Protocolul TCP/IP

A fost creat pentru a permite interconectarea rețelelor de calculatoare. A devenit standard în Internet și se bazează pe adresele IP.
Orice calculator care are acces la Internet are implementat protocolul TCP/IP și deține o adresă IP unică. A înlocuit protocolul IPX/SPX care permite și el interconectarea rețelelor.

Nevoia de interconectare vine din faptul că rețelele locale au un număr limitat de stații care pot funcționa optim.

Adresarea pe bază de MAC nu este practică pentru interconectare, deoarece adresele MAC nu sunt administrate de administratorul rețelei/rețelelor.

O adresare eficientă trebuie să se bazeze pe adrese care combină o adresă specifică rețelei cu una specifică computerului (nodului) din rețea:

Adresă rețea	Adresă nod	Număr port/socket

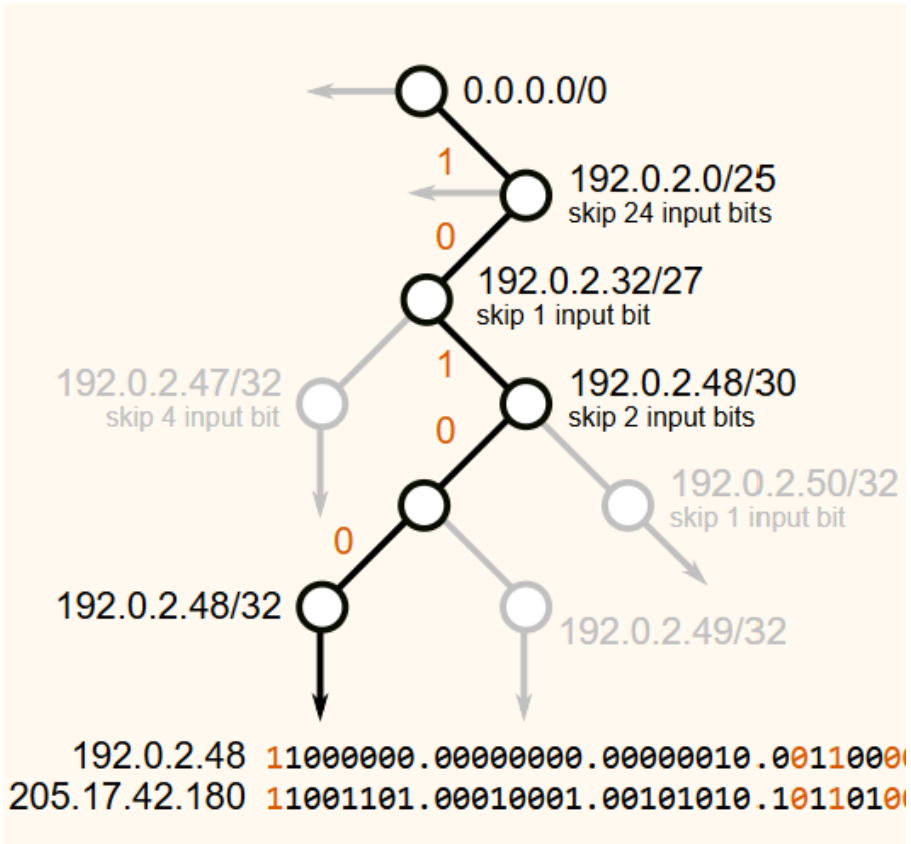
*Fac excepția adresele private care se „ascund” în spatele unei adrese IP publice, unică.

Protocolul TCP/IP

Adresarea IPX/SPX folosește adresa MAC ca adresă a nodului în timp ce adresa rețelei are lungime fixă de 4 octeți. Numărul socket-ului are 2 octeți (4 cifre hexazecimale) și identifică un anumit proces sau serviciu care rulează pe un nod.

Adresele IP au adresa numărului de rețea de lungime variabilă în timp ce lungimea totală a adresei este fixă. Adesa IP a unui nod din rețea este unică (combinația număr rețea și număr nod este unică)

În prezent există în uz două versiuni de adrese IP: IPV4 pe 32 biți și IPV6 pe 128 biți. Cea de a doua, mai puţin răspândită dar aflată în plin proces de generalizare, a fost elaborată pentru a creşte numărul de adrese IP disponibile şi pentru a îmbunătăţi schema pe 4 octeţi.
În format ușor de citit de către om, adresele IPV4 se scriu ca o succesiune de 4 octeți în format zecimal, octeți separați prin punct zecimal: 192.168.0.1. Cele din clasa IPV6 se scriu în format hexazecimal, în grupuri de cîte 4 cifre separate prin :, de exemplu: 2001:0db8:85a3:0000:0000:8a2e:0370:7334



Întreg spațiul adreselor IP este divizat în 5 clase notate cu litere de la A la E, din care doar primele 3 au utilizare publică. Ideea care a stat la baza împărțirii adreselor în clase este că orice adresă IP să fie formată din două părți: prima parte să reprezinte adresa rețelei iar partea a doua să reprezinte adresa host-ului în rețea.

S-a convenit ca pentru clasa A primul octet să reprezinte numărul rețelei iar restul de trei octeți să reprezinte adresa host-ului. Primul bit al primului octet trebuie să fie 0.
La clasa B primii doi octeți dau adresa rețelei iar ultimii doi adresa host-ului. Prefixul pentru primul octet din adresa rețelei trebuie să fie 10.

În fine, la clasa C primii trei octeți dau adresa rețelei iar ultimul octet furnizează adresa host-ului. Prefixul primului octet al adresei rețelei trebuie să fie 110. O altă convenție este ca nicio adresă, fie ea de rețea sau de host, să nu aibă toți biții cu valoarea 0 sau 1.

Clasele adreselor IPv4

Clasa	prefix	Adresa început	Adresă sfârșit
A	0	1.0.0.1	127.255.255.254
B	10	128.0.0.1	191.255.255.254
C	110	192.0.0.1	223.255.255.254
D	1110	224.0.0.1	239.255.255.254
E	1111	240.0.0.1	255.255.255.254

Clasele D si E sunt clase speciale, care nu au utilizare publică, în sensul că adresele din aceste clase nu sunt alocate clienților și serverelor în mod obișnuit. Adresele din clasa D sunt folosite pentru multicasting.
Multicast-ul este un mecanism de definire a unui grup de noduri de rețea către care se trimit simultan pachete de date folosind adresarea IP. Multicast-ul este folosit în principal de rețelele de cercetare.

Clasa E este o clasă rezervată pentru destinații speciale. Host-urile care folosesc adrese din aceste clase nu vor putea comunica corect.

O situație aparte o reprezintă adresa 255.255.255.255 din clasa E folosită pentru broadcasting în rețelele locale. Un pachet IP cu această adresă va fi recepționat de către toate nodurile rețelei locale dar nu și de alte host-uri din Internet. Din acest motiv procedeul se numește broadcast limitat.

Convenție

Nicio adresă de host sau de rețea nu poate să aibă toți biții cu valoarea 0 sau 1.

În cazul rețelelor din clasa A, primul octet desemnează rețeaua iar primul bit are valoarea 0. Aceasta înseamnă că cea mai mică adresă posibilă se obține când toți biții sunt 0 iar cea mai mare când toți biții sunt 1, cu excepția primului care rămâne 0

Bit	1	2	3	4	5	6	7	8	Valoarea în zecimal
	0	0	0	0	0	0	0	0	→ 0
	0	.	.	.	.	.	.	.	
	0	1	1	1	1	1	1	1	→127

Rezultă că spațiul adreselor valide este 0.0.1 - 255.255.254, de unde și valorile din Tabelul 1. Concluzia este că în clasa A sunt un număr de 127 de rețele și 16777214 hosturi în fiecare rețea.

Pentru rețelele din clasa B, primii 2 octeți din adresa IP sunt alocați numărului rețelei iar ultimii 2 numărului host-ului. Primii doi biți ai primului octet fiind rezervați pentru prefixul rețelei, rămân 14 biți pentru stabilirea numărului rețelei.

1	2	3	4	5	6	7	8		9	10	11	12	13	14	15	16	Valoarea zecimală
1	0	0	0	0	0	0	0	.	0	0	0	0	0	0	0	0	→ 128.0
1	0	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	
1	0	1	1	1	1	1	1	.	1	1	1	1	1	1	1	1	→191.255

Numărul total de rețele din clasa B este de 214 = 16384, din care adrese valide sunt cu două mai puțin, adică 16382, iar numărul de host-uri din fiecare rețea este de 216 – 2 = 65534.

La clasa C, primii 3 octeți sunt rezervați pentru numărul rețelei iar ultimul pentru numărul host-ului. Se găsește că adresa cea mai mică pentru o rețea din clasa C este 192.255.255 iar cea mai mare 223.255.255, numărul total de adrese de rețea fiind 2097152. Fiecare rețea poate conține 28 –2 = 254 de host-uri.

Adrese rezervate

Clasa A
10.0.0.0 până la 10.255.255.255
127.0.0.0 până la 127.255.255.255 Loopback
Clasa B
172.16.0.0 până la 172.31.255.255 - LAN fără acces la Internet
Clasa C
192.168.0.0 – 192.168.255.255 - LAN fără acces la Internet

Alocarea adreselor IP

Adresele IP, atât cele pe 4 cât și cele pe 6 octeți, sunt gestionate, la nivel global de IANA (Internet Assigned Numbers Authority).

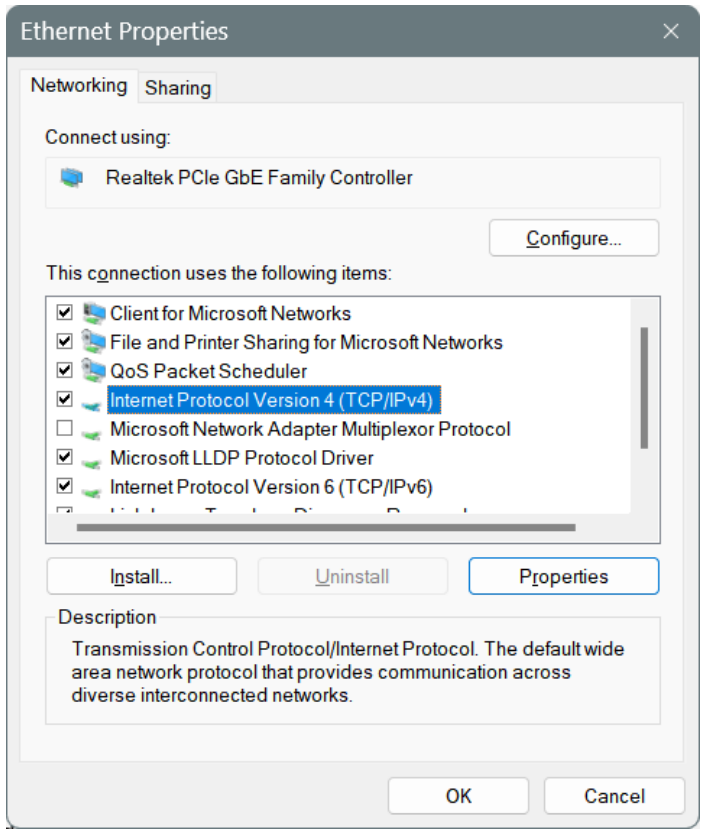
Registre regionale Internet

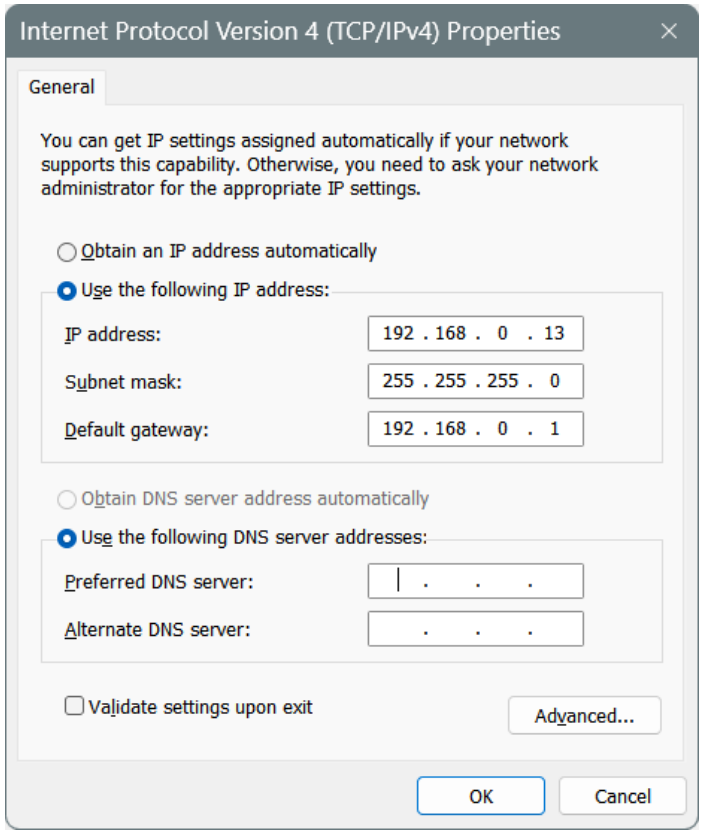
- AfriNIC (African Network Information Centre) – regiunea Africa
- APNIC (Asia Pacific Network Information Centre) – regiunea Asia/Pacific
- ARIN (American Registry for Internet Numbers) – regiunea America de Nord
- LACNIC (Regional Latin-American and Caribbean IP Address Registry) – America Latină și câteva insule din Caraibe
- RIPE NCC (Réseaux IP Européens) – regiunea Europa, Orientul mijlociu și Asia Centrală.

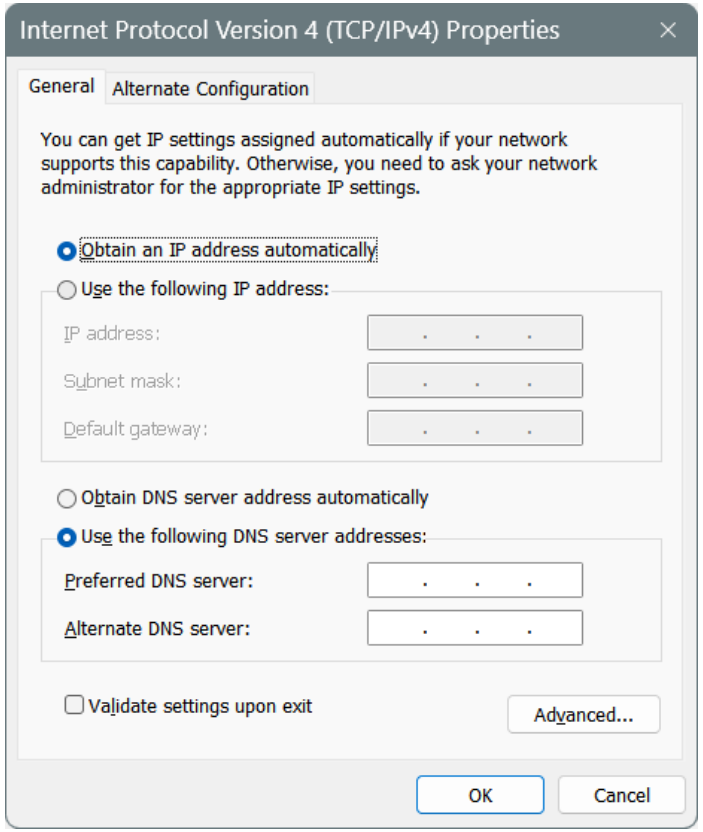
Registrele regionale repartizează blocuri de adrese autorităților naționale din țările arondate. Pentru România: ICI - Institutul de Cercetări în Informatică. Acestea repartizează și ele blocuri de adrese Furnizorilor de Servicii Internet (ISP).

Atribuirea adreselor IP

Orice dispozitiv, DTE sau DCE care este conectat la Internet trebuie să aibă o adresă IP. Atribuirea adreselor se poate face în două moduri: - Manual | - Automat, cu ajutorul protocolului DHCP Dynamic Host Configuration Protocol.



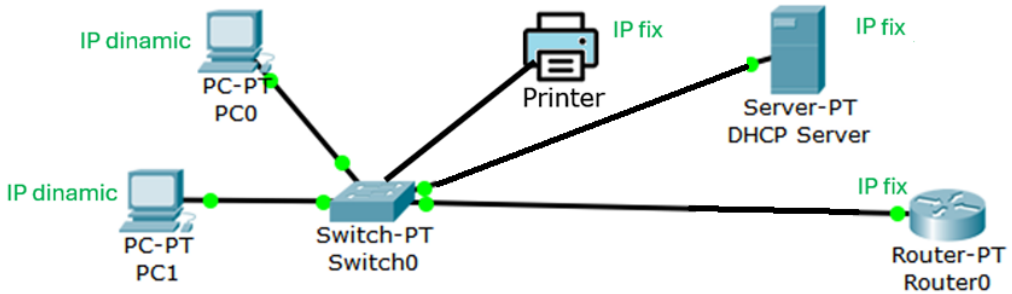




Atribuirea statică este potrivită pentru rețele mici, localizate pe orie restrânsă (LAN). Adresele sunt introduse manual de administratorul rețelei, care ține evidența lor. Ineficientă în cazul rețelelor mari cu dispozitive îndepărtate.

Atribuirea atomată este potrivită rețelelor cu multe calculatoare (și alte echipamente, precum imprimante) și necesită un server DHCP. Atunci când un echipament este alimentat, dacă este configurat pentru obținere automată a adresi IP, el va lansa o cerere pe adrea IP de broadcast 255.255.255.255. Dacă în rețea se află un server DHCP, acesta va răspunde pe adresa MAC inclusă în cerere, iar răspunsul va conține toate informațiile necesare de configurare, pe lângă adresa IP.

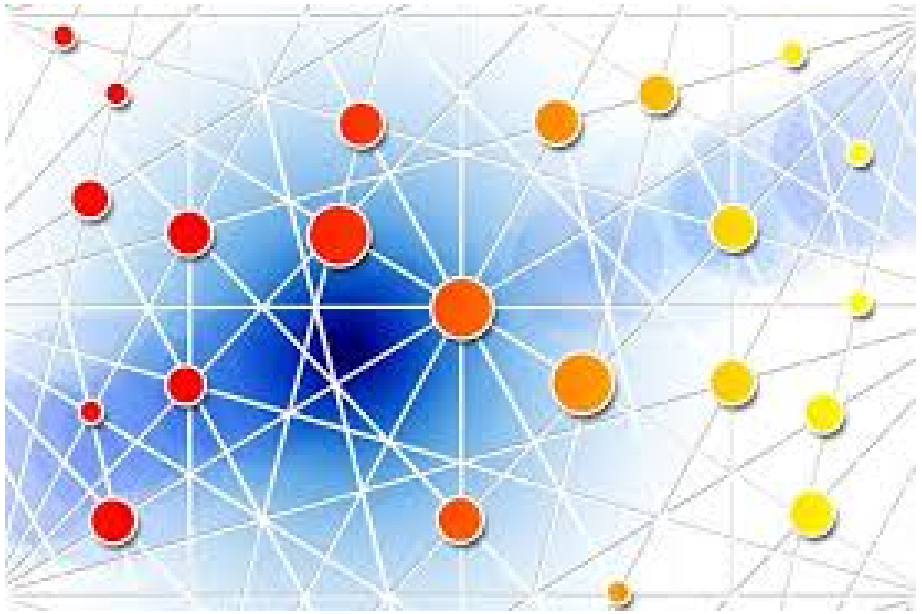
Atribuirea automată poate fi **Statică** sau **Dinamică**. Atribuirea statică alocă mereu aceeași adresă IP pe baza adresi MAC a interfeței de rețea. Atribirea dinamică închiriază aleatoriu adrese IP calculatoarelor la fiecare pornire, dacă adresa atribuită în sesiunea anterioară nu se află în perioada de închiriere.



Exemplu de alocare automată a adreselor IP

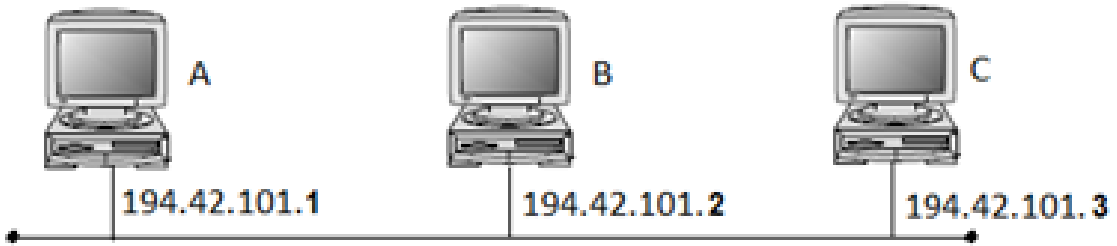
```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek 8821CE Wireless LAN 802.11ac PCI
   Physical Address. . . . . . . . . : FC-B0-DE-00-3B-2D
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2a02:2f0e:fa0a:9900:5852:e696:a2fa:40ff(
   Temporary IPv6 Address. . . . . . : 2a02:2f0e:fa0a:9900:c101:bdef:64ec:631d(
   Link-local IPv6 Address . . . . . : fe80::9560:267c:d5bb:e538%16(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.134(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : duminică, 12 octombrie 2025 03:20:27
   Lease Expires . . . . . . . . . . : marți, 14 octombrie 2025 13:54:54
   Default Gateway . . . . . . . . . : fe80::1%16
                                       192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 284995806
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2E-BC-48-3D-04-BF-1B-B6-11-E
   DNS Servers . . . . . . . . . . . : fe80::1%16
                                       192.168.1.1
                                       fe80::1%16
```

Fundamentele rutării IP



Rutarea simplă - rutarea directă

Se poate determina adresa MAC a fiecărei stații pe baza adresei IP prin utilizarea protocolului „Protocol de Rezoluție a Adreselor” (ARP – Address Resolution Protocol) care permite descoperirea dinamică a adreselor Ethernet .



Adresă IP sursă: 194.42.101.1	Adresă Ethernet sursă: 00-10-DC-49-8A-20
Adresă IP țintă: 194.42.101.2	Adresă Ethernet țintă: FF-FF-FF-FF-FF-FF
Adresă IP țintă: 194.42.101.3	Adresă Ethernet țintă: FF-FF-FF-FF-FF-FF

Răspuns nodul B

Adresă IP sursă: 194.42.101.2
Adresă Ethernet sursă: 00-27-AE-49-FF-A4
Adresă IP țintă:194.42.101.1
Adresă Ethernet țintă: 00-10-DC-49-8A-20

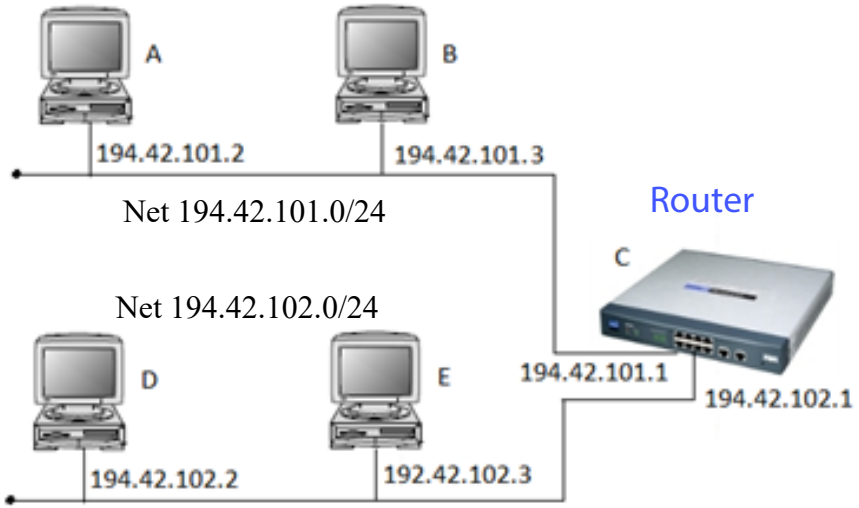
Răspuns nodul C

Adresă IP sursă: 194.42.101.3
Adresă Ethernet sursă: 00-16-7E-3C-FB-44
Adresă IP țintă:194.42.101.1
Adresă Ethernet țintă: 00-10-DC-49-8A-20

Răspunsurile nodurilor B și C sunt recepționate de nodul A care completează, în memoria cache, o tabelă de corespondențe între adresele IP și adresele MAC ale calculatoarelor din rețea, de genul:

Adresă IP:	Adresă Ethernet:
194.42.101.1	00-10-DC-49-8A-20
194.42.101.2	00-27-AE-49-FF-A4
194.42.101.3	00-16-7E-3C-FB-44

Rutarea simplă - rutarea indirectă



Router-ul alege calea potrivită pentru pachetele din rețea pe baza adreselor IP de destinație ale pachetelor pe care le primește pe cele două interfețe și pe baza unei tabele de rutare rezidentă în router.

Dacă nodul A trimite un pachet nodului E, el trebuie mai întâi să îl trimită pe interfața nodului C din rețeaua în care se află A. Pe baza tabelei de rutare, care în acest caz este foarte simplă, router-ul trimite pachetul pe interfața din rețeaua în care se află nodul E. Nodul C determină adresa Ethernet a nodului E folosind protocolul ARP, așa cum s-a arătat mai devreme. Pentru exemplul de mai sus, tabela de rutare arată astfel:

C 192.168.101.0/24 is directly connected, FastEthernet0/0

C 192.168.102.0/24 is directly connected, FastEthernet1/0 *

Tabela de rutarea poate fi introdusă manual - *rutare statică* sau se obține automat de către ruter - *rutare dinamică*.

*Pentru desemnarea unei rețele se obișnuiește să se folosească notația *adresă_rețea.adresă_host_0/*

nr_biți_adresă rețea. Ex: Clasă A: 80.0.0.0/8 Clasă B: 128.50.0.0/16 Clasă A: 200.10.30.0/24

Rutarea IP avansată

Masca de subrețea

Face parte din setul de configurare al oricărui host conectat la o rețea care folosește prorocolul TCP/IP

Este folosită pentru determinarea rețelei de destinație. Are următoarele valori standard : clasa A - 255.0.0.0

clasa B - 255.255.0.0

clasa C - 255.255.255.0

Cum se folosește

Adr. IP nod E: 194.42.102.3 Adresă host destinație

1	1	0	0	0	0	1	0	.	0	0	1	0	1	0	1	0	.	0	1	1	0	0	1	1	0	.	0	0	0	0	0	0	1	0

Netmask: 255.255.255.0

1	1	1	1	1	1	1	1	.	1	1	1	1	1	1	1	1	.	1	1	1	1	1	1	1	1	.	0	0	0	0	0	0	0	0

Adr. Rețea: 194.42.102 Adresă rețea destinație

1	1	0	0	0	0	1	0	.	0	0	1	0	1	0	1	0	.	0	1	1	0	0	1	1	0	.	0	0	0	0	0	0	0	0

Subrețele

Fie o rețea de clasă C 192.42.102.0/**24** care are 254 de hosturi. Dacă scriem ultimul octet în format binar

192.42.102| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Putem reține un număr de biți, de exemplu 2 din octetul rezervat host-ulu pe care să-i atribuim subrețelelor formate cu ei:

192.42.102| x | x | 0 | 0 | 0 | 0 | 0 | 0 | Rezultă 4 subrețele 00, 01, 10, 11 cu adresele

subnet

192.42.102.0/**26**
192.42.102.64/**26**
192.42.102.128/**26**
192.42.102.192/**26**

Masca de subrețea rezultă punînd pe 1 toți biții din mască din dreptul biților de subrețea

255.255.255. | 1| 1| 0 | 0 | 0 | 0 | 0 | 0 | => 255.255.255.192

Exemplu de împărțire în subrețele a rețelei de clasă A 10.0.0.0/8

Dorim împărțirea într-un număr de subrețele care să conțină, fiecare, 256 de host-uri.

Aflăm de câți biți avem nevoie pentru adresa de host: $2^x = 256$ -> x=8. Deci, ultimii 8 biți ai adresei vor fi ai adresei host-ului.

Clasa A 10.0.0.0/8, Masca de subrețea 255.0.0.0 , Adresă de broadcast: 10.255.255.255

După împărțire: 10.0.0.0/24 Masca de subrețea 255.255.255.0 , Adresă de broadcast: variabilă de la o subrețea la alta

Prima subrețea este cea în care toți biții împrumutați de la host sunt 0 -> 0.0 Adresa completă este 10.0.0.0/24

A doua subrețea este cea în care cel mai puțin semnificativ bit din cei împrumutați de la host este 1 -> 0.1 Adresa completă este 10.0.1.0/24

La următoare subrețea, la octeții împrumutați de la host se mai adaugă o unitate -> 0.2

Procesul se repetă până toți biții împrumutați de la host sunt 1 -> 255.255 Adresa completă este 10.255.255.0/24

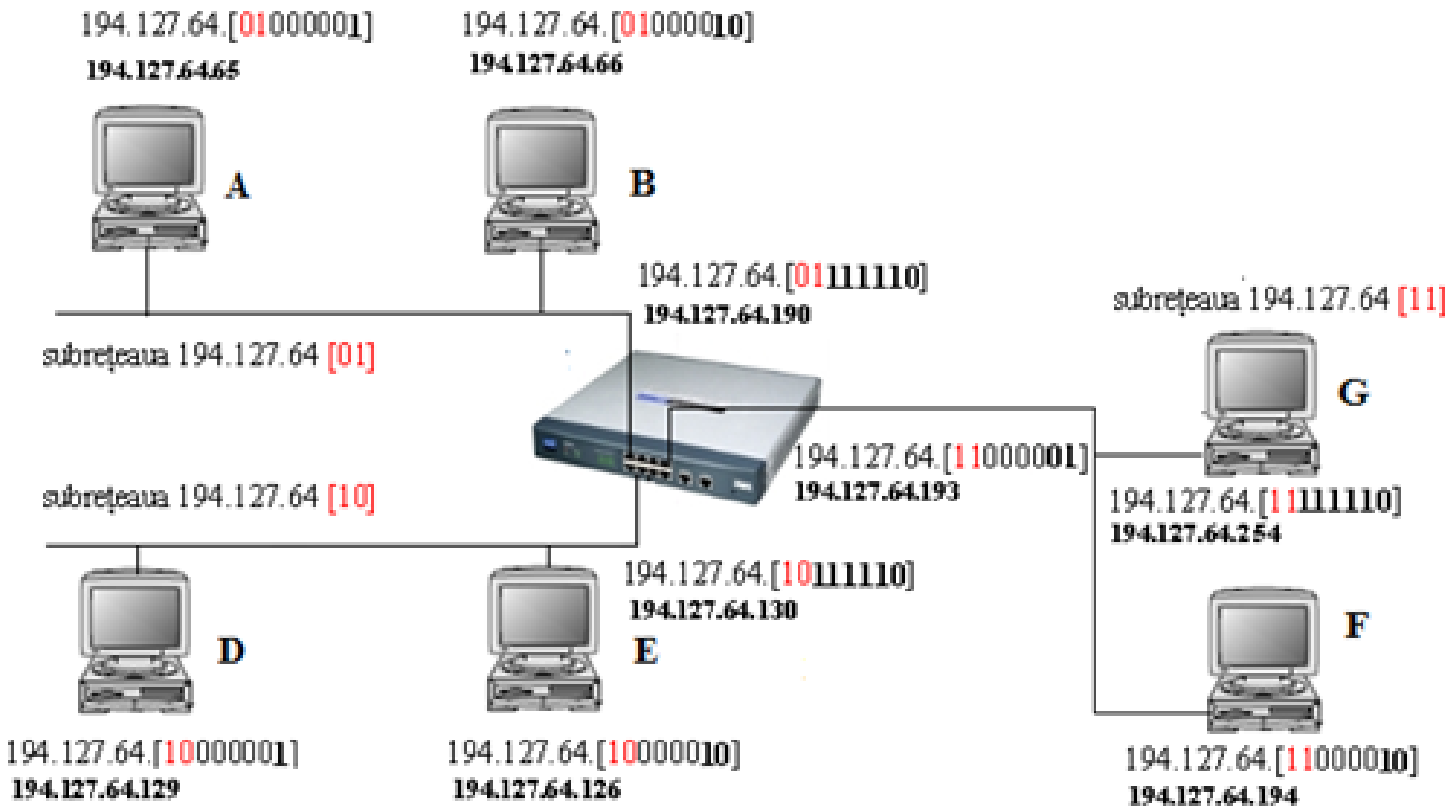
Pentru fiecare subrețea, adresa de broadcast se obține punând pe 1 toți biții corespunzători adresei host-ului:
subnet 10.0.2.0/24 ->10.0.2.255

Net ID Host Net ID

Rezultatul este sintetizat în tabelul alăturat

Subrețea	Adresa de Rețea	Adresa de Broadcast	Interval de Hosturi
Prima	10.0.0.0/24	10.0.0.255	10.0.0.1 - 10.0.0.254
A doua	10.0.1.0/24	10.0.1.255	10.0.1.1 - 10.0.1.254
A treia	10.0.2.0/24	10.0.2.255	10.0.2.1 - 10.0.2.254
...	...	...	...
Ultima	10.255.255.0/24	10.255.255.255	10.255.255.1 - 10.255.255.254

Exemplu de interconectare a 3 subrețele ale rețelei 192.127.64.0/24



Masca de subrețea este, pentru toate subrețelele, 255.255.255.192

Exemplu de interconectare a 4 rețele rezolvat în Packet Tracer

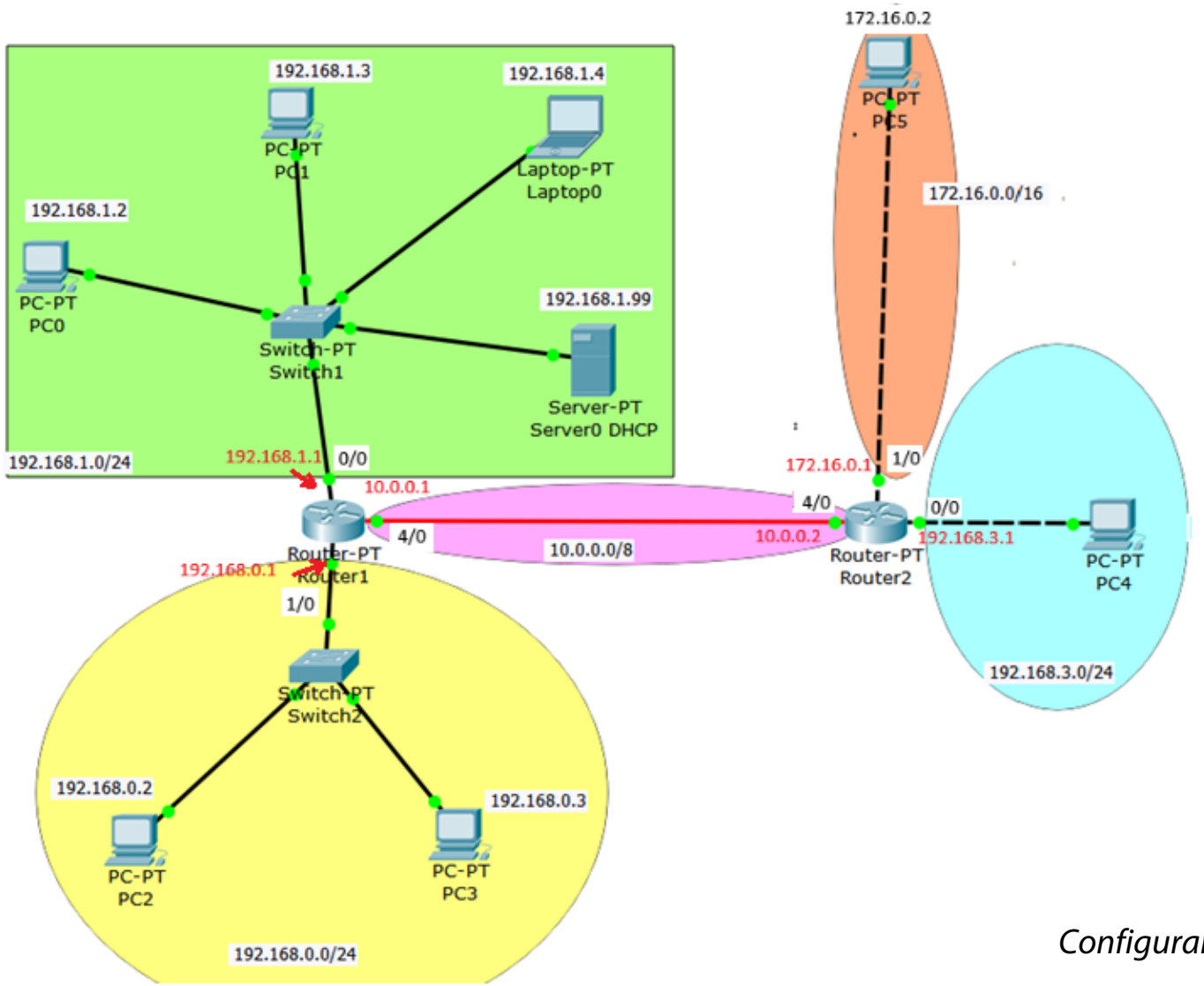
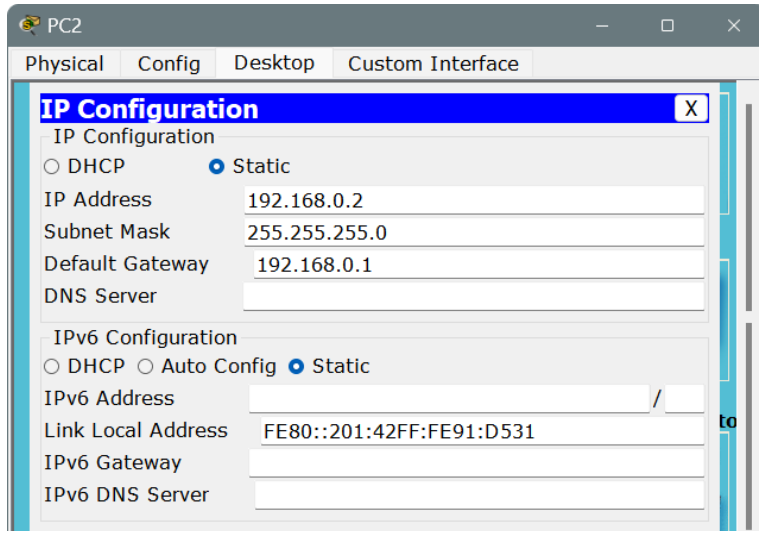


Tabela de rutare pentru Router1

C 10.0.0.0/8 is directly connected, FastEthernet4/0
S 172.16.0.0/16 [1/0] via 10.0.0.2
C 192.168.0.0/24 is directly connected, FastEthernet1/0
C 192.168.1.0/24 is directly connected, FastEthernet0/0
S 192.168.3.0/24 [1/0] via 10.0.0.2

Tabela de rutare pentru Router2

C 10.0.0.0/8 is directly connected, FastEthernet4/0
C 172.16.0.0/16 is directly connected, FastEthernet1/0
S 192.168.0.0/24 [1/0] via 10.0.0.1
S 192.168.1.0/24 [1/0] via 10.0.0.1
C 192.168.3.0/24 is directly connected, FastEthernet0/0



Configurarea IP a PC4

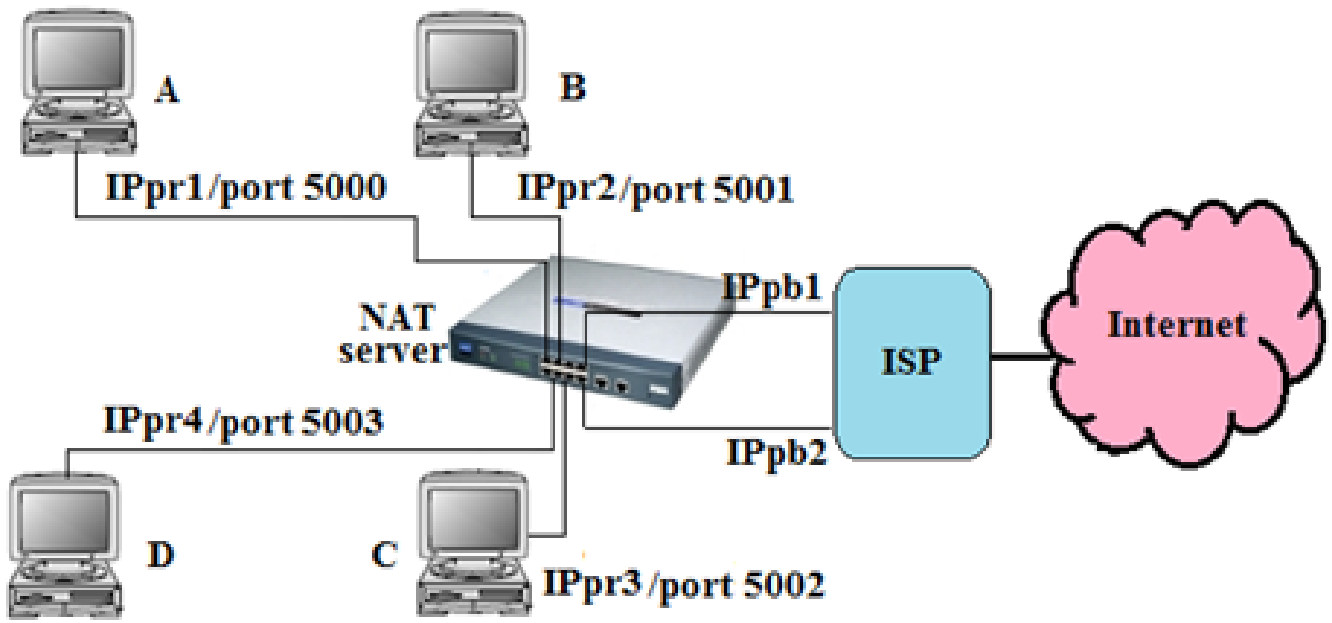
Accesul calculatoarelor cu IP privat la Internet

Adresele private au fost gândite pentru utilizare în rețele care folosesc protocolul TCP/IP dar nu sunt conectate la Internet. Ele nu sunt rutate de către rutere. Pachetele care conțin adrese private sunt distruse.

Pentru a nu fi risipite ele pot fi folosite, totuși, folosind un serviciu de translare a adreselor private în adrese publice, numit **NAT** (Networc Address Translator)

Un server NAT are alocate un număr *n* de adrese IP publice, prin care comunică în Internet, și un număr *m* de adrese private către rețeaua locală. Numărul conexiunilor cu adrese publice este mai mic decât cel al conexiunilor cu adrese private, **n<m**.

Un caz particular îl reprezintă situația în care numărul conexiunilor publice este n=1, adică se utilizează o singură adresă IP publică. Este cazul celor mai multe rețele casnice (HAN) și al firmelor mici, cu câteva zeci de calculatoare.



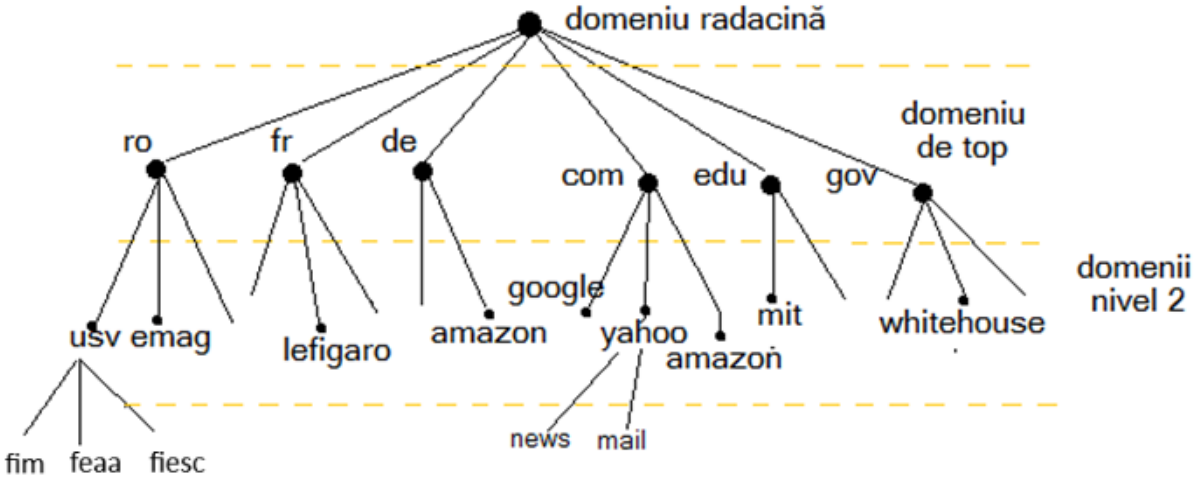
În funcție de numărul de calculatoare din rețeaua privată se determină și banda necesară pe conexiunea publică, care trebuie să fie cu atât mai mare cu cât numărul de calculatoare este mai mare. Pentru o rețea privată cu până la 10 calculatoare, o viteză a conexiunii publice de 100Mb/s este suficientă.

Toate routere-le wireless de uz general includ un server NAT, deoarece ele alocă adrese IP private (de regulă în domeniul 192.168.0.0 - 192.168.255.255), pe care le rutează pe o conexiune IP publică.

Serviciul DNS

Oamenilor le este greu să memoreze adresele IP în forma numerică, în schimb reţin mai uşor numele unor site-uri. Este nevoie de un sistem care să „traducă” numele prietenoase în adrese IP, cu care lucrează calculatoarele.

Acest sistem se numeşte DNS (Domain Name System) şi este organizat într-o structură ierarhică şi distribuită de servere, ca în figură.



Cum funcţionează DNS-ul

Sunt implicate două tipuri de servere DNS: servere ***Resolver*** şi ***autoritative***. Serverele de tip resolver sunt deţinute de ISP la cere utilizatorul este abonat. Serverele autoritative se găsesc la domeniile de top TLD şi au evidenţa tuturor serverelor din domeniul respectiv, cu IP şi numele de domeniu.

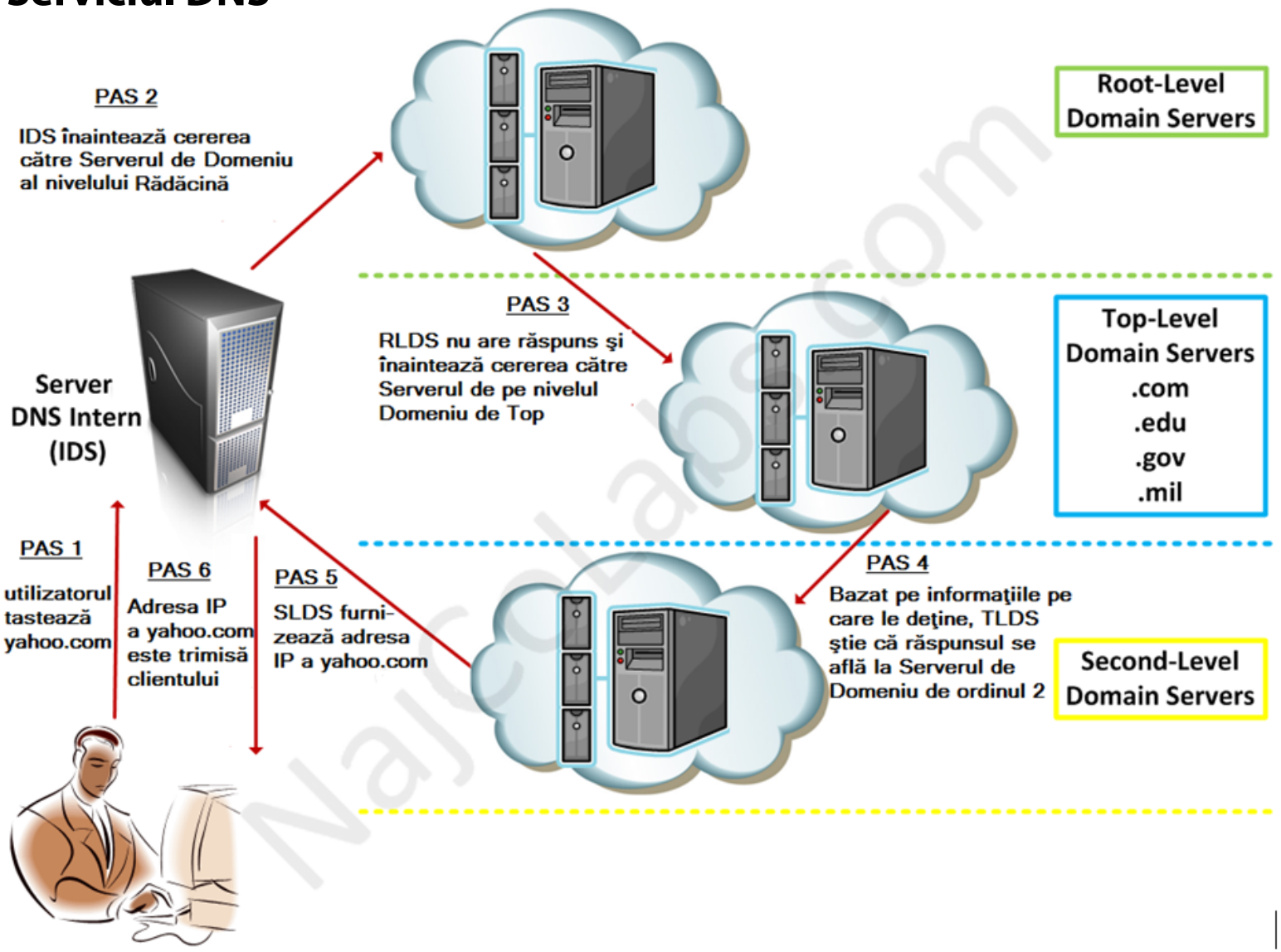
1. Verificarea memoriei cache locale: Browserul utilizatorului verifică mai întâi memoria cache locală pentru a vedea dacă a fost accesat recent domeniul. Dacă găseşte adresa IP corespunzătoare, o foloseşte direct fără a interoga serverele externe.

2. Interogare DNS Resolver: Dacă adresa IP nu se află în memoria cache locală, computerul trimite o solicitare către un DNS Resolver. Resolver-ul este de obicei furnizat de furnizorul de servicii Internet (ISP) sau de setările reţelei.

3. Server DNS rădăcină: Dacă Resolverul nu are răspunsul, trimite solicitarea către un server DNS rădăcină Serverul rădăcină nu cunoaşte adresa IP exactă a domeniului căutat dar ştie ce server de domeniu de nivel superior (TLD) să interogheze pe baza extensiei domeniului (de exemplu, .ro).

4. Server TLD: Serverul TLD al domeniului direcţionează resolver-ul către serverul DNS autoritativ pentru domeniul căurat, ex. usv.ro.

Serviciul DNS



5. Server DNS autoritativ: Acest server deține înregistrările DNS reale usv.ro, inclusiv adresa IP a serverului site-ului web. Trimite această adresă IP înapoi către resolver.

6. Răspuns final: Resolverul DNS trimite adresa IP către computerul utilizatorului, permițându-i să se conecteze la serverul site-ului web și să încarce pagina.

Rezultatele interogărilor sunt meorate în memoria cache a browser-elor și a serverelor Resolver, pentru o perioadă limitată de timp (Time-to-Live). Aceasta ajută la reducerea numărului de interogări ale serverelor din sistem.

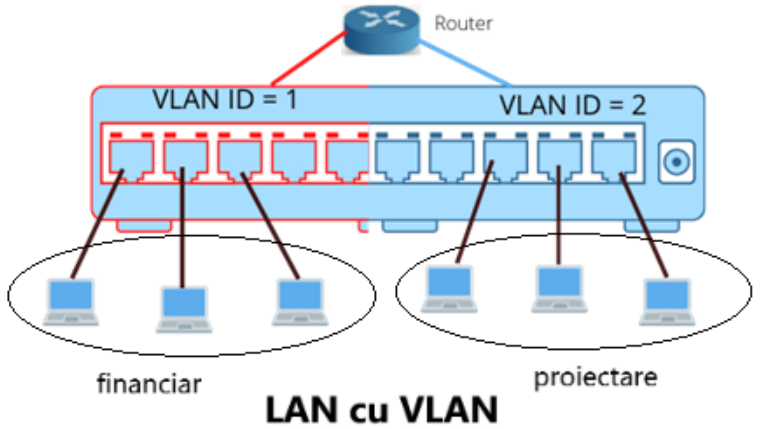
Pe lângă traducerea numelor în adrese IP, DNS mai face și:
Direcționează e-mailurile către serverul de mail corect folosind înregistrări MX .
Autentifică expeditorii pentru a securiza livrarea e-mailurilor.

Rețele LAN virtuale - VLAN și Rețele virtuale private - VPN

VLAN

O VLAN (rețea locală virtuală) este o rețea logică ce grupează dispozitivele în domenii de broadcast separate, în cadi singure rețele fizice.

Permit administratorilor de rețea să segmenteze o rețea în unități mai mici, independente, prin organizarea dispozitivelor în grupuri pe baza funcției sau departamentului, mai degrabă decât a locației fizice. Acest lucru îmbunătățește securitatea rețelei prin izolarea traficului, crește performanța prin reducerea traficului de difuzare și crește flexibilitatea prin simplificarea gestionării și modificărilor rețelei.



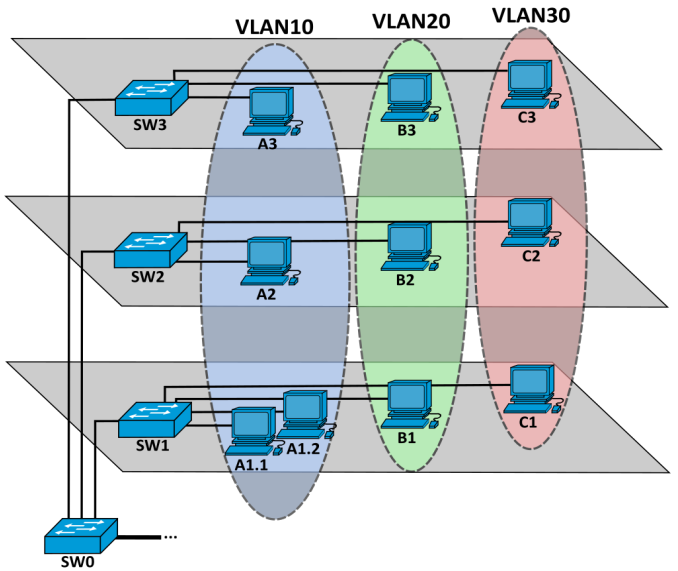
LAN cu VLAN

Cum funcționează

Segmentare logică : În loc să creeze rețele fizice separate, VLAN-urile utilizează software pentru a împărți logic o rețea fizică în mai multe rețele virtuale.
Domenii de difuzare: Fiecare VLAN acționează ca propriul domeniu de difuzare, ceea ce înseamnă că traficul de difuzare este limitat la acel VLAN specific și nu este trimis către alte VLAN-uri.
Etichetare : Etichetarea VLAN IEEE 802.1Q este utilizată pentru a identifica VLAN-ul căruia îi aparține un cadru de date pe măsură ce acesta se deplasează prin comutatoarele de rețea.

Comunicare inter-VLAN: Dispozitivele din VLAN-uri diferite nu pot comunica direct; traficul trebuie să treacă printr-un router sau un switch de nivel 3, similar comunicării dintre două rețele separate fizic.

Segmentarea rețelei în VLAN se realizează la nivel de switch, care trebuie să fie cu management. Fiecare cadru Ethernet conține o etichetă de patru octeți care specifică cărui VLAN aparține .



Rețele LAN virtuale - VLAN și Rețele virtuale private - VPN

VPN

Stabilește o conexiune digitală între un computer și un server aflat la distanță, deținut de un furnizor VPN, creând un tunel punct-la-punct care criptează datele personale, maschează adresa IP și permite ocolirea blocajelor site-urilor web și firewall-urile de pe Internet.
Acest lucru asigură că experiențele online ale utilizatorului sunt private, protejate și mai sigure.

Există două tipuri: **Remote Access VPN** și **Site-to-Site VPN**

Remote Acess VPN

Utilizatorul se conectează la serverul VPN al furnizorului (poate fi al companiei unde lucrează utilizatorul) și introduce credențialele.
Dacă acestea sunt corecte, serverul stabilește o conexiune securizată punct-la-punct între utilizator și server, prin rețeaua Internet.
Conexiunea securizată prin criptare face ca datele schimbate între utilizator și server să nu poată fi accesate de nimeni care ascultă rețeaua, nici măcar de furnizorul de servicii Internet ISP al clientului sau al companiei.

Serverul VPN dă acces utilizatorului aflat la distanță la aceleași resursele informaționale ale companiei ca și când acesta s-ar afla la sediul companiei.
Accesul la alte resurde din Internet se face prin adresa IP a severului VPN, care maschează adresa IP a utilizatorului.