprezintă singura conexiune dintre rețeaua privată și cea publică, la nivelul său se poate monitoriza traficul de pachete și se verifică drepturile de acces ale utilizatorilor din afara rețelei interne (prin operația de *login*).

În prezent, se utilizează două tipuri de firewall:

1. **Poartă de aplicații** (*Application Gateway*) - varianta tradițională de firewall.

Orice conexiune între două rețele se face prin intermediul unui program de aplicații (*proxy*). O sesiune deschisă în rețeaua privată este încheiată de proxy, după care acesta creează o nouă sesiune spre nodul de destinație.

Programul proxy se bazează pe particularitățile suitei TCP/IP și este restrictiv pentru alte suite de protocoale. Execuția acestui program necesită resurse relativ mari din partea CPU.

La nivelul firewall-ului sunt admise numai acele protocoale pentru care sunt configurate aplicații proxy specifice. Cadrele bazate pe alte tipuri de protocoale sunt automat rejectate.

În practică, se configurează și firewall-uri transparente, care transferă cadrele între cele două sesiuni fără analiza prealabilă a datelor.

2. **Modul de inspecție dependent de stare** (*Stateful Inspection*) sau de **filtrare dinamică a pachetelor**, denumit și nod de control a accesului în funcție de context (CBAC - *Context-Based Access Control*) - concept relativ nou de implementare a firewall-ului.

În această tehnologie, se preiau pachetele de date și se citesc antetele introduse de protococolul de rețea (IP) și de cele corespunzătoare nivelelor OSI și TCP/IP superioare, până la nivelul de aplicație.

Firewall-ul verifică fiecare pachet care urmează să fie transferat și acordă dreptul de acces în funcție de adresele sursei și destinației, precum și de serviciul solicitat. Acest tip de firewall realizează controlul fluxului cu memorie, astfel încât echipamentul este capabil să recunoască acele pachete transmise din rețeaua publică (în particular, Internet) ca răspuns la o cerere adresată de un nod din rețeaua internă (*intranet*), prin monitorizarea sesiunilor TCP. În paralel, se rejectează toate pachetele transmise din rețeaua publică în cea internă, dar care nu provin din traficul inițiat intern.

Prin acest nou concept, se asigură o procesare rapidă și eficientă a traficului de informații dintre Internet și rețelele private, perfect adaptată noilor aplicații Internet și realizată cu resurse hardware relativ reduse.

Implementarea firewall-ului cu routere se face prin filtrarea dinamică a pachetelor și controlul traficului pe baza regulii care stabilește că:

- orice pachet transmis din rețeaua internă către o destinație externă este transferat de firewall necondiționat, cu excepția cazurilor în care se impun constrângeri;

- transferul oricărui pachet din rețeaua publică spre o destinație din rețeaua privată este blocat de firewall, cu excepția cazurilor în care se admite accesul acestora în mod explicit, prin configurarea adecvată a interfețelor publice referitor la accesul din exterior.

Interfețele firewall-ului sunt deschise numai pe durata sesiunii inițiate de un utilizator cu drept de acces.

Firewall-ul intercepteaza orice conexiune stabilită prin TCP și o continuă numai după verificarea prealabilă a legăturii.Acest lucru previne atacurile din exterior asupra rețelei private, prin distrugerea cadrelor transmise prin TCP fără drept de acces.

Firewall-ul poate fi configurat în vederea limitării accesului utilizatorilor din rețeaua internă în cea publică.

Mesajele generate prin ICMP pot fi transferate sau blocate de firewall în funcție de modul de configurare a acestuia.

Pentru evenimentele semnificative care apar la nivelul firewall-ului se pot trimite mesaje de înștiințare către nodurile de destinație accesate.

Echipamentele de tip firewall admit diverse protocoale de aplicație: FTP, NETBIOS, GRE, OSPF, RSVP (*ReSerVation Protocol*), VDOnet's VDOLive, Microsoft's NetShow etc.

Firewall-ul protejează rețeaua privată față de **atacurile externe** de tip "inundare" cu pachete (*flooding*), cu pachete PING ilegale sau ICMP generate în număr excesiv, atacuri
Smurf cu pachete având adresă IP din spațiul de adrese alocat rețelei private, de cele mai multe ori fiind chiar adresa de broadcast a acesteia, scanare a porturilor.

Firewall-ul permite controlul și monitorizarea accesului (*Logging Facility*) în rețeaua privată dar numai pentru sesiunile create pe baza protocolului Internet, nu și pentru alte suite de protocoale (Appletalk, DECnet, IPX/SPX).

Politica de securitate aplicată de firewall stabilește regulile pe baza cărora se admite sau se blochează transferul pachetelor între rețeaua privată și cea publică.

Un firewall devine activ numai după ce au fost configurate cel puțin o interfață publică și una privată și s-au stabilit regulile de acces la nivelul acestora.

Traficul între două interfețe ale firewall-ului nesupuse politicii de securitate se desfășoară normal, fără restricții.

Transferul pachetelor de la o interfață nesecurizată către una securizată este automat blocat.

Firewall-ul controlează traficul de pachete pe baza adreselor fizice sau IP, a porturilor de aplicație și chiar a zilei sau orei la care se accesează rețeaua.

Politica de securitate se aplică pe baza **listelor de acces** stocate în routere sau în servere RADIUS (*Remote Authentication Dial In User Service*).

RADIUS este un protocol de autentificare, configurare și contorizare a transferurilor între firewall, ca server de control a accesului (*Network Access Server*) și un server RADIUS care deține baza de date cu informații despre utilizatorii rețelei (nume de utilizatori și parole), modul de configurare a rețelei (adrese IP, măști de rețele și de subrețele etc), precum și despre sesiunile stabilite anterior, sub forma unui istoric al evenimentelor din rețea.

Firewall-ul este clientul RADIUS care adresează cererea de autentificare către serverele RADIUS, pentru accesarea listelor de acces. Acestea sunt fișiere de tip 'text' (.txt), codate ASCII, care includ liste de adrese IP sau MAC.

Listele de acces bazate pe adrese IP includ adrese IP individuale, eventual numele calculatoarelor-gazdă, domeniul de adrese IP al unei rețele și eventual unele comentarii care facilitează administrarea acestor liste.

Listele de acces cu adrese fizice includ adrese MAC individuale ale componentelor rețelei, eventual numele stațiilor și comentarii ajutătoare.

Numărul maxim de liste de acces care pot fi stocate pe un router precum și dimensiunile acestora este în general limitat.

Pentru un spațiu de adrese extins se preferă utilizarea unui server RADIUS care să gestioneze eficient aceste liste, pentru a reduce întârzierile de trafic produse de routere.

În acest caz, routerul devine un simplu client RADIUS care adresează cererea de autentificare către serverul RADIUS și primește un răspuns din partea acestuia.

Observații:

1. Filtrarea dinamică a pachetelor se realizează la nivelul firewall-ului prin politica de securitate dar și prin procedeele de translare a adreselor private în adrese publice (NAT; ENAT - *Enhanced NAT*). Pentru a evita dubla filtrare a pachetelor în routere, se dezactivează serviciul NAT pe durata activării firewall-ului.
2. Se poate monitoriza activitatea firewall-ului, mai precis evenimentele care se desfășoară la nivelul său:
   - accesarea adreselor de e-mail;
   - desfășurarea sesiunilor Telnet de acces de la distanță în rețeaua privată;
   - comunicarea pe porturi asincrone (de exemplu, interfețe seriale);
   - accesarea agenților SNMP.