



# ÎNVAȚĂ REȚELELE DE CALCULATOARE

---

GHIDUL TĂU INTRODUCȚIV  
ÎN REȚELISTICĂ



Ramon Nastase

© **Copyright 2018 Ramon Nastase – Toate drepturile rezervate.**

Continutul acestei carti nu poate fi reprodus, duplicat sau transmis fara permisiunea directa scrisa din partea autorului. In nici un caz nu va fi suportata raspunderea juridica sau vina de catre editor pentru orice reparare, dauna sau pierderi financiare datorate informatiilor din aceasta carte, direct sau indirect.

**Aviz juridic**

Aceasta carte este protejată prin drepturi de autor. Acest lucru este numai pentru uz personal. Nu puteți modifica, distribui, vinde, utiliza, cita sau parafraza orice parte sau continutul acestei carti fara consimtamantul autorului.

**Notificare privind renuntarea la raspundere**

Retineti ca informatiile continute in acest document sunt numai pentru scopuri educationale si divertisment. Au fost facute toate incercarile de a furniza informatii exacte, actualizate si fiabile. Nu sunt exprimate sau implicate garantii de niciun fel. Citorii recunosc ca autorul nu se angajeaza în furnizarea de consultanta juridica, financiara, medicala sau profesionala. Continutul acestei carti a fost derivat din diverse surse.

Prin citirea acestui document, cititorul este de acord ca în nici un caz autorul nu este responsabil pentru orice pierderi, directe sau indirecte, care apar ca urmare a utilizarii informatiilor continute in acest document, inclusiv, dar fara a se limita la, omisiuni sau inexactitati.

# Introducere

Felicitari pentru descarcarea acestui ghid. Asta arata ca esti interesat de domeniul IT si mai ales ca iti doresti sa dobandesti abilitati noi, sa cresti si sa te dezvolti profesional si personal.

Din acest ghid te poti astepta sa intelegi:

- cum functioneaza **Internetul**,
- cum **comunica** Dispozitivele (telefon, laptop, server etc) in Internet
- cum functioneaza **retelele** si de cate **tipuri** sunt,
- ce este un **Router**, **Switch**, adresa **IP**, adresa **MAC**, etc.
- si cum le poti **configura** pentru a obtine conectivitate end-to-end.

Aceasta ghid este structurat in 5 capitole care cuprind diferite teme, apartinand bazelor retelisticii. Aceasta carte acopera o parte mica din materia [modulelor 1 si 2 ale cursului CCNA](#). Daca iti doresti o cariera in Retele de Calculatoare, atunci iti recomand sa te axezi pe obtinerea acestei certificari, iar cea mai buna varianta este sa-ti dai certificarea **CCENT** (din materia CCNA 1 & 2).

Daca iti doresti sa inveti si mai multe despre Retele de Calculatoare si sa-ti dezvolti o cariera in directia asta, atunci [iti recomand cursul meu online de Retele](#) care te va duce pas cu pas prin notiunile de **care ai nevoie pentru a-ti lua certificarea CCENT si ulterior sa te angajezi in domeniu**.

Iti urez spor la treaba, iar daca ai intrebari nu ezita sa ma contactezi pe [email](#), [Facebook](#) sau [YouTube](#).

Ramon Nastase (cel care te sustine in procesul tau de crestere).

# Cuprins

<b>Capitolul 1 - Introducere in Retele de Calculatoare</b>	<b>6</b>
1) Dimensiunea unei retele	6
2) Componentele unei retele	6
3) Cum reprezentam o retea prin Topologii Fizice si Logice	9
<b>Capitolul 2 – Switch-uri, Ethernet si adrese MAC</b>	<b>12</b>
Concepte de Baza despre Switch	12
<b>Capitolul 3 – Routere, adrese IPv4 si IPv6</b>	<b>16</b>
Adrese IP Publice si Private	17
Clasele de IP-uri	17
IPv6	18
Concepte de Baza despre Router	21
<b>Capitolul 4 – TCP, UDP, Port-uri si Aplicatii de Retea</b>	<b>23</b>
<b>Capitolul 5 - Cisco IOS &amp; Introducere in CLI</b>	<b>26</b>
Introducere in CLI - Configurari de Baza	26
a) Nivele de Acces	26
b) Setarea numelui unui dispozitiv (Hostname)	28
c) Securizarea accesului pe Router	28
d) Setarea unei adrese IP pe Router	30
f) Configurare access remote pe Router (Telnet, SSH)	31
<b>Laborator Practic #1</b>	<b>34</b>
<b>Capitolul 6 - Serviciul de Retea DHCP</b>	<b>35</b>
DHCP	35
Cum functioneaza DHCP ?	36
Configurare DHCP pe Router	36
Configurare adresa IP dinamica (prin DHCP) pe Windows	38
<b>Laborator Practic #2</b>	<b>42</b>

# Capitolul 1 - Introducere in Retele de Calculatoare.

## Notiuni si Principii de Baza

O **retea** reprezinta un **ansamblu de dispozitive** (PC-uri, Routere, Switch-uri etc.) interconectate, care pot comunica (schimba informatii) intre ele.

### 1) Dimensiunea unei retele

Retelele pot fi de mai multe tipuri:

- **LAN** – Local Area Network – ex: retea ta (prin cablu) de acasa
- **MAN** – Metropolitan Area Network – ex: retea extinsa, pe suprafata unui oras
- **WAN** – Wide Area Network – ex: Internetul
- **WLAN** – Wireless LAN – retea ta, wireless, de acasa
- etc.

[Poti urmarii acest video pentru a vedea lucrurile si din alt punct de vedere.](#)

### 2) Componentele unei retele

O retea este alcatuita din:

- **End-device** (PC, Laptop, Smartphone, Servere etc.)
- **Switch** - interconecteaza mai multe end-device-uri intr-o retea
- **Router** - interconecteaza mai multe retele
- **Firewall** - ne protejeaza retea de posibile atacuri din Internet
- **Mediu de transmisie** – cablu (cupru), lumina (fibra optica), wireless (aer)

Acum, propun sa discutam despre cateva elemente de retea (din cele enumerate mai sus). Primele componente ale unei retele vor fi chiar end-device-urile:

## I. END-DEVICE

In general noi suntem cei care avem in componenta un dispozitiv terminal (end-device). Fiecare dintre noi avem un Laptop, PC sau smartphone cu care ne conectam la Internet. Aceasta conexiune poate fi facuta prin 1 sau mai multe medii de transmisie (curent, lumina, aer).

In momentul in care ne conectam cu smartphone-ul la Internet, cel mai probabil vom folosi **mediul wireless**. Daca folosim un **Laptop**, il putem conecta fie prin **wireless** fie prin **cablu** de retea (UTP).



Figura 1.1

Conexiunea prin fibra optica are loc atunci cand dorim sa conectam mai multe echipamente de retea sau servere intre ele (ex: switch – switch, server – switch). Motivul este simplu: o legatura prin Fibra Optica poate fi mult mai rapida fata de cea prin cablu UTP sau prin Wireless.

## II. SWITCH

Switch-ul este un echipament de retea care interconecteaza mai multe PC-uri (si nu numai: imprimante, telefoane IP, AP-uri, etc) la ACEEASI retea locala (LAN).

El este caracterizat de un numar mare de port-uri (in general 24 sau 48) toate fiind capabile de viteze intre 100 Mbps si 1 Gbps (sau chiar 10Gbps). Switch-ul foloseste adresele MAC. (vom vorbi mai in detaliu in Capitolul 2).

Iata o imagine cu un **Switch** profesional Cisco:



Figura 1.2

### III. ROUTER

Un Router este un echipament de retea care are rolul de a interconecta mai multe retele (LAN) intr-o retea mai mare (WAN -Wide Area Network). Router-ul este dispozitivul care ne conecteaza la Internet. El se ocupa de trimiterea pachetelor, catre retea destinatie din Internet.

In comparatie cu Switch-ul, Router-ul are mult mai putine port-uri (intre 2 – 5 ) la viteze asemanatoarea ( 100 Mbps – 10Gbps, depinde de model).

Dupa cum spuneam scopul acestui echipament este sa interconecteze retelele. Toate aceste retele au nevoie de un mod de identificare si astfel Routerule folosesc adresele IP (despre care vom vorbi in Capitolul 3).

Acesta este un **Router** profesional Cisco:



Figura 1.3

[Da click AICI pentru a vedea aceste echipamente in actiune !](#)

### 3) Cum reprezentam o retea prin Topologii Fizice si Logice

Reteaua o putem **reprezenta** printr-o **topologie**. Aceasta poate fi de 2 feluri: fizica sau logica. Topologia fizica descrie echipamentele si modul in care sunt acestea conectate, cablurile folosite.

Alt exemplu avand in componenta 2 Routere, 1 PC si 1 Server. Unul dintre Routere este conectat la Internet – **Exemplu #1 Topologie Logica**

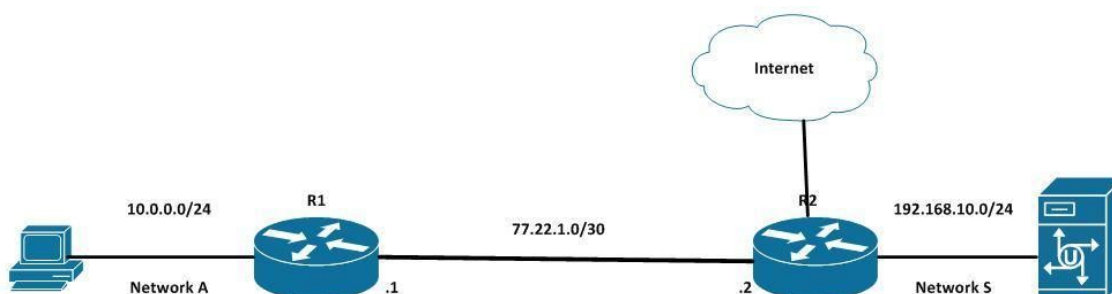


Figura 1.4

Aceasta retea contine 1 Switch, 3 Routere, 2 PC-uri si 1 Server – **Exemplu #2 Topologie Logica**

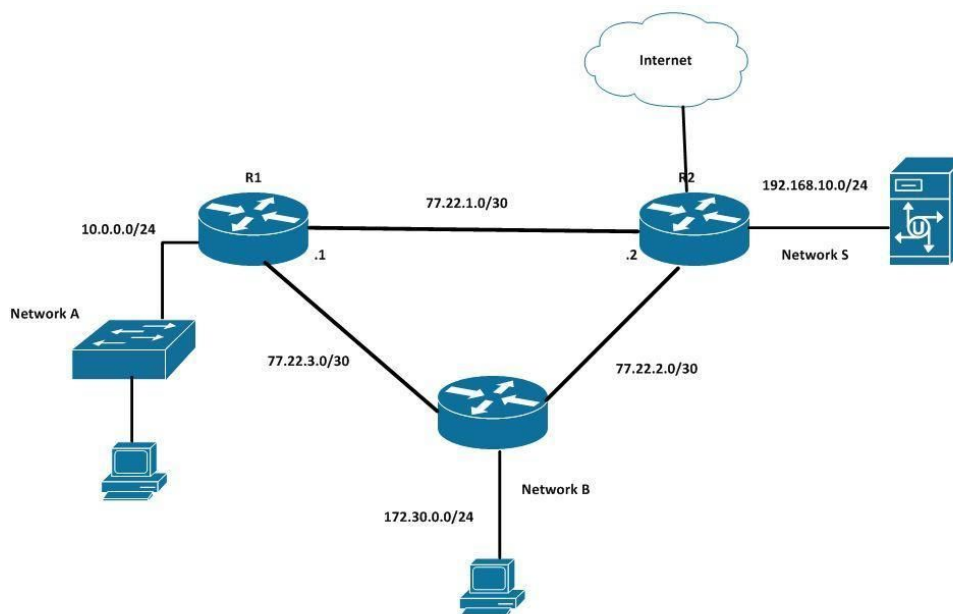


Figura 1.5



In exemplul celor de la Cisco, din figura de mai jos, putem vedea o reprezentare fizica (**Topologie Fizica**) a unei retele.

Ea defapt ne arata unde vor fi amplasate echipamentele si ce scop vor avea ele (conectarea la retea a PC-urilor unui departament, conectarea serverelor din Data Center la retea, conectarea punctelor de acces wireless la retea etc.)

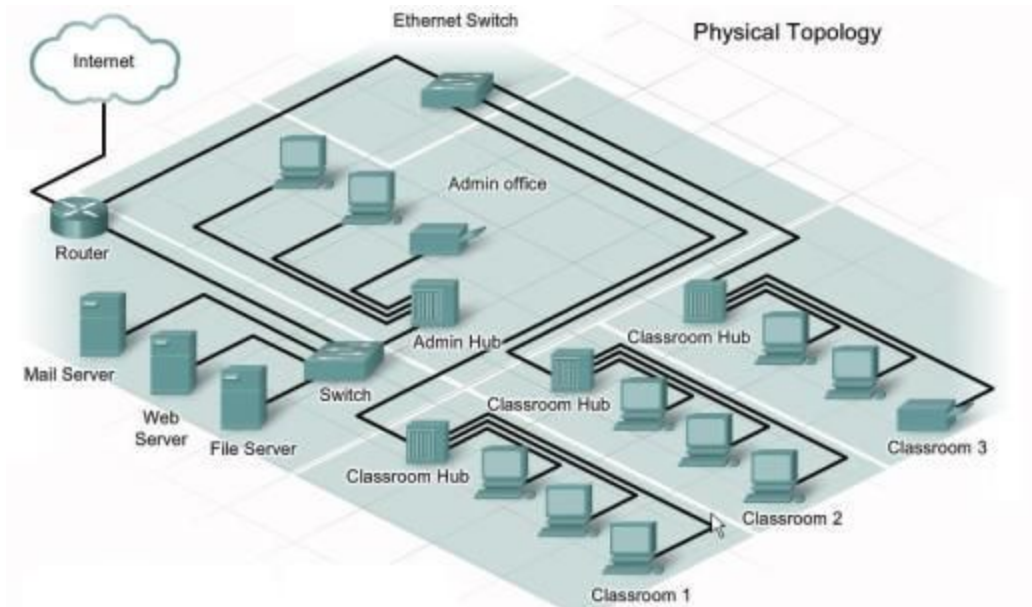


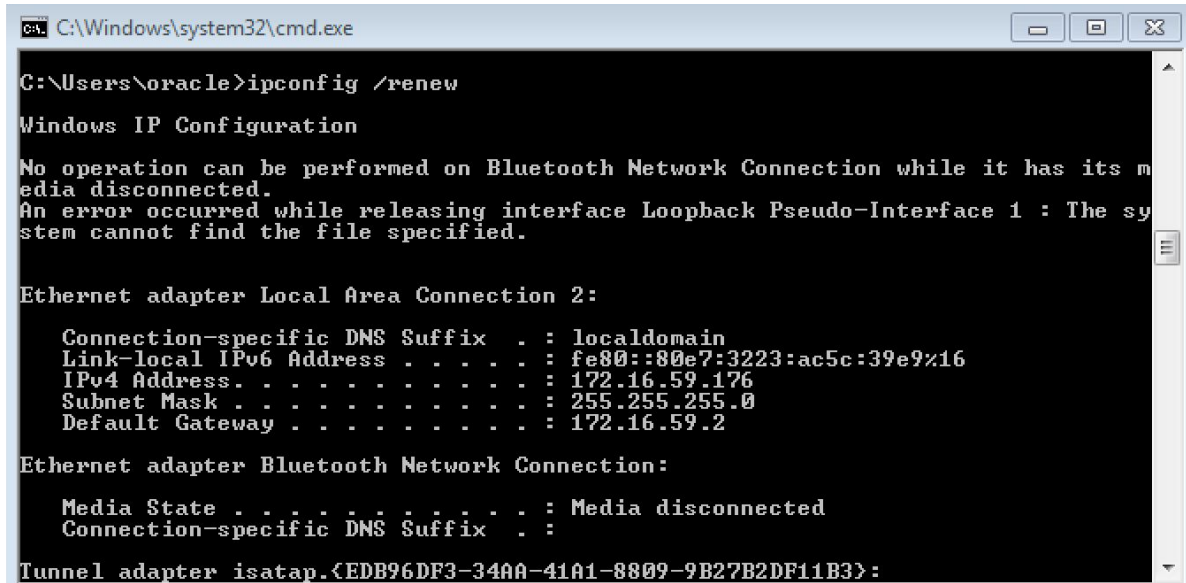
Figura 1.6

#### 4) Cum comunica calculatoarele in retea ?

Pentru a putea comunica, dispozitivele (PC-uri, routere, switch-uri, etc) trebuie sa aiba un identificator unic. In acest caz este vorba de **IP (Internet Protocol)**.

IP-ul este modul prin care identificam un dispozitiv intr-o retea. El trebuie sa fie unic. Nu pot exista 2 IP-uri la fel in aceeasi retea, deoarece va aparea un conflict la nivelul acesteia.

Hai sa ne gandim la IP ca la un CNP pentru device-uri. Ce rol are CNP-ul ? De a identifica in, mod unic, fiecare persoana din Romania. Statul ne identifica prin CNP (aka IP), iar oamenii ne identifica prin Nume sau Prenume (aka. adresa MAC).



```
C:\Windows\system32\cmd.exe

C:\Users\oracle>ipconfig /renew

Windows IP Configuration

No operation can be performed on Bluetooth Network Connection while it has its media disconnected.
An error occurred while releasing interface Loopback Pseudo-Interface 1 : The system cannot find the file specified.

Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::80e7:3223:ac5c:39e9%16
    IPv4 Address. . . . . : 172.16.59.176
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.16.59.2

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Tunnel adapter isatap.<EDB96DF3-34AA-41A1-8809-9B27B2DF11B3>:
```

Figura 1.7

Exemplu de mai sus este luat din linia de comanda din Windows (**cmd**).

Aceste este alt exemplu de IP:

**10.0.0.1/24**, unde /24 reprezinta masca de retea,

Masca de retea (Subnet Mask) determina dimensiunea retelei ( adica cate dispozitive se pot afla in aceeasi retea la un moment dat – 14 - (/28), 126 - (/25), 254 - (/24), 510 - (/23) etc).

Elementele necesare unui end-device pentru a comunica cu succes in Internet:

**IP-ul** = identifica, in mod unic, un dispozitiv conectat intr-o retea

**Masca de Retea** = determina dimensiunea retelei (ca numar de IP-uri disponibile)

**Default Gateway** = calea de iesire din retea (de obicei spre Internet printr-un Router)

**Server DNS** = "transforma" un nume (precum google.ro) intr-un IP (ex: 173.23.85.91)

## Capitolul 2 – Switch-uri, Ethernet si adrese MAC

### Concepte de Baza despre Switch

Switch-ul este un echipament de retea care functioneaza la **nivelul 2 al modelului OSI**. Scopul acestuia este de a conecta mai multe device-uri (PC-uri, Laptop-uri, Servere, Imprimante, etc.) in aceeasi retea locala (LAN). Acest echipament contine mai multe **port-uri (24 sau 48, depinde de model)** care ii permit sa faca legatura in retea.



Figura 2.1

Switch-ul trimite datele de la un dispozitiv la celalalt pe **baza adreselor MAC** (sursa si destinatie). O **adresa MAC** reprezinta un mod de identificare unic, al fiecarui device dintr-o retea. Acesta este scrisa, din fabrica, pe placa de retea a fiecarui PC, smartphone, laptop, tableta si are urmatoarea forma:

```
C:\Windows\system32\cmd.exe
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : localdomain

Ethernet adapter Local Area Connection 2:

Connection-specific DNS Suffix . : localdomain
Description . . . . . : Intel(R) PRO/1000 MT Network Connection #
2
Physical Address. . . . . : 00-50-56-2B-12-94
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::80e7:3223:ac5c:39e9%16(Preferred)
IPv4 Address. . . . . : 172.16.59.176(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Monday, August 14, 2017 12:11:21 PM
Lease Expires . . . . . : Monday, August 14, 2017 12:47:34 PM
Default Gateway . . . . . : 172.16.59.2
DHCP Server . . . . . : 172.16.59.254
DHCPv6 IAID . . . . . : 352324649
DHCPv6 Client DUID. . . . . : 00-01-00-01-1D-C2-0B-B2-00-0C-29-98-5C-60
DNS Servers . . . . . : 172.16.59.2
```

Figura 2.2

Este reprezentata in format hexadecimal, pe **48 de biti** (12 caractere, 4 biti fiecare caracter). **Primii 24 de biti** (00-1B-63) reprezinta partea specifica vendor-ului (ex: Cisco, Apple, Intel etc.), iar urmatorii 24 de biti (84-45-E6) reprezinta partea specifica device-ului, care il identifica in mod unic in retea.

Switch-ul retine in memorie o **tabela CAM** (Content-Addressable Memory) care descrie ce **adresa MAC** (sursa) se afla pe un **port** (altfel spus, face o mapare/asociere adresa MAC sursa - port) - **exemplu**: Adresa MAC X se afla pe portul Fa0/5, Adresa MAC G se afla pe portul Fa0/9.

[Pentru a afla mai multe despre modul in care functioneaza un Switch, urmareste ACEST clip.](#)

## Ce este Ethernet ?

De aceasta tehnologie sunt absolut sigur ca ai mai auzit pentru ca: 1) am amintit putin mai devreme de ea si 2) pentru ca Routerul tau de acasa foloseste o astfel de tehnologie (la fel si PC-ul / Laptop-ul - interfata de retea).

**Ethernet** este cea mai raspandita tehnologie (pe echipamente de retea) din ziua de astazi datorita acestor 2 lucruri:

- **viteza crescute** (10/40/100 Gbps)
- **forma de adresare** (adresele **MAC**)

Fiecare port al Switch-urilor sau al Router-elor este construit pe tehnologia Ethernet si este notat diferit, in functie de viteza :

- **FastEthernet** - 100Mbps ( aka. Fa0/1 ... Fa0/24 )
- **GigabitEthernet** - 1000Mbps ( aka Gi0/1 ... Gi0/24 )

Astfel pe masura ce device-urile trimit trafic in retea, Switch-ul va invata adresele (MAC) lor sursa si le va asocia cu porturile de pe care provin (portul la care e conectat device-ul - ex: Fa0/1, Fa0/10 sau Gi0/4 etc.) Iata in figura 2.3 poti vedea cum arata headerul Ethernet:

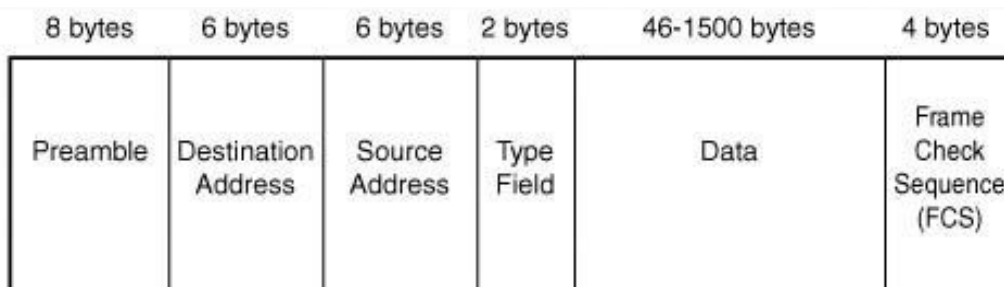


Figura 2.3

Structura headerului este in felul urmatoar:

**1. Preamble**

- sir de biti care indica inceputul unui nou frame (“pachet”)

**2. Destination Address**

- adresa MAC destinatie

**3. Source Address**

- adresa MAC sursa

**4. Type Field**

- Indica versiunea de Ethernet folosita si lungimea frameului

**5. Data**

- reprezinta datele efective transmise (impreuna cu headerele nivelelor superioare)

**6. FCS**

- mecanism de stabilire a integritatii pachetelor

**7. EoF (End of Frame bits)**

- desi nu apare in imaginea de mai sus, exista un sir de biti speciali care indica terminarea frameului

Acum, hai sa vedem cum arata headerul Ethernet intr-un scenariu real din Wireshark (figura 2.4):

No.	Time	Source	Destination	Protocol	Length	Info
114	4...	64.233.166.125	10.0.1.43	TCP	68	5222 → 63140 [ACK] Seq=1 Ack=35 Win=251 Len=0 TSval=229438:
115	4...	10.0.1.43	64.233.166.125	TCP	67	[TCP segment of a reassembled PDU]
116	4...	104.16.16.194	10.0.1.43	TCP	56	[TCP ACKed unseen segment] 443 → 52983 [ACK] Seq=1 Ack=2 W
117	4...	fe80::a495:19b6:d9...	ff02::1:3	LLMNR	86	Standard query 0xcd9d A isatap
118	4...	10.0.1.25	224.0.0.252	LLMNR	66	Standard query 0xcd9d A isatap
119	4...	64.233.166.125	10.0.1.43	TCP	68	5222 → 63140 [ACK] Seq=1 Ack=36 Win=251 Len=0 TSval=229438:
120	4...	10.0.1.43	64.233.166.125	TCP	67	[TCP segment of a reassembled PDU]
121	4...	64.233.166.125	10.0.1.43	TCP	68	5222 → 63140 [ACK] Seq=1 Ack=37 Win=251 Len=0 TSval=229438:
122	4...	10.0.1.43	64.233.166.125	TCP	67	[TCP segment of a reassembled PDU]
123	4...	163.53.33.61	10.0.1.43	UDP	62	62348 → 26085 Len=20
124	4...	fe80::a495:19b6:d9...	ff02::1:3	LLMNR	86	Standard query 0xcd9d A isatap
125	4...	10.0.1.25	224.0.0.252	LLMNR	66	Standard query 0xcd9d A isatap
126	4...	64.233.166.125	10.0.1.43	TCP	68	5222 → 63140 [ACK] Seq=1 Ack=38 Win=251 Len=0 TSval=229438:
127	4...	10.0.1.43	64.233.166.125	TCP	67	[TCP segment of a reassembled PDU]
128	4...	10.0.1.43	54.228.222.202	TCP	66	53003 → 443 [FIN, ACK] Seq=1 Ack=1 Win=4096 Len=0 TSval=13:
129	5...	64.233.166.125	10.0.1.43	TCP	68	5222 → 63140 [ACK] Seq=1 Ack=39 Win=251 Len=0 TSval=229438:
130	5...	10.0.1.43	64.233.166.125	TCP	67	[TCP segment of a reassembled PDU]
131	5...	10.0.1.43	23.64.232.189	TCP	54	52987 → 443 [ACK] Seq=1 Ack=1 Win=4100 Len=0

▶ Frame 127: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0  
 ▶ Ethernet II, Src: Apple\_c8:c0:01 (ac:bc:32:c8:c0:01), Dst: Routerbo\_06:39:4f (e4:8d:8c:06:39:4f)  
   ▶ Destination: Routerbo\_06:39:4f (e4:8d:8c:06:39:4f)  
   ▶ Source: Apple\_c8:c0:01 (ac:bc:32:c8:c0:01)  
     Type: IPv4 (0x0800)  
 ▶ Internet Protocol Version 4, Src: 10.0.1.43, Dst: 64.233.166.125  
 ▶ Transmission Control Protocol, Src Port: 63140 (63140), Dst Port: 5222 (5222), Seq: 38, Ack: 1, Len: 1

Figura 2.4

Dupa cum poti vedea in figura 2.4, un flux de date de tip TCP intre 2 device-uri care contine pe langa porturi, adrese IP (lucruri despre care vom discuta in capitolele urmatoare), mai contine si un camp (layer/nivel) special **Ethernet II**, unde poti identifica cu usurinta cele **2 adrese MAC** (*destinatie si sursa*).

Acum ca am vorbit despre ce inseamna standardul Ethernet si de ce este folosit propun sa discutam despre Switch-uri si sa vedem cum foloseste el acest standard (mai degraba cum foloseste adresele MAC pentru a facilita comunicarea in aceeasi retea - LAN).

## Capitolul 3 – Routere, adrese IPv4 si IPv6

**Protocolul IPv4** a fost dezvoltat in anii '80 si s-a propus folosirea a 32 de biti pentru definirea unei adrese (ex: 192.168.1.1). In fiecare camp din aceste 4 pot fi alocati 8 biti:

8 biti \* 4 campuri = 32 biti.

Acum, hai sa ne gandim putin la acest numar de biti, 32. Acesta ne poate spune ceva legat de numarul maxim de adrese IP care pot fi generate:  $2^{32} \approx 4.2$  Miliarde ! Da, ai citit bine, 4.2 miliarde de adrese IPv4... si **s-au terminat**.

**TIP:** de ce  $2^{32}$  ? deoarece fiecare bit poate lua valoare 0 sau 1, asadar daca avem 32 de biti vom putea genera aproximativ 4.2 miliarde de numere unice.

In anul 2011, mai exact in vara aceluia an, **IANA** (Internet Assigned Numbers Authority) a alocat ultimul spatiu de adrese IPv4. Asta inseamna ca nu mai putem conecta alte dispozitive la internet ? Nicidecum, de atunci si pana acum (2016) internetul a crescut foarte mult ca numar de dispozitive conectate. Iata urmatorul grafic:

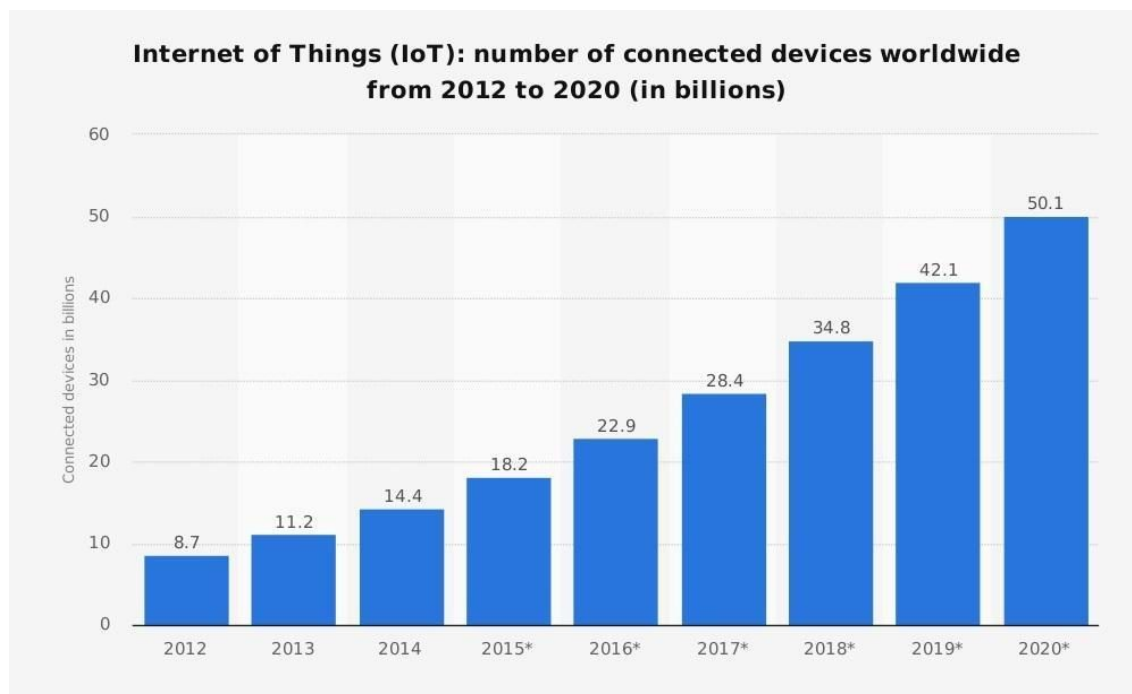


Figura 3.1



Dupa cum spuneam si mai devreme, numarul maxim de adrese IPv4 este de aproximativ **~4.2 Miliarde**. In anul 2016 se estimeaza ca numarul total de dispozitive conectate la Internet este in jur de ~30 Miliarde, numar care depaseste cu mult limita adreselor IPv4.

Datorita acestei probleme s-au luat masuri de incetinire a "consumului" de adres IPv4 prin tehnici precum NAT (si totodata introducerea conceptului de IP Public si IP Privat).

O alta masura, mult mai bine fata de NAT, este introducerea protocolului IPv6, despre care vom discuta mai tarziu.

## Adrese IP Publice si Private

IP-urile Publice, dupa cum le spune si numele, sunt folosite pentru a comunica (tranzita) in Internet, iar cele Private sunt folosite in Retelele Locale (LAN), cum ar fi reseaua noastra de acasa.

Astfel, IP-urile Private nu vor ajunge niciodata in Internet, deoarece se foloseste un procedeu numit NAT (Network Address Translation) care "transforma" IP-urile Private in IP-uri Publice.

## Clasele de IP-uri

Dupa cum am spus si la inceputul acestui articol, fiecare camp (4 in total) al unei adrese IP poate avea orice valoarea intre 0 - 255 (8 biti/camp, deci in total 256 de valori;  $2^8 = 256$ ). Astfel, adresele IP se imparte in mai multe clase:

- A** 0.0.0.0 - 127.255.255.255
- B** 128.0.0.0 - 191.255.255.255
- C** 192.0.0.0 - 223.255.255.255
- D** 224.0.0.0 - 239.255.255.255
- E** 240.0.0.0 - 255.255.255.255

**Clasele A, B, C** sunt **cele folosite** in Internet, clasa D fiind rezervata pentru Adresele de tip Multicast, iar clasa E este o clasa experimentală si nu este folosita.

## Adrese IP Private

Dintre aceste clase se disting urmatoarele **IP-uri PRIVATE**:



- A 10.0.0.0 - 10.255.255.255
- B 172.16.0.0 - 172.31.255.255
- C 192.168.0.0 - 192.168.255.255

**NOTE: Restul adreselor IP sunt PUBLICE !**

**Scopul adreselor Private este de a ramane Private** (ele nu pot ajunge in Internet; sunt valabile doar pentru LAN). Iar aici intervine **[NAT \(Network Address Translation\)](#)** un mecanism folosit pentru "translatarea" adreselor Private in Publice (si invers).

Practic NAT (configurat pe Router) ne permite sa accesam Internetul pentru ca Routerul are o adresa IP publica (iar noi, din LAN o vom folosi pe aceasta - tehnica numita **[PAT - Port Address Translation](#)**).

## IPv6

Astfel a aparut nevoia pentru **IPv6**, un nou protocol de adresare care introduce un nou format de adresare (in hexadecimal) si un spatiu mult, mult mai mare de adrese. IPv6 este pe 128 de biti (asta insemnand ca putem avea  $2^{128}$  de adrese disponibile) care reprezinta un spatiu infinit mai mare fata de IPv4 care este pe 32 de biti.

Conform [Wikipedia](#), acest numar arata cam asa:

"340,282,366,920,938,463,463,374,607,431,768,211,456 sau  $3.4 \times 10^{38}$  (340 [trillion](#) trillion trillion)"

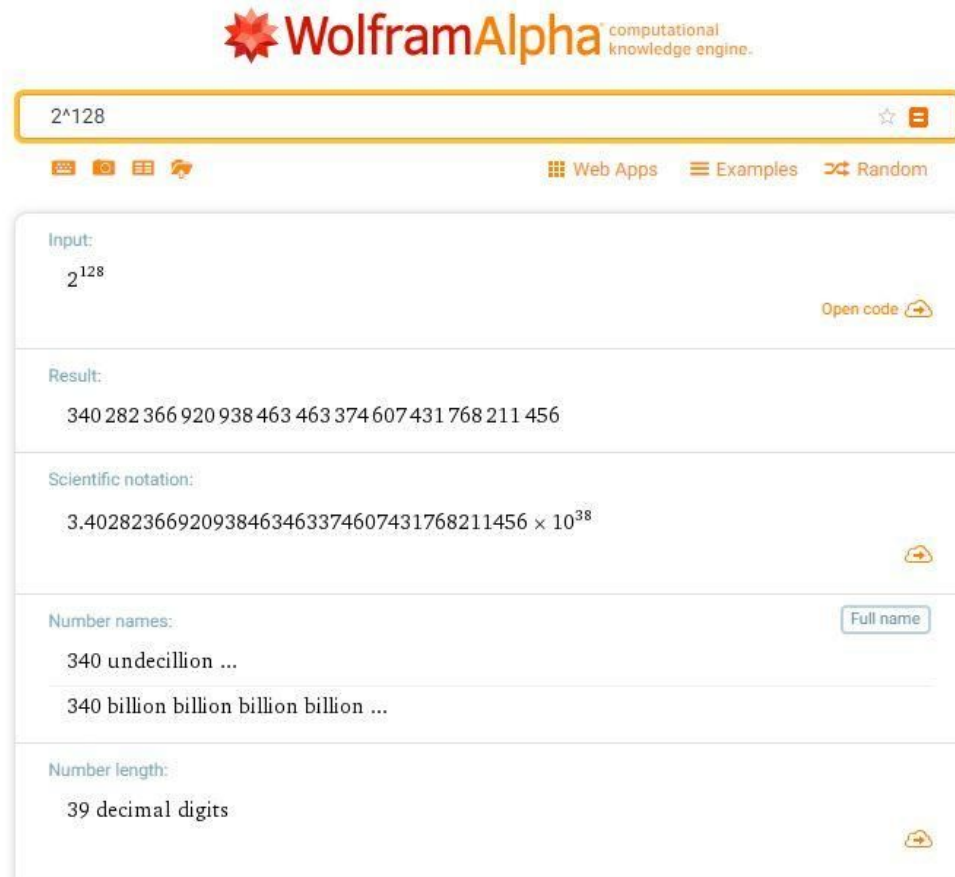


Figura 3.2

lata cateva exemple de adrese IPv6:

- **2001:DB8:85A3:8D45:119:8C2A:370:734B /64**
- **FE80::C001:37FF:FE6C:0/64**
- **2001::1/128**

Dupa cum poti vedea adresele IPv6 sunt in format **hexadecimal** (include pe langa cifre de la **0 – 9** si literele **A – F**). O adresa IPv6 este compusa din maxim **8** campuri si o masca de retea (care indica cat de mare dorim sa fie reseaua – ca numar de adrese).

Notatii: Fiecare camp al adresei IPv6 este separat de ":", dar exista si exceptii:

**2002:ABCD:1234:BBBA:0000:0000:0000:0001/64** poate fi scris in mai multe moduri:

- 2002:ABCD:1234:BBBA:**0:0:0**:1/64
- 2002:ABCD:1234:BBBA::**1**/64

Daca dorim sa reducem un lant intreg de 0-uri il vom simplifica prin "::".

**ATENTIE ! "::"** poate fi folosit **o singura data**.

In figura de mai jos vei putea vedea o adresa IPv6 (prin comanda `>ipconfig`) din CMD care incepe cu notatia **FE80**:... Aceasta adresa IPv6 este una speciala in sensul ca poate fi folosita doar in reseaua locala (LAN) pentru comunicarea cu celelalte dispozitive.

Aceasta adresa se numeste **Link-Local** si este **generata automat** (alt feature important al IPv6 - autoconfigurarea adreselor).

```
C:\Windows\system32\cmd.exe
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List . . . . . : localdomain

Ethernet adapter Local Area Connection 2:

Connection-specific DNS Suffix . : localdomain
Description . . . . . : Intel(R) PRO/1000 MT Network Connection #
2
Physical Address. . . . . : 00-50-56-2B-12-94
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::80e7:3223:ac5c:39e9%16(Preferred)
IPv4 Address. . . . . : 172.16.59.176(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Monday, August 14, 2017 12:11:21 PM
Lease Expires . . . . . : Monday, August 14, 2017 12:47:34 PM
Default Gateway . . . . . : 172.16.59.2
DHCP Server . . . . . : 172.16.59.254
DHCPv6 IAID . . . . . : 352324649
DHCPv6 Client DUID. . . . . : 00-01-00-01-1D-C2-0B-B2-00-0C-29-98-5C-60

DNS Servers . . . . . : 172.16.59.2
```

Figura 3.3

## Concepte de Baza despre Router

Scopul unui Router este **de a interconecta mai multe rețele LAN**, intr-o retea mai mare (adesea numita WAN). Tot ce trebuie sa faca acesta este sa ia urmatoarea decizie pentru fiecare pachet in parte:

"Pe ce interfata trebuie sa trimit acest pachet ? Daca nu stiu unde sa-l trimit il voi arunca (drop)."



Figura 3.4

**ATENȚIE!** By default, **un Router cunoaste** doar rețelele **Direct Conectate**. Acesta nu stie cum sa trimita mai departe de aceste rețele, pachetele. Aici intervenim noi, cei care administram aceste echipamente si configuram rutele pe device.

In momentul in care porneste, un Router, invata mai intai de rețelele direct conectate (cele care incep cu C, in tabelul de mai jos). In figura de mai jos poti vedea **Tabela de Rutare** a unui Router Cisco, care contine rutele/rețelele direct conectate (C) si adresa IP a lui R1 de pe acele interfete (L).

```
R1#
R1#
R1#
R1#sh
R1#show ip ro
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

 10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    10.0.0.0/24 is directly connected, GigabitEthernet2/0
L    10.0.0.1/32 is directly connected, GigabitEthernet2/0
 77.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    77.22.1.0/30 is directly connected, GigabitEthernet1/0
L    77.22.1.1/32 is directly connected, GigabitEthernet1/0
R1#
```

Figura 3.5

Pentru a putea face posibila toate acestea, [Routerul](#) foloseste adresele IP ca mod de referinta (de la cine vine traficul ? - **sursa** - si catre cine trebuie sa trimit acest trafic ? - **destinatia**).

Pentru a putea trimite traficul (pachetele) spre destinatie, Routerule trebuie sa cunoasca, in primul de rand, acele destinatii. Iar aici intervin mai multe moduri prin care un **Router poate invata anumite retele**:

- [Manual](#) - prin Rute Statice
- [Dinamic](#) - prin Protocoale de Rutare ([RIP](#), [OSPF](#), [EIGRP](#))

**[Afla mai multe despre cum functioneaza un Router accesand acest LINK !](#)**

## Capitolul 4 – TCP, UDP, Port-uri si Aplicatii de Retea

### 1) TCP si UDP

In retelistica exista 2 mari protocoale care decid modul de functionare al aplicatiilor de retea, TCP si UDP.

Avem de ales intre aceste 2 moduri pe operare (in functie de nevoile aplicatiei):

- Dorim ca aplicatia de retea sa functioneze fara intarziere (ex: Voce, Video - **VoIP**) si ne asumam pierderea unor pachete - **UDP**
- Suntem interesati ca aplicatia sa ne livreze tot continutul exact asa cum este el pe server (ex: pagina **Web**), asta implicand un mic delay - **TCP**

Aceste protocoale se numesc **TCP** (Transmission Control Protocol) si **UDP** (User Datagram Protocol).

**TCP** este considerat un protocol de incredere care garanteaza retransmiterea pachetelor in cazul pierderii acestora. El stabileste o conexiune intre client si server (numita 3 Way Handshake) folosind mesaje de sincronizare (SYN) si confirmarea (ACK) a primirii pachetelor.

Dezavantajul TCP-ului este schimbul de mesaje (stabilirea unei conexiuni, terminarea ei, transmiterea de pachete SYN, confirmarea lor – ACK) care adauga un delay (timp de asteptare). Aplicatiile de retea precum HTTP (Web), FTP (Transfer de Fisiere), SSH (conexiune remote) folosesc acest protocol.

**UDP** este fix opusul TCP-ului (nu retransmite pachete, nu are un mod de stabilire a conexiunilor, etc.). UDP pur si simplu trimite pachetele de la o anumita sursa catre o destinatie fara sa-l intereseze starea acestora. Avantajul folosirii acestui protocol este reprezentat de latenta scazuta (delay) si permite fluiditatea aplicatiei fara intarzieri.

Asadar **UDP** este un protocol **potrivit pentru aplicatiile real-time** (ex: Voce, Video) care pur si simplu au nevoie sa ajunga la destinatie cat mai repede posibil.

Metrici pentru traficul de Voce (**VoIP**):

- **Delay: < 150 ms** (Deschide CMD si scrie ping 8.8.8.8 pentru a vedea ce delay ai)
- **Pierdere de pachete: < 1%** (1 secunda de voce = 50 pkt de 20 ms audio fiecare => 1% din 50 = 0,5; adica la 2 secunde de audio se poate pierde maxim un pachet)
- **Jitter (delay variabil) - < 30ms**

## 2) Port-uri

Un port identifica in mod unic o aplicatie de retea (server Web, DNS etc.) pe un dispozitiv dintr-o retea. Fiecare port are un identificator – un numar care poate avea o valoare de la **1 – 65535**.

In momentul in care un PC trimite o cerere (pentru o pagina Web) catre un server, aceasta cerere va contine (printre altele) urmatoare informatii:

**IP Sursa:** PC

**IP Destinatie:** Server

**Port Sursa:** 29813 (generat random de catre Browser)

**Port Destinatie:** 80

Altfel spus, toate acestea reprezinta: Browser-ul (29813) PC-ului (sursa) cere pagina web (80) de la server (Destinatia).

## 3) Aplicatii de Retea

Iata cateva protocoale des intalnite ale aplicatiilor de retea:

### HTTP

- **Descriere:** folosit pentru traficul Web (transporta fisierele HTML de la server la client)
- **Port:** 80
- **Protocol de Transport:** TCP

### HTTPS

- **Descriere:** folosit pentru traficul Web intr-un mod **securizat**
- **Port:** 443
- **Protocol de Transport:** TCP

### FTP

- **Descriere:** permite transferul de fisiere intre un client si un server
- **Port:** 20/21
- **Protocol de Transport:** TCP

### DNS

- **Descriere:** gaseste IP-ul unui nume de domeniu (ex: google.ro -> 173.253.81.9)
- **Port:** 53
- **Protocol de Transport:** UDP (client), TCP (server)

### Telnet

- **Descriere:** permite conexiunea **nesecurizata** de la distanta catre un echipament (Switch, Router)
- **Port:** 23
- **Protocol de Transport:** TCP

### SSH

- **Descriere:** permite conexiunea **securizata** de la distanta catre un echipament (Switch, Router)
- **Port:** 22
- **Protocol de Transport:** TCP

### DHCP

- **Descriere:** aloca in mod dinamic adrese IP, masca si default gateway device-urilor din retea
- **Port:** 67/68
- **Protocol de Transport:** UDP



## Capitolul 5 - Cisco IOS & Introducere in CLI

Cand vine vorba de echipamentele Cisco (Routere si Switch-uri) toate au un lucru comun: Sistemul de Operare, **Cisco IOS**. IOS vine de la **I**nternet**o**perating **S**ystem si este “motorul” care ofera puterea acestor echipamente. Noi putem lucra cu IOS in 2 moduri **CLI** sau **GUI**.

Acronimul **CLI** reprezinta **C**ommand **L**ine **I**nterface si este linia de comanda in care vom configura toate aceste dispozitive. Astfel vom avea **acces total** asupra Router-ului sau a Switch-ului si ii vom putea influenta comportamentul in retea.

GUI reprezinta **G**raphical **U**ser **I**nterface si cel mai des il folosim atunci cand configuram echipamente de retea mici precum Routerele Wireless (Wi-Fi) de acasa.

In cele ce urmeaza vom vedea cum putem interactiona cu acest IOS prin **CLI** si vom folosi versiunea **15.2** sau **12.4**.

### Introducere in CLI - Configurari de Baza

In aceasta sectiune vom trece la partea practica si anume vom incepe cu setarile de baza pe Routere Cisco. Pentru inceput iti recomand sa folosesti simulatorul [Cisco Packet Tracer versiunea 6.2 pe care il gaseti AICI](#).

Configuratiile de baza includ urmatoarele:

- Numele dispozitivului (Hostname)
- Parole (criptate sau in clear text)
- Adrese IP pe interfete
- Setare acces remote prin Telnet sau SSH

#### a) Nivele de Acces

In Cisco IOS avem mai multe nivele de acces, in care, utilizatorul poate *face teste de conectivitate* (>) folosind comenzi precum *ping* sau *traceroute*, **vedea** anumite setari (#), poate **schimba setarile** - (config)#.

Pentru a trece dintr-un nivel de acces in altul trebuie sa dam fie comanda **enable**, fie comanda **configure terminal**. In momentul in care te conectezi la un echipament de retea Cisco (Router, Switch, Firewall etc.) te vei afla in **user exec mode (>)**.

In acest mod (**user exec**) esti **limitat din punct de vedere al comenzilor** pe care le poti da pe echipament (in general comenzi precum ping, traceroute, etc.) Pentru a trece in urmatorul nivel de acces (in care ai mai multe privilegii) trebuie sa introduci comanda:

```
Router>enable
```

In urma aceste comenzi te vei afla in nivel **priviledged mode - R1#**. Aici poti sa vezi tot ce se intampla pe echipament (prin comenzi de **show**), dar **NU poti face modificari**.

```
Router>enable
```

```
Router#
```

Pentru a putea face modificari pe echipament trebuie sa treci intr-un nivel de acces cu si mai multe privilegii si anume **global configuration mode**:

```
Router#configure terminal
```

```
Router(config)#
```

Acum poti face **orice modificare** doresti pe aceste echipamente de retea. Acest *global configuration mode* este echivalentul **Administrator**-ului din Windows sau **root**-ului de pe sistemele Linux. Iata toate comenzile cu care este recomandat sa fii familiar:



```
R1 con0 is now available

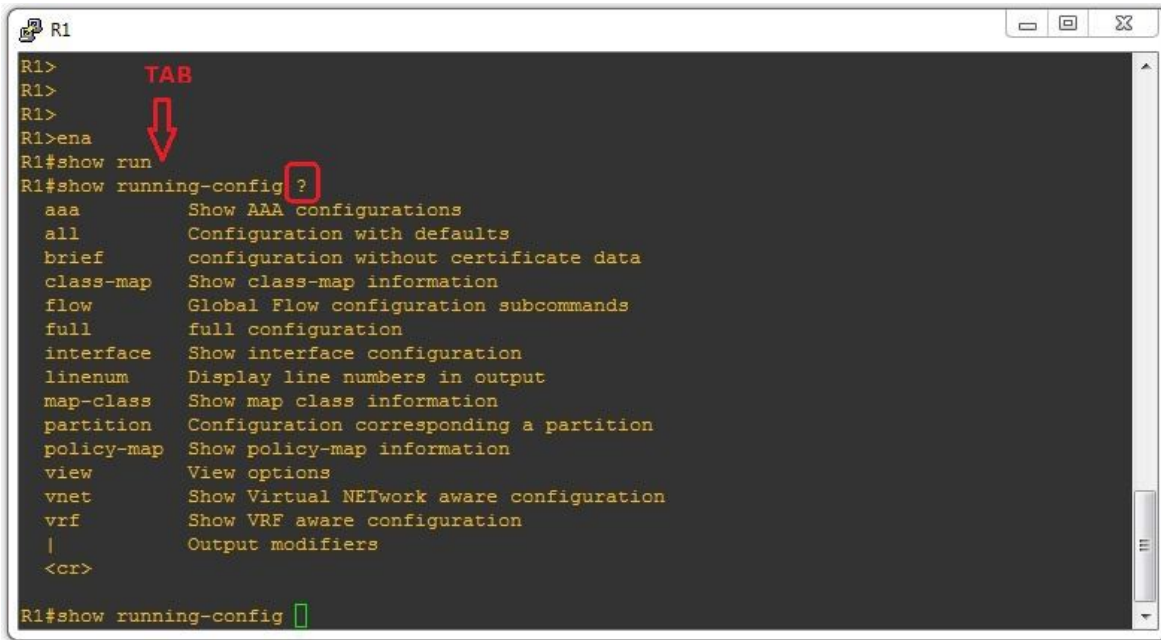
Press RETURN to get started.

R1>
R1>
R1>
R1>enable
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#exit
R1#
*Mar 20 16:59:10.143: %SYS-5-CONFIG_I: Configured from console by console
R1#
```

Figura 8.1

Daca vrem sa scriem o comanda mai lunga (si nu avem chef sa o tastam :D ) avem o solutie care garanteaza scrierea acesteia mai rapida (si corecta).

Daca scriu comanda R1#**show run**, si apas tasta **TAB**, va face **autocomplete** comenzii. De asemenea “?” ne va afisa comenzile (urmatoare) disponibile.



```
R1
R1>
R1>
R1>ena
R1#show run
R1#show running-config ?
aaa          Show AAA configurations
all          Configuration with defaults
brief       configuration without certificate data
class-map   Show class-map information
flow        Global Flow configuration subcommands
full        full configuration
interface   Show interface configuration
linenum     Display line numbers in output
map-class   Show map class information
partition   Configuration corresponding a partition
policy-map  Show policy-map information
view        View options
vnet        Show Virtual NETWORK aware configuration
vrf         Show VRF aware configuration
|           Output modifiers
<cr>
R1#show running-config
```

Figura 8.2

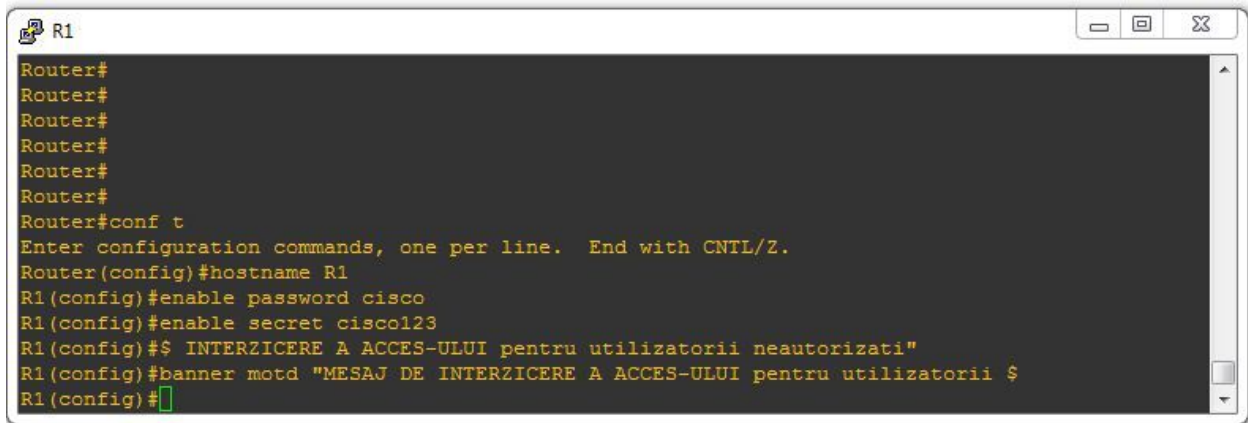
## b) Setarea numelui unui dispozitiv (Hostname)

In exemplul de mai sus, pentru a schimba numele Router-ului (sau al Switch-ului) trebuie sa introducem urmatoarea comanda:

```
Router(config)#hostname NUME_ROUTER
NUME_ROUTER(config)#
```

## c) Securizarea accesului pe Router

Acum sa vedem cum putem securiza accesul pe Router prin setarea unei parole. Setarea unei **parola** la nivelul **priviledged mode (#)**:



```
R1
Router#
Router#
Router#
Router#
Router#
Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#enable password cisco
R1(config)#enable secret cisco123
R1(config)# $ INTERZICERE A ACCES-ULUI pentru utilizatorii neautorizati"
R1(config)#banner motd "MESAJ DE INTERZICERE A ACCES-ULUI pentru utilizatorii $
R1(config)#
```

Figura 8.3

```
Router(config)#hostname R1
```

```
R1(config)#enable password cisco
```

*sau*

```
R1(config)#enable secret cisco
```

Setarea unui **banner** de atentionare la *logarea* pe echipament:

```
R1(config)#banner motd "MESAJ DE INTERZICERE A ACCES-ULUI pentru utilizatorii
neautorizati"
```

Poate te intrebi care este diferenta intre *enable password* si *enable secret* ? Ei bine, iata diferenta (figura 8.4):

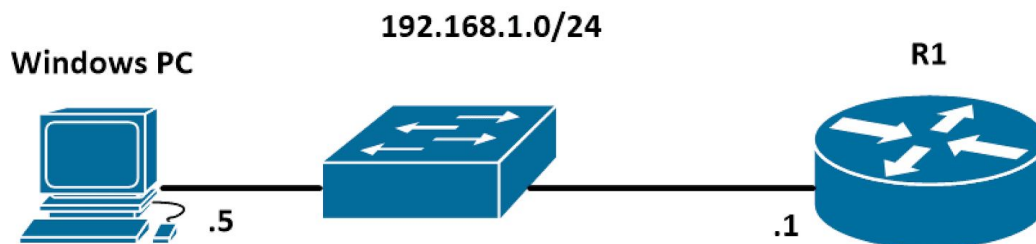
```
R1
R1(config)#do sh run
Building configuration...

Current configuration : 1579 bytes
!
! Last configuration change at 13:48:44 UTC Mon Jul 24 2017
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname R1
!
boot-start-marker
boot-end-marker
!
enable secret 4 1wLgDhbOLsU0GdsP0B9e5YU2KA7gxZujqOLWf0j48q6
enable password cisco
!
no aaa new-model
!
```

Figura 8.4

Dupa cum poti vedea una este stocata intr-un **mod criptat** (*#enable secret*), iar cealalta este stocata in **clear text** (*#enable password*).

Haide sa aruncam o privire la topologia de mai jos si sa incepem sa configuram Routerul pentru accesul la retea:



#### d) Setarea unei adrese IP pe Router

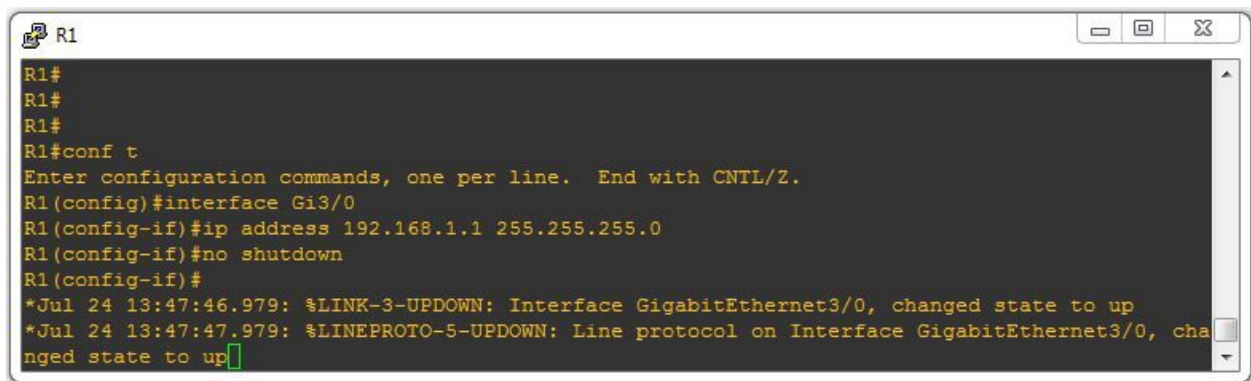
Routerul **interconecteaza** mai multe retele prin **porturi** (de obicei 2 - 3). Denumirea de **porturi** este valabila cand ne referim din punct de vedere **fizic**. Cealalta denumire este de **interfeta** si este valabila cand ne referim din punct de vedere **logic** (mai exact ceea ce vom configura noi, putin mai tarziu).

**Port = Fizic**

**Interfata = Logic**

**De exemplu:** “noi vom seta o adresa IP (logic) pe o interfata si vom conecta cablul (fizic) intr-un port”

Aceste interfete trebuie sa aiba *configurata o adresa IP* pentru a putea comunica cu retea si interfata trebuie sa fie **PORNITA**. Setarea unei adrese IP pe o interfata se face in felul urmatoar:

A screenshot of a terminal window titled 'R1'. The terminal shows the following commands and output:

```
R1#
R1#
R1#
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface Gi3/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#
*Jul 24 13:47:46.979: %LINK-3-UPDOWN: Interface GigabitEthernet3/0, changed state to up
*Jul 24 13:47:47.979: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet3/0, changed state to up
```

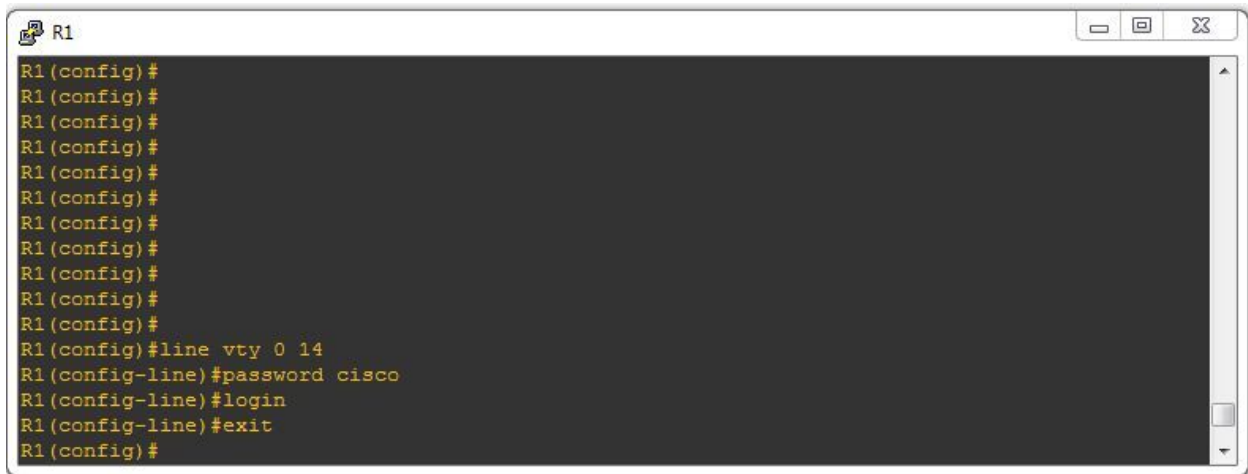
Figura 8.5

```
R1(config)#interface FastEthernet0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
```

## f) Configurare access remote pe Router (Telnet, SSH)

Putin mai devreme in acest capitol am invatat ce este Telnet, respectiv SSH, acum a sosit momentul sa le si configuram pe Router:

## Telnet



```
R1
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#line vty 0 14
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#
```

Figura 8.6

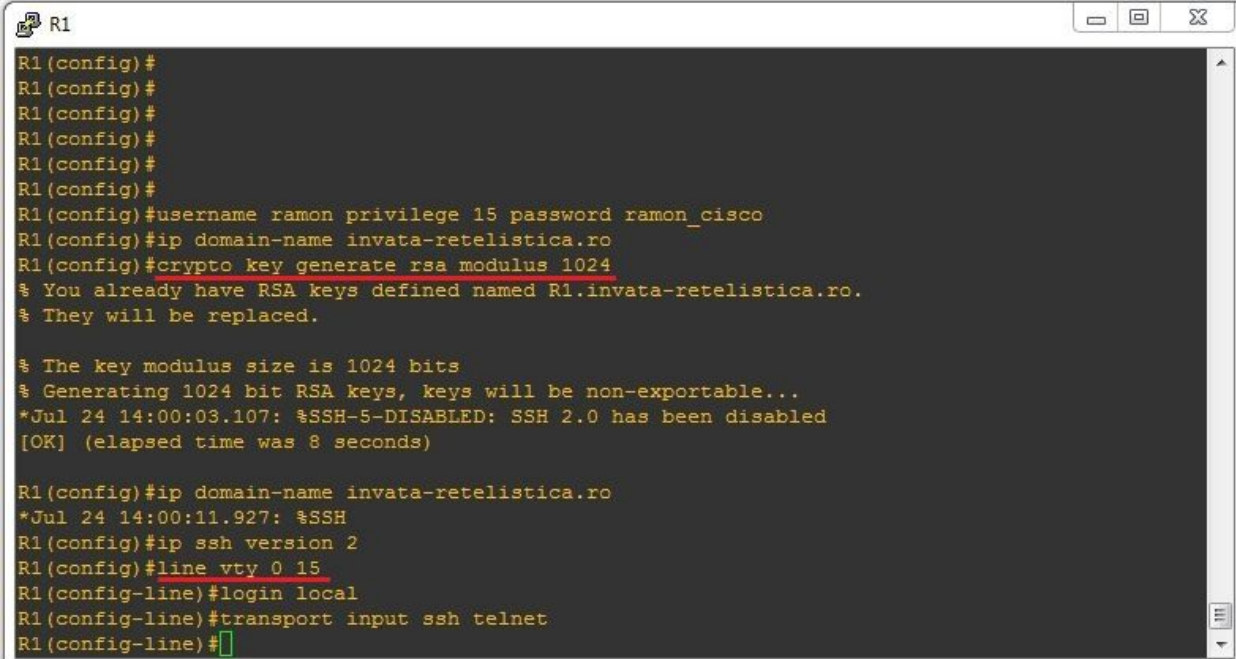
```
R1(config)#line vty 0 14
R1(config-line)#password cisco
R1(config-line)#login
```

Vom intra pe linile virtuale (15 in total), vom seta parola “cisco” si vom porni procesul (Telnet) prin comanda #login.

## SSH

Dupa cum am vorbit si in capitolul 7, SSH-ul este un protocol care ne asigura conectarea remote catre un echipament din LAN sau din Internet, intr-un mod securizat. **Pentru a configura SSH** pe un echipament Cisco vom parcurge urmatoorii pasi:

1. *Crearea unui user & parola*
2. *Nume de domeniu*
3. *Pereche de chei publica si privata*
4. *Pornirea procesului pe linile virtuale (vty) prin #login local*



```
R1
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#username ramon privilege 15 password ramon_cisco
R1(config)#ip domain-name invata-retelistica.ro
R1(config)#crypto key generate rsa modulus 1024
% You already have RSA keys defined named R1.invata-retelistica.ro.
% They will be replaced.

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
*Jul 24 14:00:03.107: %SSH-5-DISABLED: SSH 2.0 has been disabled
[OK] (elapsed time was 8 seconds)

R1(config)#ip domain-name invata-retelistica.ro
*Jul 24 14:00:11.927: %SSH
R1(config)#ip ssh version 2
R1(config)#line vty 0 15
R1(config-line)#login local
R1(config-line)#transport input ssh telnet
R1(config-line)#
```

Figura 8.7

```
R1(config)#username ramon privilege 15 password ramon_cisco
```

```
R1(config)#ip domain-name invata-retelistica.ro
R1(config)#crypto key generate rsa modulus 1024
R1(config)#ip ssh version 2
```

```
R1(config)line vty 0 15
R1(config-line)#login local
R1(config-line)#transport input ssh telnet
```

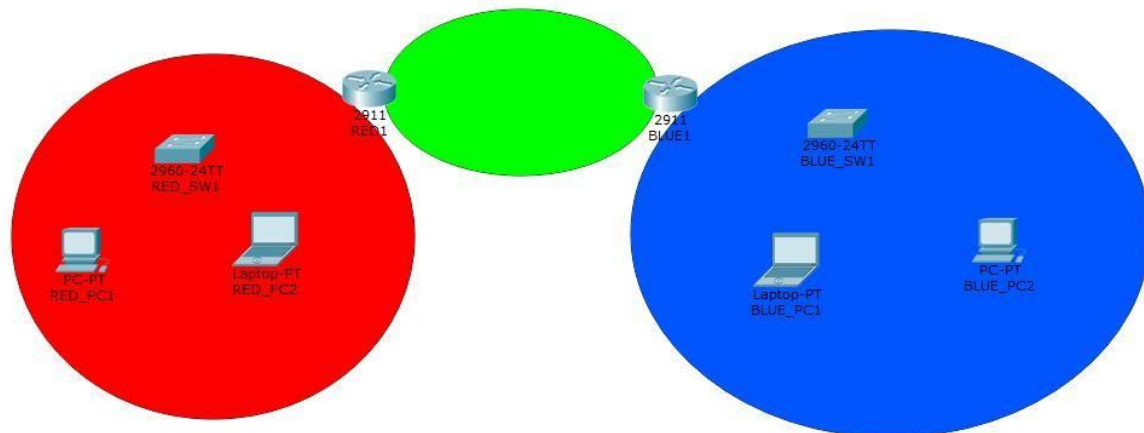


## Laborator Practic

Acum ai destul de multe cunostinte pentru a putea pune lucrurile in practica; asadar te rog sa descarci topologia de [AICI](#), impreuna cu programul [Cisco Packet Tracer](#) (programul de simulare a retelelor de calculatoare).

Urmareste cerintele existente in laborator si configureaza corespunzator acestora, dispozitivele existente.

**SCOP:** Acomodarea cu CLI. Configurari de baza pe Routere si Switch-uri



**SFAT:** Foloseste-te de **manualul de comenzi** pentru a rezolva cu succes exercitiul !

PS: Ti-a placut acest ghid de Retelistica ? Vrei sa inveti mai multe despre Retele de Calculatoare ? [Atunci iti recomand sa intrii AICI](#).

## Capitolul 6 - Serviciul de Retea DHCP

In urmatoarea sectiune vom vorbi despre serviciul de retea DHCP. Vom folosi ca referinta, topologia de mai jos:

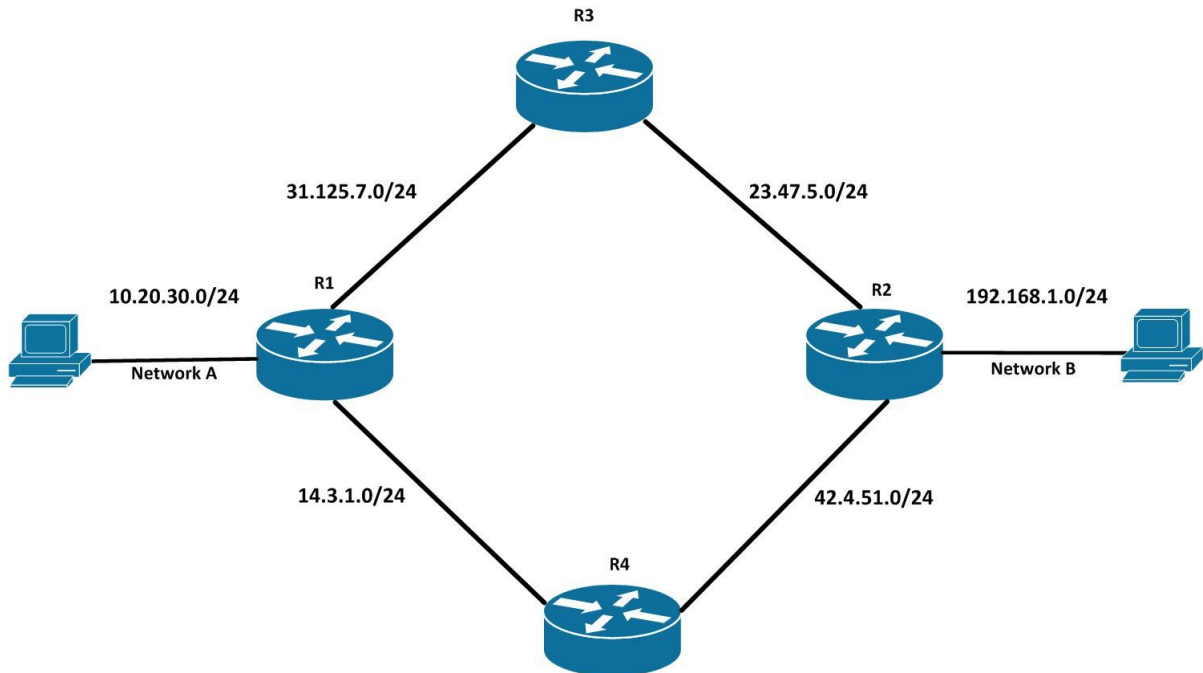


Figura 6.1

### DHCP

**DHCP** (Dynamic Host Configuration Protocol) este un protocol de retea care ne ofera in **mod dinamic** urmatoarele informatii:

- 1) *Adresa IP + Masca*
- 2) *Default Gateway*
- 3) *DNS Server*

*Adresa IP si masca de retea* ne vor ajuta sa identificam fiecare dispozitiv din retea (IP-ul) si sa stabilim dimensiunea retelei (masca de retea).

**Serverul DNS** ne ajuta cu “**translatarea**” **numelui** (ex: google.ro) intr-o adresa IP (216.58.214.227) Toate aceste informatii sunt furnizate de un server (in retelele mai mici, de asta se ocupa Routerul).

## Cum functioneaza DHCP ?

In momentul in care un dispozitiv (PC, smartphone, tableta, SmartTV etc.) se conecteaza la retea va trimite o cerere Broadcast (catre toate dispozitivile din retea) in speranta ca va gasi un server care sa-i aloce o adresa IP :

### 1) DHCP Discover

In momentul in care un server DHCP (in retele mici va fi in general un Router Wi-Fi) vede un astfel de mesaj in retea, va raspunde imediat cu un:

**2) DHCP Offer** (care contine informatiile enumerate mai sus)

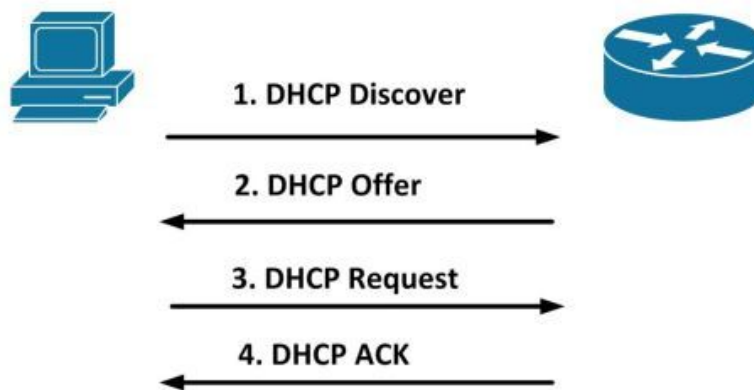


Figura 6.2

In final, dispozitivul (PC-ul in acest caz) va fi de acord cu “oferta” propusa de server DHCP si va trimite o cerere pentru aceasta:

### 3) DHCP Request

Dupa ce primeste acest mesaj serverul DHCP va raspunde cu un

**4) DHCP ACK** // in semn de confirmare a cererii primite de la dispozitiv (PC)

## Configurare DHCP pe Router

Pentru a configura un Router ca DHCP Server trebuie sa avem in vedere urmatoarele elemente:

- 1) Adresa de retea si masca - (10.20.30.0/24)
- 2) Adresa IP a gateway-ului (router-ului) - (10.20.30.1)
- 3) Adresa IP a serverului DNS - (8.8.8.8)

Fiecare din aceste 3 elemente sunt esentiale pentru asigurarea conectivitatii la Internet la orice end-device (PC, telefon, server etc). Iata si cum le putem configura:

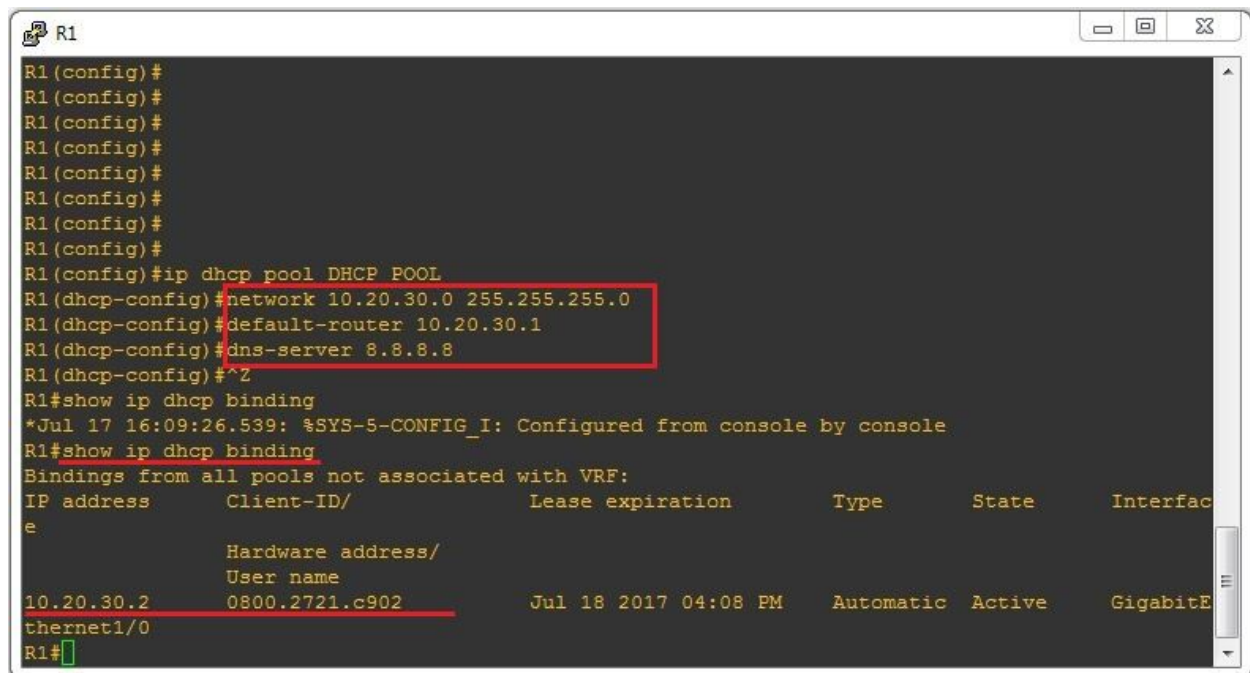
```
R1(config)#ip dhcp excluded-address IP_1 IP_2
```

```
R1(config)#ip dhcp pool NUME
```

```
R1(config-dhcp)#network 10.20.30.0/24
```

```
R1(config-dhcp)#default-router 10.20.30.1
```

```
R1(config-dhcp)#dns-server 8.8.8.8
```



```
R1
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#
R1(config)#ip dhcp pool DHCP POOL
R1(dhcp-config)#network 10.20.30.0 255.255.255.0
R1(dhcp-config)#default-router 10.20.30.1
R1(dhcp-config)#dns-server 8.8.8.8
R1(dhcp-config)#^Z
R1#show ip dhcp binding
*Jul 17 16:09:26.539: %SYS-5-CONFIG_I: Configured from console by console
R1#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address      Client-ID/
e
Hardware address/
User name
10.20.30.2      0800.2721.c902      Jul 18 2017 04:08 PM      Automatic      Active      GigabitE
thernet1/0
R1#
```

Figura 6.3

Iata si cateva comenzi de verificare:

```
R1#show ip dhcp binding
```

```
R1#show run | dhcp
```

Iata-ne si pe Ubuntu (Linux) alocand o adresa IP dinamica de la serverul DHCP creat mai devreme. Folosim `#dhclient enp0s3` (care reprezinta numele interfetei) si comanda `#ifconfig`, respectiv ping, pentru a verifica adresa IP si conectivitatea cu routerul R1.

```
root@ubuntu: ~  
  
root@ubuntu:~# dhclient enp0s3  
root@ubuntu:~# ifconfig  
enp0s3  Link encap:Ethernet  HWaddr 08:00:27:21:c9:02  
        inet addr:10.20.30.2  Bcast:10.20.30.255  Mask:255.255.255.0  
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
        RX packets:5184 errors:0 dropped:0 overruns:0 frame:0  
        TX packets:1215 errors:0 dropped:0 overruns:0 carrier:0  
        collisions:0 txqueuelen:1000  
        RX bytes:6740512 (6.7 MB)  TX bytes:94126 (94.1 KB)  
  
lo      Link encap:Local Loopback  
        inet addr:127.0.0.1  Mask:255.0.0.0  
        inet6 addr: ::1/128 Scope:Host  
        UP LOOPBACK RUNNING  MTU:65536  Metric:1  
        RX packets:103 errors:0 dropped:0 overruns:0 frame:0  
        TX packets:103 errors:0 dropped:0 overruns:0 carrier:0  
        collisions:0 txqueuelen:1  
        RX bytes:8197 (8.1 KB)  TX bytes:8197 (8.1 KB)  
  
root@ubuntu:~# ping 10.20.30.1  
PING 10.20.30.1 (10.20.30.1) 56(84) bytes of data.  
64 bytes from 10.20.30.1: icmp_seq=1 ttl=255 time=8.69 ms  
^C
```

Figura 6.4

## Configurare adresa IP dinamica (prin DHCP) pe Windows

Acum vom lua un alt exemplu si vom vedea modul in care putem aloca o adresa IP prin DHCP pe Windows XP / 7 / 8 / 10. Vom vedea cum putem face asta atat din linie de comanda (CMD) cat si din modul grafic.

## 1) DHCP din CMD

Modul in care putem aloca o adresa IP prin DHCP in Windows, din CMD, este prin comanda **>ipconfig /renew**

```
C:\Windows\system32\cmd.exe
C:\Users\oracle>ipconfig /renew
Windows IP Configuration

No operation can be performed on Bluetooth Network Connection while it has its media disconnected.
An error occurred while releasing interface Loopback Pseudo-Interface 1 : The system cannot find the file specified.

Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::80e7:3223:ac5c:39e9%16
    IPv4 Address. . . . . : 172.16.59.176
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.16.59.2

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Tunnel adapter isatap.<EDB96DF3-34AA-41A1-8809-9B27B2DF11B3>:
```

Figura 6.5

Rezultatul ? O adresa IP, masca si default gateway-ul. Daca dorim sa aflam mai multe informatii (precum DNS-ul, adresa MAC sau chiar serverul DHCP) avem la dispozitie comanda:

**>ipconfig /all**

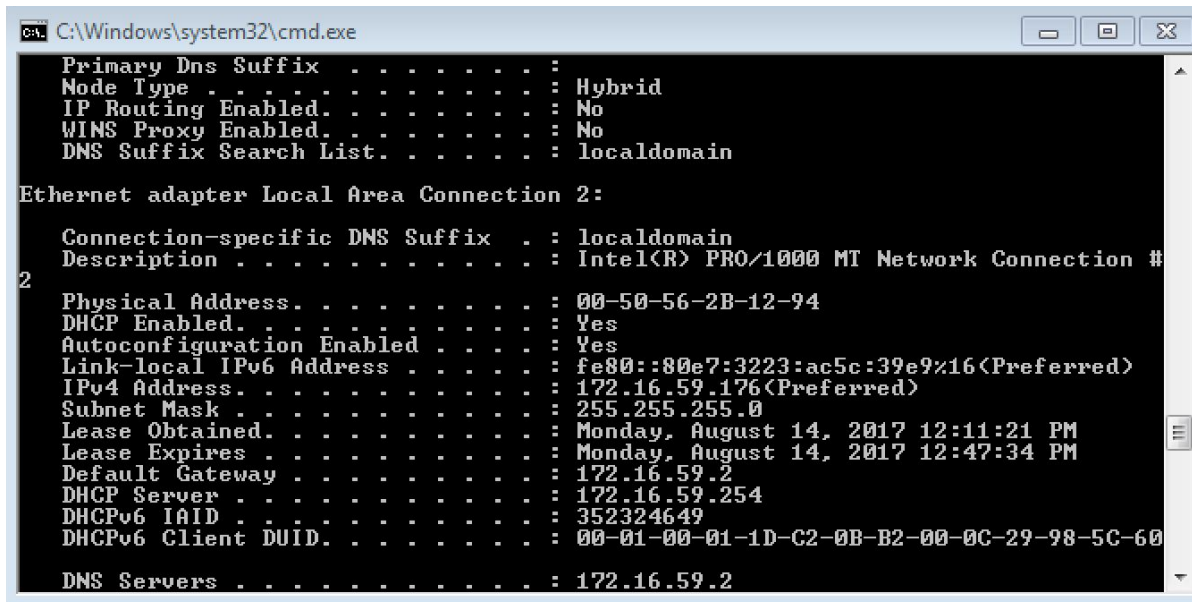


Figura 6.6

## 2) DHCP prin Modul Grafic

Odata ajunsi in acest punct in care putem configura o adresa IP:

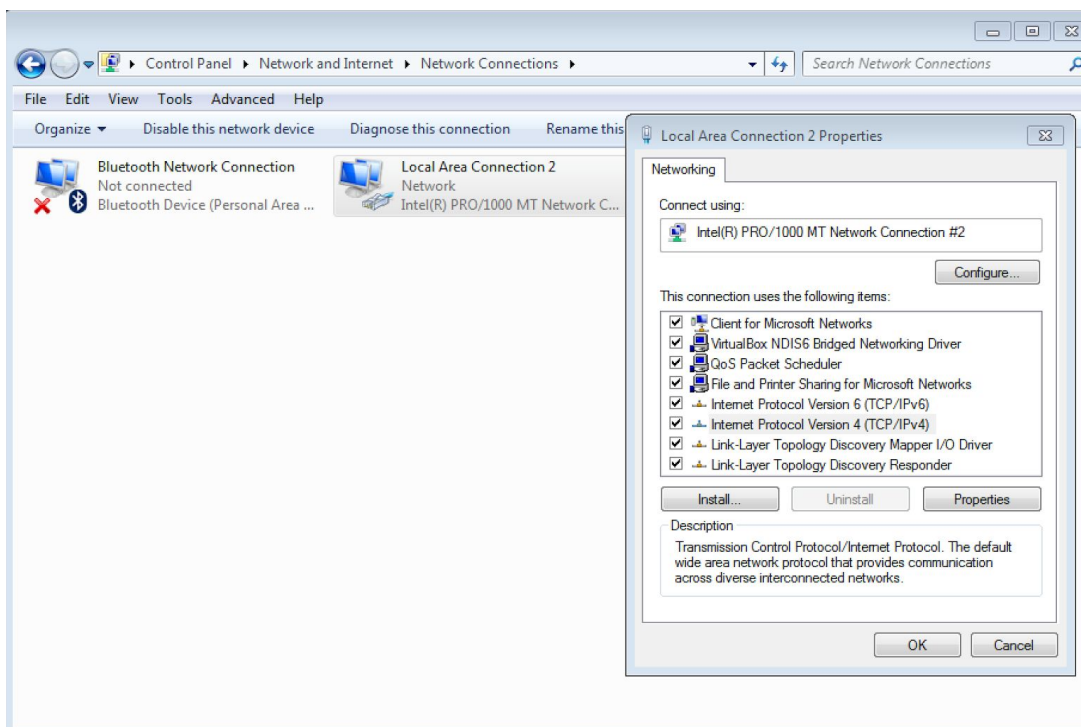


Figura 6.7



Vom selecta IPv4 -> **“Properties”** si avom ajunge la fereastra din figura de mai jos:

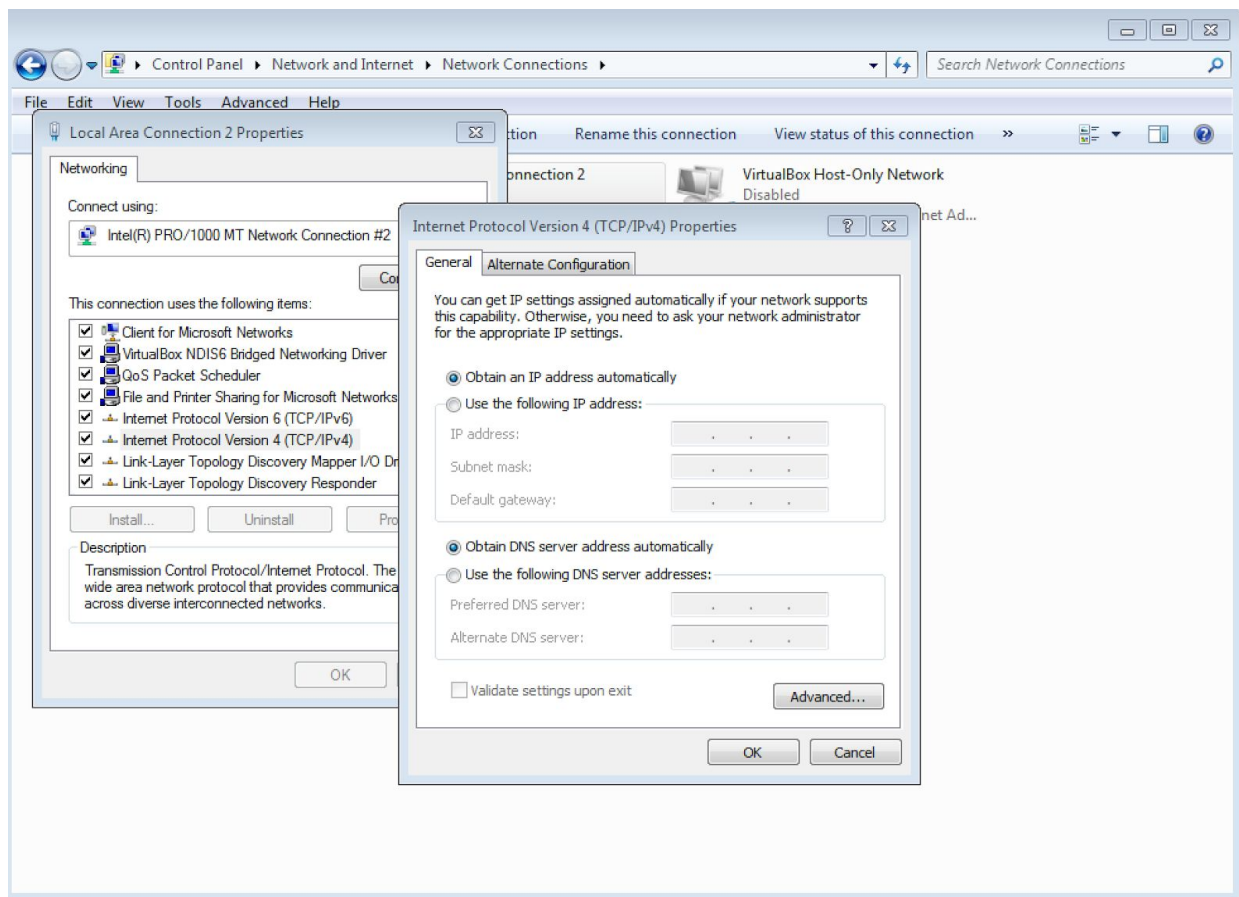


Figura 6.8

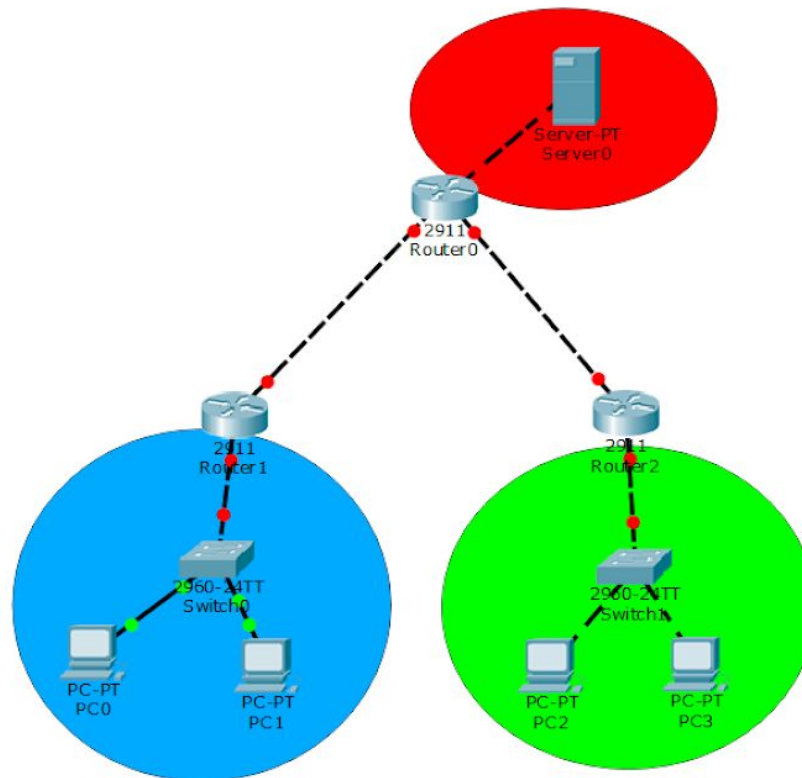
Aici vom selecta **“Obtain an IP address automatically”** si **“Obtain DNS server address automatically”**. Aceste 2 optiuni vor spune PC-ului sa trimita o cerere DHCP in retea pentru o adresa IP dinamica.



## Laborator Practic #2

Acum am ajuns la partea de laborator (partea practica), care o ai inclusa in atasamente. Aici urmeaza sa implementam cele discutate mai sus. Urmareste cerintele existente in laborator si configureaza corespunzator acestora, dispozitivele existente.

**SCOP:** Configurare DHCP in retele LAN



**SFAT:** Foloseste-te de **manualul de comenzi** pentru a rezolva cu succes exercitiul !

PS: Ti-a placut acest ghid de Retelistica ? Vrei sa inveti mai multe despre Retele de Calculatoare ? [Atunci iti recomand sa intrii AICI.](#)