Nivelul Retea

Lenuta Alboaie

adria@info.uaic.ro

Cuprins

- Nivelul Retea
  - Protocolul IPv4
    - Problematica
    - Caracterizare
    - Subretele
  - Retele Private
  - ICMP
  - Rezolutia adreselor
  - IPv6 – imagine generala
    - Detalii -> Curs Viitor

Preliminarii

- **Situatia initiala**

  - Inainte de Internet doar nodurile din aceeasi retea puteau comunica intre ele

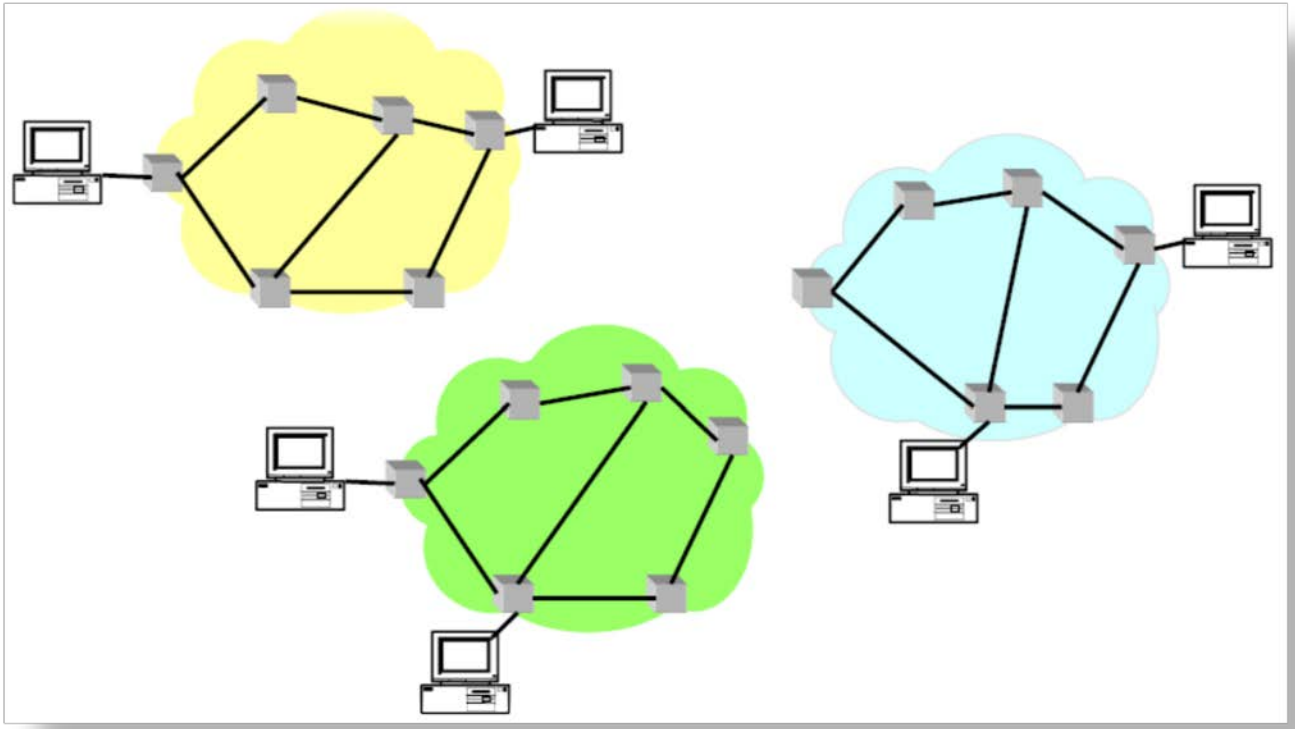
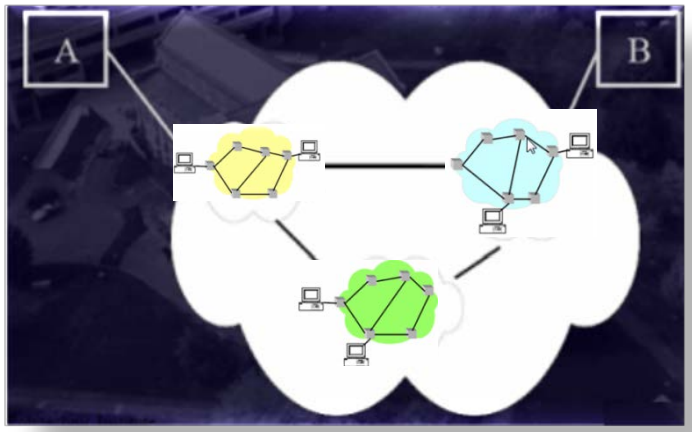


Figura: Retele individuale

Preliminarii

- Probleme
  - Cum se pot transporta pachete intr-un mediu eterogen?

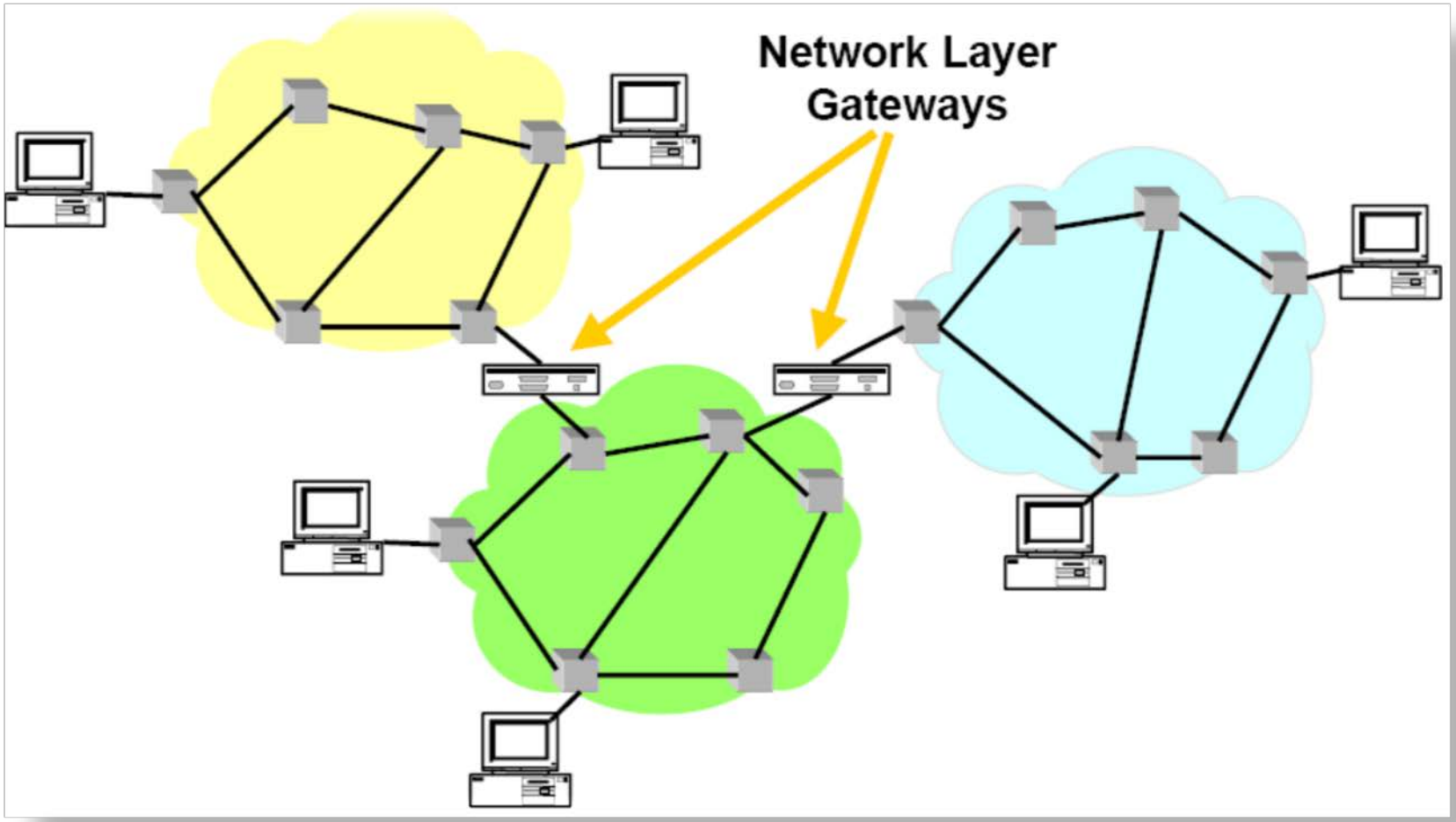
  - **Eterogenitate**
    - La nivelurile inferioare: cum se poate face interconectarea unui numar mare de retele independente?
    - La nivelurile superioare: cum se poate oferi suport pentru o mare varietate de aplicatii?



- **Scalare**: cum s-ar putea suporta un numar mare de noduri si aplicatii intr-un astfel de sistem de retele interconectate?

Solutia

- **IP – Internet Protocol**



Nivelul retea

- Protocolul IP este utilizat de sisteme autonome (*AS – Autonomous Systems*) in vederea interconectarii

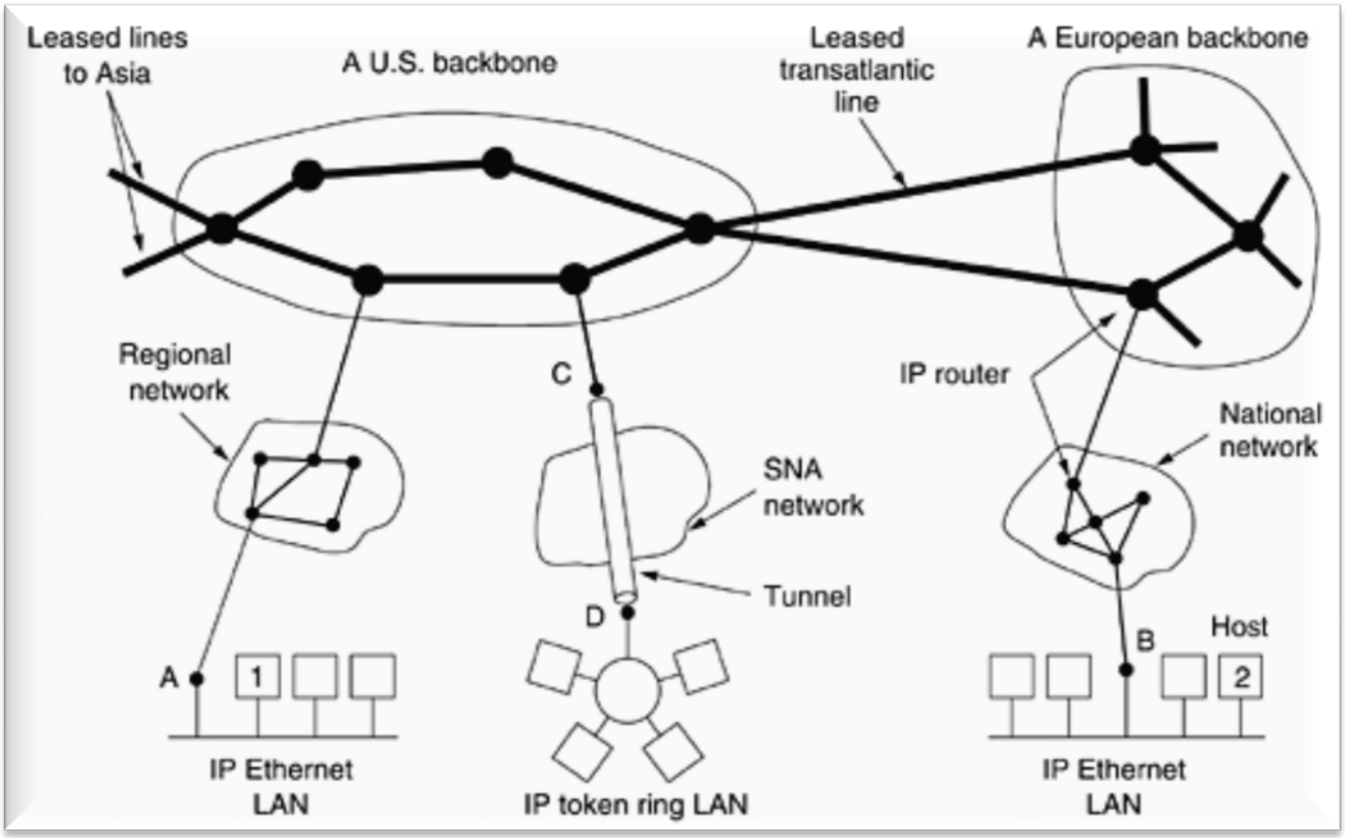


Figura: Internetul - colectie de retele interconectate

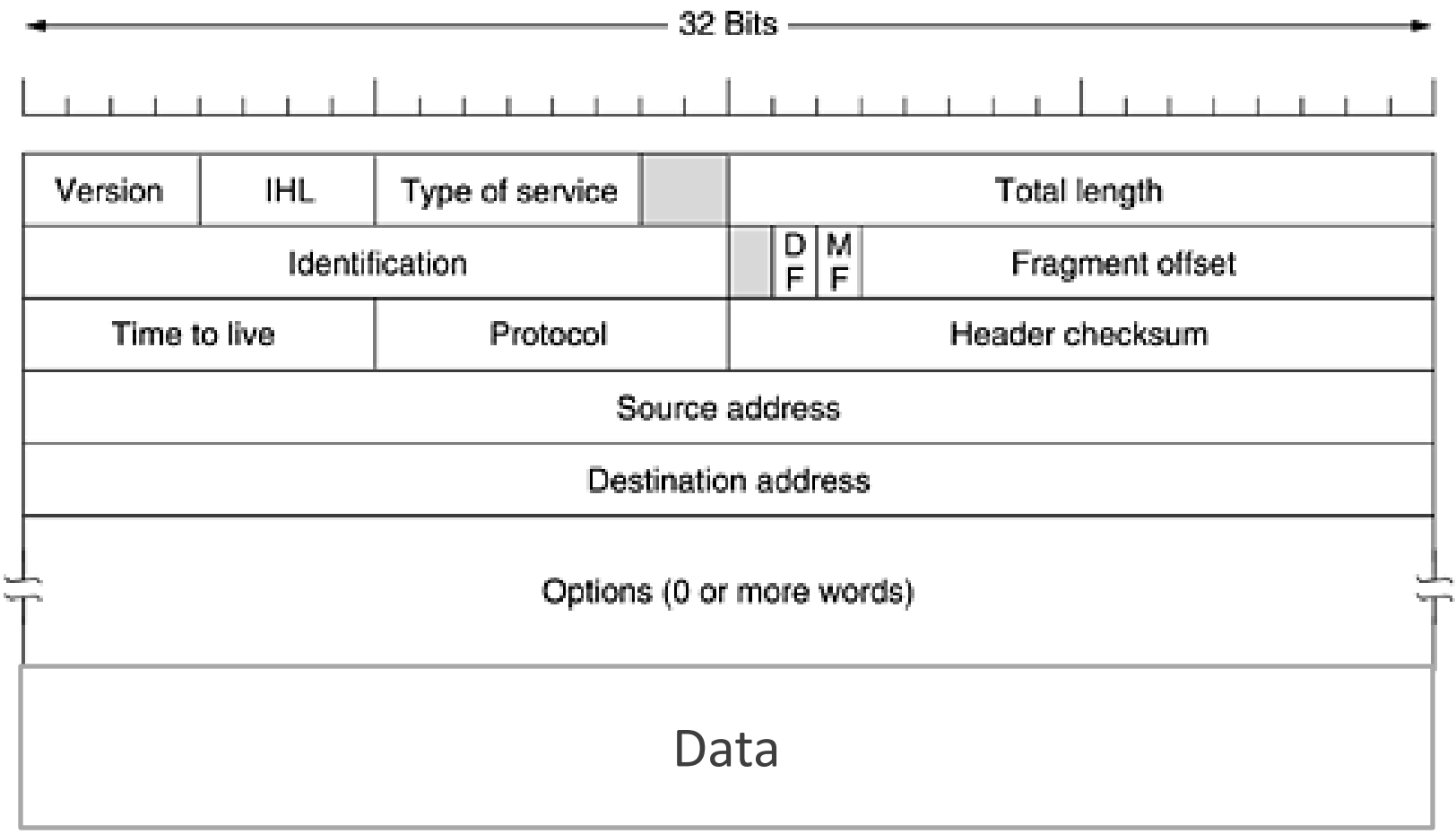
[Computer Networks, 2003 Andrew S. Tanenbaum]

Nivelul Retea

- Rol: ofera servicii neorientate-conexiune pentru a transporta **datagrame** de la sursa la destinatie; sursa si destinatia pot fi in retele diferite
- Fiecare datagrama este independenta de celelalte
- Nu se garanteaza trimiterea corecta a datagramelor (pierdere, multiplicare,…)
- +…Curs viitor

Protocolul IP

- **Datagrama IPv4**



[Computer Networks, 2003
Andrew S. Tanenbaum]

Protocolul IP

- **Datagrama IPv4**
  - Valorile uzuale ale campului *Version* sunt:
    - 4 – protocolul IP (RFC 791)

    (6 pentru protocolul IPv6 (RFC 1883))

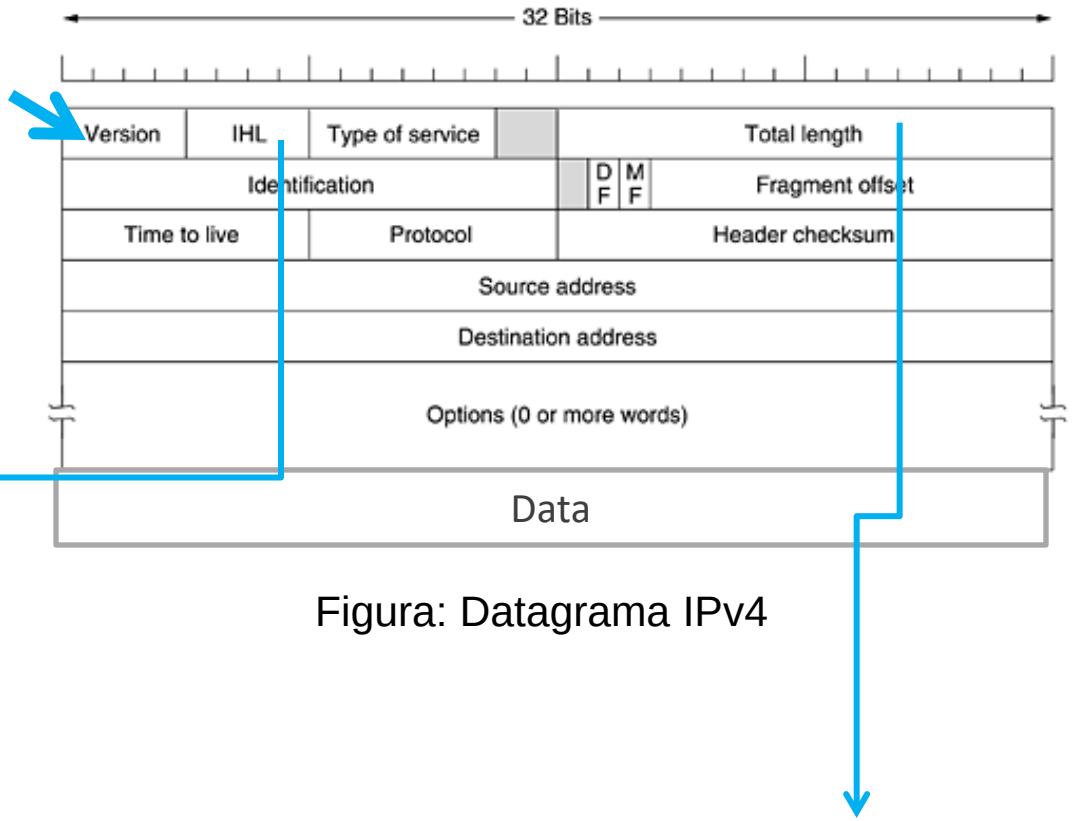


Figura: Datagrama IPv4

Protocolul IP

- **Datagrama IPv4**
  - Campul *Type of service* permite gazdei sa comunice subretelei (e.g. routere) ce tip de serviciu doreste

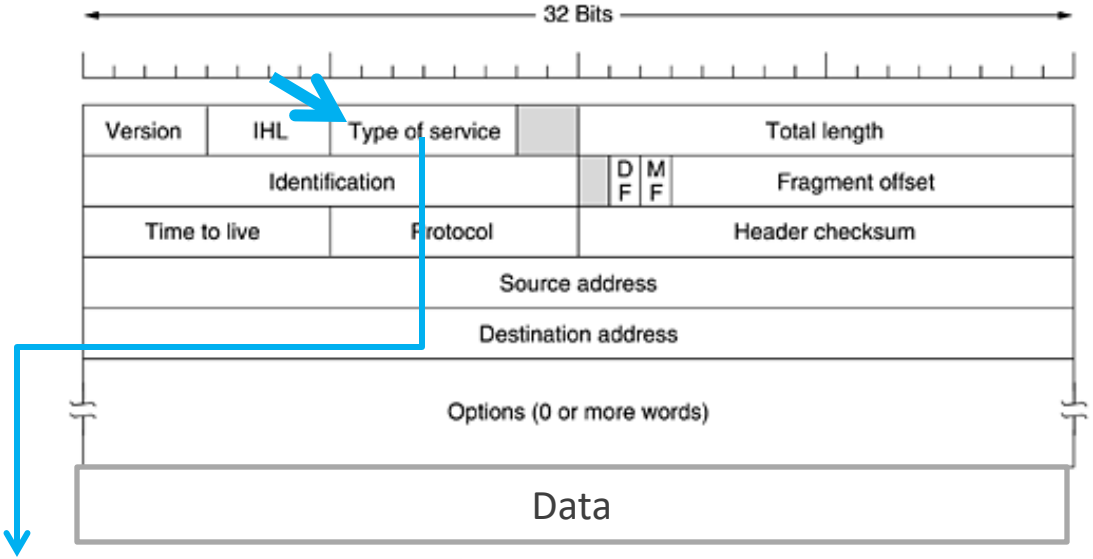


Figura: Datagrama IPv4

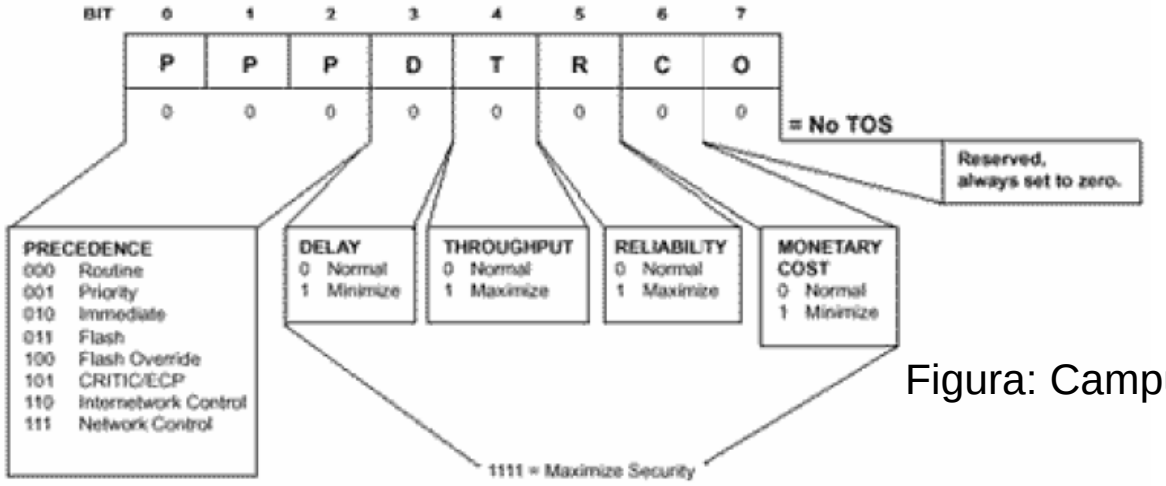
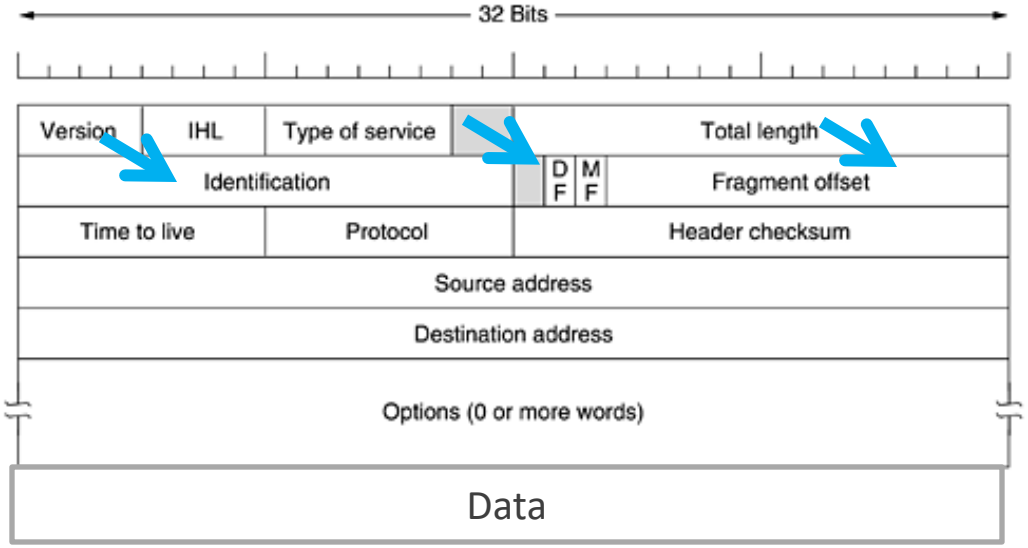


Figura: Campul *Type of Service*

Protocolul IP

- **Datagrama IPv4**
  - Campul *Identification* permite gazdei destinatie sa identifice apartenenta la o datagrama a noului fragment primit
  - Flagurile:
    - *DF (Don't Fragment)* – indica ruterelor sa nu fragmenteze datagrama
    - *MF (More Fragments)* – semnalizeaza ca pachetul este un fragment, urmat de altele; ultimul fragment are acest bit 0
  - Campul *Fragment offset* – locul fragmentului in datagrama

Figura: Datagrama IPv4



Protocolul IP

- **Datagrama IP**
  - Fragmentarea datagramelor:
    - Fiecare fragment (pachet) are aceeasi structura ca datagrama IP
    - Reasamblarea datagramelor se face la destinatar
    - Daca un fragment al unei datagrame e pierdut, acea datagrama e distrusa (se trimite la expeditor un mesaj ICMP – Internet Control Message Protocol)
    - Mecanismul de fragmentare a fost folosit pentru unele atacuri – *firewall piercing* (un fragment "special" e considerat ca fiind parte a unei conexiuni deja stabilite, astfel incat ii va fi permis accesul via *firewall)*

Protocolul IP

- **Datagrama IP**
  - Filtrarea datagramelor:
    - Se realizeaza de un *firewall:* ofera accesul din exterior in reteaua interna, conform unor politici de acces, doar pentru anumite tipuri de pachete (utilizate de anumite protocoale/servicii)
      - Preintimpina o serie de atacuri vizind securitatea
      - Firewall-ul poate fi software sau hardware
      - Firewall-ul poate juca rol de proxy sau de gateway

Protocolul IP

- **Rolul si arhitectura unui proxy:**
  - Acces indirect la alte retele (Internet) pentru gazdele dintr-o retea locala via *proxy*
  - *Proxy*-ul poate fi software sau hardware
  - Rol de poarta (*gateway*), de *firewall* sau de server de *cache*
  - *Proxy*-ul ofera partajarea unei conexiuni Internet
  - Utilizat la imbunatatirea performantei (e.g., *caching*, controlul fluxului), filtrarea cererilor, asigurarea anonimitatii

Protocolul IP

- **Datagrama IPv4**
  - Campul *TTL (Time to Live)* specifica durata de viata a pachetului;

    numarul este decrementat de fiecare *router* prin care trece pachetul

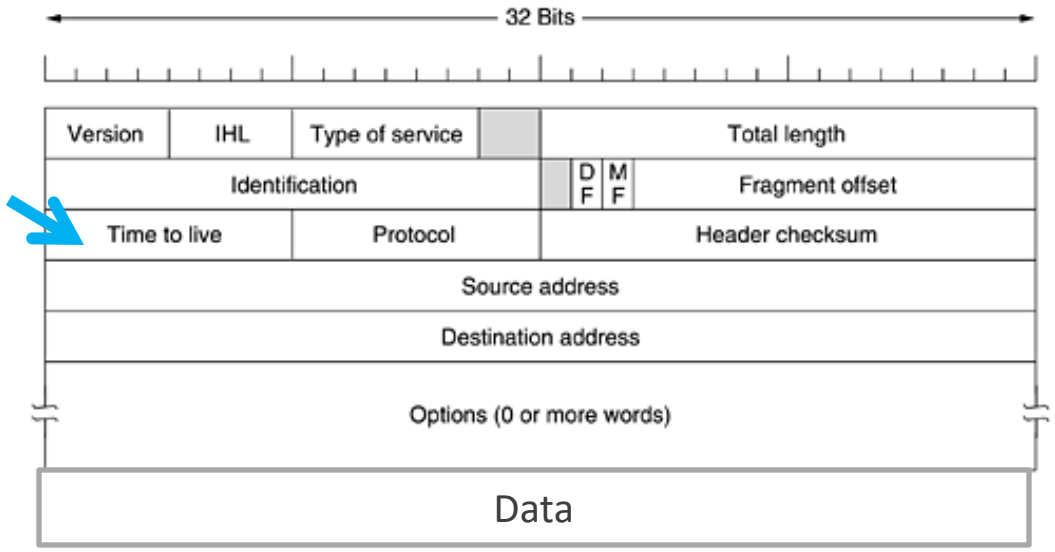
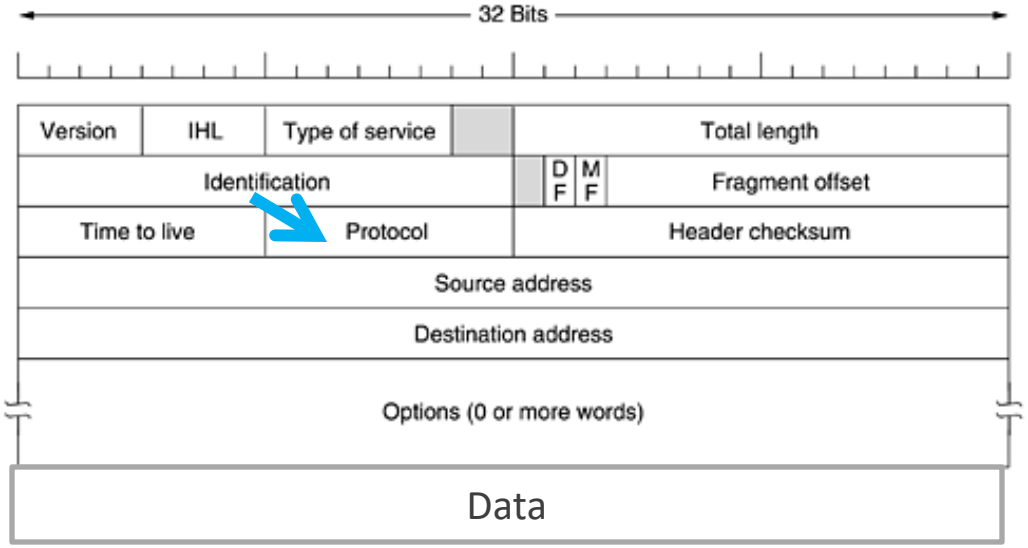


Figura: Datagrama IPv4

Protocolul IP

- **Datagrama IPv4**
  - Campul *Protocol* specifica protocolul (de nivel superior) caruia ii este destinata informatia inclusa in datagrama:

Figura: Datagrama IPv4

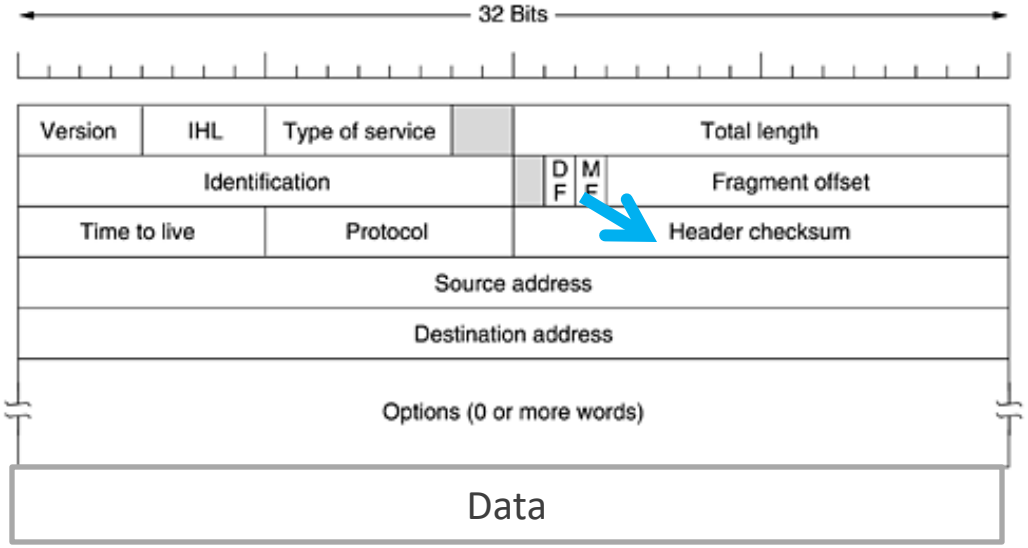


  - 1 ICMP (*Internet Control Message Protocol*)
  - 2 IGMP (*Internet Group Message Protocol*)
  - 6 TCP (*Transmission Control Protocol*)
  - 17 UDP (*User Datagram Protocol*)
  - … etc.(RFC 1700)

Protocolul IP

- **Datagrama IPv4**
  - Campul *Header checksum* folosit pentru detectarea erorilor; daca apare o eroare datagrama este distrusa

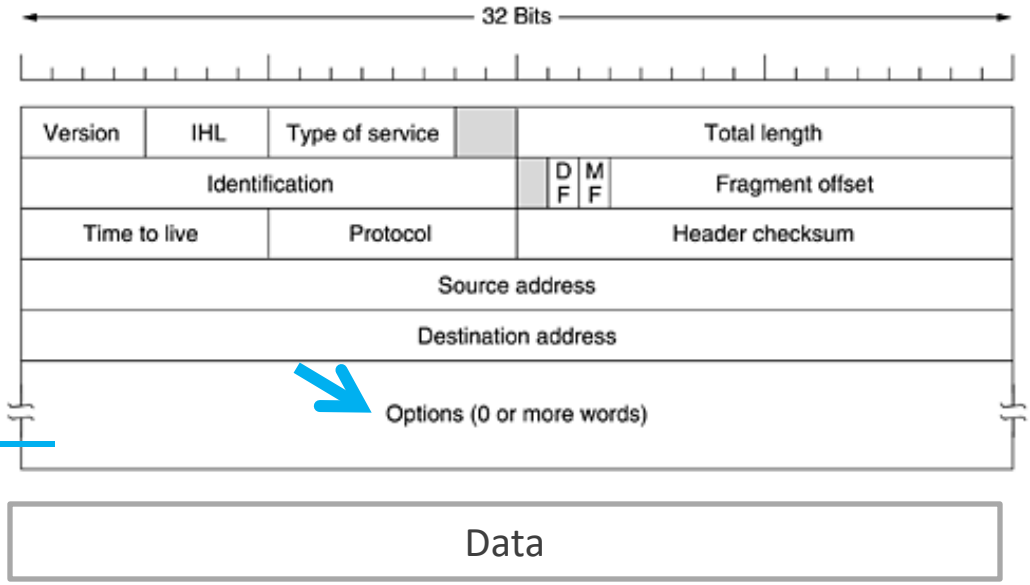
Figura: Datagrama IPv4



Protocolul IP

- **Datagrama IPv4**
  - Campul *Options*

Figura: Datagrama IPv4



Optiune	Descriere
Securitate	Mentioneaza cat de secreta este datagrama
Dirijare stricta pe baza sursei (engl. strict source routing)	Indica calea completa de parcurs
Dirijarea aproximativa pe baza sursei (engl. Loose source routing)	Indica o lista a ruterelor care nu trebuie sarite
Intregistreaza calea (engl. record route)	Face fiecare ruter sa-si adauge adresa IP
Amprenta de timp (engl. timestamp)	Face fiecare ruter sa-si adauge adresa si o amprenta de timp

Protocolul IP

- **Datagrama IPv4**
  - Campul *Source adress* si *Destination adress* indica adresa sursei si destinatiei

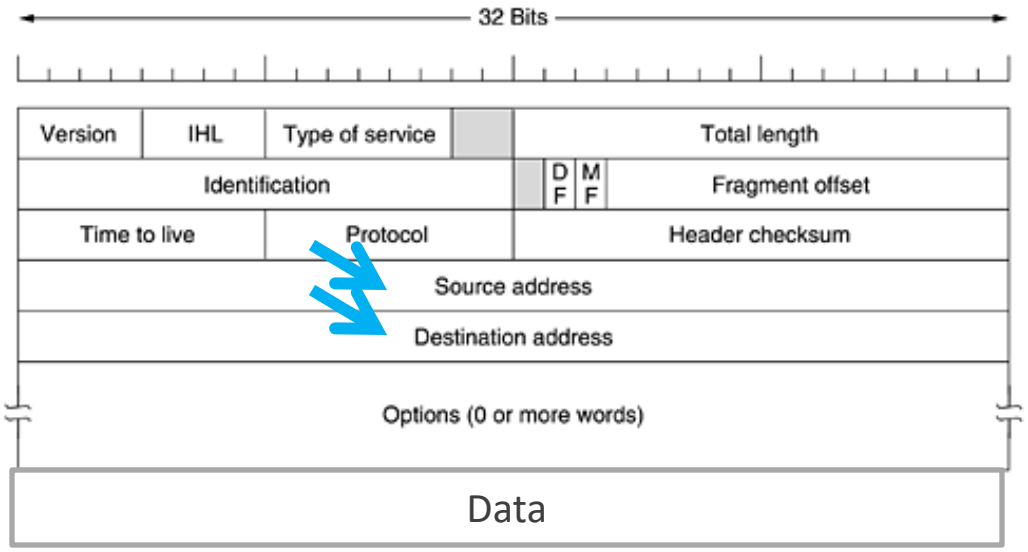


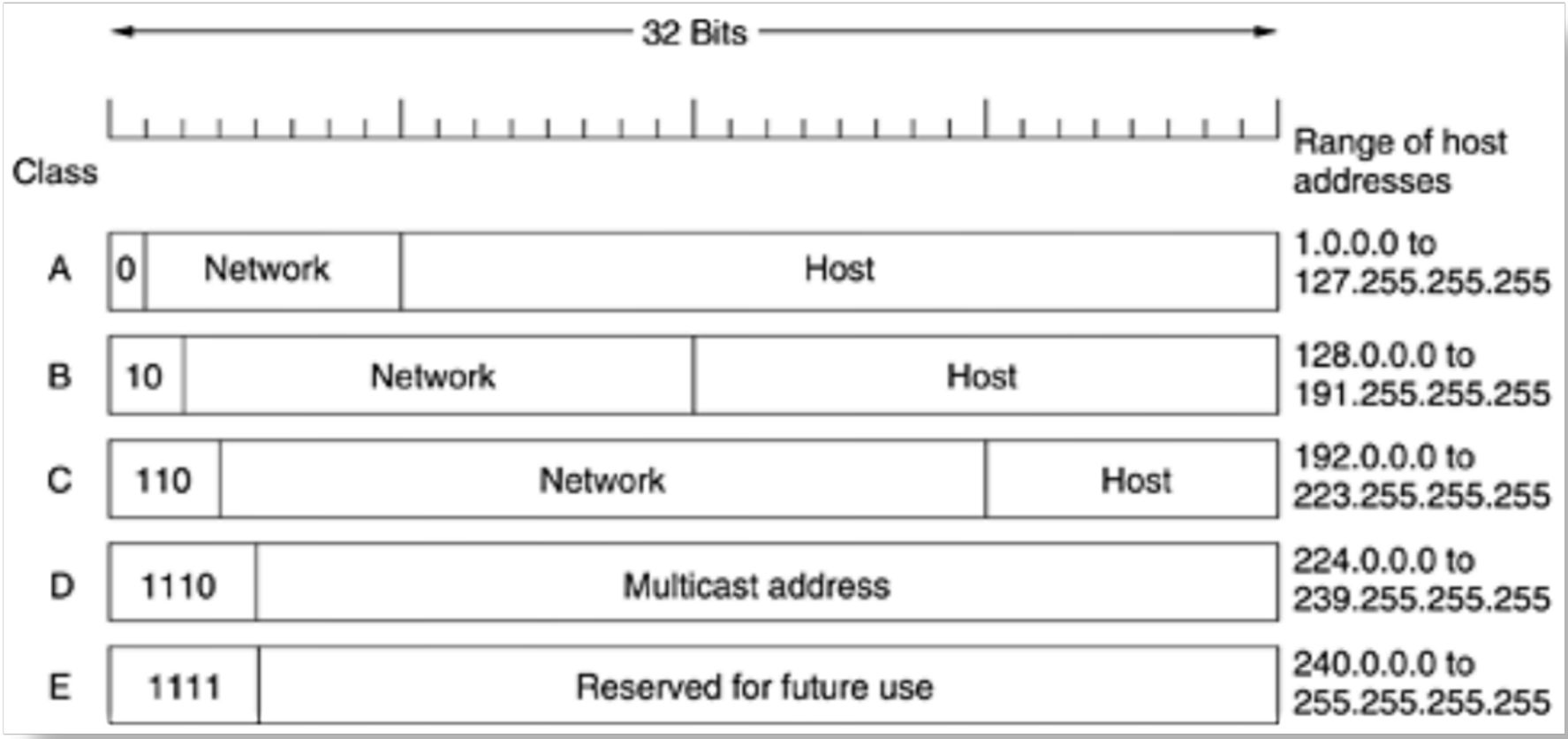
Figura: Datagrama IPv4

Protocolul IP

- **Adrese IPv4**
  - Fiecare adresa IP include un identificator de retea (NetID) si un identificator de gazda (HostID)
  - Fiecare interfata de retea are o adresa IPv4 unica
  - O adresa IPv4 are lungimea de 32 biti
  - Initial (RFC 791) exista impartirea in clase de adrese: A,B,C,D,E

Protocolul IP

- **Adrese IPv4**



[Computer Networks, 2003 Andrew S. Tanenbaum]

Protocolul IP

- **Adrese IPv4**
  - Clasa A: 128 retele posibile, 2^{24} gazde/retea
  - Clasa B: 2^{14} retele posibile, 2^{16} gazde/retea
  - Clasa C: peste 2 milioane de retele, 255 gazde/retea
  - Identificatorul de retea (NetID) este asignat de o autoritate centrala (NIC – *Network Information Center*)
  - Identificatorul de gazda (HostID) este asignat local de administratorul retelei
  - Exemplu: 85.122.23.145 – Clasa A (conventie de notatie in zecimal)

    0101 0101 0111 1010 0001 0111 1001 0001
  - Pentru IPv6 se recomanda reprezentarea hexadecimal

Protocolul IP

- **Adrese IPv4**
  - O interfata (placa) de retea are asignata o unica adresa IP
  - O gazda poate avea mai multe placi de retea, deci mai multe adrese IP
  - Gazdele unei aceleiasi retele vor avea acelasi identificator de retea (acelasi NetID)
  - Adresele de *broadcast* au HostID cu toti bitii 1
  - Adresa IP care are HostID cu toti bitii 0 se numeste adresa retelei – refera intreaga retea
    - Exemplu: adresa 85.122.23.0 (adresa *network* a masinilor 85.122.23.145 si 85.122.23.1
  - 127.0.0.1 – adresa de *loopback* (*localhost*)

Protocolul IP

- **Adrese IPv4**
  - Din spatiul de adrese ce pot fi alocate efectiv sunt rezervate urmatoarele (RFC 1918):
    - 0.0.0.0 – 0.255.255.255
    - 10.0.0.0 – 10.255.255.255 (adrese private)
    - 127.0.0.0 – 127.255.255.255 (pentru *loopback*)
    - 172.16.0.0 - 172.31.255.255 (adrese private)
    - 192.168.0.0 - 192.168.255.255 (adrese private)
  - Adrese private: adrese care nu sunt accesibile spre exterior (Internetul “real”), ci doar in intranetul organizatiei

Retele private

- Aspecte:
  - Cresterea exponentiala a numarului de gazde
  - Nu toate masinile gazda ofera resurse accesibile de pe Internet
- Solutia: NAT (*Network Address Translation*) – RFC 3022, 4008
  - Se reutilizeaza adresele private (RFC 1918)
  - Se bazeaza pe inlocuirea adresei private cu adresa IP neprivata (*IP masquerading*)

Retele private

- Functionalitate:

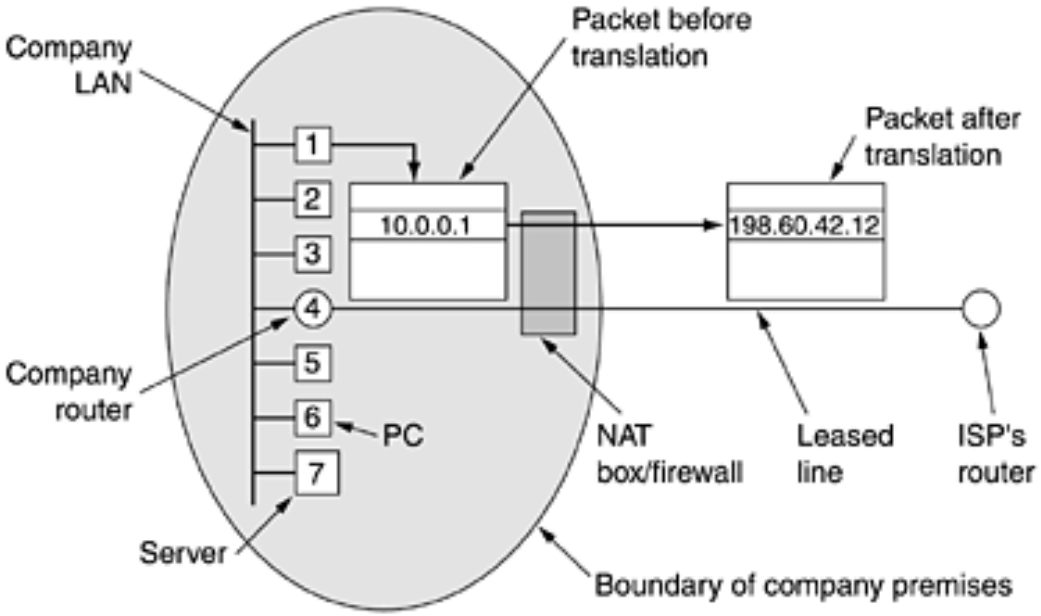


Figura: Functionare NAT

- Ruterele in mod normal ignora datagramele continind adrese private => pot fi folosite adrese IP private in cadrul intranet-ului organizatiei
- Accesul spre exterior (Internetul “real”) se realizeaza via o poarta (mediating gateway) ce rescrie adresele IP sursa/destinatie

[Computer Networks, 2003 Andrew S. Tanenbaum]

Protocolul IP

- **Subretele folosind masti de retea**
  - A aparut ca solutie pentru problema epuizarii spatiului de adrese IP
  - Simplifica rutarea
  - Subretelele nu pot fi detectate ca subretele din exterior

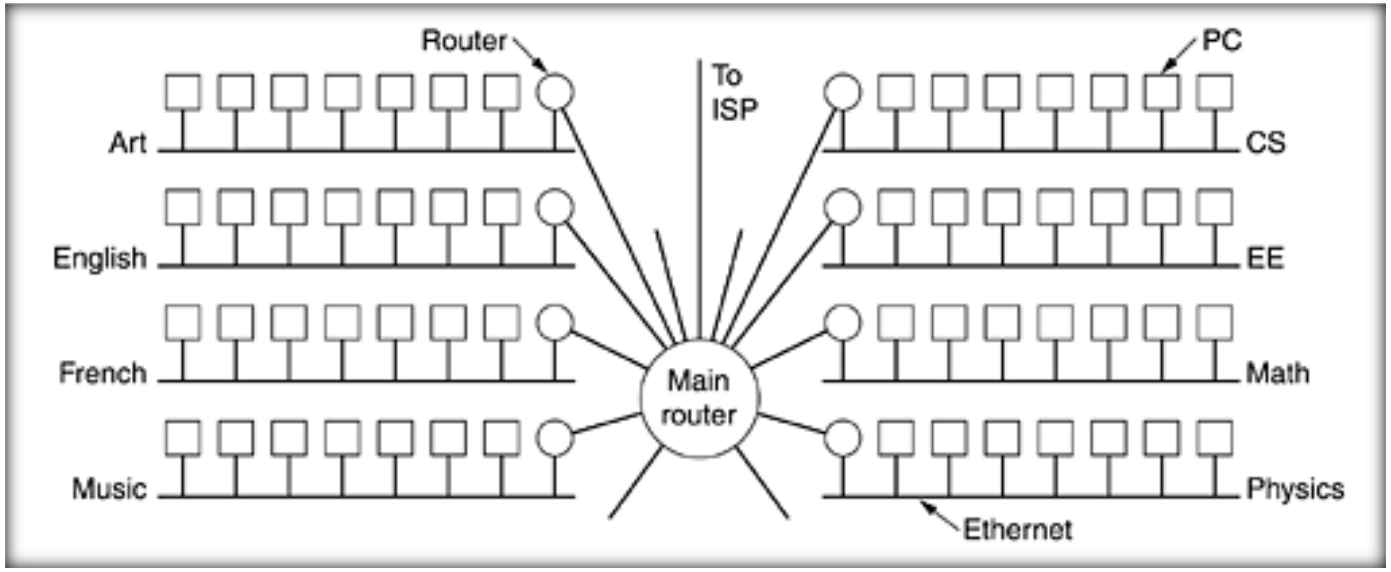


Figura: Reteaua unui campus

Protocolul IP

- **Subretele folosind masti de retea**
  - Divizarea in subretele se va face via masca de retea (*netmask*): bitii NetID sunt 1, bitii HostID sunt 0
  - Identificatorul subretelei (SubnetID) este utilizat in general sa grupeze calculatoarele pe baza topologiei fizice

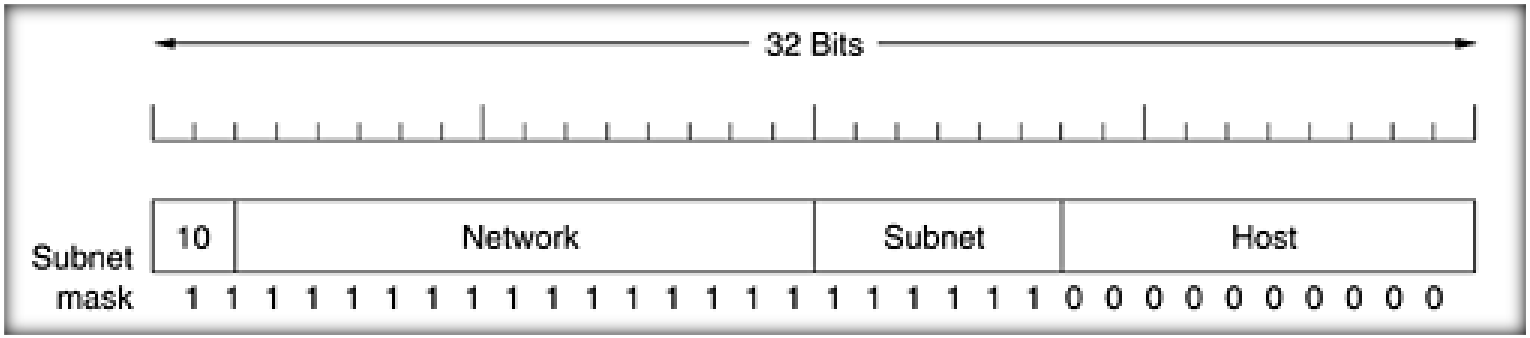


Figura. O cale de a crea o subretea dintr-o retea de clasa B

Protocolul IP

- **Subretele folosind masti de retea**
  - Exemplu:
    - Fie adresa IP: 160.0.6.7

      10100000 00000000 00000110 00000111
    - Masca de retea: 255.255.252.0

      11111111 11111111 11111100 00000000

      
    - Adresa de retea: 160.0.4.0

      10100000 00000000 00000100 00000000

  Adresa retelei = masca de retea AND adresa IP

- Masti de subretea implicite:
  - 255.0.0.0 Clasa A
  - 255.255.0.0 Clasa B
  - 255.255.255.0 Clasa C

Protocolul IP

- **Conventii de notare**: x.x.x.x/m inseamna ca se aplica o masca de m biti adresei IP precizata de x.x.x.x
- Exemplu:
  - 10.0.0.0/12 – se aplica o masca de 12 biti adresei 10.0.0.0, selectindu-se valorile posibile in ultimii 20 de biti (=32-12) de adresa
  - 85.122.16.0/20 – se aplica o masca de 20 biti adresei 85.122.16.0

Nivelul Retea

- Protocoale
  - ICMP (RFC 792)
  - ARP (RFC 826)
  - RARP (RFC 903)
  - BOOTP (RFC 951,1048,1084)
  - DHCP
- De la IPv4 la IPv6

Protocolul ICMP

- **ICMP – Internet Control Message Protocol**
  - Utilizat pentru schimbul de mesaje de control
  - Foloseste IP
  - Mesajele ICMP sunt procesate de software-ul IP, nu de procesele utilizatorului
  - Tipuri de mesaje :

Tipul mesajului	Descriere
8 Echo Request	Intreaba o masina daca este activa
0 Echo Replay	“Da, sunt activa”
3 Destination Unreachable	Pachetul nu poate fi livrat (e.g. DF setat)
5 Redirect	Schimbarea rutei
11 Time Exceeded	A expirat timpul
… etc (RFC 792)	http://www.iana.org/assignments/icmp-parameters

Protocolul ICMP

- Utilizat de:
  - comanda ping (Packet Internet Gropher)
  - comanda traceroute
    - Se trimite un pachet cu TTL=1 (1 hop)
    - Primul router ignora pachetul si trimite inapoi un mesaj ICMP de tip "*time-to-live exceeded*"
    - Se trimite un pachet cu TTL=2 (2 hop-uri)
    - Al doilea router ignora pachetul si trimite inapoi un mesaj "*time-to-live exceeded*"
    - Se repeta pina cind se primeste raspuns de la destinatie sau s-a ajuns la numarul maxim de hop-uri

Rezolutia adreselor

- **Adrese IP <-> adrese hardware (fizice)**
  - Procesul de a gasi adresa hardware a unei gazde stiind adresa IP se numeste rezolutia adresei (*address resolution*) – protocolul ARP (RFC 826)
    - ARP – protocol de tip broadcast (fiecare masina primeste cererea de trimitere a adresei fizice, raspunde doar cea in cauza)
  - Procesul de a gasi adresa IP pe baza adresei hardware se numeste rezolutia inversa a adresei (*reverse address resolution*) – protocolul RARP (RFC 903)
    - Utilizat la boot-are de statiile de lucru fara disc
    - BOOTP (RFC 951,1048,1084)
    - DHCP (*Dynamic Host Configuration Protocol*) RFC 2131,2132

IPv6

- Context:
  - Probleme de adresabilitate via IPv4 clasic:
    - Cresterea exponentiala a numarului de gazde
    - Aparitia unor tabele de rutare de mari dimensiuni
    - Configuratii tot mai complexe, utilizatori tot mai multi
    - Imposibilitatea asigurarii calitatii serviciilor (QoS)
  - Presiuni din partea operatorilor de telefonie mobila

IPv6

- Obiective pentru un nou protocol:
  - Suport pentru miliarde de gazde
  - Reducerea tabelelor de rutare
  - Simplificarea protocolului
  - Suport pentru gazde mobile
  - Compatibilitatea cu vechiul IP
  - Suport pentru evolutiile viitoare ale Internet-ului
- RFC 2460, 2553

IPv6

- 6 Iunie 2012

IPv6

- Aspecte:
  - Adresele IPv6 au lungime de 16 octeti - 2^{128} adrese
  - Notatie: 16 numere hexa, fiecare de 2 cifre, delimitate de ":"
    - Exemplu: 2001:0db8:0000:0000:0000:0000:1428:57ab
    - Daca unul sau mai multe din grupurile de 4 cifre este 0000, zerourile pot fi omise si inlocuite (o singura data) cu "::"
      - Exemplu: 2001:0db8::1428:57ab
  - Pentru pastrarea compatibilitatii: adresele IP publice sunt considerate un subset al spatiului de adrese IPv6
  - Adresele IPv4 in IPv6 pot fi scrise astfel:

10.0.0.1 -> ::10.0.0.1 sau 0:0:0:0:0:0:A00:1

IPv6

- ICMPv6
  - Ofera functiile ICMP (raportarea transmiterii datelor, erorilor, etc.) plus:
    - Descoperirea vecinilor (*Neighbor Discovery Protocol – NDP*) - Inlocuieste ARP
    - Descoperirea ascultatorilor multicast (*Multicast Listener Discovery*) – inlocuieste IGMP (*Internet Group Management Protocol*)
  - Detalii in RFC 4443

IPv6

- **…continuare -> Curs viitor**

Rezumat

- Nivelul Retea
  - Protocolul IPv4
    - Problematica
    - Caracterizare
    - Subretele
  - Retele Private
  - ICMP
  - Rezolutia adreselor
  - IPv6 – imagine generala

Intrebari?