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.

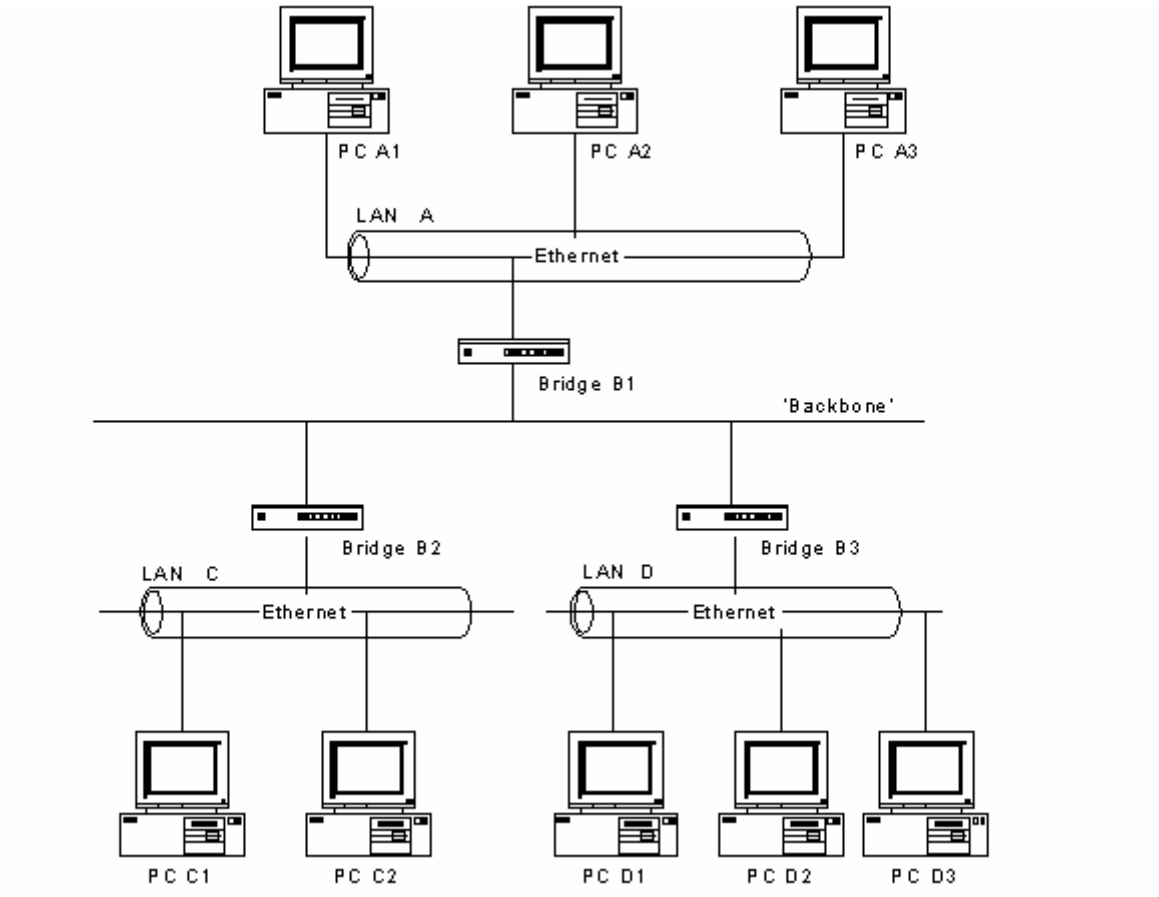

Fig. VI.1 Exemplu de LAN extins cu punți

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 fiec

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 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.

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

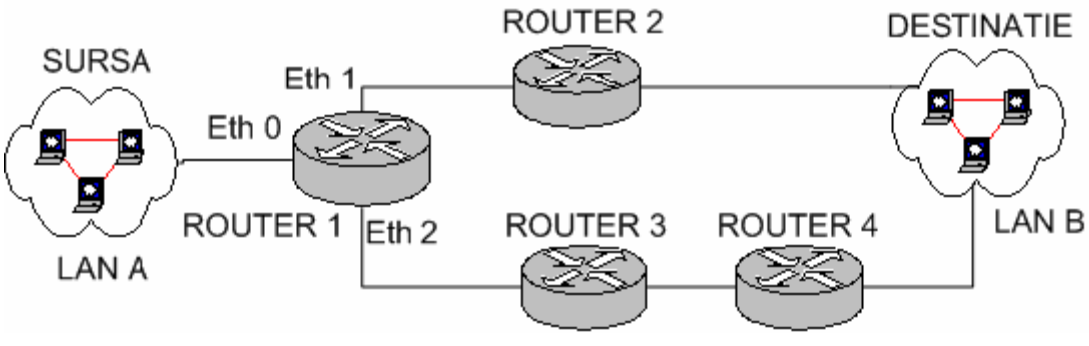

Fig.VI.2 Exemplu de LAN-uri interconectate cu routere în WAN

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 ieşire	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)**.**

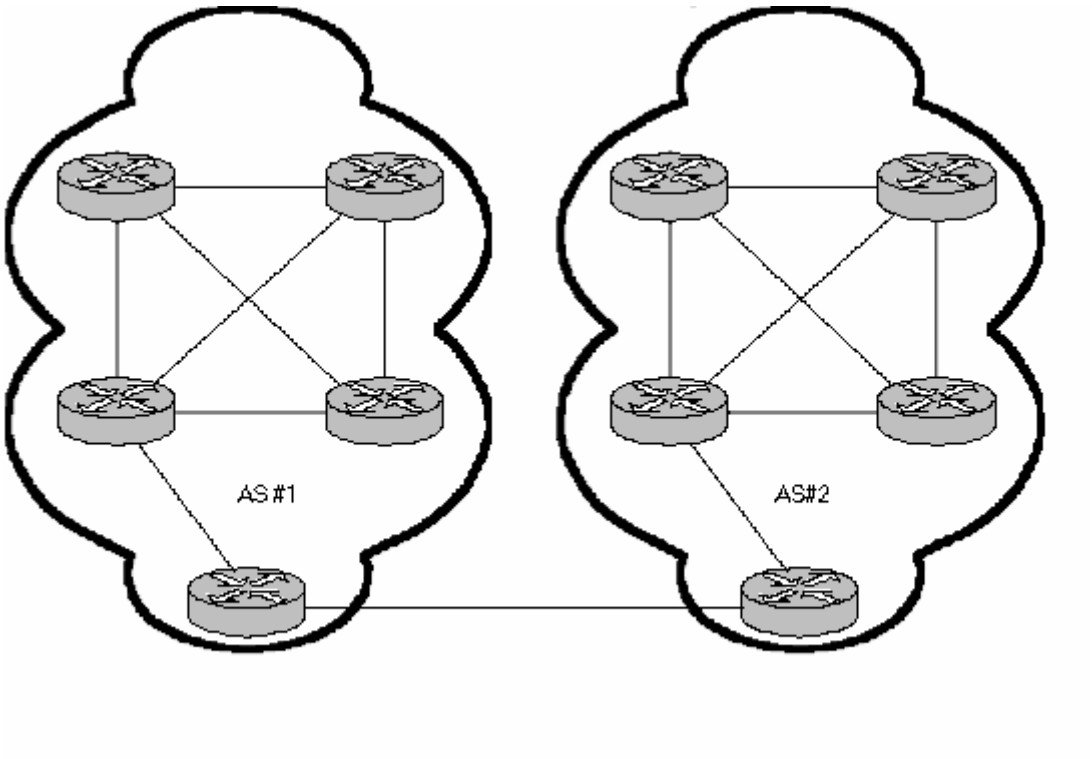

Fig.VI.3 Interconectarea unor sisteme autonome

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.

Rutarea IP se poate face în două moduri:

1. **static**, caz în care administratorul de rețea introduce manual rutele în tabelul de rutare, specificând pentru fiecare adresă a rețelei de destinație:

- adresa interfeței de ieșire din router;
- adresa următorului router (*next Hop*);
- eventual metrica de cale.

Rutarea se face simplu, pe baza tabelului de rutare. Din adresa destinației, prin aplicarea măștii de rețea, se deduce adresa rețelei de destinație și pachetul este transferat pe portul de ieșire corespunzător. Metoda nu asigură deducerea căii optime și nu elimină riscul congestiilor de trafic.

2. **dinamic**, prin reactualizarea tabelelor de rutare atunci când apar modificări ale adreselor rețelelor sau subrețelelor, ale metricii utilizate sau coliziuni în WAN. Acest mod de rutare permite deducerea căii optime dintre rețeaua-sursă și cea destinație pentru reducerea timpului, a costurilor de transmisie sau a riscului de coliziune.

Rutarea IP dinamică presupune alegerea protocolului de rutare (de exemplu, RIP, OSPF), stabilirea adreselor și a măștilor de rețea pentru toate rețelele direct conectate la acel router.

Întrucât spațiul de adrese IP este limitat, în numeroase rețele se alocă utilizatorilor adrese IP private care nu trebuie confundate cu adresele IP reale (*public*) alocate de InterNIC. Rutarea pachetelor se face pe baza adreselor IP reale alocate interfețelor ruterelor de ieșire în WAN, folosind procedeul NAT de translare a adreselor.

Pentru rutarea cu adrese private, se încapsulează pachetele IP transmise în Internet cu antete suplimentare prin așa-numitul **mecanism GRE** (*Generic Routing Encapsulation*), descris în RFC 1701. Pachetului inițial (*payload packet /original packet*) i se adaugă un antet GRE (*GRE Header*) și un antet privind modul de transfer specificat conform protocolului de rețea (*delivery header*) (Fig.VI.4).

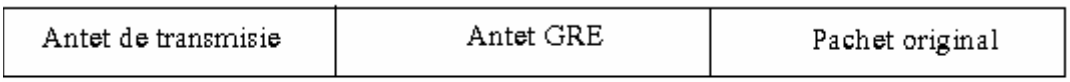

Fig. VI.4 Încapsularea GRE

Prin GRE se asigură transparența adreselor intermediare și securitatea transmisiei, prin realizarea unui așa-numit "tunel de transmisie" (*tunnelling*) .

Uzual este cazul încapsulării pachetelor IP pentru transmisii cu IP (*IP over IP*) conform RFC 1702, standard definit pentru GRE.

Conform RFC 1597, anumite spații de adrese IP din clasele A, B și C sunt rezervate pentru procedeul GRE și sunt numite **adrese private** (*private*):

10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255.

Aceste adrese IP pot fi utilizate în încapsularea GRE astfel încât cadrul să fie interpretat ca fiind încapsulat GRE și routerele 'de la distanță' să extragă adresa de destinație privată din pachetul original.

Exemplu: Să presupunem existența a două rețele locale de calculatoare A și B având alocate adresele IP private 192.168.3.0 și 192.168.4.0.

Aceste rețele sunt conectate în WAN prin intermediul a două routere cu adresele IP publice alocate interfețelor: 193.162.35.110 și 195.16.23.12.

Cele două routere comunică prin intermediul unui al treilea router cu adresa 194.225.140.1.

Un pachet trimis de la adresa 192.168.3.2 către 192.168.4.5 va fi încapsulat prin procedeul GRE specificându-se în antetul de transmisie numai adresele IP private ale routerului-sursă și respectiv routerului-destinație fără a se menționa adresa routerului intermediar. Adresa acestuia este inclusă doar în tabelele de rutare nefiind vizibilă din exterior. Urmează ca în LAN-ul B să se extragă datele și să se citească adresa IP alocată local destinației .

Observații:

1. Există protocoale similare celor de rutare IP pentru rețelele care folosesc IPX/SPX, DECnet sau AppleTalk, eventual cu alte valori ale intervalelor de timp privind reactualizarea informațiilor (de exemplu, routerele IPX RIP transmit prin broadcast informațiile lor de stare la fiecare 60 de secunde). Fenomenul de broadcast este dificil de administrat în rețelele comutate (ISDN).

2. SAP (*Server Advertising Protocol*) este utilizat în rețele Novell, pentru transmisia periodică prin broadcast a informațiilor privind rutarea către serverele din rețea, la fiecare 60 de secunde. Routerele construiesc tabelele SAP pe care le transmit celorlalte routere din WAN, urmând ca fiecare să transmită aceste informații prin broadcast în LAN-uri, la servere.

3. Routerele IP admit definirea rețelelor locale virtuale (VLAN - *Virtual LAN*), constând în gruparea logică a nodurilor rețelei, fără a ține cont de segmentul fizic de care aparțin. În rețelele Ethernet și Fast Ethernet bazate pe VLAN-uri, se utilizează protocolul STP (*Spanning-Tree Protocol*), pentru a elimina buclele din graf și a evita apariția fenomenului "*broadcast storm*", care determină creșterea la infinit a numărului pachetelor transmise prin broadcast într-o rețea redundantă. STP configurează porturile pentru a realiza transferul sau blocarea pachetelor pe anumite căi.