NIVELUL REŢEA

Nivelul reţea este un nivel complex care oferă conectivitate şi selectează drumul de urmat între două sisteme gazdă care pot fi localizate în reţele separate geografic. Acesta este nivelul cel mai important în cadrul Internetului, asigurând posibilitatea interconectării diferitelor reţele. Tot la acest nivel se realizează adresarea logică a tuturor nodurilor din Internet. La nivelul reţea operează ruterele.

Nivelul Reţea este stratul cu numărul 3 corespunzător modelului OSI –figura 1.

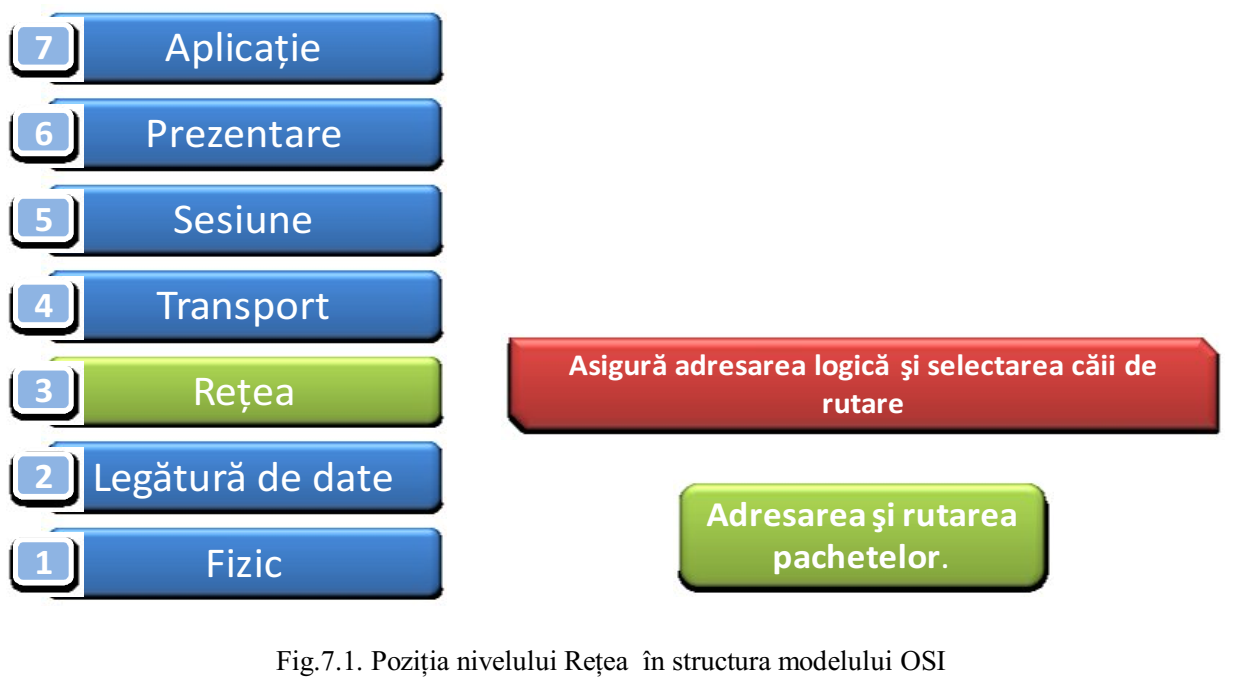


Fig. 1 Nivelul Rețea în structura modelului ISO OSI

În cadrul nivelului Reţea are loc un nou proces de încapsulare prin adaugare antetul propriu ce transformă segmentele de la nivelul Transport în pachete. Cele mai importante informaţii conţinute de acest antet sunt adresele logice ale sursei, respectiv destinaţiei. Nivelul reţea are ca sarcină principală transferul datelor de la sursă la destinaţie prin trecere din nod în nod de-a lungul reţelei. Transferul datelor la nivel reţea se poate face în modul orientat pe conexiune sau neorientat pe conexiune. Şi într-un caz şi în altul, reţeaua trebuie să poată face dirijarea pachetelor în noduri, adică să facă rutarea. Nodurile de reţea care fac dirijare se numesc rutere. Ele trebuie să fie echipamente inteligente, capabile să ia decizii de rutare optime, să aleagă calea cea mai potrivită de urmat dintre multe variante posibile. Pentru aceasta, ruterele trebuie să cunoască topologia reţelei, să aibă mereu informaţii despre starea rutelor, să poată folosi diferite criterii de performanţă pentru a compara rutele, să poată utiliza algoritmi de rutare în timp real. Prin deciziile de rutare trebuie să se asigure o încărcare cât mai uniformă posibilă a reţelei, fără a congestiona unele rute şi a lăsa neîncărcate altele. Dacă pachetele sau fluxurile de date traversează reţele diferite, interconectarea dintre ele se face prin conversie de protocol de către echipamente speciale numite porţi (gateways) care operează la nivel transport. În fiecare reţea omogenă operează protocoale specifice de nivel reţea care asigură ruterea în acea reţea. Principalul protocol implementat la acet nivel este Ipv4 (Internet Protocol version 4)

**1 Funcţiile nivelului Reţea**

Nivelul reţea, controlează operaţiile din subreţea prin crearea, menţinerea şi apoi întreruperea unei conexiuni virtuale a nivelurilor transport al calculatoarelor aflate în comunicaţie. Nivelul reţea, în cazul comunicaţiei dintre două calculatoare care aparţin unei reţele WAN, are rolul de a proteja nivelurile superioare de arhitectura fizică a reţelelor LAN, deoarece se interconectează reţele de calculatoare care au fost realizate de diferite firme care au dezvoltat propriile tipuri de reţele, bazate pe propriile standarde. În consecinţă, este important ca nivelurile superioare să nu fie dependente de tehnologia utilizată în reţelele LAN.

Principalele funcţii realizate la acest nivel sunt:

● Alegerea traseelor pentru mesajele dintre utilizatorii finali şi eventuala modificare a acestora, pentru a asigura transmiterea lor pe un traseu optim. Altfel spus se realizează alegerea traseului (path) sau căii (route), adică a succesiunii de canale fizice de la calculatorul emițător la cel receptor, pe care este transportat fiecare pachet. Procesul se numeste rutare.;

● Alocarea adreselor logice ale calculatoarelor şi efectuarea conversiilor între aceste adrese şi adresele fizice ale respectivelor calculatoare;

● Rezolvarea strangulărilor (bottleneck) provocate de prezenţa simultană a prea multor pachete în subretea, fie prin realegerea traseelor, fie cerând nivelului transport să oprească temporar emisia mesajelor;

● Realizarea conversiei dintre diferite protocoale, în situatia în care mesajele parcurg reţele eterogene, adică realizate cu tehnologii diferite (Ethernet, FDDI, Token Ring, etc).

**2. Protocolul IPv4**

Principalalul protocol al nivelului retea este protocolul IP. Acesta este un protocol fără conexiune, care asigură o transmisie nefiabilă a pachetelor de date. Un astfel de protocol este caracterizat prin faptul că fiecare pachet este considerat o entitate independentă, care nu are legătură cu celelalte pachete transmise. Adresa unică, atribuită fiecărui echipament de comunicatie dintr-o retea, se numeste adresă IP având o lungime de 4 bytes sau 32 de biţi. Procesul prin care se face alocarea adresei IP unui echipament din reţea se numeste adresare. Fiecare pachet de date, contine atât adresa IP a calculatorului sursă, cât si adresa IP a calculatorului destinatie, astfel încât poate fi transmisă si rutată independent de celelalte pachete. Protocolul IP este nefiabil, pentru că nu garantează că pachetele vor ajunge la destinaţie şi nici că transmisia lor pe canalul de comunicaţie va fi fără erori. Totuşi, pachetul IP conţine o sumă de control a antetului. Dacă antetul unui pachet IP nu este corespunzător, întreg pachetul este anulat şi nu mai este transmis nivelului superior, nivel care verifică toate datele conţinute de pachet. Protocolul IP este responsabil cu rutarea pachetelor în Internet şi cu o posibilă fragmentare a datelor. Fragmentarea unui pachet este făcută de un gateway atunci când pachetul este prea mare pentru a parcurge reţeaua prin care se va transmite, aceasta fiind o reţea de alt tip (Ethernet, Token Ring, FDDI, etc.). În acest caz, fragmentele rezultate sunt transmise în continuare ca pachete IP independente şi sunt reasamblate la destinaţie, reconstituind astfel pachetul initial. Dacă unul dintre fragmente este eronat sau pierdut, se anulează întregul pachet. În cadrul nivelului Reţea are loc o nouă împachetare a datelor. Această împachetare constă în lipirea unui antet, noile entităţi de transmisie şi de recepţie purtând numele de pachete.

Un pachet constă dintr-un antet de 20 de octeţi (plus o parte opţională cu lungime variabilă) urmat de zero sau mai mulţi octeţi de date - figura 2.

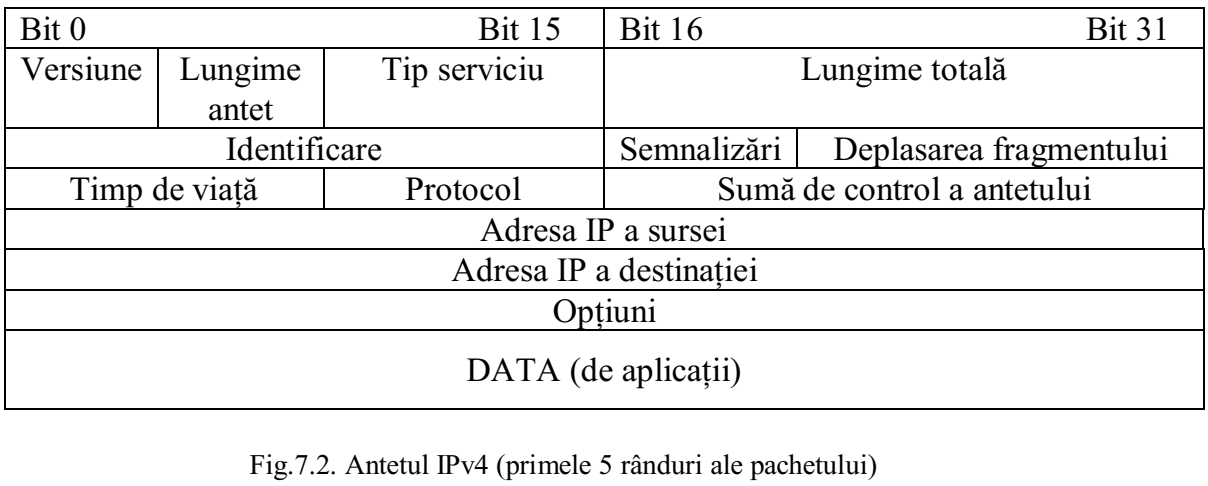


Fig. 2 Antetul IPv4 (primele 5 rînduri ale pachetului)

Semnificaţia informaţiilor introduse în antet este următoarea:

● Versiune - 4 biţi - versiunea protocolului IP utilizat. Versiunea actuală este versiunea 4, notată cu IPv4;

● Lungime antet - 4 biţi - Lungimea antetului ataşt segmentului (sau datagramei). Când a fost concepută structura unei pachet, s-a stabilit ca antetul să fie multiplu de 32 biti.

Un antet are în mod normal 20 de octeti, adică 5 blocuri de cîte 4 octeti. Ca urmare, acest câmp va contine, de cele mai multe ori, valoarea 5. Mai exact, valoarea acestui câmp este numărul binar 0101. Datele încapsulate în pachet urmează imediat după antet. Examinând câmpul Lungime antet se poate determina pozitia la care încep datele;

● Tip serviciu – 8 biţi (1 octet) – precizează informaţii referitoare la prioritatea pachetului de date. Acest câmp este împărtit la rândul său în 6 subcâmpuri care permit stabilirea priorităţilor pentru pachetul IP. Echipamentul de retea, citeşte valoarile din acest câmp, poatând lua decizii corecte pentru gestiunea datelor. Într-o reţea, sau în internet, circulă nu numai pachete de date, ci si pachete de control (informatii de routare, etc). Utilizând acest câmp se pot acorda priorităţi diferite pachetelor de control faţă de cele de date;

● Lungime totală – 16 biţi (2 octeţi) – este o valoare care specifică lungimea totală a pachetului (în octeti), incluzând şi antetul. Având 16 biti, rezultă că dimensiunea teoretică maximă este de 65.535 octeţi. La stabilirea acestei valori s-a ţinut cont de nivelul Legăturii de Date al reţelei, nivel care încapsulează diferit pachetele pentru tipuri diferite de reţele. Fiecare tip de reţea defineşte o valoare pentru dimensiunea maximă a unui pachet. Aceasta valoare se numeste unitate maximă de transfer a reţelei (MTU – Maximum Transfer Unit). Astfel, reţelele Ethernet au un MTU de 1500 octeţi, Token Ring au unitatea maximă de transfer a reţelei de 4464 octeţi.

Alte tipuri de reţea pot avea valori mult mai mici ale unităţii maxime de transfer a reţelei, chiar până la 128 octeţi. Dacă o aplicaţie încearcă să transporte un pachet IP mai mare decât MTU, se produce fragmentarea datelor, la destinaţie urmând să se producă reasamblareastora;

● Identificare – 16 biţi (2 octeţi) – permite (împreună cu câmpurile de adrese şi protocol), identificarea, pe parcursul reasamblării, a diferitelor fragmente ale pachetelor de către;

● Semnalizări – 3 biţi - este un câmp de informaţie de control format din 3 biti (un bit nefolosit), care conţine 2 indicatori:

◦ DF setat pe 1 interzice fragmentarea; DF setat pe 0 precizează că pachetul a fost fragmentat;

◦ MF setat 1 precizează că mai urmează fragmente; MF poziţionat pe 0 indică ultimul fragment al pachetului;

● Deplasarea fragmentului – 13 biţi – precizează poziţia fragmentului curent în cadrul pachetului. Toate fragmentele dintr-un pachet, cu excepţia ultimului, trebuie să fie un multiplu de 8 octeţi - unitatea de fragmentare elementară. Din moment ce sunt prevăzuţi 13 biţi, există un maxim de 8192 de fragmente pe pachet, obţinîndu-se o lungime maximă de 65536 octeţi, cu unul mai mult decît cîmpul lungime totală;

● Timp de viaţă – 8 biţi (1 octet) - este un contor folosit pentru a limita durata de viaţă a pachetelor. A fost introdus pentru a împiedica pachetele să rătăcească prin Internet. La primirea pachetului, fiecare router dintre calculatorul sursă şi calculatorul destinaţie decrementează acest câmp cu o unitate. Atunci când un pachet atinge valoarea =0TTL este distrus. În acest caz sursa este anuntată printr-un mesaj generat de protocolul ICMP (Internet Control Message Protocol). În concluzie este imposibil ca un pachet să circule la infint, deoarece după ce trece prin maximum 255 de device-uri (de exemplu routere) este distrus;

● Protocol – 8 biţi (1 octet) - permite specificarea tipului de protocol de nivel superior (nivelul Transport) utilizat (TCP, UDP, etc);

● Suma de control a antetului – 16 biţi (2 octeţi) - verifică numai antetul. O astfel de sumă de control este utilă pentru detectarea erorilor generate de locaţii de memorie proaste din interiorul unui router. Suma de control pentru toate datele încapsulate este calculată de protocoalele de nivel superior care au creat datele respective. În cazul unui segment eronat, protocolul IP nu obligă calculatorul destinaţie să trimită calculatorului emiţător (sursă) un mesaj de eroare;

● Adresa IP a sursei - 32 biţi (4 octeţi) – indică adresa logică a sursei;

● Adresa IP a destinaţiei - 32 biţi (4 octeţi) – indică adresa logică a destinaţiei;

**3. Adresarea IP**

Pentru orice comunicare în reţea trebuie să existe un mecanism de adresare, care să permită recunoaşterea unică a calculatoarelor conectate. La conceperea protocolului IP s-a impus utilizarea unui mecanism de adresare care să identifice unic fiecare dispozitiv gazdă din reţea.

O adresă IP este un număr binar pe 32 de biti, reprezentat prin 4 numere zecimale separate prin puncte, fiecare număr fiind reprezentat prin 8 biţi. Un exemplu de adresă IP este: 192.0.128.64. Această notaţie este cunoscută sub numele "dotted decimal".

Adresa IP este reprezentată în calculator în forma binară:

11000000 00000000 10000000 01000000.

*a) Clase de adrese IP; Adresarea IP pe baza claselor de adrese (Classful IP Addressing)*

Orice adresă IP este formată din două părti, una care identifică reţeaua (Network ID) şi una care identifică nodulsau gazda (Host ID). Deşi această exprimare facilitează semnificativ lucrul cu adresele IP, există unele limitări legate de uşurinta de a discerne între porţiunea de reţea şi cea de staţie din cadrul adresei IP. Încercarea de a păstra reprezentarea zecimală ca model de referinţă pentru adresa IP şi de a permite să se facă uşor distincţia între cele două componente ale adresei IP, a condus la definirea claselor de adrese IP. Au fost definite 5 clase diferite de adrese IP: A, B, C, D si E.

Se poate determina clasa din care face parte adresa IP prin examinarea primilor 4 biţi ai adresei IP:

● Adresele de clasă A sunt adresele care încep cu 0xxx, de la 1 la 126 în zecimal;

Adresele de clasă A sunt destinate reţelelor de dimensiuni mari. La aceste adrese IP, pentru definirea reţelei (network) se foloseste primul octet, iar ceilalţi trei octeţi sunt utilizaţi pentru identificarea gazdei (host), figura 3.

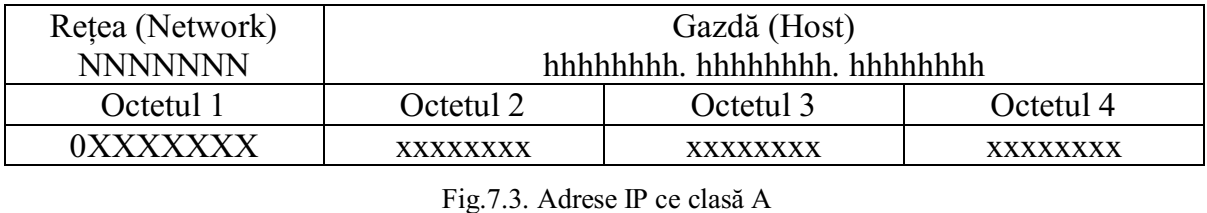
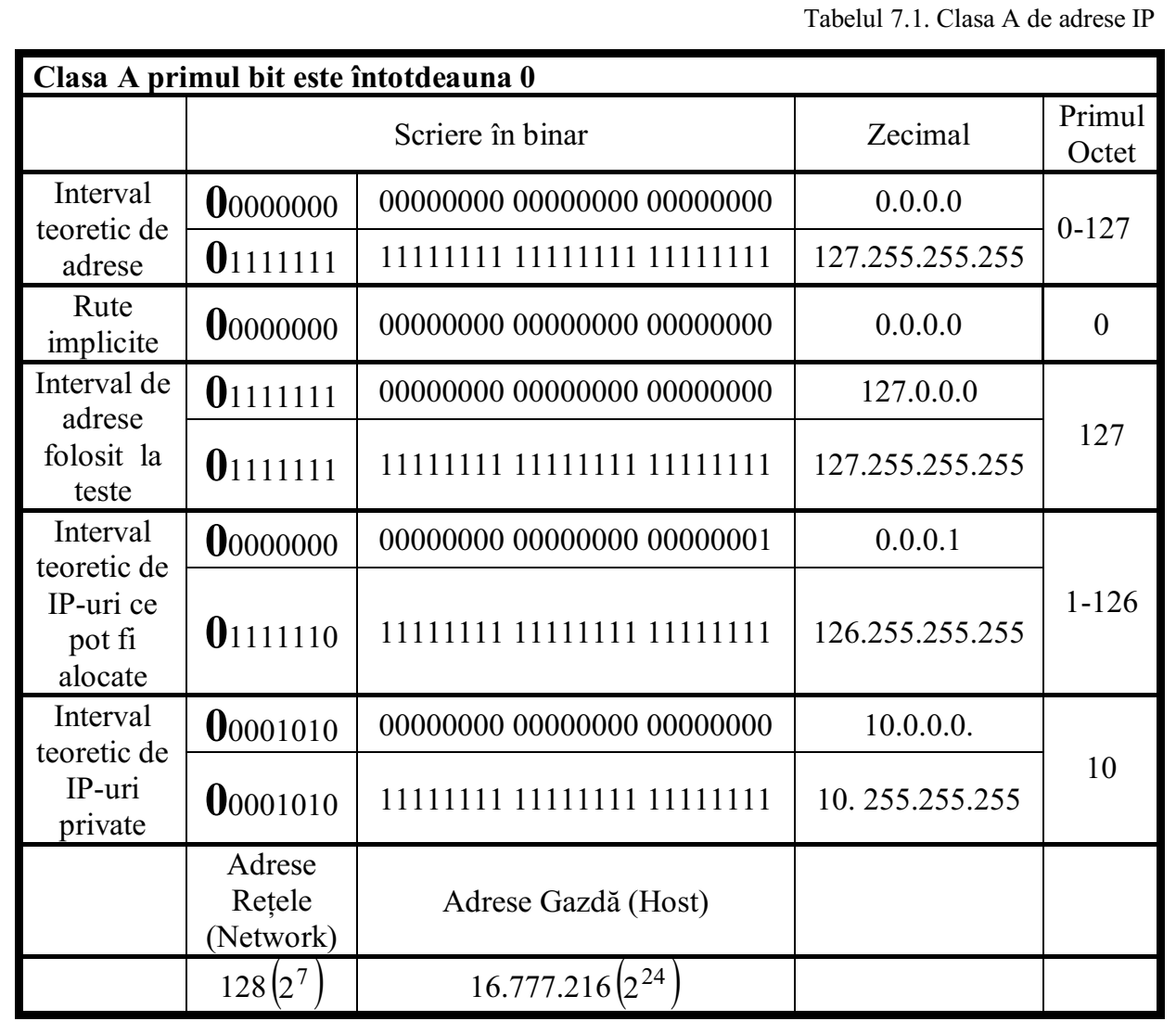


Fig. 3 Adresele IP de clasa A

Domeniul de valori pentru adresele din clasa A este de la 1 la 126, adică adresele de la 0.0.0.1 până la 126.255.255.255. Clasa de adrese 0.0.0.0 nu este folosită datorită posibilelor confuzii cu rutile implicite, iar clasa 127.0.0.0 este rezervată pentru adrese de loopback, în scopul monitorizării şi testării reţelei locale. Adresa de loopback nu poate fi accesată decât local, orice pachet trimis va avea ca destinatie exact calculatorul de pe care sunt trimise pachetele. În tabelul 1 este prezentată succint clasa A de adrese IP.

Tabelul 1 Clasa A de adrese IP



Cei 24 de biţi folositi pentru identificarea hostului, permit adresarea a 16.777.216 hosturi. Rezultă că reţelele de clasă A sunt reţele foarte mari, datorită numărului foarte mare hosturi ce pot fi adresate, folosite de companii mari şi de unele ţări.

● Adresele de clasă B sunt adresele care încep cu 10xx, de la 128 la 191 în zecimal;

Adresele de clasă B sunt destinate reţelelor de dimensiuni mai mici decât cele de clasă A. La aceste adrese IP, pentru definirea reţelei (network) se folosesc primii doi octeţi, iar următorii doi octeţi sunt utilizati pentru identificarea gazdei (host), figura 4.

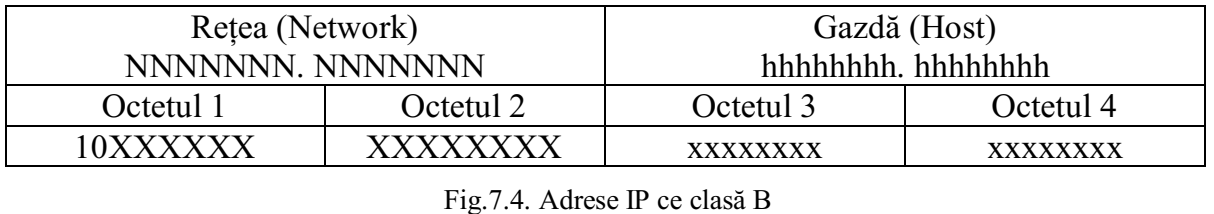
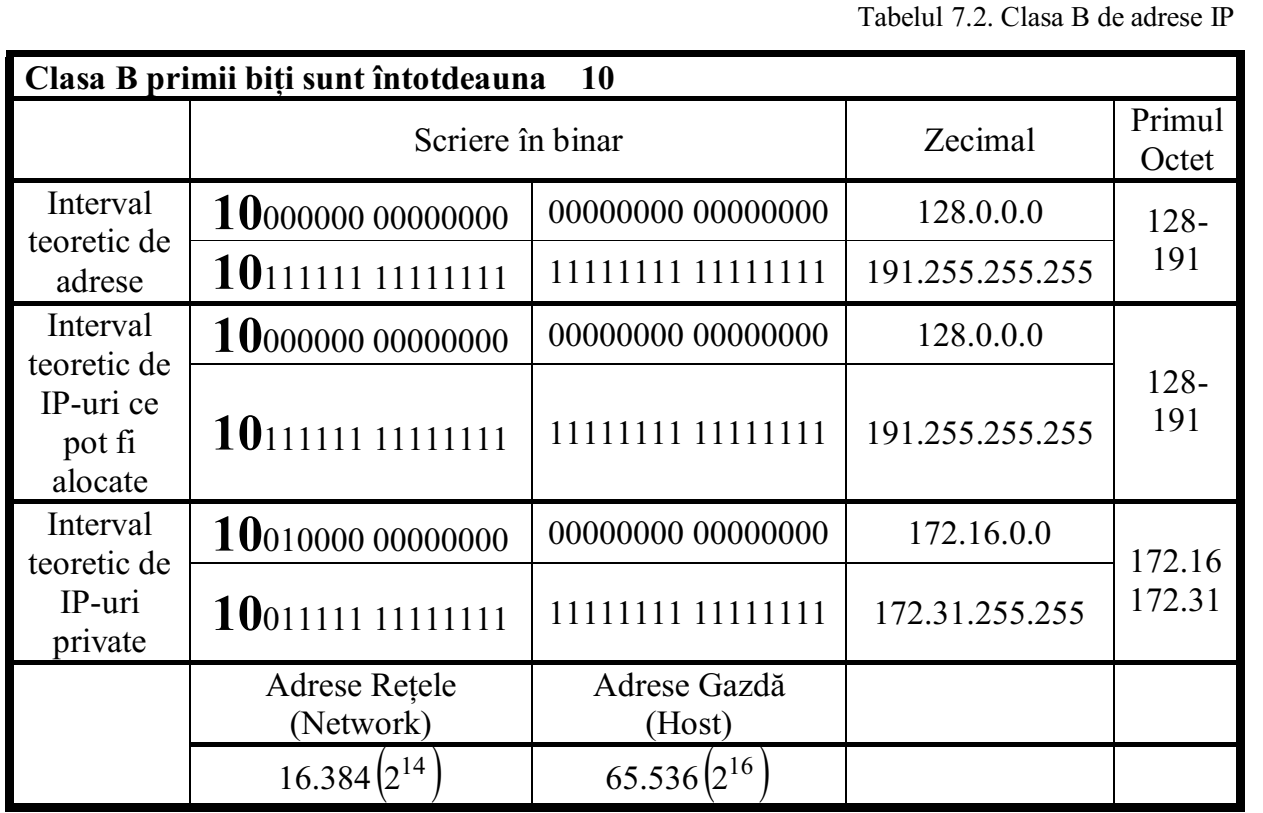


Fig. 4 Adresa IP de clasa B

Domeniul de valori pentru adresele de clasă B este de la 128 la 191, adică adresele de la 128.0.0.0 până la 191.255.255.255.

În tabelul 2 este prezentată succint clasa B de adrese IP.

Tabelul 2 Clasa B de adrese IP



În acest interval se pot adresa 16.324 reţele. Cei 16 biţi folosiţi pentru identificarea hostului permit adresarea a 65.534 hosturi. Rezultă că reţelele de clasă B sunt reţele medii spre mari, datorită numărului de hosturi ce pot fi adresate, cum ar fi cele folosite în universităţi.

● Adresele de clasă C sunt adresele care încep cu 110x, de la 192 la 223 în zecimal;

Adresele de clasă C sunt destinate reţelelor de dimensiuni mici. La aceste adrese IP, pentru definirea reţelei (network) se folosesc primii trei octeţi, ultimul fiind utilizat pentru identificarea gazdei (host), figura 5.

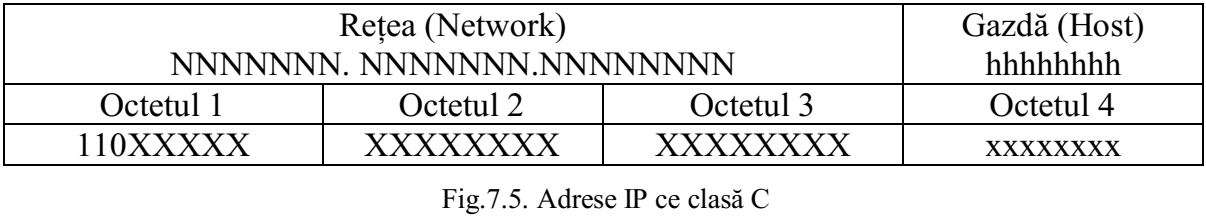
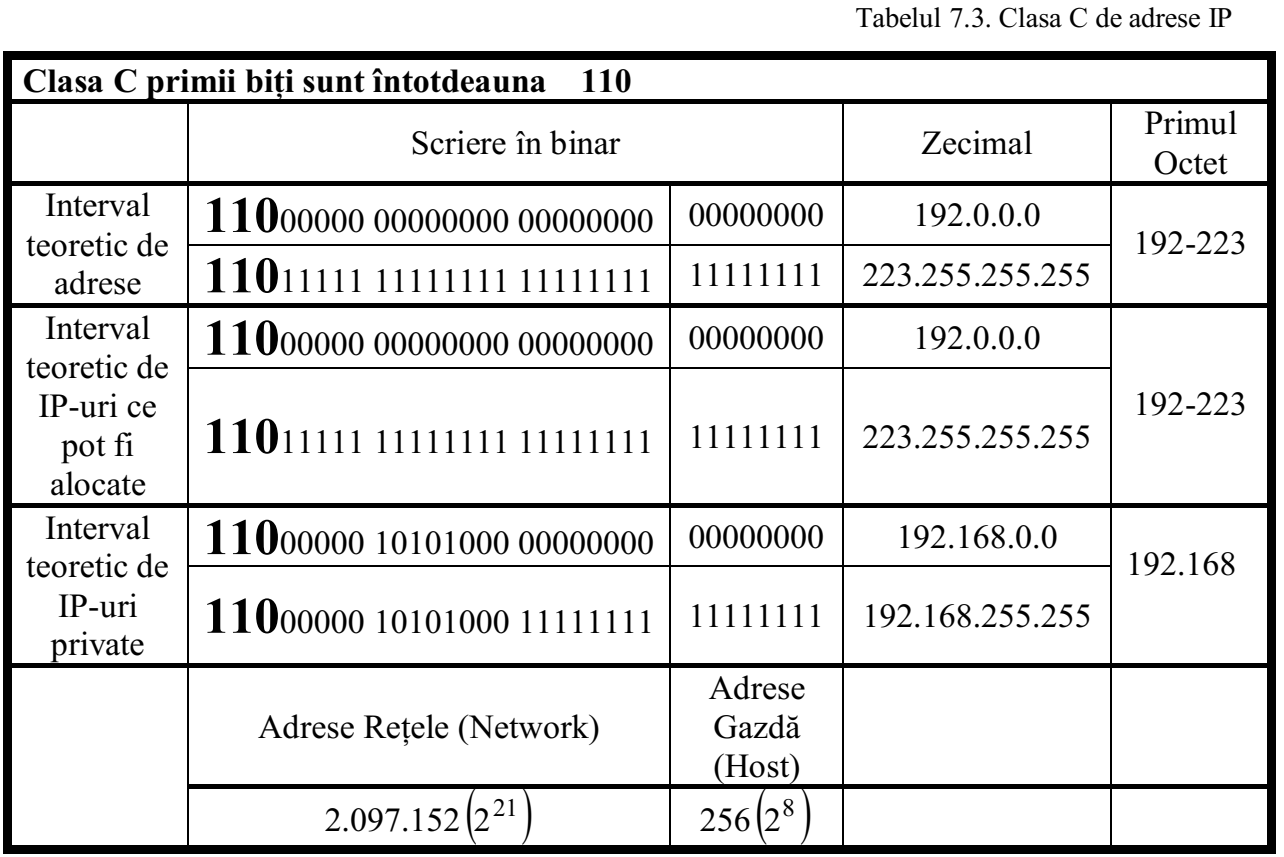


Fig. 5. Adrese IP de clasa C

Cei 8 biţi folosiţi pentru identificarea hostului permit adresarea a 256 hosturi. Rezultă că reţelele de clasă C sunt reţele mici, datorită numărului de hosturi ce pot fi adresate, cum ar fi cele folosite în departamentele universităţilor.

În tabelul 3 este prezentată succint clasa C de adrese IP.

Tabelul 3 Clasa C de adrese IP



În afară de cele trei clase de IP-uri au mai fost definite încă două, cu observaţia că aceste adrese nu vor fi alocate unor reţele.

● Adresele de clasă D sunt adresele care încep cu 1110, de la 224 la 239 în zecimal;

Adresele de clasă D sunt destinate traficului multicast, toţi cei patru octeţi fiind alocaţi pentru identificarea reţelei, figura 6.

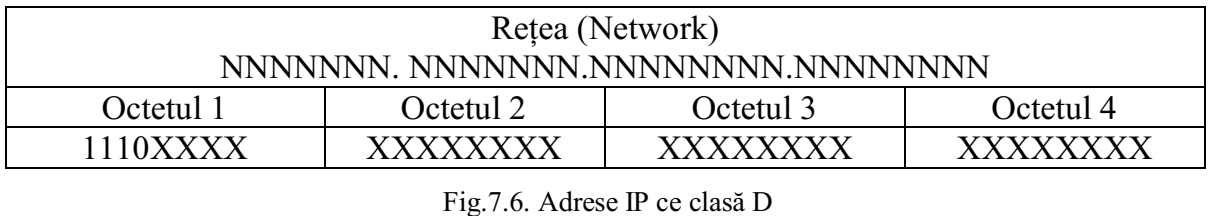


Fig 6 Adresa IP De clasa D

Domeniul de valori pentru adresele de clasă D este de la 224 la 239, adică adresele de la 224.0.0.0 până la 239.255.255.255.

● Adresele de clasă E sunt adresele care încep cu 1111, de la 240 la 254 în zecimal;

Adresele de clasă E sunt destinate utilizărilor experimentale. Domeniul de valori pentru adresele de clasă se întinde de la 240.0.0.0 până la 254.255.255.255. IANA (Internet Asigned Numbers Authority) a definit ca spaţiu de adresare private intervalele:

● 10.0.0.0 - 10.255.255.255 (clasa A);

● 172.16.0.0 - 172.31.255.255 (clasaB);

● 192.168.0.0 - 192.168.255.255 (clasa C)

Totodată intervalul 169.254.0.0 -169.254.255.255 este rezervat pentru adresarea IP automată privată (APIPA - Automatic Private IP Addressing) utilizată pentru alocarea automată a unei adrese IP la instalarea iniţială a protocolului TCP/IP peste anumite sisteme de operare. Adresele private sunt ignorate de către echipamentele de rutare ele putând fi utilizate pentru conexiuni nerutate, în reţelele locale. Restul adreselor au statutul de adrese IP publice beneficiind de vizibilitate potenţială la nivelul reţelei mondiale Internet. După cum s-a precizat anterior protocolul IPv4 defineşte adrese pe 32 de biţi, rezultând un număr de maxim de 232 (4.294.967.296) de adrese. Alocarea spaţiilor de adrese nu a fost făcută în mod eficient, acest lucru constituind în prezent un motiv care determină iminenta epuizare a adreselor IPv4. A doua problemă este cauzată de creşterea dimensiunii tabelelor de rutare. Routerele care formează coloana vertebrală (backbone) a Internetului trebuie să memoreze informaţii complete de rutare. Problema rutării nu se rezolvă doar prin instalarea unor memorii suplimentare în routere cu scopul de putea stoca tabele de rutare mai mari, ci este nevoie şi de putere de calcul sporită, astfel încât să nu fie eliminată nici o rută din cauza creşterii volumului de trafic şi a intrărilor în tabele de rutare. Soluţia acestor probleme constă în implementarea noului protocol IPv6 (IP Next Generation – IPng), însă tranziţia de la IPv4 la IPv6 nu este simplu de realizat, fiind necesar consensul marilor furnizori de servicii Internet la nivel mondial. Adresarea IP este o adresare de tip ierarhic. Acesta este motivul pentru care cei 32 de biţi ai adresei IP este împărţită în două categorii (biţii de reţea-network- respectiv biţii gazdei-host). Atunci când protocolul IP a fost standardizat (1981), specificaţiile prevedeau ca o gazdă (PC-uri, routere, imprimante, camere web, telefoane VoIp, etc) conectată la o reţea să aibă alocată o adresă unică pe 32 de biţi. Dacă o gazdă conţinea mai multe interfeţe (conexiuni la mai multe reţele), atunci fiecare interfaţă trebuia să aibă alocată propria adresă unică pe 32 de biţi. Modelul de adresare IP era format din două nivele, un nivel identifica reţeaua în care se afla gazda, iar celălalt nivel identifica gazda din reţeaua respectivă. Toate staţiile dintr-o reţea au acelaşi prefix de reţea (adrese reţele, figurile 3, 5), însă trebuie să aibă un număr de staţie unic (adrese gazdă, figurile 3, 5). În mod similar, două gazde aflate în reţele diferite trebuie să aibă prefixe diferite de reţea, însă pot avea acelaşi număr de staţie. Specificaţiile IP iniţiale împărţeau spaţiul de adrese IP în trei clase principale: A, B şi C (classful addressing). Fiecare clasă defineşte în mod diferit zona prefixului de reţea şi zona numărului de staţie. Astfel, fiecare adresă conţine o cheie care identifică în mod precis locul de demarcaţie dintre prefixul de reţea şi numărul de staţie. Această abordare simplifica procesul de rutare în trecut, deoarece protocoalele de rutare iniţiale nu furnizau o cheie de descifrare sau o mască de reţea asociată fiecărei rute pentru identificarea lungimii. Pentru împărţirea adresei IP în numărul reţelei şi a gazdei este utilizată masca IP, ce conţine 32 de biţi.

În forma binară masca de reţea este formată dintr-o:

● succesiune de biţi de valoare 1 ce corespund zonei de biţi reţea (network) a IP-ului;

● succesiune de biţi de valoare 0 ce corespund zonei de biţi gazdă (host) a IP-ului;

Masca de reţea ce este asociată adreselor IP corespunzătoare claselor A, B sau C se numeşte mască implicită (default network mask).

În figura 7 este prezentată asocierea dintre IP şi mască în cazul adresării IP pe baza claselor de adrese (Classful IP Addressing)

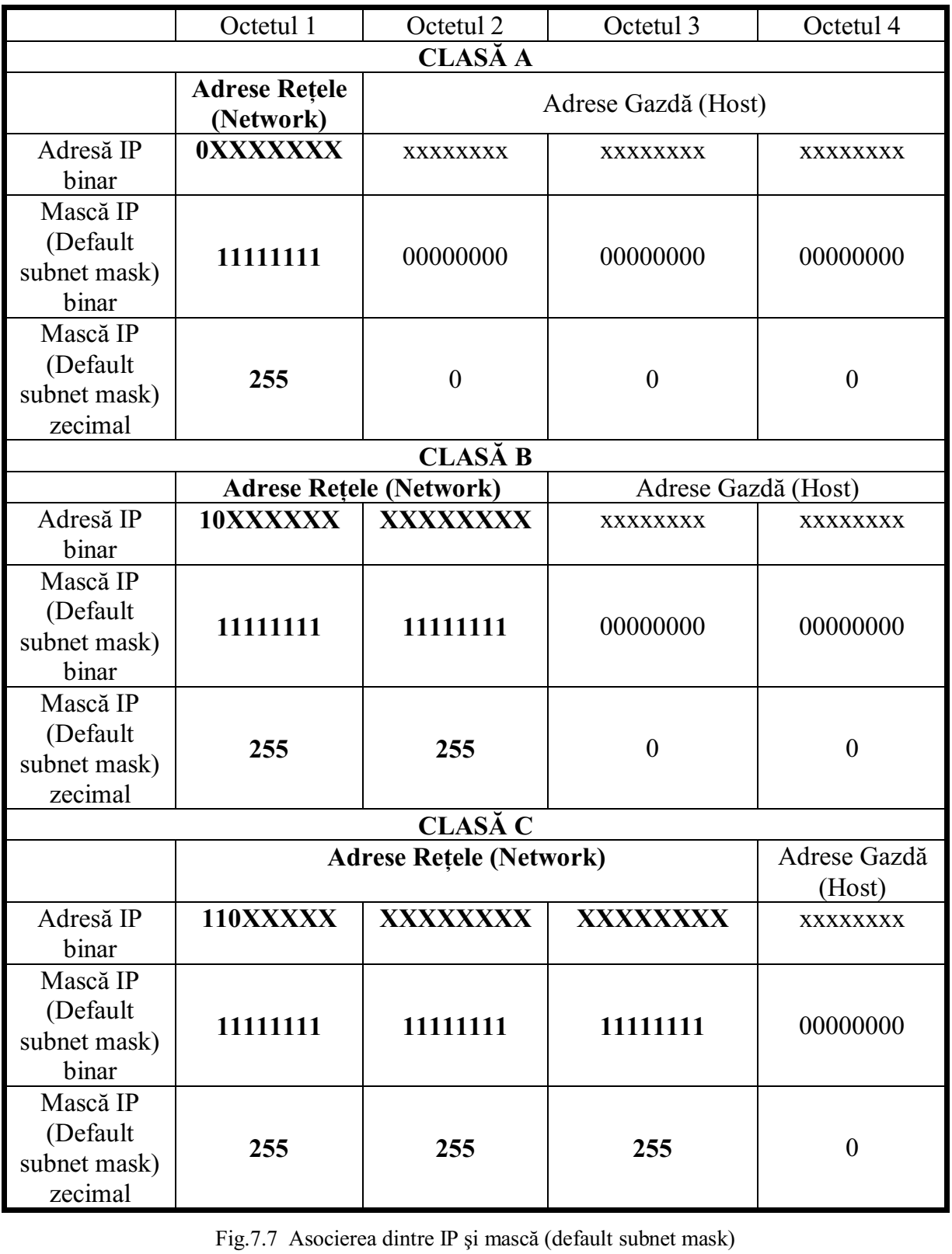


Fig. 7 Asocierea dintre IP și mască (default subnet mask)

În concluzie orice IP este insoţit de mască. În exemplul următor se prezintă această asociere pentru trei IP-uri.

● **10.**28.34.87 **255.**0.0.0

● **172.17.**56.239 **255.255.**0.0

● **192.168.0.**4 **255.255.255.**0

Există să o altă variantă (mai simplă) de a nota asocierea dintre un IP şi mască lui aferentă:

● IP/nr biţi ai reţelei

Acestă scriere poartă numele de “scriere cu prefix”, figura 8.

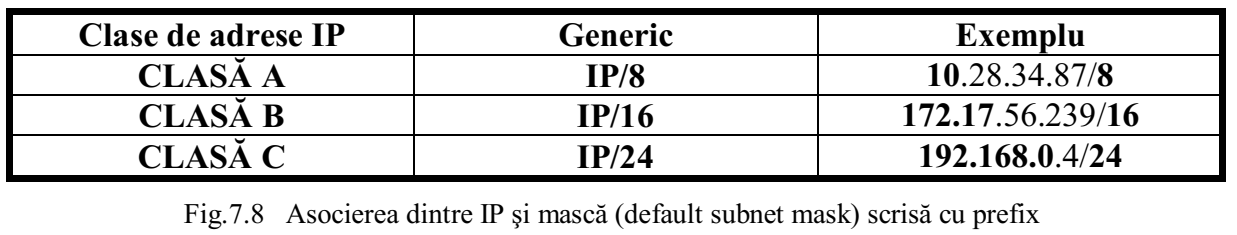


Fig.8 Asocierea dintre IP și mască (default subnet mask) scrisă cu prefix

*b) Adrese IP – CIDR - clasaless inter-domain routing*

Deoarece, la ora actuală, se conectează la Internet câte o nouă reţea la fiecare câteva minute, Internetul se confruntă cu două probleme critice:

● Depăşirea numărului de adrese IP disponibile;

Există un număr maxim de reţele şi gazde cărora le pot fi alocate adrese IP unice de 32 biţi. Iniţial s-au utilizat clasele de adrese A, B ,C. Utilizând clasele, schema de adresare în Internet poate suporta:

◦ 126 reţele de clasă A (cu maximum 16,777,214 gazde/reţea fiecare);

◦ 65,000 reţele de clasă B (cu maximum 65,534 gazde/reţea fiecare);

◦ peste 2 milioane reţele clasă C (cu maximum 254 gazde/reţea fiecare);

Deoarece adresele de pe Internet au fost alocate conform schemei de adresare pe clase (Classful IP Addressing), au rezultat o mulţime de adrese neutilizate. De exemplu, dacă sunt necesare 120 de gazde, va fi alocat un domeniu de clasă C rămânând neutilizate 134 de adrese. CIDR a fost creat pentru a permite o alocare mult mai eficientă a adreselor IP.

● Depăşirea capacităţii tabelelor de rutare globale;

Odată cu creşterea numărului de reţele conectate la Internet a crescut şi numărul de rute. S-a estimat că, în câţiva ani, routerele de pe backbone-urile Internetului vor atinge limita numărului de rute pe care le pot suporta. Chiar utilizând cele mai noi tehnologii în domeniul routerelor, valoarea teoretică maximă a numărului de intrări intr-o tabelă de rutare este de approximativ 60.000. Dacă nu s-ar fi făcut nimic Internetul şi-ar fi oprit creşterea.

Pentru rezolvarea problemei s-au dezvoltat două soluţii:

● Agregarea ierarhică a rutării în scopul minimizării numărului de intrări în tabelele de rutare;

● Restructurarea alocării adreselor IP în scopul creşterii eficienţei;

CIDR (Clasaless Inter-Domain Routing) înlocuieşte sistemul clasic de alocare al adreselor IP pe baza claselor, prin utilizarea unui”prefix” generalizat de reţea. În locul limitării ID-urilor de reţea (sau "prefixelor") la 8, 16 sau 24 biţi, CIDR utilizează în mod curent prefixe cuprinse între 10 şi 30 de biţi. Astfel, pot fi alocate blocuri de adrese de gazdă cuprinse între 2 şi peste 500.000 . Aceasta permite alocarea de domenii de adrese mult mai apropiate ca număr de necesităţile unei organizaţii. În cadrul CIDR nu mai există o delimitare rigidă între ID-ul de reţea şi cel de gazdă (pe bază de octeţi). Separarea între ID-ul de reţea şi cel de gazdă se poate face oriunde în interiorul unui octet. Adresa CIDR arată ca o adresă IP standard de 32-biţi, dar se termină cu prefixul IP de reţea (IP network prefix). De exemplu, în adresa CIDR 192.168.0.4/**26**, "/26" indică faptul că primii 26 biţi sunt utilizaţi pentru identificarea reţelei, iar restul biţilor – 6 - sunt pentru identificarea gazdei.