

Lucrarea 2 : Scheme ierarhice de adresare in Internet

Problema : aceste scheme au fost propuse ca solutii la problema epuizarii spatiului de adrese IP. Sunt scheme de tip “classless”, provizorii pana la implementarea pe scara larga a tehnologiei IPv6.

Proprietati ale acestor solutii :

- alocarea eficienta a resurselor.
- faciliteaza segmentarea retelelor la nivel trei, in vederea cresterii performantelor (reduce domeniul de coliziune si de difuzare, utilizeaza mai eficient banda de transmisie intre statii).
- faciliteaza aplicarea politicilor de securitate si ascunderea topologiei retelei locale (transparența din rețeaua externă).

1 Tipuri de retele

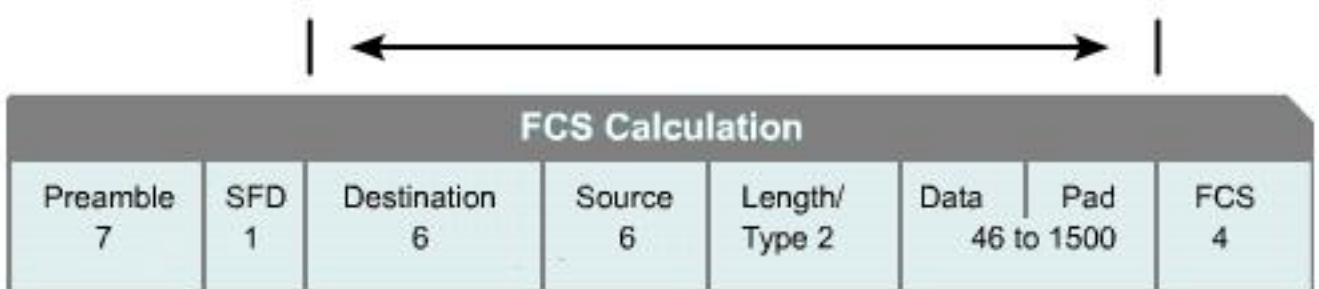
Retelele locale sau așa numitele LAN-uri (Local Area Network), sunt rețele private localizate într-o singură clădire sau într-un campus de cel mult câțiva kilometri. Ele sunt frecvent utilizate pentru a conecta calculatoarele personale și stațiile de lucru din birourile companiilor și fabricilor, în scopul de a partaja resurse (imprimante de exemplu) și a schimba informații.

Retelele metropolitane sau așa numitele MAN-uri (Metropolitan Area Network), deservește un întreg oraș. Cel mai bun exemplu de o rețea metropolitană este rețeaua de televiziune prin cablu disponibilă în cele mai multe orașe.

Retelele larg răspândite geografic sau așa numitele WAN-uri (Wide Area Network), acoperă o arie geografică întinsă, deseori o țară sau un continent. Rețeaua conține o colecție de mașini utilizate pentru a executa programele utilizatorilor (aplicațiile).

Tehnologia cea mai răspândită în domeniul rețelisticii în momentul de față este tehnologia Ethernet. Ethernet-ul nu este în sine o singură tehnologie, ci reprezintă o familie de tehnologii LAN. Este o tehnologie atât LAN cât și MAN și WAN.

Standardul care definește tehnologia Ethernet este standardul 802.3. Structura unui frame Ethernet este următoarea :



IEEE 802.3 Ethernet

- câmpul Preambul (Preamble) este de fapt un pattern de 1 și 0 care alternează (10101010) și este folosit pentru sincronizare în implementările asincrone de Ethernet. De la Fast Ethernet

incolo, deoarece aceste tipuri de Ethernet sunt sincrone, informatia corespunzatoare este redundanta, dar se pastreaza pentru compatibilitate.

- campul SFD (Start Frame Delimiter) este, de fapt, un octet care marcheaza sfarsitul informatiei de sincronizare, si contine secventa de biti : 10101011.
- campul Destinatia (Destination) contine adresa MAC a masinii destinatie.
- campul Sursa (Source) contine adresa MAC a masinii sursa.
- campul Lungime/Tip (Length/Type) suporta doua folosiri. Daca valoarea este mai mica decat 1536 in decimal (0x600H), atunci campul indica lungimea. Daca insa valoarea este egala sau mai mare decat 1536 decimal atunci campul indica tipul protocolului folosit.
- campul Data&Tampon (Data/Pad) poate fi de orice lungime, atata timp cat nu depaseste lungimea maxima admisa pentru un frame Ethernet. Un frame Ethernet trebuie sa aiba cel putin 46 octeti si cel mult 1500 octeti. Un tampon de marime nespacificata este introdus imediat dupa datele utilizatorului daca marimea frame-ului nu atinge cel putin 46 de octeti.
- campul FCS (Frame Check Sequence) contine o valoare CRC pe 4 octeti care este creata de masina care trimite si este recalculata de masina destinatie pentru a se indentifica erori. Aceasta valoare se calculeaza pe baza bitilor cuprinsi intre sfarsitul campului SFD si inceputul campului FCS.

2 Modelul OSI

Organizația Internațională de Standardizare (ISO) a stabilit în anul 1977 un subcomitet care să se ocupe de dezvoltarea standardelor pentru interconectarea sistemelor deschise (OSI). Astfel, în 1979 a apărut modelul de referință pentru protocoalele de comunicație, numit PRM (Protocol Reference Model).

Prin adoptarea internațională a acestui model se asigură o bază comuna pentru coordonarea dezvoltării standardelor de telecomunicații în vederea interconectării sistemelor deschise, rezolvându-se astfel, într-o oarecare măsură, problema compatibilității între sisteme si echipamente provenind de la producători diferiți, fără a impune, însă, anumite soluții tehnice.

Principala caracteristică a modelului OSI este structurarea schimbului de informații între utilizatorii sistemului de comunicație pe 7 straturi (niveluri). De aceea, acest model de numește și ”Modelul cu 7 straturi”.

Principiile de bază ale arhitecturii OSI sunt :

- partajarea sarcinilor între straturi trebuie făcută în mod flexibil (în mai multe moduri).
- straturile inferioare trebuie să asigure servicii in mod transparent către straturile superioare.
- schimbul de informații între straturi trebuie optimizat.



Stratul 1 - numit si stratul “fizic” - este stratul de bază, care asigură serviciile fizice. Nivelul fizic definește specificațiile electrice, mecanice, procedurale si funcționale pentru activarea, menținerea si dezactivarea legăturii fizice între sistemele finale. Totodata, el controlează specificațiile mediului de transmisie, controlează tensiunea, semnalele, viteza de transmisie, distanțele, conectorii.

Stratul 2 - numit si stratul “legatura de date” - permite transferul informației între sistemele interconectate. Acest strat transmite datele printr-o legatură fizică. Aceasta este partea fizică a unei rețele care se ocupă cu adresarea “fizică”, topologia rețelei, accesul la rețea, sesizarea erorilor, transportul cadrelor cerute și controlul fluxului.

Stratul 3 - stratul “rețea” - este cel mai complex nivel, care conectează si asigură ruta potrivită dintre două gazde aflate pe două rețele total diferite. Nivelul 3 se ocupa cu selectarea rutelor si adresarea.

Stratul 4 - stratul “transport” - asigură transportul informației între procesele de aplicație, efectuând controlul cap-la-cap al conexiunii si optimizează utilizarea resurselor în funcție de tipul și caracteristicile comunicației.

Stratul 5 - stratul “sesiune” - asigură organizarea transferului de informație și modul de structurare a dialogului între aplicații, de exemplu : dialoguri alternative (semi-duplex) sau duplex integral (full-duplex). Oferă date stratului “prezentare”. Ajută două gazde să își sincronizeze dialogul și administrează schimbul de date. Oferă resursele pentru un transfer de date eficient și raportează erorile proprii sau ale nivelelor superioare.

Stratul 6 - stratul “prezentare” - verifică dacă datele sunt într-un format care poate fi înțeles de ambele părți implicate în comunicare. Daca nu, le convertește la un format comun. Acționează ca un translator într-o conversație.

Stratul 7 - stratul “aplicație” - oferă servicii de rețea pentru aplicațiile utilizatorilor. Având în vedere ca se afla in vârful stivei, nu ofera sevicii pentru alte straturi, ci pentru aplicațiile exterioare. Nivelul de aplicații verifică partenerii de comunicare, integritatea si sincronizarea datelor. Ca regulă generala, se poate face urmatoarea afirmație : pentru straturile de la baza stivei modelului de referinta OSI (straturile 1 - 4) serviciile care trebuie asigurate sunt relativ simple, dar mecanismele necesare pentru asigurarea lor sunt complexe, iar pentru straturile superioare (straturile 5 - 7), serviciile care trebuie asigurate sunt complexe, însă mecanismele necesare pentru asigurarea lor sunt relativ simple.

Diferențe între modelul OSI și TCP/IP

Suita de protocoale TCP/IP este organizată pe 5 niveluri conceptuale (Aplicație, Transport, Internet, Legătură de date, Fizic).

Există două diferențe –subtile, dar importante- între modelul conceptual al arhitecturii TCP/IP și modelul de referință OSI, diferențe ce rezultă din modul în care sunt gândite soluțiile privind asigurarea fiabilității și amplasarea „inteligenței” în întregul sistem.

O diferență principală între protocoalele TCP/IP și protocoalele OSI constă în modul de abordare a problemei furnizării unor servicii fiabile de transfer de date. În modelul OSI, programele de protocoale detectează și soluționează erorile la toate nivelurile, în timp ce modelul arhitectural al TCP/IP își bazează suita de protocoale pe ideea că fiabilitatea este o problemă între utilizatorii finali. Eliberarea “nivelului de interfață de rețea” de sarcina verificării corectitudinii transmiterii datelor face ca software-ul TCP/IP sa fie mai ușor de înțeles și de implementat.

O altă diferență între modelul TCP/IP și modelul OSI provine din alegerea locului unde se am-

plasează autoritatea și de unde se face conducerea. În concluzie, o rețea (de calculatoare) este un sistem complex, independent și deschis, la care pot fi atașate calculatoare relativ simple, întrucât calculatoarele participă în foarte mică măsură la funcționarea rețelei. Ca regulă generală, rețelele implementate după modelul OSI aderă la ideea că o rețea de calculatoare este un mijloc care oferă servicii de transport de informații. În opoziție cu acest concept, TCP/IP pretinde calculatoarelor să participe la aproape toate protocoalele de rețea.

3 Adrese IP

Adrese IPv4 :

- au 32 de biti organizati in 4 grupe de 8 biti.
- sunt organizate in clase de adrese : Clasa A, Clasa B, Clasa C, Clasa D, Clasa E.
- clasele A, B, C reprezinta adrese de unicast.
- clasa D - clasa adreselor de multicast.
- clasa E este rezervata (neutilizata pentru a da adrese hosturilor si dispozitivelor de retea).
- adresele IP de unicast contin adresa rețelei din care face parte hostul și adresa hostului.
- adresa rețelei se obtine punand bitii din host address pe 0.
- fiecare adresa IPv4 este insotita de o masca de retea (masca de retea are 32 de biti organizati in 4 grupe de 8 biti).
- o adresa IP se specifica insotita de masca sa (de ex. IP = 10.2.3.1 255.0.0.0 sau 10.2.3.1/8).

Clasa A :

ID clasa 7 biti

0	ID retea	ID gazda
---	----------	----------

Cuprinde adrese de la 1.0.0.0. pana la 127.255.255.255, masca implicita 255.0.0.0

Clasa B :

ID clasa 14 biti

10	ID retea	ID gazda
----	----------	----------

Cuprinde adrese de la 128.0.0.0. pana la 191.255.255.255, masca implicita 255.255.0.0

Clasa C :

ID clasa 21 biti

110	ID retea	ID gazda
-----	----------	----------

Cuprinde adrese de la 192.0.0.0. pana la 223.255.255.255, masca implicita 255.255.255.0

Clasa D :

1110	ID grup
------	---------

Cuprinde adrese de la 224.0.0.0 pana la 239.255.255.255

Clasa E :

11110	Rezervat pentru o folosire ulterioara
-------	---------------------------------------

Cuprinde adrese de la 240.0.0.0 pana la 247.255.255.255

Adrese IP private :

- adrese private de clasa A = 10.0.0.0 - 10.255.255.255
- adrese private de clasa B = 172.16.0.0 - 172.31.255.255
- adrese private de clasa C = 192.168.0.0 - 192.168.255.255
- adresele de clasa A care incep cu 127 sunt rezervate pentru depanare și management (de ex. 127.0.0.1 este adresa de loopback)

Adrese IPv6 :

- au 128 de biti organizati in 8 grupe de 16 biti. Fiecare grupa de 16 biti se reprezinta prin 4 cifre hexazecimale.
- fiecare grup de 16 biti se trece in baza 16, rezultand astfel 4 cifre hexazecimale.
- daca includ adrese de IPv4, acestea se reprezinta in baza 10 și ocupa ultimi 32 de biti ai

- adresei : IPv6 = x :x :x :x :x :x :d.d.d.d
- adresele IPv6 nu sunt organizate in clase de adrese.
 - sunt de trei tipuri : unicast, multicast si anycast.
 - nu exista adrese de broadcast - acestea sunt forme particulare ale adreselor de multicast.
 - orice adresa care incepe cu FF este de multicast si orice adresa care incepe cu orice alte cifre hexazecimale este de unicast (anycast).
 - adresele de anycast sunt adrese de unicast care se atribuie numai routerelor pentru functii speciale (mai multe interfete apartinand diverselor routere au aceeaasi adresa de unicast, pachetul ajunsa insa la interfata “cea mai apropiata”).
 - adresa de loopback in IPv6 este : 0 :0 :0 :0 :0 :0 :0 :1
 - pentru perioada de tranzitie IPv4 – IPv6 exista moduri de generare a adreselor Ipv6 din Ipv4 :IPv4 compatible IPv6 address, Ipv4 mapped IPv6 address.

4 Subnetizare

Problema principala a adresarii bazate pe clase : clasele A si B sunt mult prea mari, iar clasa C este prea mica pentru unele institutii si prea mare pentru altele. Spatiul de adrese IP este limitat si acest tip de adresare risipeste cea mai mare parte a adreselor, deoarece retelele de clasa A si B au teoretic milioane sau zeci de mii de host-uri si practic numai o parte din acest numar se folosesc in cadrul unei singure retele. Este de dorit realizarea fizica a cat mai multe retele avand un numar cat mai mic (zeci) de hosturi.

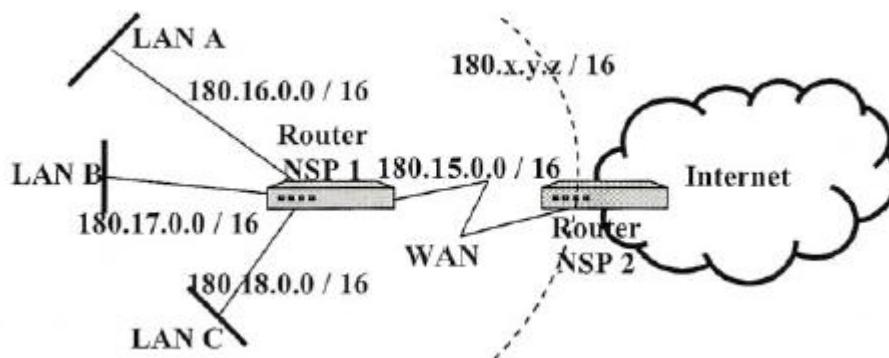
Solutie : se renunta la clasa (adresarea classless). Se elimina masca implicita cu specificarea explicita a mastii alaturi de adresa ; protocoalele de rutare trebuie sa stie acest lucru.

Se creeaza subretele prin impartirea unei retele de clasa A, B, C in 2, 4, 8, 16, etc (puteri ale lui 2) retele mai mici, adica, prin imprumutarea unei secvente de biti din ID gazda se va obtine un ID subretea.

10	ID retea	ID subretea	ID gazda
----	----------	-------------	----------

Numarul de subretele este egal cu $2^{|ID_{subretea}|}$. Se utilizeaza o masca pentru a indica adresa de subretea (ID-ul retelei + ID-ul de subretea). Masca este de lungime fixa pentru toate segmentele de subretea nou create. Este o schema de adresare rigida, care nu ia in seama numarul de gazde pe fiecare segment de retea.

Astefl, o institutie care primeste o retea de clasa A (16 milioane de host-uri) poate crea prin subnetting foarte multe subretele cu un numar mic de hosturi, si totusi sa apara in internet ca detinand o singura retea de clasa A, deci o singura intrare in tabela de rutare. Exemplu de subnetizare : se considera configuratia din figura



In continuare se va arata cum utilizand numai domeniul de adrese 180.15.0.0 255.255.0.0 este suficient pentru a aloca adrese tuturor subretelelor din figura.

10110100.00001111.00000000.00000000 = 180.15.0.0
 11111111.11111111.00000000.00000000 = 255.255.0.0

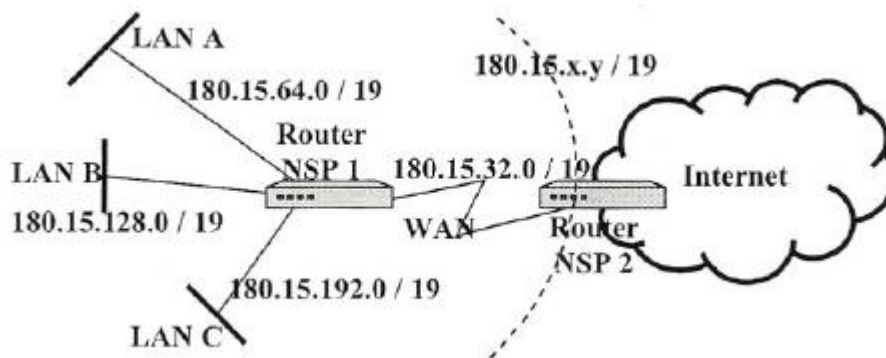
Se observa ca sunt 4 subretele care trebuie sa aiba prefixul de retea diferit. In acest scop se extinde acest camp, imprumutand biti din campul de identificare al gazdelor (dupa relatia de mai sus). Rezulta masca de subretea pe 19 biti :

11111111.11111111.11100000.00000000 = 255.255.224.0 (masca de subretea)

Prefixele rezultate se asociaza ad hoc la subretele :

WAN	180.15.32.0/19
LAN A	180.15.64.0/19
LAN B	180.15.128.0/19
LAN C	180.15.192.0/19

Dupa subnetizare, topologia logica rezultata este urmatoare :



Adresele 180.16, 180.17, 180.15.160, 180.15.96 raman in acest mod neutilizate fiind disponibile pentru a fi alocate altor entitati.

Ex. 1 : Dati exemple de adrese de clasa A, B de difuzare, C, D, E.

Ex. 2 : Carei clase de adrese ii apartine adresa 170.168.175.255/20? In total cate gazde pot exista in aceasi subretea ?

Ex. 3 : Sa se proiecteze trei subretele stiind ca adresa de retea primita de la ISP este 172.168.0.0. Sa se precizeze care sunt adresele de subretea, respectiv de difuzare.

5 Metoda VLSM de subnetizare

Se mai numeste subnetizare de subretele. Aceasta schema de adresare permite utilizarea la maximum (subnetizarea nu utiliza eficient spatiul de adrese) a spatiului de adrese alocat unui domeniu administrativ.

Acest lucru este posibil prin utilizarea mai multor masti de retea de lungime diferita in functie de necesitati.

Exemplu

Se considera aceeasi configuratie fizica si logica a subretelelor determinata mai sus. In plus se presupune ca din totalul de adrese alocate pentru fiecare subretea sunt utilizate efectiv numai o parte, asa cum este precizat in figura de mai de jos :

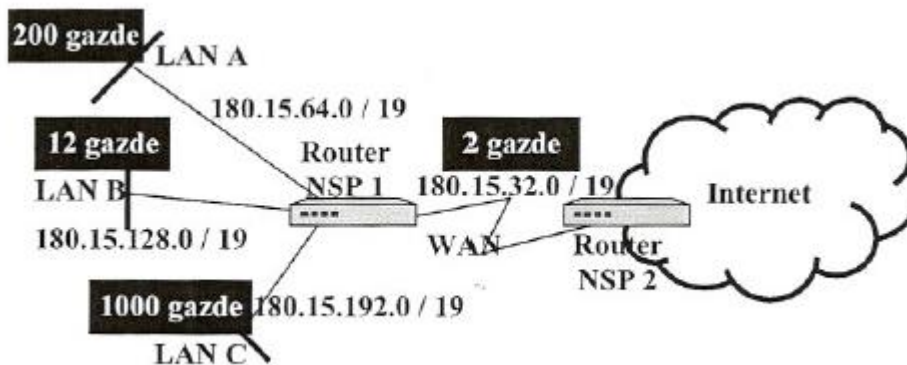
Se observa ca gradul de utilizare a spatiului de adrese este urmatorul :

$$\eta_{LANA} = 200/(2^{13} - 2) = 2,4\%$$

$$\eta_{LANB} = 12/(2^{13} - 2) = 0,1\%$$

$$\eta_{LANC} = 1000/(2^{13} - 2) = 12,2\%$$

$$\eta_{WAN} = 2/(2^{13} - 2) = 0,02\%$$



Determinarea lungimii mastii pentru fiecare subretea in functie de necesitati :

LAN A : pentru 200 de gazde, $|ID_{gazda}| = 8$ biti, $|masca| = 24(255.255.255.0)$

LAN B : pentru 12 de gazde, $|ID_{gazda}| = 4$ biti, $|masca| = 28(255.255.255.240)$

LAN C : pentru 1000 de gazde, $|ID_{gazda}| = 10$ biti, $|masca| = 22(255.255.252.0)$

WAN : pentru 2 de gazde, $|ID_{gazda}| = 2$ biti, $|masca| = 30(255.255.255.252)$

Spatiul de adrese gazda definit de 180.15.32.0/19 este suficient de mare ($2^{13} - 2 = 8190$) pentru a acoperi toate gazdele ($200 + 12 + 1000 + 2 = 1214$) din configuratia data. Se vor aloca deci adrese din acest spatiu, astfel :

LAN C : (180.15.32.1 - 180.15.35.232)/22

LAN A : (180.15.36.1 - 180.15.36.200)/24

LAN B : (180.15.37.1 - 180.15.37.12)/28

WAN : (180.15.37.17 - 180.15.37.18)/30

