6. Nivelul retea

Nivelul retea

- direcționarea (*rutarea) datelor între rețele* şi cu *adresarea inter-rețea*
- *rutere* sau echipamente de nivel 3;
- Serviciile nivelului rețea au fost proiectate astfel încât:
  - să fie independente de tehnologia subrețelei;
  - nivelul transport să fie independent de numărul, tipul şi topologia subrețelelor existente;
  - adresele de rețea accesibile nivelului transport trebuie să folosească o schemă de numerotare uniformă (pt. LAN şi WAN).
- Nivelul rețea oferă nivelului transport 2 clase de servicii:
  - servicii fără conexiune (datagram)
  - servicii orientate pe conexiune (circuit virtual)
- AS-Autonomous System = un ansamblu de porți (gateways) şi rețele care au o administrație unică
- AS= totalitatea rețelelor interconectate dintr-o organizație

Nivelul retea

- 10 principii pe care se bazează nivelul rețea în Internet (RFC1958):

1. fiţi siguri ca funcţionează;
2. menţine-l simplu;
3. faceţi alegeri clare;
4. exploataţi modularitatea;
5. aşteptaţi-vă la medii eterogene;
6. evitaţi opţiuni şi parametrii statici;
7. căutaţi o proiectare cât mai bună, nu neapărat perfectă;
8. fiţi stricţi când trimiteţi şi toleranţi când recepţionaţi;
9. gândiţi-vă la scalabilitate;
10. luaţi în considerare performanţele şi costurile.

6.1. Rutarea

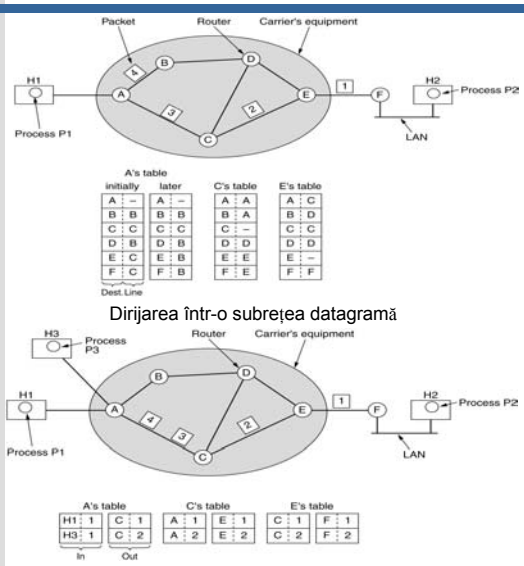
- ***Tipuri de pachete*** :

- *pachete de date* – protocoalele folosite se numesc *protocoale rutate* (routed protocols); exp.: IP, IPX;
- *pachete cu informații de reîmprospătare a rutelor* - protocoalele folosite se numesc *protocoale de rutare* (routing protocols); exp.: RIP (Routing Information Protocol), EIGRP (Enhanced Interior Gateway Routing Protocol), OSPF (Open Shortest Paths First).

- **Tabela de rutare***:*
  - adrese de rețea,
  - numele interfeței,
  - metrica

- **Rutarea:**
  - ***statică***
  - ***dinamică***

6.1.1. Implementarea serviciilor



Dirijarea într-o subrețea datagramă

Dirijarea într-o subrețea cu circuite virtuale (CV)

6.1.1. Implementarea serviciilor (*)

Problemă	**Subrețea datagramă**	**Subrețea cu CV**
Stabilirea circuitului	Nu este necesară	Obligatorie
Adresare	Fiecare pachet conține adresa completă pentru sursă și destinație	Fiecare pachet conține un număr mic de CV
Informații de stare	Ruterele nu păstrează informații despre conexiuni	Fiecare CV necesită spațiu pt. tabela ruterului per conexiune
Dirijare	Fiecare pachet este dirijat independent	Calea este stabilită la inițierea CV și este urmată de toate pachetele
Efectul defectării ruterului	Nici unul, cu excepția pachetelor pierdute în timpul defectării	Toate circuitele virtuale care trec prin ruterul defect sunt anulate
Calitatea serviciului	Dificil	Simplu, dacă pt. fiecare CV pot fi alocate resurse suficiente în avans
Controlul congestiei	Dificil	Simplu, dacă pt. fiecare CV pot fi alocate resurse suficiente în avans

Comparație între subrețelele datagramă și CV

6.1.2. Algoritmi de rutare

- *algoritmi neadaptivi*
- *algoritmi adaptivi*

- *algoritmi statici*
  - *dirijarea pe cale cea mai scurtă* - Dijkstra
  - *Inundarea*
- *algoritmi dinamici*
  - *dirijarea după vectorul distanțelor* – Bellman-Ford și Ford-Fulkerson
  - *După starea legăturii*

- *algoritmi* pt. rutare ierarhică
- *algoritmi* pt. rutare pentru gazde mobile
- *algoritmi* pt. rutare pentru difuzare – trimitere simultană a unui pachet către toate stațiile
- *algoritmi* pt. rutare multidestinație
- *algoritmi* pt. rutare în rețele punct-la-punct

- Algoritmi pentru **controlul congestiei**

6.1.3. Protocoale de rutare

- Tipuri de protocoalele de rutare:
  - vector de distanță (**distance vector)**- RIP, IGPR, EIGPR,BGP
  - starea legăturii (**link-state**) - OSPF, IS-IS

- RIP (Routing Information Protocol)
- IGRP (Interior Gateway Routing Protocol)
- EIGRP(Enhanced Interior Gateway Routing Protocol)
- BGP (Border Gateway Protocol)
- OSPF (Open Shortest Paths First)
- IS-IS (Intermediate System- Intermediate System)

6.1.3. Protocoale de rutare (*)

- **RIP** (Routing Information Protocol) – cel mai folosit protocol pentru transferul informațiilor rutare între rutere direct conectare.

- A apărut în 1998 și este specificat în RFC 1058.
- Ruterul alege drumul din rețea pe care se vor transmite datele pe baza vectorului de distanță (distance-vector). Când datele trec printr-un ruter, se consideră un „hop trecut". Dacă există mai multe rute până la destinație, protocolul alege ruta cu număr minim de hopuri, care nu este neapărat și cea mai rapidă. Dacă numărul de noduri intermediare depășește 15, pachetul este ignorat.
- Informațiile de împrospătare sunt trimise o dată la 30 de secunde către toți vecinii, sub forma tabelei complete de rutare.

- **IGRP** (Interior Gateway Routing Protocol)- Protocolul de rutare pentru porti interioare – este dezvoltat la mijlocul anilor '80 de Cisco Systems cu scopul de a obține o dirijare robusta in interiorul AS-urilor.

- Este de tipul vector de distanță.
- Calculează distanțele până la destinație, permițând ruterelor să-și împrospăteze tabelele de rutare la intervale programabile (de obicei la fiecare 30 –90 secunde);
- foloseste o metrica compusa care este calculata pe baza valorilor intarzierilor,a latimii benzii,a sigurantei si a traficului. Administratorii retelelor pot stabili proportiile in care aceste valori formeaza metrica si trebuie sa fie foarte atenti deoarece aceste valori au un domeniu de valori foarte mare. Administratorii isi mai pot defini si o serie de constante, cu ajutorul carora sa influenteze alegerea caii de catre ruter.
- Dezavantaj- generează trafic suplimentar;
- Succesul IGRP-ului se datoreaza similaritatii cu RIP-ul si caracteristicilor sale. Lipsindu-i suportul pentru variabila lungimii subnet masks (VLSM), in loc sa se dezvolte o noua versiune s-a preferat realizarea unui nou protocol : EIGRP.

6.1.3. Protocoale de rutare (*)

- **EIGRP** (Enhanced Interior Gateway Routing Protocol),

- este varianta îmbunătățită a lui IGRP, proprietate Cisco;
- este de tip vector de distanță îmbunătățit (combinație între vector de distanță și de stare a legăturii);
- folosește algoritmi pt. repartizarea uniformă a încărcării;
- folosește algoritmul DUAL (Diffused Update Algorithm) pentru a calcula drumul cel mai scurt până la destinație;
- informațiile de împrospătare sunt trimise tuturor vecinilor o dată la 90 de secunde sau când apar schimbări topologice.

- **BGP (Border Gateway Protocol)-**

- specificat în RFC 1771 și 1774;
- este un protocol de rutare externă de tip vector de distanță, dar destul de diferit de majoritatea celorlalte cum ar fi RIP. In loc sa mentina doar costul pana la destinatie, fiecare ruter BGP memoreaza calea exacta folosita.
- se folosește între furnizorii de servicii Internet sau între furnizorii și clienții acestora;
- se folosește pentru rutarea traficului între sistemele autonome;
- trebuie să țină cont de politici, care sunt configurare manual pentru fiecare ruter
- Dat fiind interesul special al BGP-ului pentru traficul in tranzit, retelele sunt grupare in trei categorii:
  - *retelelor ciot* (stub networks), care au doar o conexiune la graful BGP. Acestea nu pot fi folosite pentru traficul in tranzit deoarece nu este nimeni la capatul celalalt.
  - *retelele multiconectate*- pot fi folosite pentru traficul in tranzit, cu exceptia ce ele refuza.
  - *retelele de tranzit*- cum ar fi coloanele vertebrale, care sunt doritoare sa manevreze pachetele altora, eventual cu unele restrictii.
- Perechile de rutere BGP comunica intre ele stabilind conexiunni TCP. Operarea in acest mod ofera comunicatie sigura si ascunde toate detaliile retelelor transversate

6.1.3. Protocoale de rutare (*)

- **OSPF** (Open Shortest Paths First) – protocol deschis, specificat în RFC 2328, apărut în 1990 ca standard elaborat de IETF;

- este de tip stare a legăturii si se foloseşte în cadrul unui sistem autonom (AS – Autonom System;
- foloseşte algoritmul Dijkstra pentru a calcula drumul minim până la o destinaţie;
- pachetele de împrospătare sunt trimise prin întreaga reţea doar când apar schimbări în topologie.
- Suportă o varietate de metrici de distanţă, incluzând distanţa fizică, întârzierea;
- Este dinamic, se adaptează automat şi repede la schimbările în topologie;
- Suportă dirijarea bazată pe tipul de serviciu; dirijează traficul în timp real într-un mod iar alt tip de trafic în alt mod;
- Realizează echilibrarea încărcării, divizând încărcarea pe mai multe linii; (majoritatea protocoalelor anterioare trimit pachetele pe calea cea mai bună, calea secundară nefiind folosită);
- Suportă sisteme ierarhice, astfel încât nici un ruter să nu trebuiască să cunoască întreaga topologie;
- Introduce pentru prima dată un sistem minim de securitate (ruterele erau conectate la Internet printr-un tunel, pentru a evita cazurile în care ruterele primeau informaţii de dirijare false);
- Suportă 3 tipuri de conexiuni şi reţele: linii punct-la-punct între 2 rutere, reţele multiacces cu difuzare (LAN-uri), reţele multiacces fără difuzare (WAN_uri cu comutare de pachete).
- O reţea multiacces poate să conţină mai multe rutere, fiecare dintre lele comunicând direct cu celelalte; abstractizarea reţelei se face printr-un graf orientat, în care fiecare arc are un cost (distanţă, întârziere); calculează distanţa cea mai scurtă pe baza ponderilor arcelor, care pot fi diferite.

6.1.3. Protocoale de rutare (*)

- **IS-IS** (Intermediate System- Intermediate System)- protocol bazat pe starea legaturilor; a fost proiectat pentru DECnet si apoi adoptat de ISO pentru a fi folosit cu protocolul neorientat pe conexiune de la nivelul retea, CNPL.
- De atunci a fost modificat pentru a se descurca cu alte protocoale, cel mai important fiind IP.
- Este folosit in numeroase coloane vertebrale ale Internet-ului (inclusiv vechiul NSFNET) si in unele sisteme digitale celulare cum ar fi CDPD. Novell NetWare foloseste o varianta simplificata IS-IS (NLSP) pentru a dirija pachete IPX.
- In principiu IS-IS distribuie o imagine a topologiei ruterelor, pe baza caruia se calculeaza calea cea mai scurta. Fiecare ruter anunta, in informatia de stare a legaturilor sale, ce adrese la nivelul retea poate sa acceseze direct.
- Aceste adrese pot fi IP, IPX , AppleTalk, sau oricare alte adrese.
- IS-IS poate accepta chiar mai multe protocoale ale nivelului retea in acelasi timp.

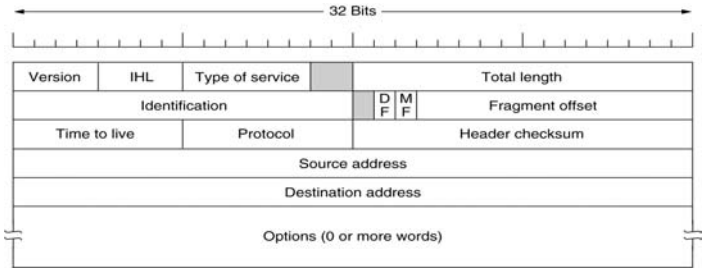
6.1.4. Protocoale rutate

- IPv4,
- IPv6,
- IP Mobile,
- IP multicast

IPv4

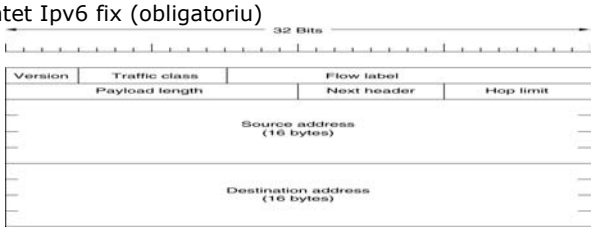
- Datagrama IP constă din:
  - Antet – parte fixă de 20 B + parte opțională de lungime variabilă
  - text

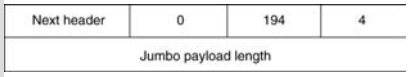
Transmisă în ordinea „big endian”



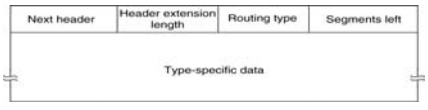
IPv6

Antet Ipv6 fix (obligatoriu)





Antet de extensie salt-după-salt pentru datagrame mari (jumbograme)

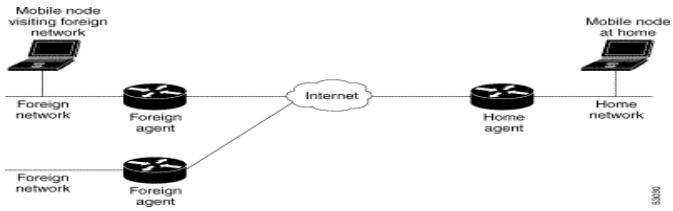


Antet de extensie pentru rutare

IP mobil

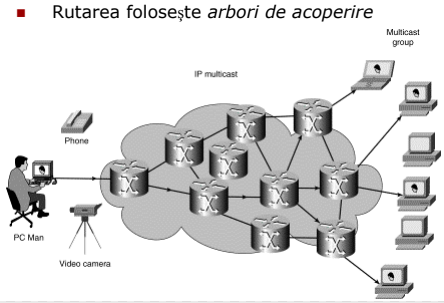
- Fiecare site care oferă servicii de mobilitate asigură un *agent local*, iar site-urile care permit accesul mobil trebuie să ofere un *agent pentru străini*. Când o *gazdă mobilă* apare la un site străin, ea contactează *gazda străină* de acolo şi se înregistrează. Gazda străină contactează agentul local şi îi dă o adresă a intermediarului, adică adresa IP a agentului pentru străini.
- Mobile IP permite nodului mobil sa foloseasca doua adrese IP:
  - adresă locală (*home address)*
  - *Care-of address: a agentului străin, asociata*
- Etape ale rutarii Mobile IP:

1. Descoperirea agentului
2. Inregistrarea
3. Rutarea



IP multicast

- Permite trimiterea simultană de la un emiţător la mai mulţi receptori;
- Foloseşte *adrese de clasă D*: fiecare adresă identifică un grup de gazde, pe 28 de biţi (adică pot exista simultan 250 milioane de grupuri). Pachetul este trimis tuturor celor din grup, dar nu garantează ca ajunge la toţi.
- Suportă 2 *tipuri de adrese: permanente* si *temporare*
- Se implementează cu *rutere speciale de trimitere multiplă*, care pot să lucreze simultan cu cele standard sau nu.
- **IGMP** (Internet Group Management Protocol – protocol de gestiune a grupurilor Internet), asemănător cu ICMP, de tip întrebare-răspuns, descris în RFC 1112.
- Are *2 tipuri de pachete*: întrebare şi răspuns
- Rutarea foloseşte *arbori de acoperire*



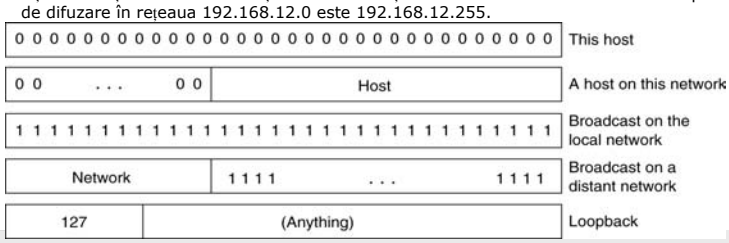
Link Local Addresses Address	Usage
224.0.0.1	All systems on this subnet
224.0.0.2	All routers on this subnet
224.0.0.5	OSPF routers
224.0.0.6	OSPF designated routers
224.0.0.12	DHCP server/relay agent

6.2. Adresare

- conectare la Internet => TCP/IP => adresa IP unica
  - nu este cazul la alte protocoale (IPX şi NetBEUI), deoarece acestea au un mecanism automat de atribuire a adreselor staţiilor, bazat pe adresele fizice ale plăcilor de reţea.
- IANA alocă furnizorilor de servicii Internet (ISP - Internet Service Provider) seturi de adrese pe care le pot folosi pentru reţelele care se conectează la ei.
- Unicitate adrese => adresele sunt atribuite centralizat
- 2 cazuri:
  - organizaţia nu doreşte o conectare permanentă la Internet
  - compania doreşte să ofere informaţii şi servicii către Internet

6.2.1. Tehnica adresării IP

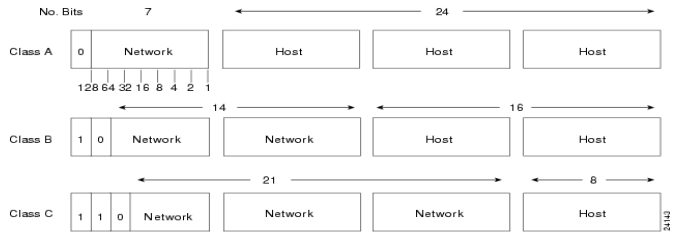
- protocolului IP versiunea 4, (RFC 791): adresă de 32 de biţi, reprezentată sub forma a 4 numere zecimale, corespunzătoare celor 4 octeţi, numerele fiind separate prin puncte (*notaţie zecimală cu punct*). De exemplu, 192.168.12.34.
- Adresa IP *are două componente*:
  - *adresa de reţea* - este porţiunea comună tuturor staţiilor din aceeaşi reţea logică IP;
  - *adresa de staţie*- permite identificarea unică a staţiilor din aceeaşi reţea.
- adresele IP se împart în mai multe *clase,* în funcţie de numărul de biţi alocaţi adresei de reţea şi adresei de staţie
- Adrese IP speciale:
  - zero pe toţi biţii corespunzători numărului de staţie - defineşte adresa reţelei din care face parte staţia. Exp.: adresa staţie 192.168.12.34, adresa de reţea este 192.168.12.0.
  - biţii rezervaţi numărului de staţie sunt unu- acţiunea de difuzare sau *broadcast*. Exp.: adresa de difuzare în reţeaua 192.168.12.0 este 192.168.12.255.



6.2.1. Tehnica adresării IP

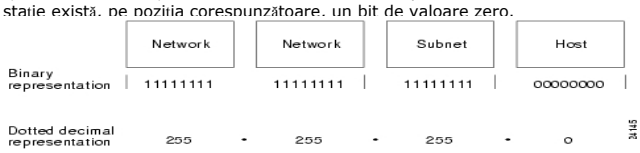
- Formatul adreselor IP

Clasă	Primii biti	Număr de biti pentru reţea	Număr de retele	Număr de biti pentru staţie	Număr de statii	Interval
A	0	8	126	24	16777214	1.0.0.0 - 127.255.255.255
B	10	16	16382	16	65534	128.0.0.0 - 191.255.255.255
C	110	24	2097152	8	254	192.0.0.0 - 223.255.255.255
D	1110	Adrese de trimitere multiplă				224.0.0.0 - 239.255.255.255
E	11110	Rezervat pentru folosire viitoare				240.0.0.0 - 247.255.255.255



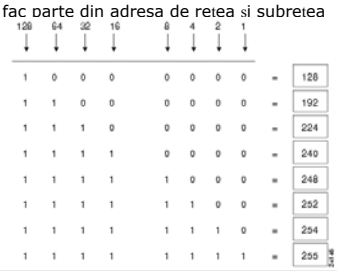
6.2.2. Subreţele

- Divizarea unei retele in parti pentru uz intern, din exterior fiind o singura retea;
- criterii organizaţionale, geografice
- biţii alocaţi adresei de staţie sunt folosiţi pentru a identifica adresa de subreţea
- *mască de reţea* (*mască de subreţea*)- pentru fiecare bit din adresa de subreţea există, pe aceeaşi poziţie în masca de reţea, un bit de valoare unu, iar pentru fiecare bit care face parte din adresa de staţie există, pe poziţia corespunzătoare, un bit de valoare zero.



- Masca de reţea poate fi indicată în două moduri:
  - prin reprezentarea zecimală cu punct (ca o adresă IP obişnuită),
  - prin indicarea directă a numărului de biti care fac parte din adresa de reţea şi subreţea

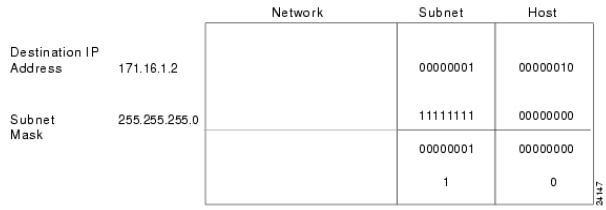
▪adresa de clasă *C*, 192.168.12.34, în adresa de subreţea intră 25 de biţi prin masca 255.255.255.128 sau prin forma echivalentă 192.168.12.34/25. Masca de reţea este diferită de valoarea ei implicită (255.255.255.0), care poate fi dedusă pe baza clasei din care face parte adresa IP.



6.2.2. Subrețele

- Subretele ale clasei C

Number of Bits	Subnet Mask	Number of Subnets	Number of Hosts
2	255.255.255.192	2 +2 (0,1)	62 +2 (0,1)
3	255.255.255.224	6	30
4	255.255.255.240	14	14
5	255.255.255.248	30	6
6	255.255.255.252	62	2



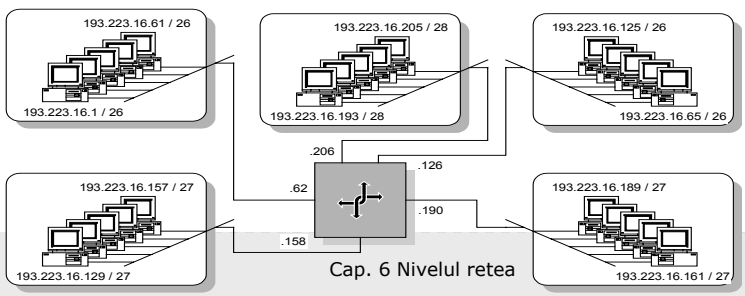
SI logic intre adresa IP si masca de subretea =>numar de subretea

Adresa IP: 130. 97. 16.132 = 1000 0010.0100 1101.0001 0000.1000 0100
Masca subretea: 255.255.255.192= 1111 1111.1111 1111.1111 1111.11-- --------
SI LOGIC = 1000 0010.0100 1101.0001 0000.1000 0000 = adresa subretelei 130.97.16.128
----------.---00 0100=adresa host 4

6.2.2. Subrețele

- organizație care are alocată adresa IP, de clasă C, 193.223.16.0. (maxim 254 de adrese)
- Crearea de subrețele, câte una pentru fiecare din cele 4 departamente (maxim 62 de stații, iar adresele lor vor fi 193.223.16.0/26, 193.223.16.64/26, 193.223.16.128/26 și 193.223.16.192/26); patru subrețele prin utilizarea a încă doi biți din adresa de stație pentru partea de rețea
- IT are nevoie de subretea proprie; administrativ=62, cercetare=62, producție=30, marketing=30, IT=14

Administrativ	de la 193.223.16.1 la 193.223.16.62	masca 255.255.255.192
Cercetare	de la 193.223.16.65 la 193.223.16.126	masca 255.255.255.192
Productie	de la 193.223.16.129 la 193.223.16.158	masca 255.255.255.224
Marketing	de la 193.223.16.161 la 193.223.16.190	masca 255.255.255.224
IT	de la 193.223.16.193 la 193.223.16.206	masca 255.255.255.240.



6.2.3. Tehnica de alocare CIDR

- CIDR (Classless InterDomain Routing) – dirijare fara clase intre domenii - tehnica de dirijare care să nu țină cont de clasa din care face parte adresa IP;
- foloseşte o mască prin care se stabileşte câte staţii pot fi într-o reţea. Numărul de biţi unu din cadrul măştii poate fi mai mare decât numărul de biţi unu din masca implicită a clasei C, nepermis la subreţele (*mască de superreţea*).
- *reducerea numărului de intrări din tabelele de dirijare* a router-elor care fac parte din backbone-ul principal al Internet-ului.
- aplicabilitate redusă, datorită, noilor tehnici de translatare a adreselor de reţea

6.2.4. Translatarea adreselor şi porturilor de reţea

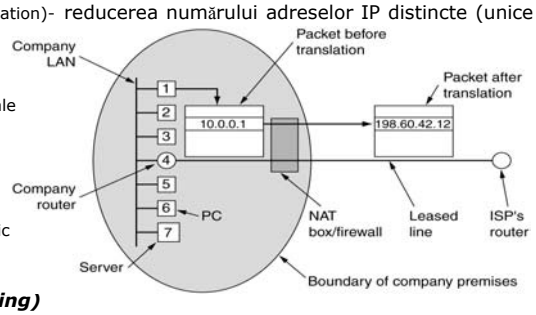
- concept: modificarea de către un echipament intermediar, plasat între sursă şi destinaţie, a unei informaţii din antetul IP, TCP sau UDP. Informaţia modificată poate fi adresa sursă a pachetului, adresa destinaţie, portul sursă sau portul destinaţie;
- *nu necesită modificări la nivelul staţiilor sau router-elor*, ci doar intercalarea unor dispozitive de translatare a adreselor.

IP NAT – (Network Address Translation)- translatarea adreselor, RFC 1631, 3022, folosita de sine stătător, cât şi în conjuncţie cu CIDR.

- *adresele IP,* pe care le folosesc societăţile, *pot fi duplicate* (nu este nevoie să fie unice global, ci doar local), cât timp acestea sunt folosite doar în interiorul societăţii şi nu sunt "exportate" către Internet.
- Pentru a putea comunica în Internet, calculatoarele cu adrese unice local au nevoie de dispozitiv de translaţie a adreselor, care să convertească *temporar*, pe durata unei sesiuni de comunicare, adresa locală într-o adresă unică global, primită de la furnizorul de servicii Internet
- Pentru a putea realiza conversia, *translatorul de adrese* trebuie să analizeze cele cinci componente implicate în orice comunicaţie Internet:
  - protocolul, cu variantele TCP, UDP, ICMP etc.;
  - adresa IP a sursei pachetului;
  - portul (TCP sau UDP) sursei pachetului;
  - adresa IP a destinaţiei pachetului;
  - portul (TCP sau UDP) destinaţiei pachetului.

Translatarea clasică a adreselor

- **NAT** – (Network Address Translation)- reducerea numărului adreselor IP distincte (unice global) din Internet.
- Translatarea poate fi:
  - *statică* - spaţiul adreselor locale (folosit în reţea) şi spaţiul real (folosit pentru Internet) au dimensiuni egale, simplu de implementat
  - *dinamică* - numărul adreselor IP reale disponibile este mai mic decât numărul adreselor locale



Deghizarea *(IP Masquerading)*

- caz particular de translatare dinamică, în care numărul de adrese IP reale este foarte mic (de obicei, egal cu unu) => router-ul NAT trebuie să modifice şi numerele de port asociate
- mai multe conexiuni TCP sunt multiplexate prin intermediul schimbării numărului de port, motiv pentru care tehnica se numeşte *NAPT (Network Address and Port Translation*).
- numărul conexiunilor simultane din reţeaua internă spre Internet este limitat de numărul porturilor TCP disponibile la nivelul router-ului NAT
- **Un avantaj** - este *folosirea unei singure adrese IP*, care poate fi obţinută chiar prin *conectarea cu protocol PPP* (Point-to-Point Protocol) pe o linie telefonică comutată. Astfel, nu trebuie făcută o investiţie pentru o adresă de clasă *C*

6.3. Protocoale de control în Internet

- ICMP
- ARP
- RARP
- BOOTP
- DHCP

ICMP (The *Internet Control Message Protocol*- protocolul mesajelor de control din Internet) - furnizează pachete de mesaje pentru raportul erorilor şi al altor informaţii privind calea pachetelor IP de la sursă la destinaţie.

- Este specificat în RFC 792.
- ICMP emite mesaje doar despre erorile primului fragment din datagramele IP fragmentate; mesajele nu sunt răspunsuri la mesajele de eroare ICMP şi nici ca răspunsuri la adrese IP de tip broadcast sau multicast.
- Mesajul ICMP este emis prin datagrama IP, dacă câmpul *Protocol* are valoarea 1.

ICMP

- Structura mesajului, variază în funcție de natura lui, dar primii 32 de biți sunt standard:
  - *Tip* (8biți)- natura mesajului de control emis (exp.: 0-răspuns ecou, 3-destinație inaccesibilă, 5-redirectare, 8-ecou, 11-timp depășit etc.)
  - *cod* (8biți)- parametrii de bază ai mesajului, în funcție de tipul mesajului;
  - *control eroare* (16biți)- verifică validitatea mesajului;
  - *date* (32biți) –în funție de tipul mesajului; conține informația mesajului.
- Are o multitudine de mesaje (www.iana.org/assignements/icmp-parameters), dintre care amintim:

Tip mesaj	Descriere	Utilizare
Destinație inaccesibilă	Pachetul nu poate fi livrat	Subrețeaua sau ruterul nu pot localiza destinația sau un pachet cu bitul DF nu poate fi trimis în rețea cu pachete mici
Timp depășit	Câmpul de viață este 0	Buclarea pachetelor, congestii sau valoare ceas prea mică
Problemă de parametru	Câmp invalid în antet	Eroare în programul IP al emițătorului sau al ruterului tranzitat
Oprire sursă	Pachet de șoc	Limitează traficul gazdelor care trimit prea multe pachete; îngreunează și mai mult traficul și se folosește f.rar
Redirectare	Ruterul învață topologia	Ruterul răspunde emițătorului că un pachet a fost rutat greșit
Cerere de ecou	Întreabă o mașină dacă este activă	Verifică dacă destinația este accesibilă și activă
Răspuns ecou	Da, mașina este activă	Idem
Cerere de amprentă de timp	Idem ca cererea de ecou +amprentă de timp	Idem + timpul de sosire a mesajuluișI plecare a răspunsului. Măsoară performanța rețelei
Răspuns cu amprentă de timp	Idem ca răspunsul ecou +amprentă de timp	Idem

ARP

ARP (Address Resolution Protocol) – protocolul de rezoluție a adresei, definit în RFC 826, realizează corespondența dintre adresa IP și adresa fizică.

- Fiecare placă Ethernet vine cu o adresă Etherent de 48 biți, dată de o autoritate centrală (MAC address- de 6B). Plăcile trimit și primesc cadre pe bază acestei adrese, și nu cea IP, pe care n-o cunosc.

- Adresele IP sunt transformate la nivelul legătură de date în adrese MAC, în mod dinamic, astfel:
  - există *un fișier de configurare* care face transformarea adresă IP-adresă MAC – inutil în rețelele cu mii de calculatoare, deoarece actualizarea fișierului este mare consumatoare de timp și poate genera erori;
  - trimiterea unui *pachet de difuzare*, care întreabă toate calculatoarele din acea rețea despre proprietarul adrese IP (a destinatarului). Gazda cu adresa IP din pachet va răspunde cu adresa sa MAC.

- Când modulul ARP al unui host primește o cerere de translatare a unei adrese IP, verifică mai întâi dacă se găsește în fișierul (tabelul) său. Dacă o regăsește, returnează adresa Ethernet; dacă nu, ARP difuzează un pachet stațiilor din rețea, care conține adresa IP a destinatarului pentru care se caută adresa MAC. Dacă destinatarul recunoaște adresa IP, va răspunde către emițător, prin emiterea unui mesaj cu adresasa MAC. Răspunsul va fi plasat în tabelul ARP. Dacă nu primește răsouns, atunci nu va fi plasat în tabelul ARP

RARP

- RARP (The Reverse Address Resolution Protocol) se foloseşte pentru maparea adresei MAC la adresa IP.
- Este specificat în RFC 903.
- Este inversul logic al lui ARP şi poate fi folosit de staţiile fără hard, care nu-şi cunosc adresa IP atunci când boot-ează.
- Are nevoie de un server RARP care conţine un tabel cu corespondenţele adreselor MAC-IP.
- Când o staţie porneşte, îşi difuzează adresa MAC (de pe placa de reţea) şi îşi caută adresa IP. Serverul RARP vede cererea, caută adresa în fişierele de configurare şi îi trimite adresa IP corespunzătoare (dacă adresa IP ar fi fixată în imagine, atunci fiecare staţie ar avea nevoie de propria imagine).
- Dezavantaj – pentru a ajunge la serverul RASP se foloseşte o adresă de difuzare (formată din 1-uri), nepropagate de rutere, motiv pt. care este nevoie de un server în fiecare reţea. Se rezolva acest lucru cu BOOTP.

BOOTP

- RFC 951, 1048, 1084
- Este un protocol de pornire alternativ, care foloseşte mesaje UDP, propagate prin rutere.
- O staţie fără disc va beneficia de informaţii suplimentare, cum ar fi adresa IP a serverului cu imaginea de memorie, adresa IP a ruterului implicit, masca de subreţea.
- Necesită configurarea manuală a corespondenţelor dintre adresa IP şi adresa MAC.
- Pentru a elimina acest pas predispus la erori, a fost extins şi redenumit în DHCP.

DHCP

- DHCP (Dynamic Host Configuration Protocol) se bazează pe un server special care atribuie adrese IP host-urile care cer.
- Serverul nu trebuie să fie în aceeaşi reţea cu hostul, deci nu va fi accesibil prin difuzare, necesitând un *agent de legătură DHCP (DHCP relay agent).*
- Pentru aflarea adresei IP, o maşină difuzează un pachet *DHCP DISCOVER*. Agentul de legătură interceptează difuzările, iar când găseşte un astfel de pachet, îl trimite ca *pachet unicast* serverului DHCP (agentul are nevoie doar de adresa serverului DHCP).
- Atribuirea adresei IP se face pe o perioadă fixă de timp, folosind *tehnica de închiriere*. Înainte de expirarea perioadei, gazda trebuie să ceară o reînnoire a adresei IP, altfel o va pierde.