

# Adresarea în rețea

Stratul de rețea este responsabil pentru navigarea datelor în cadrul unei rețele. Funcția stratului de rețea este de a găsi calea cea mai bună în cadrul unei rețele. Dispozitivele utilizează schema de adresare a stratului de rețea pentru a determina destinația datelor pe măsură ce sunt deplasate în cadrul rețelei.

Suita de protocoale TCP/IP are o schemă de adresare a stratului de rețea, numită *adresare IP*. Versiunea originală a IP, IP versiunea 4 (IPv4), utilizează o adresă binară pe 32 biți. Pentru a se adapta la diferite dimensiuni de rețea, adresarea IPv4 a fost descompusă în cinci clase, de la clasa A la clasa E. În anii 1980, IPv4 a oferit o strategie de adresare care, deși scalabilă pentru un timp, a avut ca rezultate o alocare ineficientă a adreselor. În cursul ultimelor două decenii, inginerii în domeniul rețelelor au modificat cu succes IPv4 astfel încât ar putea să supraviețuiască creșterii exponențiale a Internetului. Între timp, a fost definită și dezvoltată o versiune de IP mult mai extensibilă și scalabilă, IP versiunea 6 (IPv6).

Acest capitol examinează adresarea IP și cele cinci clase de adrese IP. Acest capitol discută, de asemenea, adresele IP rezervate, care sunt adresele IP care au fost lăsate deoparte și nu pot fi atribuite pentru nici o rețea din Internet.

În final, acest capitol explorează evoluția și extensia standardului IPv4, incluzând una dintre particularitățile cheie de scalabilitate pe care inginerii au adăugat-o în cursul anilor – rutarea interdomeniu fără clase (CIDR – classless interdomain routing).

## Adresarea IP

Într-o rețea IP, stațiile finale comunică cu serverele sau cu alte stații finale. Această comunicație necesită un mod de a identifica cele două părți ale conversației. Suita de protocoale TCP/IP utilizează o adresă de 32 biți. Această adresă este denumită adresa IP. Adresa IP are o structură ierarhică. O adresă IP are două părți, după cum urmează:

- **Porțiunea de număr de rețea (network ID)** – porțiunea de număr de rețea a unei adrese IP identifică rețeaua la care este asociat un dispozitiv.
- **Porțiunea de număr de host (host ID)** – porțiunea de număr de host a unei adrese IP identifică un dispozitiv specific pe o rețea.

Împreună, aceste două părți ale adreselor ar putea identifica în mod unic oricare și în același timp toate dispozitivele conectate prin Internet. Există o combinație unică, ce cuprinde atât numărul de host, cât și numărul de rețea care face posibil accesul la orice host dat dintr-o interrețea. Adresele IP sunt la fel ca adresele pentru corespondența poștală, care descrie locația unei persoane prin furnizarea unei țări, a unui stat, a unui oraș, a unei străzi și a unui număr. Pachetul IP, care transportă informația între dispo-

zitivele din rețea, este la fel ca un plic de scrisoare conținând informația pe care utilizatorul dorește să o expedieze. În exteriorul plicului avem nevoie de adresa pentru livrare.

Un număr de rețea funcționează la fel ca un cod poștal. Un cod poștal permite sistemului poștal să direcționeze corespondența dumneavoastră la oficiu poștal local al dumneavoastră și al vecinilor dumneavoastră. De acolo, adresa de stradă orientează transportatorul la destinația corespunzătoare.

De exemplu, dacă dumneavoastră aveți o scrisoare care este adresată către „150 Tasman Drive, Los Angeles, CA 90210“, codul poștal 90210 orientează corespondența la un oficiu poștal local în Los Angeles, California. Apoi transportatorul utilizează adresa de stradă, 150 Tasman Drive, pentru a livra scrisoarea la casa corespunzătoare. În acest exemplu, codul poștal (90210) reprezintă numărul de rețea sau identificatorul de rețea (network ID) și adresa de stradă (150 Tasman Drive) reprezintă numărul de host sau identificatorul de host (Host ID).

Este important să înțelegeți semnificația identificatorului de rețea și a identificatorului de host. Secțiunile următoare discută mai detaliat despre identificatorul de rețea și identificatorul de host.

## Identificatorul de rețea (network ID)

Un *identificator de rețea* ajută ruterul să găsească o cale în cadrul interrețelei către rețeaua de destinație. Hosturile într-o rețea pot comunica direct numai cu dispozitivele care au același identificator de rețea. Ele ar putea partaja același segment fizic, dar dacă au număr de rețea diferit, de obicei nu pot comunica unul cu altul în afară de cazul când există un alt dispozitiv care poate face o conexiune între rețele.

Un identificator de rețea (network ID) permite unui ruter să pună un pachet pe segmentul de rețea adecvat.

## Identificatorul de host (host ID)

În afară față de identificatorul de rețea (network ID), protocoalele de rețea utilizează identificatorul de host (host ID). *Identificator de host (host ID) adresează* portul dispozitivului de pe rețea.

Identificatorul de host (host ID) ajută ruterul să livreze un cadru de strat 2 (cum ar fi un cadru Ethernet), încapsulând pachetul către un host specific de pe rețea. Ca rezultat, adresa IP este mapată la adresa corectă MAC (Media Access Control), necesară pentru procesarea de strat 2 pe ruter pentru a crea cadrul Ethernet. Reamintim din capitolul 17, că ARP (Address Resolution Protocol) este utilizat la determinarea adresei MAC a unui dispozitiv, dând adresa IP.

De la anumite protocoale ale stratului de rețea, un administrator de rețea atribuie numărul de host (gazdă) în concordanță cu un plan predeterminat de adresare în rețea, dezvoltat de el. Pentru alte protocoale ale stratului de rețea, atribuirea numărului de host (gazdă) este parțial sau complet dinamică sau automată. Figura 18-1 arată trei

dispozitive în rețeaua 1 (două stații de lucru și un ruter), fiecare cu un numărul de host (gazdă) unic. Figura 18-1 arată și că ruterul este conectat la două alte rețele, rețelele 2 și 3. (De notat că adresele utilizate în figura 18-1 sunt pentru ilustrarea conceptului; nu sunt adrese IP valide.)

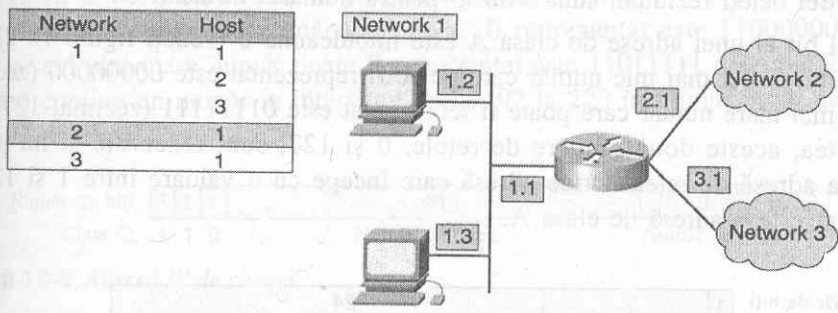


Figura 18-1 Numerele de rețea și numerele de de host-uri

## Clasele de adrese IP

Adresele IP sunt numere globale unice de 32 biți. Adresele globale unice permit dispozitivelor IP să comunice unul cu altul oriunde în lume. Pentru simplitate și claritate, acești biți sunt, în mod normal, reprezentați ca patru seturi de octeți (8 biți sau 1 byte per octet). Fiecare octet este apoi reprezentat ca număr zecimal între 0 și 255, iar numerele sunt separate prin puncte. Acest procedeu este numit *zecimală cu punct*. Așa cum se arată în următoarea listă, adresa IP 100001001010001110000000000010001 poate fi scrisă 132.163.128.17 (se citește „132 punct 163 punct 128 punct 17“):

- O adresă IP este un număr binar de 32 biți:  
100001001010001110000000000010001
- Acest număr binar poate fi divizat în patru octeți:  
10000100 10100011 10000000 00010001
- Fiecare octet (sau byte) poate fi reprezentat în zecimal:  
132 163 128 17
- Adresa poate fi scrisă în notația zecimală cu punct:  
132.163.128.17

Pentru a se adapta la diferitele dimensiuni ale rețelelor și a facilita clasificarea lor, adresele IP au fost divizate în categorii numite *clase*. Acest procedeu este numit *adresare pe clase* (*classful addressing*). Fiecare adresă IP este descompusă într-un număr de rețea (sau identificator de rețea) și un număr de host (sau identificator de host). Un bit sau o secvență de biți la începutul fiecărei adrese determină clasa adresei. Există cinci clase de adrese IP, de la clasa A la clasa E.

Secțiunile următoare descriu, mai detaliat, fiecare clasă de adrese IP.

## Adrese de clasa A

Adresele de clasa A fost proiectate să constituie suport pentru rețele extrem de mari. O adresă IP de clasa A utilizează numai primul octet pentru a indica numărul de rețea. Cei trei octeți reziduali sunt utilizați pentru numărul de host.

Primul bit al unei adrese de clasa A este întotdeauna 0 (vedeți figura 18-2). Cu acest prim bit 0, cel mai mic număr care poate fi reprezentat este 00000000 (zecimal 0), iar cel mai mare număr care poate fi reprezentat este 01111111 (zecimal 127). Cu toate acestea, aceste două numere de rețele, 0 și 127, sunt rezervate și nu pot fi utilizate ca adresă de rețea. Orice adresă care începe cu o valoare între 1 și 126 în primul octet este o adresă de clasa A.

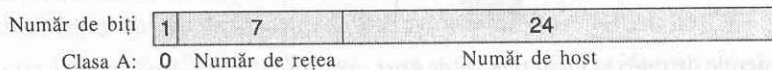


Figura 18-2 Adresă IP de clasa A

### NOTĂ

Rețeaua 0.0.0.0 este rezervată spre utilizare de către rutere, în scopul de a desemna ruta predefinită. O rută predefinită asociază o interfață specifică a ruterului cu toate adresele destinație necunoscute. Rețeaua 127.0.0.0 este rezervată pentru teste de conectare în buclă (ruterile sau mașinile locale pot utiliza această adresă pentru a expedia pachete către ele însele). Prin urmare, rețeaua 0.0.0.0 sau rețeaua 127.0.0.0 nu pot fi atribuite unei rețele.

## Adrese de clasa B

Adresele de clasa B a fost proiectate să constituie suport pentru necesitățile rețelilor de dimensiuni între medii și mari. O adresă IP de clasa B utilizează doi dintre cei patru octeți pentru a indica adresa de rețea. Ceilalți doi octeți specifică adrese de host.

Primii 2 biți ai primului octet al unei adrese de clasa B sunt întotdeauna 10 (vedeți figura 18-3). Cei 6 biți reziduali pot fi populați fie cu 1, fie cu 0. Prin urmare, cel mai mic număr care poate fi reprezentat cu o adresă de clasa B este 10000000 (zecimal 128), iar cel mai mare număr care poate fi reprezentat este 10111111 (zecimal 191). Orice adresă care începe cu o valoare în intervalul de la 128 la 191 în primul octet este o adresă de clasa B.

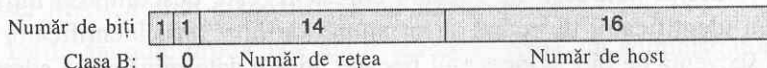


Figura 18-3 Adresă IP de clasa B



## Adrese de clasa C

Spațiul de adrese de clasa C este, în mod obișnuit, cel mai utilizat dintre clasele originale de adresă. Acest spațiu de adrese a fost proiectat să ofere suport multor rețele mici. O adresă de clasa C începe cu numărul binar 110 (vedeți figura 18-4). Prin urmare, cel mai mic număr care poate fi reprezentat este 11000000 (zecimal 192), iar cel mai mare număr poate fi reprezentat este 11011111 (zecimal 223). Dacă o adresă conține un număr în intervalul de la 192 la 223 în primul octet, aceasta este o adresă de clasa C.

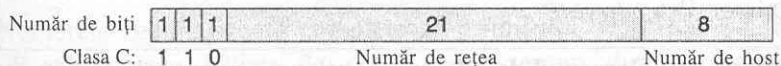


Figura 18-4 Adresă IP de clasa C

## Adrese de clasa D

Clasa de adrese D a fost creată pentru a da permite distribuția multiplă într-o adresă IP. O adresă de distribuție multiplă este o adresă unică de rețea, ce orientează pachetele cu acea adresă de destinație către grup predefinit de adrese IP. Prin urmare, o singură stație poate transmite simultan un singur flux de datagrame către beneficiari multipli.

Spațiul de adrese de clasa D, la fel ca și celelalte spații de adrese, este restricționat matematic. Primii 4 biți ai unei adrese de clasa D trebuie să fie 1110 (vedeți figura 18-5). Prin urmare, domeniul de valori al primului octet pentru adresele de clasa D este de la 11100000 la 11101111, sau de la 224 la 239. O adresă IP care începe cu o valoare în intervalul de la 224 la 239 în primul octet este adresă de clasa D.

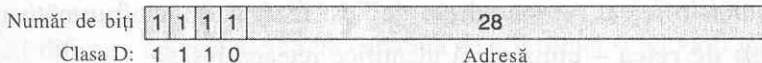


Figura 18-5 Adresă IP de clasa D

### NOTĂ

Adresele de clasa D sunt utilizate pentru grupuri de distribuție multiplă. Prin urmare, nu există o necesitate de a alocă octeți sau biți pentru a separa numărul de rețea și numărul de host.

## Adrese de clasa E

A fost definită o clasă E de adrese; cu toate acestea, Internet Engineering Task Force (IETF) rezervă aceste adrese pentru cercetările proprii. Prin urmare, nici o adresă de clasa E nu a fost autorizată pentru utilizare în Internet. Primii 4 biți ai unei adrese de clasa E sunt întotdeauna fixați la 1 (vedeți figura 18-6). Prin urmare, domeniul de valori ale primului octet pentru clasa D de adrese este de la 11110000 la 11111111, sau de la 240 la 255.

**Figura 18-6** Adresă IP de clasa E

Pentru a sumariza, tabelul 18-1 prezintă domeniul de valori al primului octet al adreselor IP (în zecimal și binar) pentru fiecare dintre cele cinci clase de adresă IP.

**Tabelul 18-1** Domeniile de adrese IP

Clasa de adrese IP	Domeniul de adrese IP (valoarea primului octet în zecimal)
Clasa A	De la 1 la 126 (de la 00000001 la 01111110) *
Clasa B	De la 128 la 191 (de la 10000000 la 10111111)
Clasa C	De la 192 la 223 (de la 11000000 la 11011111)
Clasa D	De la 224 la 239 (de la 11100000 la 11101111)
Clasa E	De la 240 la 255 (de la 11110000 la 11111111)

\*Technic, 127 (01111111) este o adresă de clasa A. Cu toate acestea, este rezervată și nu poate fi utilizată ca adresă de rețea.

## Adrese IP rezervate

Anumite adrese de host determinate sunt rezervate și nu pot fi atribuite dispozitivelor dintr-o rețea. Aceste adrese de host rezervate includ următoarele:

- **adresa de rețea** – utilizată să identifice rețeaua însăși;
- **adresa de difuzare** – utilizată la difuzarea pachetelor către toate dispozitivele dintr-o rețea.

Secțiunile următoare descriu mai detaliat adresele de rețea și adresele de difuzare.

### Adresa de rețea

O adresă IP care are 0 binar în toate pozițiile biților de host este rezervată pentru adresa de rețea. Prin urmare, să luăm ca exemplu o rețea de clasa A: 113.0.0.0 este adresa IP a unei rețele conținând hostul 113.1.2.3. Un ruter utilizează adresa de rețea IP când caută în tabelul de rutare IP locația rețelei destinație. Ca un exemplu de o rețea de clasa B, să considerăm adresa IP 176.10.0.0: este o adresă de rețea, așa cum se arată în figura 18-7.

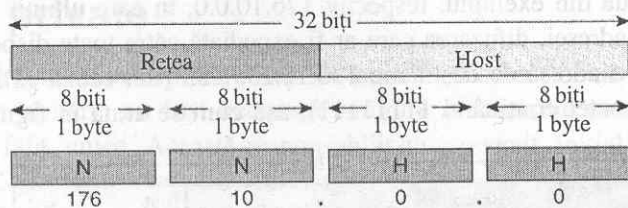


Figura 18-7 Adresă de rețea

Numerele zecimale care completează primii doi octeți într-o adresă de rețea de clasa B sunt alocate. Ultimii doi octeți conțin zerouri, din cauză că acei 16 biți sunt destinați numărului de host și sunt utilizați pentru dispozitivele asociate la acea rețea. În exemplul dat, adresa IP 176.10.0.0 este rezervată adresei de rețea; ea nu este niciodată utilizată ca adresă pentru vreun dispozitiv asociat la ea. Un exemplu de adresă IP pentru un dispozitiv de pe rețeaua 176.10.0.0 este 176.10.16.1. În acest exemplu, 176.10 este porțiunea numărului de rețea și 16.1 este porțiunea numărului de host.

## Adresa de difuzare

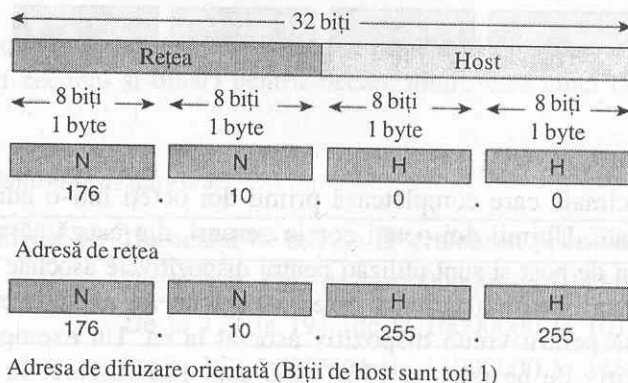
Dacă doriți să expediați date către toate dispozitivele de pe o rețea, va fi necesar ca să utilizați o *adresă de difuzare (broadcast address)*. Adresele de difuzare nu sunt niciodată valide ca adrese sursă – numai ca adrese destinație. Există diferite tipuri de adrese de difuzare, după cum urmează:

- **Difuzare locală** – Dacă un dispozitiv IP dorește să comunice cu toate dispozitivele din rețeaua locală, fixează toți biții la 1 în adresa destinație – de exemplu, 255.255.255.255 – și transmite pachetul. Această formă de difuzare nu este *niciodată* capabilă de a fi rutată și nu va fi niciodată direcționată de către rutere pe alte segmente de rețea.
- **Difuzarea orientată** – Este o difuzare locală în interiorul unei subrețele particulare, care este cea mai mică diviziune a acelei rețele locale. (Veți învăța mai mult despre subrețele în capitol 19.) O adresă de difuzare orientată conține un identificator de rețea valid (network ID) și identificator de host (Host ID) de difuzare. Difuzarea orientată este capabilă de a fi rutată. Cu toate acestea, această comportare nu este predefinită pentru ruterele Cisco. Adresele de difuzare orientată sunt discutate mai detaliat în secțiunea următoare.

### Adresa de difuzare orientată

O difuzare orientată apare când o sursă expediază date către toate dispozitivele dintr-o subrețea. Pentru a se asigura că toate dispozitive din rețea acordă atenție difuzării, expeditorul trebuie să utilizeze o adresă IP destinație pe care toate dispozitivele să o poată recunoaște și alege. Adresele IP de difuzare orientată se termină cu valoarea binară 1 în întreaga parte a adresei de host.

Pentru rețeaua din exemplu, respectiv 176.10.0.0, în care ultimii 16 biți alcătuiesc partea de host a adresei, difuzarea care ar fi expediată către toate dispozitivele din acea rețea va include o adresă de destinație 176.10.255.255 (din cauză că 255 este valoarea zecimală a unui octet conținând 11111111), așa cum se arată în figura 18-8.



**Figura 18-8** Adresa de difuzare orientată

O adresă de difuzare orientată este în întregime similară cu o corespondență poștală globală. Codul poștal orientează corespondența către zona adecvată, iar adresa de difuzare „Rezident curent“ care urmează, orientează corespondența la fiecare adresă. O adresa IP de difuzare utilizează aceeași concept. Numărul de rețea desemnează segmentul, iar restul adresei spune fiecărui host IP din acea rețea că este un mesaj de difuzare și că este necesar ca dispozitivele să acorde atenție mesajului. Toate dispozitivele din acea rețea vor recunoaște adresa de difuzare pentru rețeaua lor, la fel ca pe propria adresă de host IP.

## Hosturile pentru clasele de adrese IP

Fiecare clasă de rețele permite un număr fixat de hosturi. Într-o rețea de clasă A, primul octet este atribuit rețelei, ultimii trei octeți (24 biți) fiind lăsați spre atribuire hosturilor. Amintiți-vă că prima adresă de host în fiecare rețea (toți biții 0) este rezervată adresei concrete de rețea, iar adresa de host finală în fiecare rețea (toți biții 1) este rezervată pentru difuzare. Numărul maxim de hosturi într-o rețea de clasă A este  $2^{24} - 2$  (se scad adresele de rețea și de difuzare, care sunt rezervate), adică 16777214 hosturi.

Într-o rețea de clasă B, primii doi octeți sunt desemnați pentru rețea, cei doi octeți finali (16 biți) fiind lăsați spre atribuire hosturilor. Numărulul maxim de hosturi într-o rețea de clasă B este  $2^{16} - 2$ , adică 65534 hosturi.

Într-o rețea de clasă C, primii trei octeți sunt atribuiți rețelei. Octetul final (8 biți) rămâne a fi atribuit hosturilor, astfel că numărul maxim de hosturi este  $2^8 - 2$ , adică 254 hosturi.

## Adrese IP private

Stabilitatea Internetului depinde direct de unicitatea adreselor de rețea utilizate în mod public. Prin urmare, au fost necesare anumite mecanisme pentru a asigura că adresele erau, în fapt, unice. Această responsabilitate a revenit, inițial, unei organizații numite InterNIC (Internet Network Information Center). Această organizație este acum defunctă și a fost succedată de IANA (Internet Assigned Numbers Authority). IANA administrează cu grijă fondul rezidual de adrese IP pentru a asigura că nu se produce duplicarea adreselor utilizate în mod public. O astfel de duplicare ar cauza instabilitate în Internet și ar compromite capacitatea de a distribui datagrame în rețelele care utilizează adrese duplicate.

Hosturile Internet necesită o adresă IP unică global, rutabilă, numită *adresa publică IP* (veți învăța mai multe despre adresa publică IP ulterior în acest capitol). Cu toate acestea, hosturile private care nu sunt conectate la Internet pot utiliza orice adresă validă, atât timp cât este unică în interiorul acelei rețele private.

Aceste adrese sunt numite *adrese IP private*. Din cauză că există multe rețele private alături de rețelele publice, a căuta orbește orice adresă posibilă este o practică foarte nerecomandată. RFC 1918, „Address Allocation for Private Internets“, (Alocarea adreselor pentru interneturi private) pune deoparte trei blocuri de adrese IP (înseamnă câte un domeniu în clasa A, în clasa B și în clasa C) pentru utilizare internă, privată (vedeți tabelul 18-2). Adresele IP private sunt definite ca nerutabile pe Internet și sunt utilizate exclusiv într-o rețea privată. Adresele din acest domeniu nu sunt rutate pe magistrala Internet; ruterele Internet resping imediat adresele private.

**Tabelul 18-2** Adrese IP private

Clasa	Domeniul de adrese interne conform RFC 1918
A	De la 10.0.0.0 la 10.255.255.255
B	De la 172.16.0.0 la 172.31.255.255
C	De la 192.168.0.0 la 192.168.255.255

### NOTĂ

Puteți găsi toate RFC-urile online la [www.isi.edu/in-notes/rfc xxx txt](http://www.isi.edu/in-notes/rfc xxx txt), unde *xxxx* este numărul de RFC. Dacă nu cunoașteți numărul de RFC, îl puteți găsi făcând o căutare a subiectului pe [www.rfc-editor.org/rfcsearch.html](http://www.rfc-editor.org/rfcsearch.html).

Dacă adresați un intranet nonpublic, un laborator de testare, sau rețeaua la domiciliu, aceste adrese private pot fi utilizate în loc de adresele globale unice.

Conectarea la Internet a unei rețele care utilizează adresele private necesită o traducere a adreselor private în adrese publice. Acest proces de traducere este denumit *NAT (Network Address Translation)*. Un ruter sau un firewall este de obicei dispozitivul care efectuează NAT.



Utilizarea adreselor RFC 1918 și NAT face ca toate adresele de pe Internet să fie accesibile. Dacă erau căutate la întâmplare, secțiunea Internetului care utiliza aceea adresă înregistrată ar fi fost confundată cu intranetul local și, astfel, ar fi fost inaccesibilă.

## NOTĂ

NAT, așa cum este definit de către RFC 1631, este procesul de schimbare a unei adrese în alta în antetul pachetului IP. În practică, NAT este utilizat pentru a permite accesul la Internet al hosturilor cu adrese IP private.

Un dispozitiv capabil de NAT, cum ar fi un ruter Cisco sau un firewall, funcționează la frontiera unui domeniu buclă deschisă (*stub*) (o interrețea care are o singură conexiune cu exteriorul lumii. Când un host din interiorul acestui domeniu dorește să transmită către un host din exterior, dirijează pachetul la dispozitivul capabil de NAT. Procesele NAT caută apoi în interiorul antetului IP și, dacă este cazul, înlocuiesc adresa IP locală (interioară sau privată) cu o adresă IP globală, unică. Când hostul exterior expediază un răspuns, procesul NAT îl recepționează, verifică tabelul curent de adrese de rețea translate și înlocuiește adresa destinație cu adresa sursă interioară originală.

## Adrese IP publice

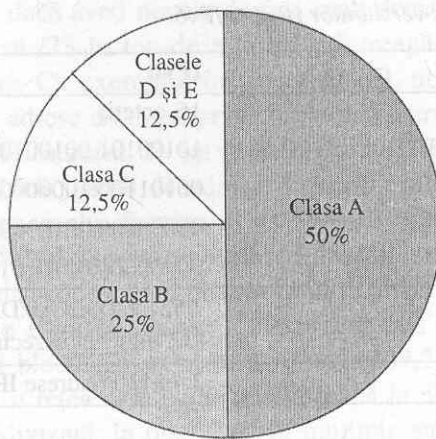
Adresele publice IP sunt unice. Nu există două mașini care să fie conectate la o rețea publică și să poată avea aceeași adresă IP: Adresele IP publice sunt globale și standardizate, iar toate mașinile conectate la Internet agreează să adere la sistem. Adresele publice IP trebuie să fie obținute de la furnizorul de servicii Internet (ISP - Internet service provider) sau să fie înregistrate cu anumite cheltuieli.

Datorită creșterii rapide a Internetului, adresele publice IP încep să se epuizeze, astfel încât, pentru a ajuta la rezolvarea problemei, au fost dezvoltate noi scheme de adresare, cum ar fi rutarea interdomeniu fără clase (CIDR - classless interdomain routing) și IPv6 (IP versiunea 6). CIDR și IPv6 sunt discutate în următoarele două secțiuni.

## IPv4 și IPv6

Când a fost introdus TCP/IP, în perioada 1980, se baza pe o schemă de adresare pe două niveluri, care în acel moment oferea o scalabilitate adecvată. Din nefericire, arhitecturii TCP/IP nu au putut să prevadă că, până la urmă, protocolul lor va susține o rețea globală de informație, comerț și distracție. Acum 20 de ani, IP versiunea 4 (IPv4) a oferit o strategie de adresare care, cu toate că a fost scalabilă pentru a timp, a avut ca rezultat o alocare ineficientă a adreselor.

Adresele de clasa A și de clasa B alcătuiesc 75 procente din spațiul de adrese IPv4, dar numai unui număr relativ mic de organizații (sub 17000) le poate fi desemnat un număr de rețea de clasa A sau de clasa B. Adresele de rețea din clasa C sunt, de departe, mult mai numeroase decât adresele de clasa A și de clasa B, deși totalizează numai 12,5 procente din cele 4 miliarde de adrese IP posibile a fi disponibile în IPv4, așa cum se arată în figura 18-9.



**Figura 18-9** Alocarea adreselor în IPv4

Din nefericire, adresele de clasa C sunt limitate la 254 de hosturi, valoare care nu îndeplinește cerințele unor organizații mai mari, dar care nu pot dobândi o adresă de clasa A sau B. Chiar dacă ar exista mai multe adrese de clasele A, B și C, prea multe adrese de rețea ar putea cauza o blocare a rutelor Internet sub povara unor dimensiuni enorme pentru tabelele de rutare necesare pentru a stoca rutele de accesare a fiecărei rețele.

Încă din 1992, Internet Engineering Task Force (IETF) a identificat două preocupări specifice:

- **Epuizarea adreselor de rețea IPv4 reziduale, nedesemnate** – înainte de anii 1990, spațiul clasei B a fost la limita epuizării.
- **Creșterea rapidă și substanțială în dimensiune a tabelelor de rutare Internet** – Pe măsură ce tot mai multe rețelele de clasa C devin online, inundarea cu noua informație de rețea care rezultă amenință capacitatea rutelor Internet de a procesa eficient informația.

În cursul ultimelor două decenii, au fost dezvoltate numeroase extensii la standardul IPv4, destinate în mod specific să îmbunătățească eficiența cu care pot fi utilizați cei 32 biți ai spațiului de adrese.

Două dintre cele mai importante sunt măștile de subrețea și rutarea interdomeniu fără clase (CIDR – classless interdomain routing), discutate mai detaliat în următoarea secțiune și în capitolul 19.

Între timp, a fost definitivată și dezvoltată o versiune de IP mult mai extensibilă și scalabilă, IP versiunea 6 (IPv6). IPv6 utilizează valori binare de 128 biți, care pot fi afișate ca 32 digiți hexazecimali. IPv6 furnizează  $3,4 \times 10^{38}$  adrese IP. Această versiune de IP ar asigura suficiente adrese pentru necesitățile viitoare, dacă vor fi utilizate cu înțelepciune. Tabelul 18-3 compară caracteristicile versiunilor IPv4 și IPv6.

IPv4	IPv6
4 octeți:	16 octeți:
11010001.10011100.11001001.01110001	10100101.00100100.01110010.11010011. 00101100.10000000.11011101.00000010. 00000000.00101001.11101100.01111010. 00000000.00101011.11101010.01110011
209.156.201.113	A524:72D3:2C80:DD02:0029:EC7A:002B:EA73 (32 digiți hexazecimali)
4294467295 adrese IP	3,4 x 10 <sup>38</sup> adrese IP

IPv6 este implementat mai lent în anumite rețele. Până la urmă, IPv6 poate înlocui IPv4 ca protocol Internet dominant.

## CIDR

Așa cum ați învățat în secțiunea precedentă, IPv4 original definește adresele IP într-o structură de cinci clase majore de adrese, de la clasa A până la clasa E. Utilizând IPv4, Internetul a depășit spațiul de adrese foarte repede.

Rutarea interdomeniu fără clase (CIDR – classless interdomain routing) este o nouă schemă de adresare pentru Internet care permite o mult mai eficientă alocare a adreselor IP decât vechea schemă cu clasele de adrese A, B și C.

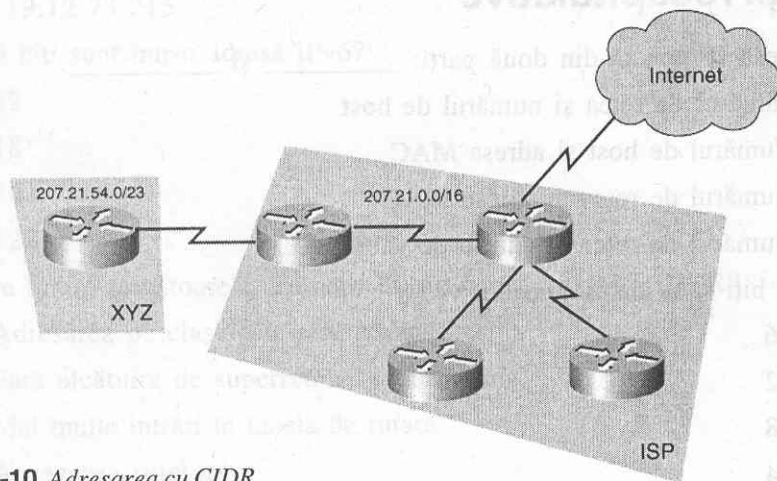
Prima dată introdusă în 1993 de către RFC-urile 1517, 1518, 1519, și 1520 și dezvoltată ulterior în 1994, CIDR îmbunătățește dramatic scalabilitatea și eficiența standardului IPv4, oferind următoarele avantaje:

- Înlocuirea adresării pe clase (classful addressing) cu o schemă fără clase mult mai flexibilă și mai puțin risipitoare.
- Agregarea îmbunătățită a rutelor, numită și *alcătuirea super-rețelelor* (*supernetting*). Pe măsură ce Internetul crește, ruterele Internet necesită tabele de memorie uriașe pentru a stoca toată informația de rutare. Alcătuirea super-rețelelor ajută la reducerea dimensiunii tabelelor de memorare ale rutelor, prin combinarea și sumarizarea intrărilor multiple ale informației de rutare într-o singură intrare. Aceasta reduce dimensiunea tabelelor de memorare ale rutelor și, de asemenea, permite o căutare mai rapidă în tabele.

O adresă de rețea CIDR arată astfel: 207.21.54.0/23.

207.21.54.0 este însăși adresa rețelei. Partea /23 înseamnă că primi 23 biți sunt partea de rețea a adresei, ultimii 9 biți rămânând pentru specificarea adresei de host. Prin comparație cu abordarea pe clase (classful approach), aceasta ar fi o adresa de clas C, cu partea de rețea de 24 biți și partea de host de 8 biți.

În abordarea CIDR, dacă aveți nevoie de mai mult decât cele 254 adrese de host, vi se poate atribui adresa /23 în loc de a risipi o întreagă adresă de clasa B, care susține 65534 de hosturi. Ca exemplu, în figura 18-10, utilizând CIDR, compania XYZ solicită un bloc de adrese de la propriul furnizor de servicii Internet (ISP), nu de la autoritatea centrală. Furnizorul de servicii Internet (ISP), evaluează necesitățile companiei XYZ și îi alocă spațiul de adrese de la propriul său *bloc* cuprinzător de adrese CIDR. În acest exemplu, furnizorul de servicii Internet (ISP) are blocul de adrese 207.21.0.0/16. ISP-ul semnalează numai această singură adresă 207.21.0.0/16 către Internet (chiar dacă acest bloc de adrese în realitate constă în multe rețele de clasa C). ISP-ul atribuie către compania XYZ blocul mai mic de adrese, respectiv 207.21.54.0/23 în cadrul blocului mai mare de adrese 207.21.0.0/16. Aceasta permite companiei XYZ să aibă o rețea care poate ajunge până la 510 hosturi ( $2^9 - 2 = 510$ ) sau o rețea poate fi subdivizată, la rândul ei, în multiple subrețele mai mici de către compania XYZ. Capitolul 19 discută mai detaliat alcătuirea subrețelilor.



**Figura 18-10** Adresarea cu CIDR

ISP-ul își asumă sarcina de a gestiona spațiul de adrese într-un sistem fără clase. Folosind acest sistem, ruterele Internet păstrează numai o singură rută centralizatoare, sau o rută de super-rețea (supernet route), către rețeaua furnizorului de servicii Internet, și numai furnizorul individual păstrează rutele care sunt mult mai specifice, către rețelele propriilor clienți.

Această metodă reduce drastic dimensiunea tabelelor de rutare Internet.