Lecţia 5. Nivelul reţea în Internet. Adresarea în Internet. Rutarea fără clase

Lecţia prezentă nivelul reţea în Internet. Sunt descrise protocolul IPv4, sistemul de adresare în Internet bazat pe clase de adrese, avantajele şi limitările actuale ale acestuia, soluţiile folosite în prezent pentru depăşirea acestor limite (IPv6, rutarea interdomenii fără clase, tehnica VLSM).

După parcurgerea şi însuşirea acestei lecţii, studentul va cunoaşte:

- *Protocolul IP şi utilizarea sa în Internet*
- *Protocoalele de control în Internet (ICMP,*
- *Sistemul de adrese IPv4 şi IPv6*
- *Clasele de adrese şi rutarea*
- *Rutarea fără clase şi tehnica VLSM*
- *Divizarea unei reţele în subreţele si alocarea optimă a adreselor*

Cuvinte cheie: Internet, protocol IP, adresă IP, mască de reţea, VLSM, QoS, CIDR, NAT, DHCP, ICMP, ARP, SIPP, IPv6, MPLS, clasa de adrese

Lucrările de laborator exemplifică practic aplicarea acestor algoritmi pentru rutarea traficului în diverse reţele locale şi de arie largă. Cu ajutorul programelor de simulare RouteSim Network Visualizer şi PacketTracer se realizează diferite scenarii şi aplicaţii de rutare. De asemenea în cadrul orelor de laborator se modelează şi simulează divizarea unei reţele în subreţele folosind tehnica VLSM şi rutarea fără clase.

Timp minim de studiu 3 ore.

Bibliografie

1. Iosif Praoveanu - Reţele de calculatoare, Ed. Universităţii Titu Maiorescu, Bucureşti 2009 - cap 4 Nivelul reţea
2. Andrew S. Tanenbaum - Reţele de calculatoare, ediţia a 4-a, Editura Byblos, Bucureşti 2004 – cap. 5 Nivelul reţea
3. Tim Parker, Mark Sportack – TCP/IP, Editura Teora, Bucureşti, 2002
4. Mike Mayers – Manualul network pentru administarea şi depanatrea reţelelor, Ed. Rosetti Educational, Bucureşti, 2008, cap. 10, cap. 11.

4.7 Nivelul rețea în Internet şi protocolul său (IP)

Internetul poate fi văzut ca **o colecție de subrețele sau sisteme autonome, interconectate ierarhic**, acoperind practic tot globul pământesc.

La baza Internetului ca structură organizatorică şi topologică stau calculatoare independente şi rețelele locale de calculatoare (LAN-uri). Ele sunt interconectate prin rețele de arie medie (MAN-uri) sau rețele regionale care la rândul lor sunt interconectate prin rețele de transport de mare viteză, numite coloane vertebrale (backbone-uri). Acestea pot avea acoperire regională, națională sau chiar continentală.

Backbone-urile sunt interconectate la rândul lor prin linii magistrale de mare capacitate şi de mare distanță, care transportă fluxuri agregate de sute Mbps sau Gbps pe canale optice, radioreleu sau satelitare. Fluxurile magistrale conțin şi alte tipuri de date decât cele provenite de la rețelele d calculatoare (canale telefonice numerice, canale radio, canale TV etc.) O structură foarte generală de astfel de rețea cu acoperire intercontinentală se poate vedea în fig.4.17.

Liantul care ține Internetul la un loc şi asigură funcționarea sa unitară este protocolul de nivel rețea **IP** (**Internet Protocol**).

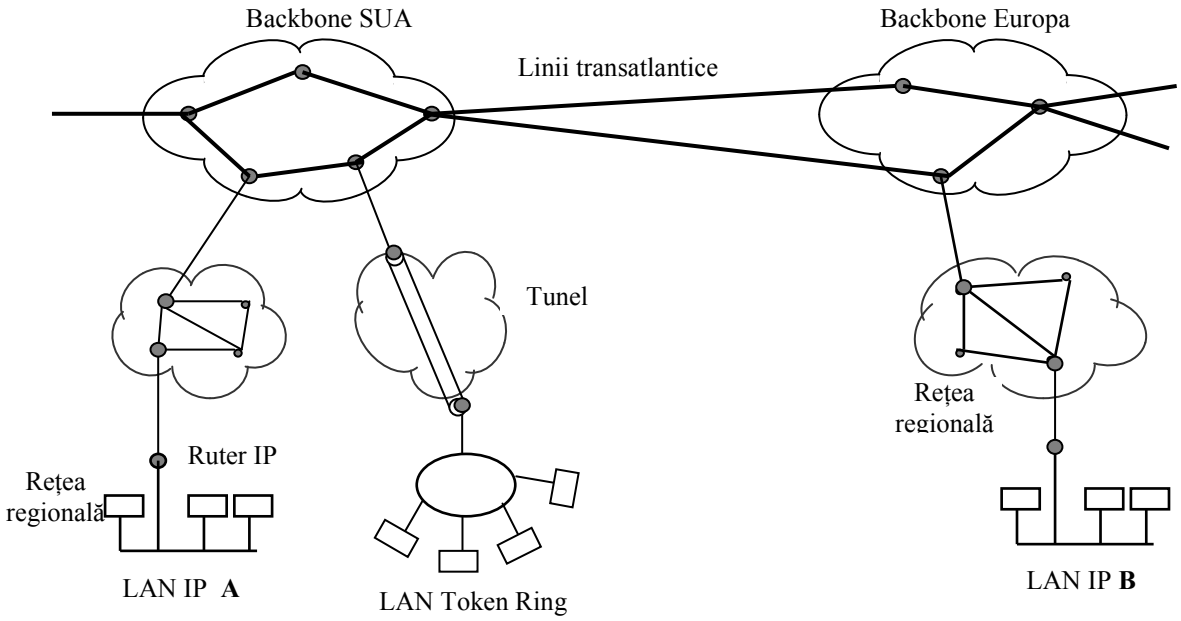

Fig. 4.17 Internetul ca o colecție de rețele interconectate

4.7.1 Protocolul IP

Protocolul IP este un protocol rutabil, capabilă să dirijeze pachetele IP prin rețea din nod în nod, de la sursă până la destinație, folosind adresele IP şi protocoalele de rutare pe baza cărora se configurează tabele de rutare din nodurile rețelei.

Un pachet IP are un antet şi o parte de date utilizator. La rândul său, antetul are o parte fixă de 20 de octeți şi o parte opțională de lungime variabilă. Pachetul este transmis începând cu cel mai semnificativ bit (**big endian**).

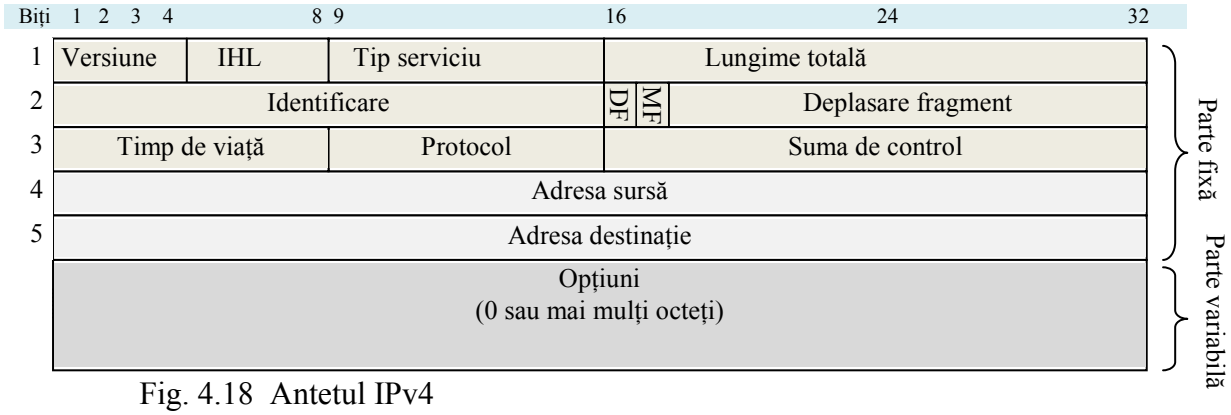

Fig. 4.18 Antetul IPv4

.

Semnificația câmpurilor din antetul pachetului IP este următoarea:

Versiune -arată cărei versiuni de protocol IP îi aparține pachetul. Aceasta face posibilă operarea simultană a mai multor versiuni, lucru necesar în perioadele de tranziție de la o versiune la alta. Unele maşini pot folosi o versiune mai veche, altele una mai nouă.

IHL – arată lungimea antetului deoarece acesta are o parte opțională de lungime variabilă.

Tip serviciu – de lungime 6 biți, permite gazdei să comunice rețelei ce tip de serviciu doreşte. Sunt posibile diferite combinații de fiabilitate şi de viteză. Pentru aplicații de transfer de voce este mai important transferul în timp real decât erorile de transmisie, pe când un transfer de fişiere este mai importantă transmisia corectă decît transmisia în timp real. La început câmpul a fost gândit astfel. Primii 3 biți erau pentru prioritate (de la 0 la 7), iar ceilalți trei pentru întârziere, productivitate şi fiabilitate. Se putea opta pentru transmisii mai puțin fiabile dar cu întârziere mică, sau o linie cu capacitate (productivitate) mare etc. În timp IETF s-a orientat pentru a folosi cei 6 biți la a indica clasele de servicii căruia aparține pachetul. Ultimii doi biți din cel de-al doilea octet nu sunt folosiți.

Lungimea totală – precizează lungimea totală a pachetului (antet plus câmpul de date). Având doi octeți pentru acest câmp, un pachet poate avea mximum 2^{16}=65 535 octeți.

Identificare – este folosit pentru a indica gazdei cărei datagrame aparține un pachet sosit. Toate pachetele unei datagrame trebuie să aibă aceeaşi valoare de identificare.

DF – înseamnă a nu fragmenta pachetele (don't fragment) pentru că destinatarul nu poate să le reasambleze. Acestă opțiune trebuie folosită cu atenție, deoarece pot apărea probleme atunci când pachetul traversează o rețea care nu acceptă pachete lungi.

MF – (more fragments) permite fragmentarea unei datagrame în mai multe fragmente. Toate fragmentele unei datagrame trebuie să aibă acest bit setat pe 1, cu exepția ultimului, care trebuie setat pe zero indicând astfel sfârşitul datagramei.

Deplasamentul fragmentului – arată locul (ordinea) fragmentului în compunerea datagramei. Toate fragmentele unei datagrame, cu excepția ultimului, trebuie să fie multiplu de 8 octeți, lungimea minimă a unui fragment.

Timpul de viață – este un contor pentru a limita durata de viață a pachetelor. Maximul de viață este 255 de secunde. El trebuie decrementat la fiecare salt dintr-o rețea în alta şi deasemenea se decrementează şi în timpul aşteptărilor în cozi. Când ajunge la zero, pachetul este distrus şi se trimite gazdei sursă un pachet de avertisment.

Protocol – spune cărui proces de nivel transport trebuie predat pachetul (protocolului TCP, UDP sau altora). Numerotarea protocoalelor este globală la nivelul Internetului şi se găseşte într-o bază de date on line, la adresa www.iana.org.

Suma de control a antetului – verifică numai antetul. Verificarea se face la fiecare salt pentru că cel puțin un bit se schimbă (bitul din câmpul timp de viață legat de salturi).

Adresa sursei **şi** ***Adresa destinației*** – indică numărul de gazdă şi numărul de rețea din care face parte gazda.

Câmpul ***Opțiuni*** – are lungime variabilă (maximum 3 cuvinte de 32 biți). El a fost introdus pentru a specifica diferite opțiuni de tipul celor descrise mai jos sau pentru folosiri ulterioare.

Câteva dintre opțiunile posibile sunt următoarele.

1. **Securitate** – menționează gradul de confidențialitate al informației.
2. **Dirijare statică de la sursă** – dă calea completă de la sursă la destinație ca o succesiune de adrese IP complete. Datagrama trebuie să urmeze această cale. Este deosebit de utilă administratorilor de rețea pentru a trimite pachete de urgență în caz de perdere a tabelelor de rutare sau pentru a realiza măsurători de timp.
3. **Dirijarea aproximativă de la sursă** – cere ca pachetul să traverseze o listă specificată de rutere şi în ordinea specificată, dar pot fi incluse în rută şi alte rutere nespecificate. Este utilă când se doreşte ca pachetele să treacă obligatoru prin unele rutere.
4. **Înregistrează calea** – obligă ruterele de pe cale să treacă în câmpul *Opțiuni* adresele IP. Este utilă în detectarea penelor în algoritmii de dirijare. Dacă pachetele trec mereu print-un ruter care, în mod normal nu ar tebui să fie în cale, indică o problemă de dirijare.

4.7.2 Adresele IPv4

Fiecare gazdă şi ruter din Internet au o adresă IP formată din două părți: **adresa de rețea** şi **adresa de gazdă**. Toate adresele sunt de 32 de biți.

Este important de precizat că o adresă IP nu se referă de fapt la o gazdă, ci la o **interfață de rețea**.

O gazdă care este conectată în două rețele are două adrese IP. Un exemplu şi mai elocvent este cel al ruterelor care interconectează două rețele: el are o adresă pentru o rețea pe o interfață şi altă adresă de rețea pe altă interfață. Tradițional, adresele IP sunt împărțite pe 5 categorii numite **clase de adrese**. În prezent acest mod de alocare nu mai este folosit, dar ajută la înțelegerea modului de organizare a rețelelor de calculatoare.

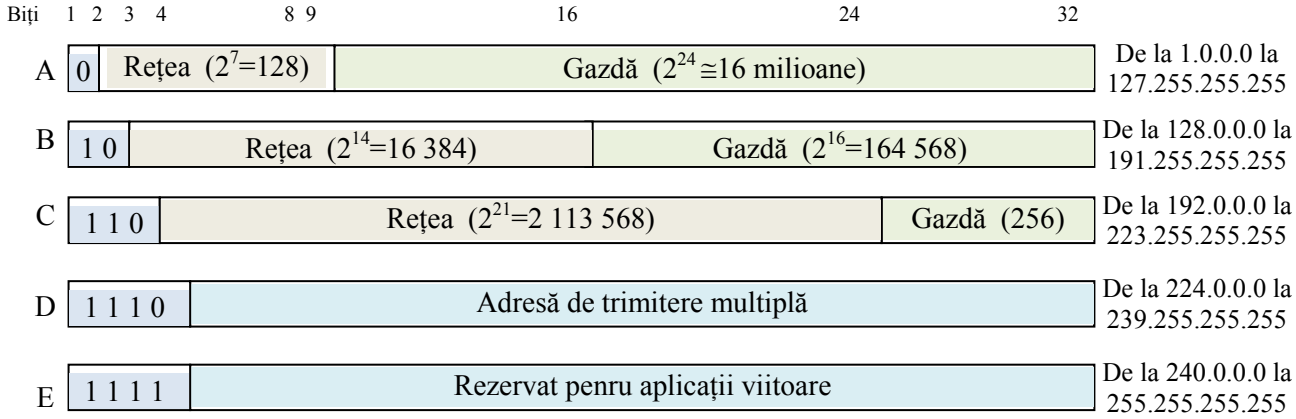

Fig. 4.19 Formatul adreselor IPv4

Formatul diferitelor adrese permite organizarea de rețele cu diverse configurații.

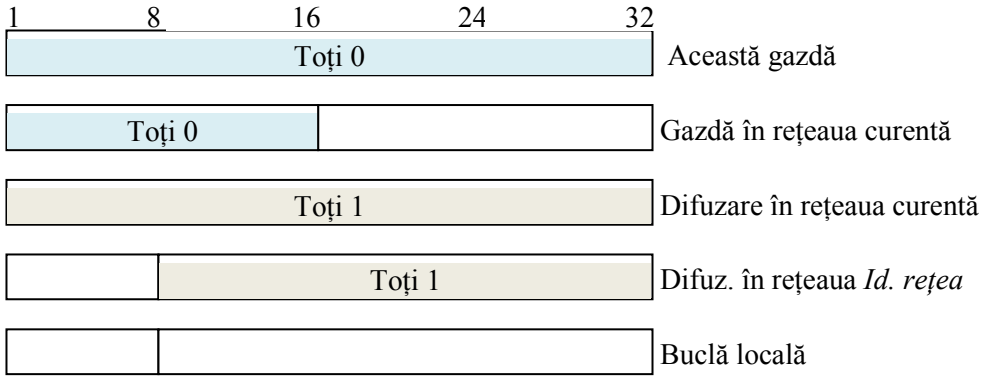

Fig. 4.20 Adrese IP speciale

Adresele care încep cu 111 au fost rezervate pentru utilizări viitoare. Există şi unele adrese speciale care permit trimiterea multiplă (multicast).

Adresele se scriu în mod curent în notația zecimală cu punct. Fiecare din cei 4 octeți poate fi scris în zecimal ca un număr între 0 şi 255. Uneori se foloseşte şi notația hexazecimală în care fiecare octet este împărțit în grupe de câte 4 biți codificat hexazecimal cu un simbol de la 0 la F.

Pentru a evita conflictele care pot apărea la atribuirea numerelor de rețea, acestea sunt administrate de **Corporația Internet pentru numere şi nume atribuite** (**ICANN – Internet Corporation for Assigned Names and Numbers**). La rândul său, ICANN a delegat diverse autorități regionale să administreze părți din spațiul de adrese de rețea, iar acestea au împărțit adrese furnizorilor de servicii Internet (ISP) şi altor companii.

4.7.3 Subrețele

Toate gazdele dintr-o rețea IP trebuie să aibă acelaşi număr (adresă) de rețea. Această particularitate a adresării IP poate crea probleme când rețeaua creşte. De exemplu o rețea LAN din clasa C poate avea cel mult 254 de maşini, iar cu timpul poate este nevoie de a introduce mai multe maşini în rețea, ceeace nu este posibil în formatul clasic de adresă IP.

Soluția problemei este divizarea unei rețele în mai multe părți de uz intern, numite **subrețele,** dar care pentru lumea externă să fie văzute ca o singură rețea. Fiecare subrețea va fi accesată printr-un ruter iar, la rândul lor, subrețelele vor fi accesate printr-un ruter principal. Tot prin acesta se va accesa şi rețeau din şi spre exterior (intrările şi ieşirile din rețea). Se crează astfel o rețea ierarhică.

Pentru a înțelege cum funcționează o rețea divizată în mai multe subrețele, se poate porni de la un exemplu de rețea de clasă B care are adresa de rețea de 16 biți şi adresa de gazdă tot de 16 biți.

Pe acesta din urmă îl împarte în 2 părți: **6 biți pentru subrețea** şi **10 biți pentru gazdă**. Această divizare permite realizarea a 64 de subrețele, cu câte 1022 de gazde fiecare (adresele 0 şi 1 fiind rezervate). În afara rețelei divizarea nu este vizibilă deoarece rețeaua este anunțată ca fiind de clasă B. Funcționarea rețelei se poate înțelege dacă se explică procesarea pachetelor IP într-un ruter. Fiecare ruter are o tabelă care memorează un număr de adrese IP de forma (**rețea,0**) şi un număr de adrese IP de forma (**această_rețea, gazdă**). Primul tip arată cum se ajunge la rețele la distanță, iar al doilea cum se accesează o gazdă din rețeaua proprie. Când soseşte un pachet IP, se citeşte adresa destinație din antet şi se caută în tabela de dirijare.

Dacă este destinat altei rețele, este transmis ruterului următor pe portul specificat în tabelă. Dacă nu găseşte adresa rețelei în tabel, trimite pachetul unui ruter implicit, care are tabele mai extinse. Dacă adresa este a unei gazde locale, pachetul este trimis imediat gazdei.

Dacă nici gazda locală nu este în tabel, întoarce un pachet de avertzare că nu există gazda respectivă. Prin urmare, fiecare ruter memorează numai rețele şi gazde, nu şi perechi (rețea, gazdă), reducând considerabil dimensiunea tabelelor de dirijare.

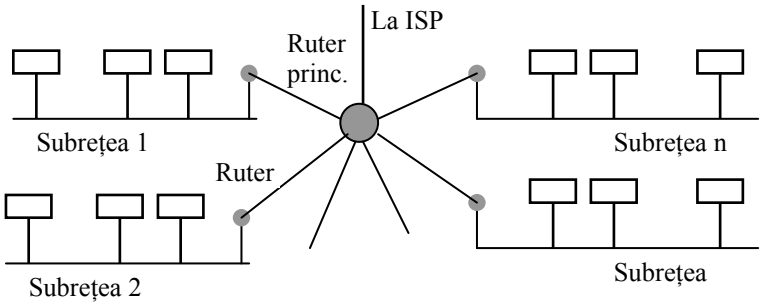

Fig. 4.21 Rețea IP cu subrețele

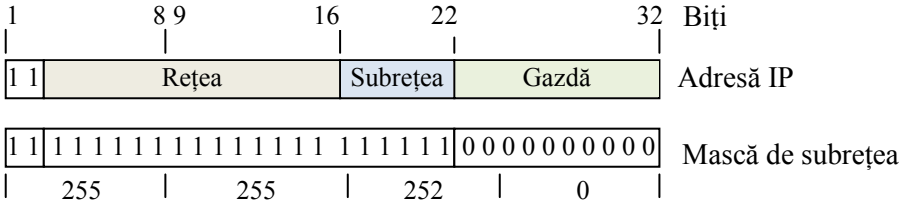

Fig. 4.22 Format de adresă şi mască de subrețea pentru o rețea IP cu 64 de subrețele

În cazul împărțirii în subrețele, tabelele de dirijare sunt schimbate, adăugînd înregistrări de forma (**această_rețea, această_subrețea, gazdă**). Astfel un ruter din subrețeaua *n* ştie cum să ajungă la toate celelalte subrețele si deasemenea la toate gazdele din subrețeaua sa. El nu trebuie să ştie detalii despre gazdele din alte subrețele.

Delimitarea dintre rețea şi subrețea se face cu ajutorul **măştilor de subrețea**.

O mască conține toți biții spațiului de rețea şi subrețea setați pe 1 şi toți biții de gazdă setați pe 0. Pentru a găsi subrețeaua, ruterul nu trebuie decât să facă un **ŞI LOGIC** dintre adresa pachetului şi masca subrețelei. Împărțirea pe subrețele crează o dirijare ierarhică pe trei nivele, rețea, subrețea şi gazdă şi reduce spațiul tabelelor de dirijare.

În afara rețelei împărțirea pe subrețele nu este vizibilă, astfel încât la alocarea unei noi rețele nu este nevoie de acordul ICANN sau de schimbarea unor baze de date externe.

În continuare se exemplifică împărțirea pe subrețele şi folosirea măştii pentru rețeaua din fig.4.21 cu adrese de clasă B, cu 6 biți pentru subrețea şi 10 pentru gazde. Se consideră o rețea a unei companii având o rețea clasă B adresa de rețea 130.50.0.0. Ea îşi propune să organizeze până la 64 de subrețele pentru a separa diferite compartimente structurale şi funcționale. Pentru aceasta împarte spațiul de 16 biți destinat gazdelor de clasă B în 6 biți pentru subrețea şi 10 biți pentru gazde. Adresele de subrețea pot fi de tipul de mai jos, fiind atribuite ruterelor de subrețea.

Subrețea 1	130.50.**4**.0	=	10000010	00110010	**000001**	|	00	00000000
Subrețea 2	130.50.**8**.0	=	10000010	00110010	**000010**	|	00	00000000
Subrețea 3	130.50.1**2**.0	=	10000010	00110010	**000011**	|	00	00000000
			Rețea		**Subrețea**		Gazdă	

Masca de subrețea va avea primii 22 de biți de valoarea 1 şi ultimii 10 de valoarea 0, adică formatul este 255.255.252.0.

Dacă ruterul principal primeşte un pachet cu adresa 130.50.15.6, el va face ŞI logic cu masca de subrețea pentru a vedea cărui ruter să-l trimită.

130.50.15.6. = 10000010 00110010 000011|11 00000110

255.255.252.0 = 11111111 11111111 111111|00 00000000

ŞI LOGOC = 10000010 00110010 000011|00 00000000 =130.50.**12**.0 = *Subrețeaua 3*

Rezultă adresa subrețelei 3. Din tabela de dirijare ruterul principal "vede" la ce port este conectat ruterul 3 şi trimite pachetul acolo.

4.7.4 Unele probleme de rutare IP şi soluții propuse

Împărțirea spațiului de adrese IP de 32 de biți în cele 3 clase uzuale (A,B,C) nu s-a dovedit a fi foarte inspirată. Cea mai utilizată clasă este B (16 384 de rețele cu câte 64 536 de gazde) a dus la epiuzarea rapidă a spațiului de adrese. Deşi teoretic sunt disponibile circa 2 miliarde de adrese, câteva sute de milioane sunt irosite prin însuşi formatul de adresă (clasa D nu foloseşte eficient primii cei mai semnificativi 3 biți). Pe de altă parte algoritmii de rutare au fost dezvoltați pe actuala structură de adrese şi au fost optimizați pentru a face prelucrare cât mai rapidă în rutere. Schimbarea claselor de adresă ar crea alte probleme.

O soluție de compromis care a dat un mic spațiu de manevră este **dirijarea fără clasă între domenii (CIDR – Classless InterDomain Routing).** Ideea de bază în CIDR este de a aloca adrese IP în blocuri de dimensiune variabilă, fără a ține cont de clase. Renunțarea la clase face însă rutarea mai complicată.

Epuizarea adreselor IPv4 a necesitat gândirea unei soluții de moment, până la introducerea IPv6. Această soluție este **translatarea adreselor de rețea** (**NAT–Network Address Translation**).

Ideea de bază a NAT este de a aloca fiecărei companii o singură adresă IP (sau cel mult câteva) pentru traficul Internet. În interiorul companiei fiecare user primeşte o adresă IP unică folosită pentru traficul intern. Când un pachet părăseşte compania şi se duce la ISP, are loc o translatare de adresă, adică o transformă în adresa reală a companiei. Translatarea o face un bloc special (unitate NAT), separată de Internet printr-un firewall. Funcționarea NAT se bazează pe nivelul transport (protocolul TCP sau UDP) şi pe porturile lui. NAT poate fi folosit

pentru a rezolva problema insuficienței adreselor IP pentru utilizatorii de ADSL şi Internet pe cablu. Cu toate acestea, mulți specialişi consideră NAT o aberație. Ea crează multe probleme:

- *violează arhitectura IP pentru că nu fiecare maşină are o adresă IP proprie;*
- *crează dependență între protocoale de pe nivele diferite;*
- *obligă folosirea TCP sau UDP, deşi ar trebui să lase loc şi altor protocoale*.

4.7.5 Protocoale de control în Internet

Pe lângă IP care este protocol de transfer de date, Internetul are protocoale de control de nivel rețea (ICMP, ARP, RARP, BOOT etc.).

Protocolul mesajelor de control în Internet (ICMP)

Funcționarea Internetului este strâns monitorizată de rutere. Când se întâmplă ceva deosebit, evenimentul este raportat prin ICMP (Internet Control Massages Protocol). Sunt definite mai multe tipuri de masaje ICMP. Fiecare tip este încapsulat într-un pachet IP.

1. *Destinație necunoscută* (destination unreachable) este folosit atunci când o rețea sau un ruter nu pot localiza destinația sau când un pachet cu bitul DF=1 nu poate fi livrat deoarece întâlneşte o rețea cu pachete mai scurte decât cel de transmis.
2. *Timp depăşit* (time exceeded) este trimis atunci când un pachet este eliminat datorită depăşirii contorului de timp (contorul ajunge la 0).
3. *Problemă de parametru* (parameter problem) indică detectarea unei valori nepermise într-un câmp din antet.
4. *Oprire sursă* (source quench) folosit pentru reglarea traficului (reducerea ratei de transmitere).
5. *Redirectare* (redirect) folosit când un ruter observă că un pachet pare a fi dirijat greşit.
6. *Cerere ecou* (echo request) şi *răspuns ecou* (echo replay) folosite pentru a vedea dacă o anumită destinație este accesibilă şi activă.
7. *Cerere amprentă de timp / Răspuns amprentă de timp* folosită pentru măsurarea întârzierilor.

Protocolul de rezoluție a adreselor (ARP)

Fiecare maşină din Internet are una (sau mai multe) adrese IP, dar ele sunt recunoscute doar la nivel rețea. De fapt ele sunt de fapt nişte puncte de acces (interfețe) de rețea.

La nivel legătură de date şi mai jos sunt alte adrese (MAC, fizice) specifice tipului de LAN la care sunt conectate calculatoarele. În prezent cele mai multe gazde unt conectate la LAN printr-o

placă de rețea care înțelege numai adresele fizice. De exemplu, orice placă Ethenet are o adresă LAN de 48 de biți implementată hard de către fabricant.

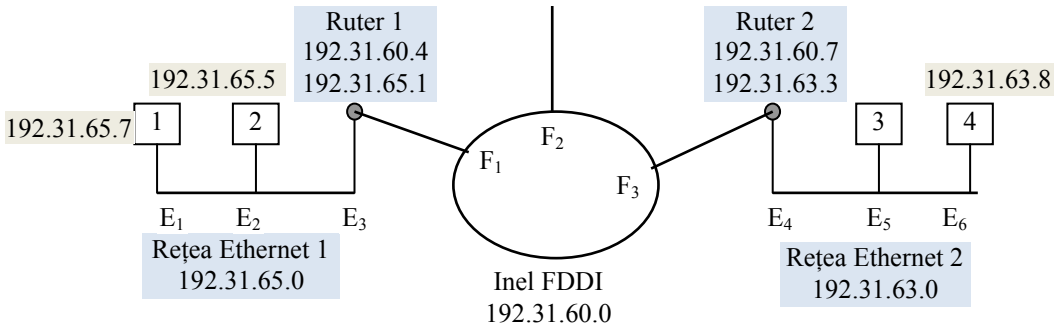

Fig.4.23 Trei rețele clasă C interconectate: două rețele Ethernet şi un inel FDDI

Administrarea adreselor LAN şi distribuirea lor producătorilor de plăci de rețea se face de către o autoritate centrală pentru ca să nu existe pe piață simultan mai multe adrese identice. Prin urmare pe un calculator gazdă se află simultan două adrese, una fizică (de 48 de biți în cazul Ethernet) şi alta IP de 32 de biți. Internetul procesează numai adrese IP iar nivelul fizic ştie numai adrese fizice. Cel care stabileşte legătura (conversia) dintre cele două adrese este ARP (Address Resolution Protocol).

Problema rezoluției de adresă se pune şi invers. Cunoscând o adresă fizică se poate afla adresa IP cu ajutorul **protocolului de rezoluție inversă a adresei** (**RARP – Reverse Address Resolution Protocol**).

4.8 Versiuni de IP

Versiunea curentă de IP este IPv4, dar devine tot mai clar că zilele sale sunt numărate. Explozia interesului față de Internet după 1990 a făcut ca să înceapă studiul unei noi versiuni care să depăşească limitele actualei versiuni. În primul rând spațiul de adrese este pe cale să se epuizeze şi trebuie căutate diferite artificii pentru accesul de noi clienți. În al doilea rând actuala versiune este destul de rigidă şi nu satisface mulțumitor noile servicii cerute de rețelele integrate, în primul rând transferul eficient de voce şi imagini video în timp real. Obiectivele majore urmărite:

1. să suporte miliarde de gazde;
2. să reducă dimensiunile tabelelor de dirijare;
3. să simplifice protocolul pentru a permite ruterelor să proceseze mai repede pachetele;
4. să asigure securitate (autentificare şi confidențialitate) mai bună decât în prezent;

5. să permită servicii diferențiate cu grad specific de QoS;
6. să permită transmiterea multiplă în rețele distante;
7. să asigure mobilitate sporită a gazdelor fără schimbarea adresei;
8. să permită operarea cu diferite tipuri de protocoale existente sau viitoare;
9. să poată conlucra încă mulți ani cu actualul IPv4.

După discuții şi propuneri diverse s-a ajuns la **Protocolul simplu îmbunătățit pentru Internet** (**Simple Internet Protocol Plus – SIPP**) cunoscut pe scurt ca **IPv6**. Menține caracteristicile bune ale IPv4, adaugă altele noi şi este compatibil cu IPv4, TCP, UDP, ICMP, IGMP, OSPF, BGP şi DNS. Este descris în RFC 2460 – 2466

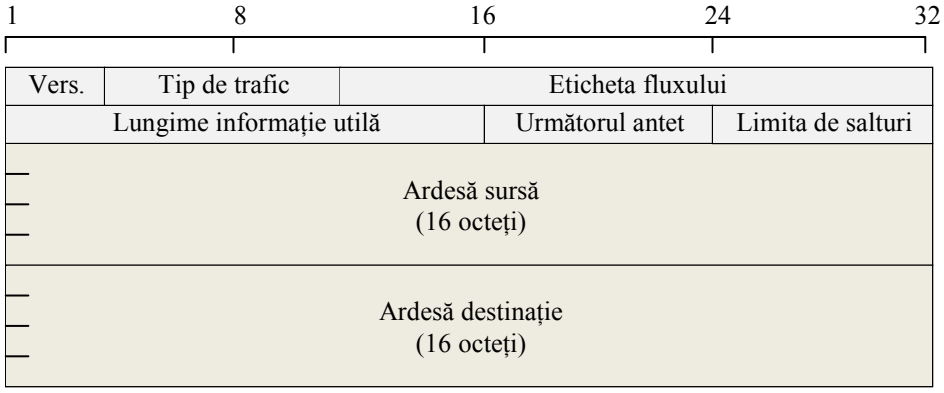

Fig. 4.24 Antetul fix IPv6

Deosebiri față de vechea versiune:

- lungimea ardeselor sursă şi destinație mult mai mare, de 16 octeți față de 4;
- simplificarea antetului care conține numai 7 câmpuri față de 13, ceea ce permite rurterelor o procesare mult mai rapidă;
- suportă mai bine opțiuni noi;
- securitate bună, permite autentificarea şi confidențialitatea;
- acordă atenție sporită tipului de serviciu.

Câmpul *Versiune* este întotdeauna 6 pentru IPv6 şi 4 pentru IPv4. Este necesar cât timp coexistă cele două versiuni pentru ca procesoarele să ştie cum să prelucreze datele din pachete.

Tip de trafic este folosit pentru a distinge pachetele care au sau nu nevoie de a fi transmise în timp real. Este util în aplicații multimedia.

Eticheta fluxului este încă experimental dar a fost gândit pentru a permite unei surse şi unei destinații să stabillescă o pseudoconexiune cu proprietăți particulare. De exemplu, rezervarea capacității de transmitere pentru un anumit şir de pachete ale unui proces aplicație între sursă şi destinație. Fiecare flux este desemnat prin cele două adrese terminale şi prin **Eticheta fluxului**. Asta înseamnă că între o pereche sursă destinație pot fi simultan mai multe

fluxuri active. Mai mult chiar, două sau mai multe fluxuri provenind de la surse diferite dar cu aceeaşi destinaţie, pot fi separate individual pe baza etichetei. În plus, ruterele de pe calea fluxului pot face comutare pe bază de etichete (**MPLS – MultiProtocol Label Switching**).

Lungimea informaţiei utile spune câţi octeţi urmează după antetul de 40 de octeţi. Dacă la IPv4 antetul are o zonă de lungime variabilă (câmpul Opţiuni) şi trebuie precizată lungimea totală, la IPv6 antetul fiind fix trebuie specificată doar lungimea informaţiei utile.

Antetul următor precizează cărui tip de protocol (TCP, UDP etc.) i se va trimite pachetul.

Limita de salturi arată cât timp poate trăi un pachet , fiind identic cu *Timp de viaţă* din IPv4.

Adresă sursă şi *Adresa destinaţie* conţin adresele respective, fiecare de câte 16 octeţi. Mărimea aleasă este considerată un compromis acceptabil între o adresă prea scurtă (4 octeţi la IPv4) şi una prea lungă. Numărul total de adrese IPv6 este $2^{128} \cong 3 \times 10^{38}$, număr foarte mare.

Pentru scrierea lor a fost inventată o nouă notaţie: 8 grupuri de câte 4 cifre hexazecimale separate prin două puncte, că în exemplul următor:

8000:000:000:000:0123:4567:89AB:CDEF

adică în total 16 octeţi. Unul sau mai multe grupuri de 16 zerouri în binar (4 zerouri în hexazecimal) pot fi înlocuite prin semnul „**:**”. În plus, un zero de la începutul unui grup de 4 cifre hexa poate fi omis, întrucât lipsa sa presupune valoarea implicită 0. Asta înseamnă că adresa de mai sus se pate scrie şi sub forma:

8000::123:4567:89AB:CDEF

O adresă IPv4 poate fi scrisă în IPv6 ca o pereche de semne :: şi vechea adresă în format zecimal cu punct:

::192.31.28.4

Câmpurile de fragmentare MF şi DF au fost eliminate deoarece Ipv6 are o abordare diferită a fragmentării. Toate gazdele şi ruterele trebuie să determine dinamic mărimea datagramei care va fi folosită, ceea ce face de la început fragmentarea mai puţin probabilă. Apoi lungimea minimă a pachetului a fost mărită de la 576 la 1280 de octeţi pentru a permite blocuri de date de 1024 octeţi. Când o gazdă trimite un pachet prea mare, ruterul care este incapabil să-l transmită dă un mesaj de avertizare gzdei să nu mai trimită lâpachete aşa lungi spre acea destinaţie.

Câmpul sumă de control a fost eliminat deoarece calculul acestuia reduce mult performanţele. Oricum nivelurile legătură de date şi transport fac asemenea verificări.

4.4 Rutarea fără clase

Strategia de adresare specifică IPv4 este în prezent depăşită şi nu mai permite dezvoltarea reţelelor la nivelul cererilor prezente şi viitoare. Până la generalizarea noii versiuni de protocol de reţea, IPv6, s-au propus diverse soluţii de depăşire a actualului impas.

O astfel de soluție care să acopere golul dintre cele două versiuni este rutarea fără clase, pe bază de adrese de lumgime variabilă (**VLSM – Subnet MaskVariable-Length**). Folosind VLS, un administrator de rețea poate folosi măşti de lungime variabilă pentru gazde aflate în cadrul aceluiaşi sistem autonom. Tehnica VLSM permite subdivizarea succesivă a unei rețele ân subrețele, desigur, cu respectarea unor reguli şi cerințe date. Una din aceste cerințe de bază este că **numai o adresă de (sub)rețea neutilizată se poate diviza**. Dacă măcar o adresă dintr-o (sub)rețea este folosită, atunci (sub)rețeaua nu se mai poate diviza în continuare. O altă cerință este că VLSM se poate folosi numai împreună cu protocoate care suportă această tehnică. Ruterele CISCO suportă VLSM împreună cu OSPF, IS-IS (Intermediate System- Intermediate System), EIGRP, RIPv2, ruterea statică etc.

VLSM este un artificiu care prmite unui singur sistem autonom să aibă rețele cu diferite măşti de subrețea. VLSM ajută să se administreze optim adresele IP, în special când este vorba de LAN-uri interconectate prin linii punct la punct. Cu o mască de rețea de lungime potrivită se asigură conexiunile din interiorul LAN-uli, iar cu alta se asigră conexiunile punct la punct. Fără VLSM, legăturile WAN trebuiesă aubă acceaşi mască de subrețea ca şi segmentele LAN.

De exemplu, dacă un client doreşte să realizeze câteva rețele locale cu un număr de ordinul zecilor de gazde (să zicem între 10 şi 60), rețele interconectate între ele, ar putea folosi câte o adresă de clasă C în fiecare rețea, adresă care admite până la 254 de gazde. Diferența de adrese până la 254 de din fiecare rețea ar fi irosită, deoarece adresa de rețea trebuie să fie diferită de la o rețea la alta. În plus, pentru interconectarea rețelelor locale, sunt necesare alte adrese de rețea, câte o pereche pentru fiecare legătură punct la punct, ceea ce înseamnă irosirea a câte 252 de adrese de gazdă.

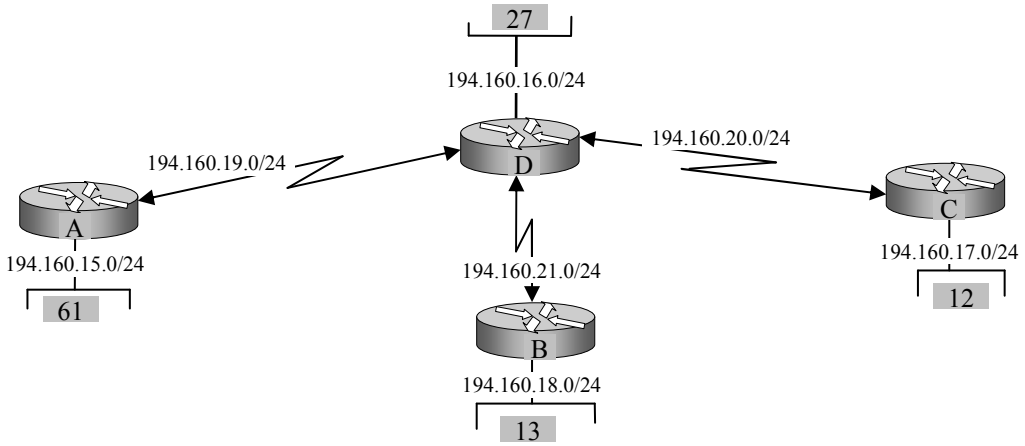

Fig. 4.11 Configurație de 4 rețele clasă C interconectate

O soluție mai bună este împrumutarea în spațiul de rețea de 24 de biți a unui număr oarecare de biți din cei 8 ai spațiului de gazdă. În cazul exemplului dat, unde numărul maxim de gazde este 60, se pot împrumuta 2 biți. Aceasta înseamnă că se poate folosi o singură adresă

clasă C, care se subdivide în 2^2=4 subrețele, fiecare cu maximum 62 de gazde. În această ipoteză, cele 4 adrese de rețea vor fi:

194.160.15.0/26
194.160.15.64/26
194.160.15.128/26
194.160.15.192/26

Mai mult chiar, dacă una sau mai multe subrețele au mai puțin de 30 gazde, se pot subdiviza la rândul lor în sub-subrețele, prin folosirea unor măşti de lungime mai mare.

Adresa de rețea locală deservită de ruterul A va fi 194.160.15.0/26. Gazdele din această rețea vor avea adresele 194.160.15.1 ... 194.160.15.62, rămânând liberă adresa 194.160.15.63.

Pentru rețeaua ruterului D cu 27 de gazde, se poate folosi o mască de 27 biți. Adresa de rețea va fi 194.160.15.64/27, iar adresele de gazdă: 194.160.15.65, 194.160.15.66 ..... 194.160.15.92. Rămân libere adresele de gazdă 194.160.15.93 ... 194.160.15.95.

Pentru rețelele ruterelor B şi C se pot folosi măşti de rețea de 28 biți (2^4-2=14 gazde).

Adresa de rețelei B va fi 194.160.15.96/28 cu adresele de gazdă 194.160.15.97 .... 194.160.15.109, ramânând liberă adresa 194.160.15.110 .

Adresa de rețelei C va fi 194.160.15.112/28 cu adresele de gazdă 194.160.15.113 .... 194.160.15.125, ramânând liberă adresele 194.160.15.126 şi 194.160.15.127.

Până aici au fost alocate optim adresele celor 4 LAN-uri , inclusiv a gazdelor din fiecare. Mai trebuie alocate adresele celor 3 legături la distanță de tip punct la punct. Deoarece fiecare link este echivalent cu o rețea cu câte două adrese de gazdă (capetele legăturii), se poate folosi următoarea rețea liberă, si anume 194.160.15.128/28, care însă poate fi subdivizată în 4 subrețele, utilizând o mască de 30 de biți.

Prima subrețea va fi 194.160.15.128/30 având adresela capetelor conexiunii punct la punct 194.160.15.129 şi 194.160.15.130.

A doua subrețea va fi 194.160.15.132/30 având adresela capetelor conexiunii punct la punct 194.160.15.133 şi 194.160.15.134.

A treia subrețea va fi 194.160.15.136/30 având adresela capetelor conexiunii punct la punct 194.160.15.137 şi 194.160.15.138.

Schema de divizare a adreselor de rețea şi subrețea este următoarea:

Ruter A : 194.160.15.0/26
Ruter D : 194.160.15.64/27
Ruter B : 194.160.15.96/28
Ruter C : 194.160.15.112/28
Link A-D: 194.160.15.128/30
Link B-D: 194.160.15.132/30
Link C-D: 194.160.15.136/30

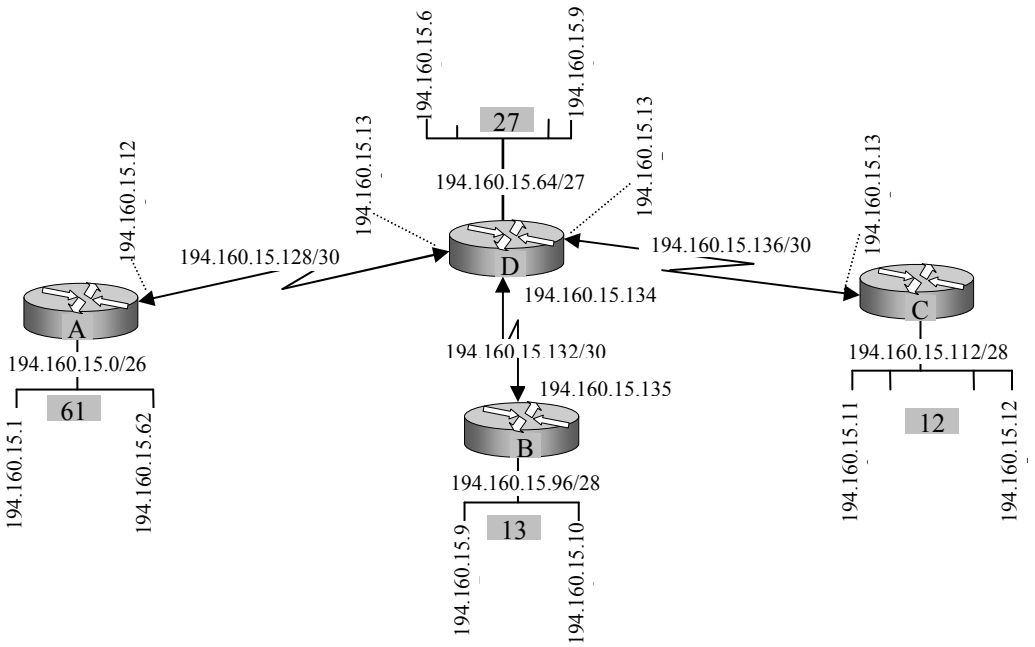

Fig. 4.12 Schema de alocare a adreselor folosind VLSM

Rezumat

Internetul este o supereţea de dimensiune globală, cu structură ierarhică, cu o mulţime de echipamente fizice, protocoale, aplicaţii şi utilizatori. Este ceea ce se cheamă un sistem deschis. Baza funcţionării Internetului este suita de protocoale definite de organizaţiile de stadardizare şi grupate în jurul a două protocoale de bază: protocolul IP şi protocolul TCP. La nivel reţea există o mare varietate de protocoale în Internet: protocoate de rutare (RIP, OSPF, BGP, IGRP etc.), protocoale de control în Internet (ICMP), protocoale de rezoluţie adrese IP cu adrese MAC (ARP, RARP). Protocolul IP şi sistemul de adrese corespunzător pe 32 biţi nu mai sunt suficiente în prezent si este în curs de generalizare versiunea nouă, IPv6. Până la generalizarea sa se folosesc unele artificii ca VLSM, CIDR, NAT.

IPv6 rezolvă problema spaţuilui de adresare în Internet şi aduce şi o serie de avantaje: simplificarea antetului, ceea ce permite rurterelor o procesare mult mai rapidă, securitate bună, permite autentificarea şi confidenţialitatea, acordă atenţie sporită calităţii serviciului etc.

Exercițiu

Stiind că VLSM ajută la setarea măştilor de subrețea ca să fie potrivite cu nevoile de segment sau de link punct la punct, să se stabilească un set de adrese IP care să asigure optim configurarea următoarei rețele, folosind o adresă de clasă B 172.20.0.0/16. Să se stabilească şi schema de divizare a adreselor.

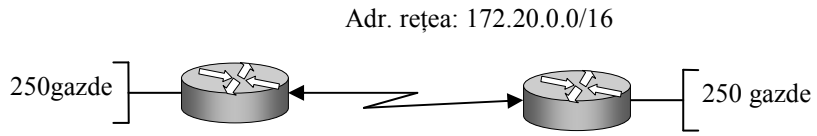

Fig. 4.13 Rețea clasă B propusă pentru confgurare de adrese

Soluție

Exemplu de mai sus conține două LAN-uri cu câte 250 de gazde. Dacă ruterele folosesc un protocol de rutare fără clase, atunci linkul WAN trebuie să fie o subrețea a aceleiaşi clase B, presupunând că administratorul nu foloseşte un IP unnumbered. Protocoalele de rutare fără clasă (RIPv1, IGRP, EGP) nu pot suporta VLSM. Fără VLSM, link-ul WAN ar trebui să aibă acceaşi mască de subrețea ca şi segmentele LAN. O mască de 24 de biți ar suporta 250 de gazde. Linkul WAN necesită doar 2 adrese, câte una pentru fiecare ruter. Asta înseamnă că ar fi irosite 252 de adrese. Dacă se foloseşte VLSM în acest exemplu, pe segmentele LAN se vor folosi în continuare măşti de 24 de biți, dar pe link o mască de 30 de biți, dintr-o subrețea neutilizată deja. Astfel, o soluție ar putea fi următoarea.

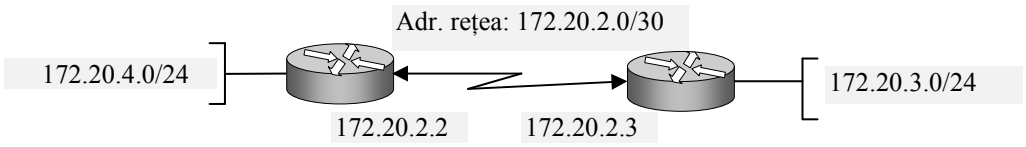

Fig. 4.14 Alocarea adreselor pentru rețeaua din fig. 4.13

Temă de casă

Descrieți un produs soft de modelare şi simulare a rețelelor de comunicații şi calculatoare.