

# **Proiect Protocole și Rețele de Comunicații**

Proiectarea unei infrastructuri rețelistice  
pentru o clădire comercială cu trei nivele

**- Tema 2 -**

**Vlad-Alexandru Bartolomei**

Grupa 30643

Profesor îndrumător: Adrian Lucian Peculea



MEMBRĂ A



Facultatea de Automatică și Calculatoare  
Universitatea Tehnică din Cluj-Napoca  
România  
Martie 2025

# Cuprins

<b>0 Specificația problemei</b>	<b>2</b>
<b>1 Etapa 1 - stabilirea topologiei tip mapătă problemei expuse</b>	<b>2</b>
1.1 Layout . . . . .	2
1.2 Comenzi . . . . .	4
1.3 Memoriu tehnic . . . . .	5
1.3.1 Minimum Spanning Tree . . . . .	5
1.3.2 Virtual Local Area Network - VLAN . . . . .	5
1.3.3 Virtual (LAN) Trunking Protocol - VTP . . . . .	6
1.3.4 VLAN pentru traficul de management . . . . .	8
1.3.5 Bridge-ul rădăcină . . . . .	9
1.3.6 Adresarea de IP-uri . . . . .	10
1.3.7 Serverul de DHCP . . . . .	10
<b>2 Etapa 2 - Adăugarea zonei demilitarizate (DMZ)</b>	<b>13</b>
2.1 Layout . . . . .	13
2.2 Comenzi . . . . .	13
2.3 Memoriu tehnic . . . . .	14
2.3.1 Hop-by-hop routing . . . . .	14
2.3.2 Zona demilitarizată - DMZ . . . . .	15
<b>3 Etapa 3 - Configurarea serviciilor din zona demilitarizată. Conectarea remote prin SSH</b>	<b>16</b>
3.1 Layout . . . . .	16
3.2 Comenzi . . . . .	16
3.3 Memoriu tehnic . . . . .	20
3.3.1 Rezolvarea adresării serverelor prin DNS . . . . .	20
3.3.2 Conectarea remote la switch-uri . . . . .	23
<b>4 Etapa 4 - Ieșirea în Internet prin Network Address Translation (NAT)</b>	<b>26</b>
4.1 Layout . . . . .	26
4.2 Comenzi . . . . .	27
4.2.1 Legătura punct-la-punct MainRouter-ISP . . . . .	27
4.2.2 Listele de acces . . . . .	27
4.2.3 Translatarea interior-exterior . . . . .	28
4.2.4 Configurarea retelei Outside . . . . .	28
4.2.5 Rutarea de la Interior la Exterior . . . . .	29
4.2.6 Mapare statică NAT . . . . .	30
4.3 Memoriu tehnic . . . . .	30
4.3.1 NAT - Network Access Translation . . . . .	30
4.3.2 PAT - Port Address Translation . . . . .	33
<b>5 Etapa 5 - Securizarea suplimentară a echipamentelor</b>	<b>35</b>
5.1 Memoriu tehnic . . . . .	35
5.1.1 Protejarea Switch-urilor . . . . .	35
5.1.2 Liste de acces extinse pe routerul principal . . . . .	36

## Rezumat

Prezenta documentație își propune să documenteze printr-un procedeu etapizat parcursul implementării acestui proiect pe durata fiecărei ședințe de lucru și să marcheze, acolo unde este cazul, noțiunile folosite în subcapitole - memorii tehnice.

# 0 Specificația problemei

## 0.1: Specificație

Se consideră o clădire comercială cu 3 nivele. Se va folosi adresa de rețea 172.16.0.0/16 pentru rețeaua intranet, adresa de rețea 210.1.1.64/27 pentru DMZ și adresa de rețea 210.1.1.32/27 pentru accesul în exterior. Se vor proiecta 4 VLAN-uri (unul pentru fiecare etaj și unul pentru traficul de management). Pentru configurarea VLAN-urilor se va folosi protocolul VTP. Prin cablarea și configurarea rețelei se va asigura redundanță. Adresele hosturilor vor fi alocate dinamic folosind un singur server de DHCP aflat în VLAN-ul corespunzător primului etaj. Numărul minim de utilizatori deserviți de către fiecare VLAN este 200. Serverele de HTTP, FTP, DNS și MAIL vor fi plasate în DMZ și vor avea adrese publice. Numele domeniului web va include numele studentului. Pentru asigurarea conectivității se vor configura rute statice. Accesul în exterior se va realiza folosind NAT pe routerul care controlează DMZ, pe următorul interval de adrese publice: 210.1.1.35-210.1.1.62.

Conecțarea la ISP se va realiza printr-o interfață de tip Ethernet având adresa 210.1.1.34/27. Adresa ISP-ului este 210.1.1.33/27. Reteaua Internet se va simula prin intermediul unui server și a unui calculator.

Pentru securizarea echipamentelor de rețea se vor realiza următoarele configurații:

- se vor defini utilizatori pe diferite nivele de privilegiu;
- criptarea parolelor;
- configurarea remote se va face doar prin ssh;
- se va securiza protocolul VTP.

Se vor prezenta și implementa două măsuri suplimentare de securizare a rețelei.

## 0.1: Precizări

1. Pentru acest proiect au fost implementate toate cerințele impuse de problemă.
2. Măsurile de securitate aditionale abordate sunt:
  - securizarea switch-urilor prin impunerea unui număr maxim de adrese MAC care se pot conecta.
  - liste de acces extinse pentru zona DMZ.

# 1 Etapa 1 - stabilirea topologiei tip mapată problemei expuse

## 1.1 Layout

De regulă, într-un astfel de proiect din lumea reală se alege o topologie de tip **stea extinsă**. Această topologie oferă scalabilitate; spre exemplu, dacă aş mai dori să mai cablez o cameră, este posibil să fie tras încă un *app link* și adăugat un *fulg nou*<sup>1</sup>. Pentru problema noastră am ales aceeași variantă, rezultând următoarea figură:

<sup>1</sup>stea extinsă

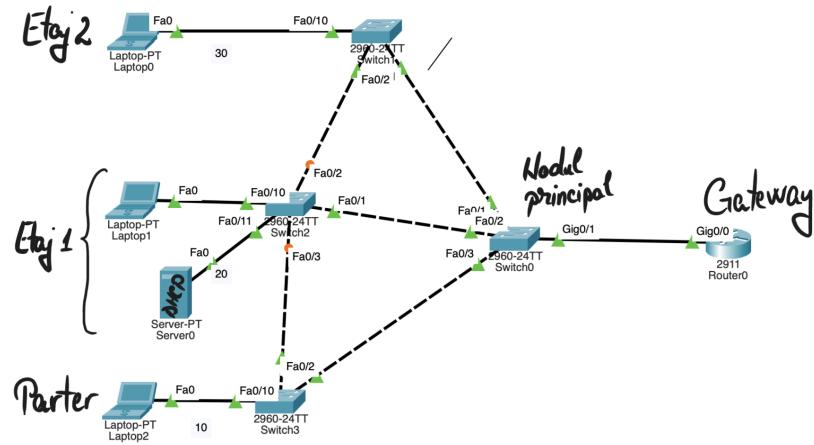


Figura 1: Reprezentarea celor trei etaje, a nodului principal și a celorlalte noduri

Figura 1 respectă specificația de redundanță în felul următor: fiecare etaj are propriul său switch; între toate switch-urile există legături, dar datorită faptului că acestea vor fi configurate pentru a funcționa pe baza algoritmului MINIMUM SPANNING TREE, legăturile redundante vor fi *down*. Algoritmul cunoaște nodul principal, iar când acesta este *down*, celelalte legături se vor activa și vor fi *up*.

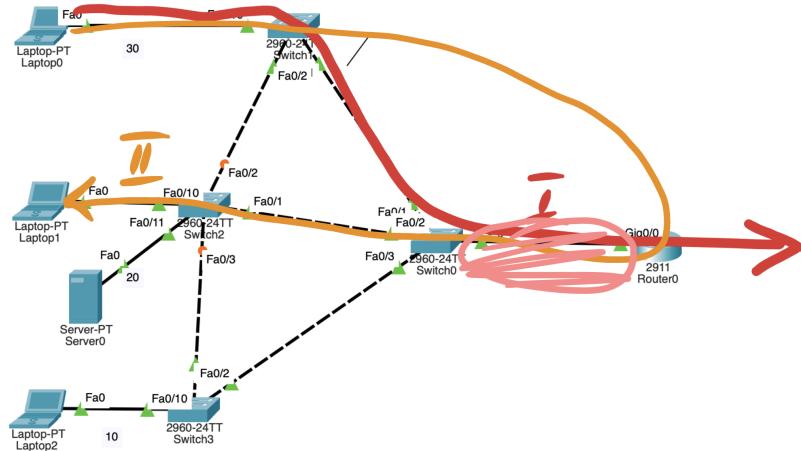


Figura 2: I: accesul stației de pe etajul 2 pe Internet; II: accesul stației de pe etajul 2 la o stație pe etajul 1, într-un alt VLAN

```

Physical Config CLI Attributes
IOS Command Line Interface
1005 trnet-default active
VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
-----
1 enet 100001 1500 - - - - 0 0
1002 fddi 101002 1500 - - - - 0 0
1003 tr 101003 1500 - - - - 0 0
1004 fdnet 101004 1500 - - - ieee - 0 0
1005 trnet 101005 1500 - - - ibm - 0 0
VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
-----
Remote SPAN VLANs
-----
Primary Secondary Type Ports
-----
MainSwitch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MainSwitch(config)#vlan 10
MainSwitch(config-vlan)#name Net10
MainSwitch(config-vlan)#exit
MainSwitch(config)#vlan 20
MainSwitch(config-vlan)#name Net20
MainSwitch(config-vlan)#exit
MainSwitch(config)#vlan 30

```

Figura 5: Crearea VLAN-urilor pe switch-ul principal

## 1.2 Comenzi

```

Switch>ena
Switch#
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#host
Switch(config)#hostname MainSwitch
MainSwitch(config)#int
MainSwitch(config)#interface ra
MainSwitch(config)#interface range fa
MainSwitch(config)#interface range fastEthernet 0/1-2
MainSwitch(config-if-range)#exit
MainSwitch(config)#interface range fastEthernet 0/1-3
MainSwitch(config-if-range)#sw
MainSwitch(config-if-range)#switchport mo
MainSwitch(config-if-range)#switchport mode acc
MainSwitch(config-if-range)#switchport mode access
MainSwitch(config-if-range)#exit

```

Figura 3: Exemplu pentru configurarea Switch-ului principal și configurarea porturilor aferente, legate la celealte Switch-uri ale fiecărui VLAN, pentru a comunica pe linii de trunk

```

MainSwitch>ena
MainSwitch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MainSwitch(config)#vtp do
MainSwitch(config)#vtp domain Adrian
Changing VTP domain name from NULL to Adrian
MainSwitch(config)#vtp pass
MainSwitch(config)#vtp password Adrian
Setting device VLAN database password to Adrian
MainSwitch(config)#vtp mode ser
MainSwitch(config)#vtp mode server
Device mode already VTP SERVER.
MainSwitch(config)#

```

Figura 4: Activarea protocolului VTP pe switch-ul principal. Captură de ecran de la laboratorul online ținut de domnul profesor Adrian Peculea, de pe stația sa

```

MainSwitch>
MainSwitch>ena
MainSwitch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MainSwitch(config)#spa
MainSwitch(config)#spanning-tree vlan 1,10,20,30,99 prior
MainSwitch(config)#spanning-tree vlan 1,10,20,30,99 priority 0
MainSwitch(config)#sh
MainSwitch(config)#do

```

Figura 6: Setarea VLAN-urilor în Spanning Tree

```

MainRouter(config-if)#exit
MainRouter(config)#int
MainRouter(config)#interface gi
MainRouter(config)#interface gigabitEthernet 0/0.20
MainRouter(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.20, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.20,
changed state to up

MainRouter(config-subif)#enc
MainRouter(config-subif)#encapsulation d
MainRouter(config-subif)#encapsulation dot1Q 20
MainRouter(config-subif)#ip add
MainRouter(config-subif)#ip address 172.16.20.1 255.255.255.0
MainRouter(config-subif)#

```

Figura 7: Configurarea serverului de DHCP. Protocolul folosit este 802.1Q, încrucișând acesta menține și informații despre VLAN-uri, iar protocolul Ethernet este insuficient.

```

MainRouter(config-subif)#enc
MainRouter(config-subif)#encapsulation dot1Q 30
MainRouter(config-subif)#ip add
MainRouter(config-subif)#ip address 172.16.30.1 255.255.255.0
MainRouter(config-subif)#ip h
MainRouter(config-subif)#ip he
MainRouter(config-subif)#ip hel
MainRouter(config-subif)#ip helpe
MainRouter(config-subif)#ip helper-address 172.16.20.2
MainRouter(config-subif)#

```

Figura 8: Exemplu de rerutare a unui DHCPDiscover request dintr-un VLAN diferit de VLAN-ul în care se află serverul de DHCP

### 1.3 Memoriu tehnic

#### 1.3.1 Minimum Spanning Tree

#### 1.3.2 Virtual Local Area Network - VLAN

Un VLAN este util pentru a virtualiza resurse. Se economisesc bani, hardware și echipamente. Ca aplicabilitate în viața reală, VLAN-urile se folosesc în cadrul același companii pentru a lega între ele stații din aceeași departamente. Spre exemplu, departamentul de Marketing are un VLAN, cel de Resurse Umane alt VLAN. Această *clusterizare* a stațiilor aduc un mare avantaj: reduc din traficul generat pe router-ul principal, ținând chestiunile interne strict pentru acel VLAN.

În locul unui VLAN, fiecare departament ar fi putut avea propriul său router, numai că aceasta ar fi implicat costuri suplimentare și overhead tehnic. Protocolul folosit este 802.1Q.

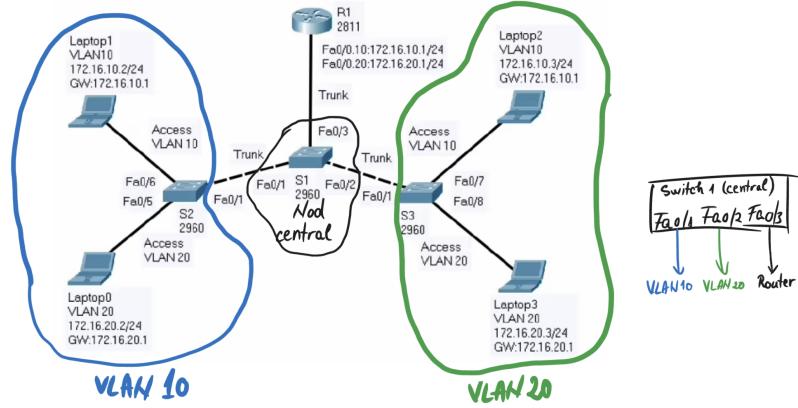


Figura 9: Exemplu cu două VLAN-uri diferite legate de un switch central și un router

Figura 9 ilustrează perfect o situație în care un VLAN poate fi aplicat. Două departamente vorbesc separat în VLAN-uri diferite (10 și 20). Pentru ca o stație din VLAN 10 să vorbească cu o alta din VLAN 20, trebuie să treacă prin Switch-ul principal, apoi prin Router (prezența acestuia este absolut necesară) și apoi să fie redirectată către VLAN-ul potrivit. Între cele trei switch-uri din poză, comunicarea se face în mod **trunk**, spre deosebire de celelalte linii, care comunică pe mode **access**.

În scenarii reale, VLAN-urile nu vor fi identificate după numere (VLAN 10, VLAN 20), ci după nume (VLAN Engineering, VLAN Accounting). Din motive de securitate, VLAN-ul 1 este un VLAN preconfigurat și el nu se schimbă.

### 1.3.3 Virtual (LAN) Trunking Protocol - VTP

Definirea de VLAN-uri în mod manual poate fi laborioasă. Adăugarea unui nou VLAN mai adaugă un număr de comenzi și nu este scalabil.

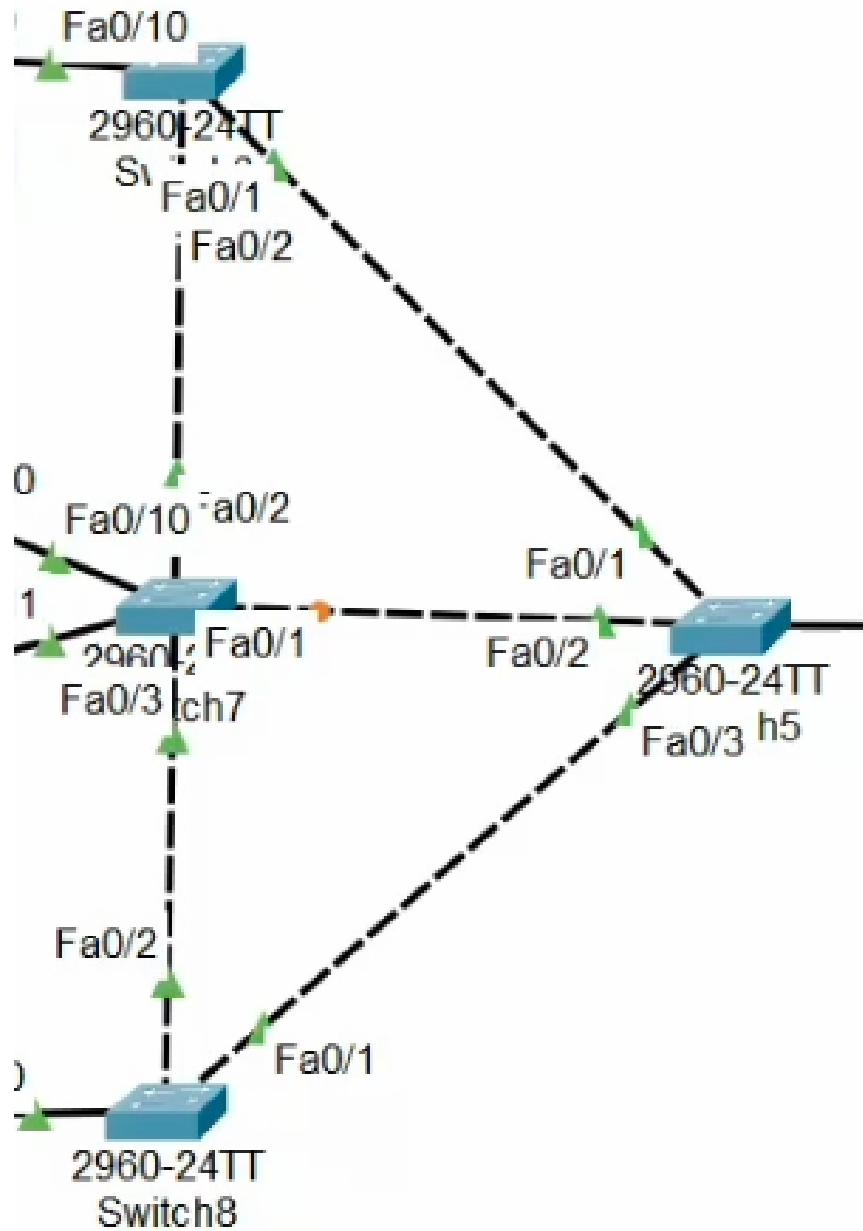


Figura 10: Numai pentru 4 VLAN-uri (10, 20, 30 și 99) avem  $12 \times 4 = 48$  de comenzi

Ca răspuns la această problemă a apărut protocolul VTP, un protocol enterprise scalabil. Acest protocol spune că eu pot așeza toate switch-urile **într-un singur domeniu**, iar ele să se autentifice unul cu celălalt prin intermediul unei **parole**<sup>2</sup>. Adițional, switch-urile trebuie să activeze într-unul dintre cele două moduri<sup>3</sup>: *server* și *client*.

<sup>2</sup>Domeniul și parola trebuie să fie **aceleași** pentru toată infrastructura de switch-uri dorită. În caz contrar, switch-urile nu se pot autentifica între ele

<sup>3</sup>sunt mai multe, însă numai despre acestea două merită discutat

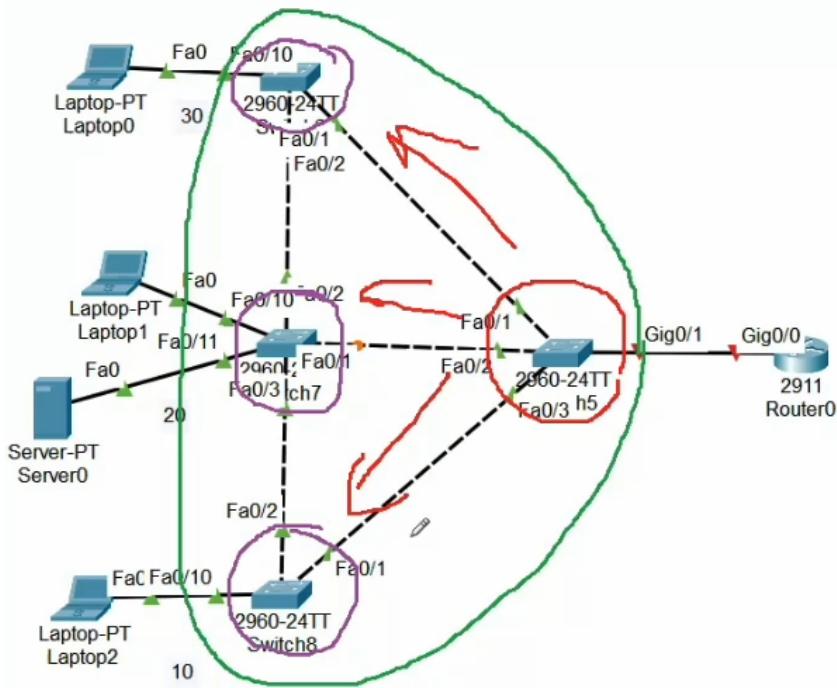


Figura 11: Switch-ul principal este considerat a fi cel în mod server; celelalte sunt în mod client

Switch-ul server (unul singur!) ține o bază de date de VLAN-uri. Procedeul de adăugare al unui nou VLAN implică:

- adăugarea VLAN-ului nou la switch-ul server
- advertise din partea switch-ului server către toate switch-urile client deja existente

Ca efect, toate switch-urile client vor învăța existența noului VLAN. În mod similar are loc stergerea unui VLAN.

#### 1.3.4 VLAN pentru traficul de management

Prin acest VLAN trece tot traficul ce ține de administrare și gestionare al echipamentelor, trafic izolat de cel al clientului. Acest VLAN este destinat folosirii de către inginerul de sistem, care de oriunde se poate conecta la VLAN și poate monitoriza traficul și echipamente; drept urmare aceste date au caracter confidențial.

### 1.3.5 Bridge-ul rădăcină

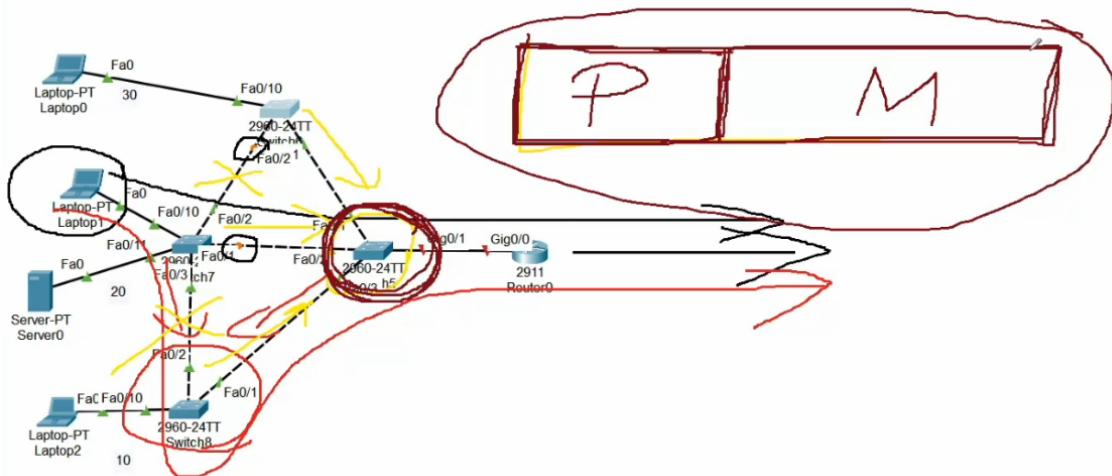


Figura 12: Laptop-ul de pe etajul 1 încearcă să comunice cu internetul (negru), însă se vede nevoie să o ia pe la parter (roșu) (a se vedea LED-urile portocalii)

Ideea de a merge pe la parter sau pe orice alt etaj în afară de cel de origine nu este bună pentru controlul traficului. În varianta ideală ar trebui ca bridge-ul rădăcină să coincidă, în acest caz, cu switch-ul principal, astfel încât fiecare switch să-și calculeze cea mai scurtă cale către nodul principal și implicit backup-ul (redundanță) să fie stabilit între etaje (semnalizat de x-urile galbene).

**Cum se alege bridge-ul rădăcină?** În funcție de identificatorul switch-ului. Structura sa constă în:

- câmpul P - Prioritate
  - cea mai semnificativă parte
  - cu cât e mai mic numărul, cu atât e mai prioritar
- câmpul M - MAC
  - cea mai puțin semnificativă parte

În mod normal, în cazul în care  $n$  switch-uri au priorități egale, bridge rădăcină devine cel cu MAC mai mic. Dar ce mă fac dacă mai adaug un switch care întămplător are MAC mai mic (și încurcă calculele)? Soluția vine din următoarea idee: oricât ar fi MAC-ul, dacă pe acest nou switch va fi setată o prioritate mai mică ca toate celelalte, el va deveni noul bridge rădăcină<sup>4</sup>.

<sup>4</sup>indiferent cât vor fi celelalte MAC-uri

### 1.3.6 Adresarea de IP-uri

**172.16.0.0/16  
255.255.0.0**

**172.16.20.0/24  
255.255.255.0  
172.16.20.1 gw  
172.16.20.2 dhcp**

Figura 13:

Din cerință cunoaștem adresa de rețea pentru rețeaua intranet și masca sa (primele două linii). În continuare știm că serverul de DHCP va funcționa în VLAN-ul 20, drept urmare va fi definit în *subrețeaua 172.16.20.0*.

### 1.3.7 Serverul de DHCP

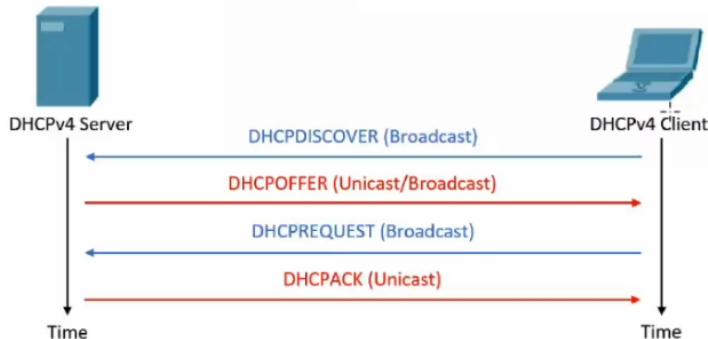


Figure 6.12 DHCP process

The previous sequence of operations can also be observed in Wireshark (Figure 6.13) when using the `ipconfig /release` and `ipconfig /renew` (on Windows OS) and `dhclient` (on Linux OS) commands:

No	Time	Source	Destination	Protocol	Length	Info
1		171.10.92.55.62	192.168.0.100	DHCP	342	DHCP Release - Transaction ID 0x9a7c44e2
2		41.17.86.1982	0.0.0.0	DHCP	342	DHCP Discover - Transaction ID 0x31d82096
3		41.17.86.6707	192.168.0.1	DHCP	590	DHCP Offer - Transaction ID 0x31d82096
4		41.17.86.9187	0.0.0.0	DHCP	366	DHCP Request - Transaction ID 0x31d82096
5		42.718.38.1342	192.168.0.1	DHCP	590	DHCP ACK - Transaction ID 0x31d82096

Figure 6.13 Wireshark capture of DHCP process

Figura 14: Prințipiul de funcționare al unui server de DHCP

Clientul nu știe inițial nimic, nici măcar unde e serverul de DHCP. Așa că el aruncă în broadcast un mesaj standard definit de **DHCP discover**. Înapoi, serverul de DHCP îi face o **ofertă** clientului: „băi, adresa ta e asta, masca ta e asta, gateway-ul tău e asta, DNS-ul asta etc.”. Mai rămâne să se întâmpăre un handshake.

Pentru a configura un server de DHCP, trebuie să se configureze pe acesta adresa serverului în sine și adresa gateway-ului.

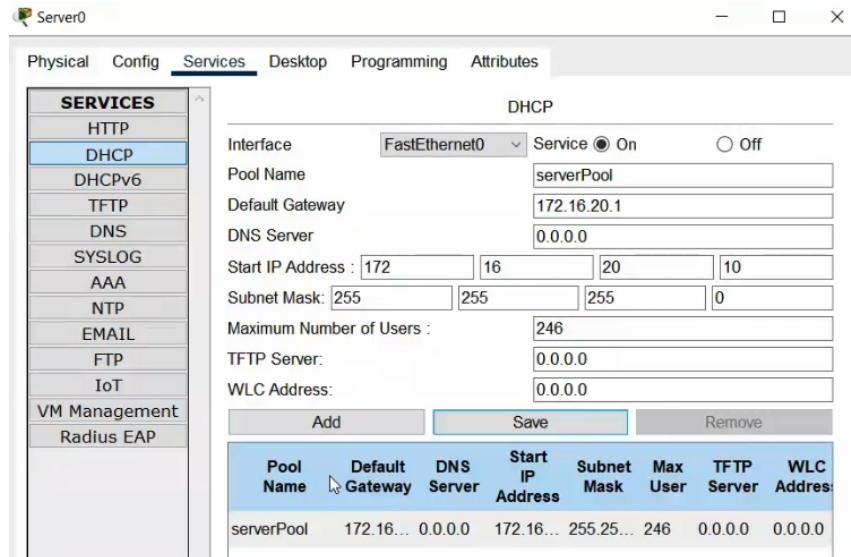


Figura 15: Configurarea serviciului de DHCP

Default gateway se setează la adresa router-ului<sup>5</sup>. DNS serverul este, în această etapă, încă necunoscut. Adresele de IP nu vor începe de la 1 (blocat de gateway), nici de la 2 (fiind adresa serverului DHCP), ci de la 10. Ca best practice, adresele 3-7 (sau alt număr de adrese) este lăsat liber ca, în cazul în care eu îmi doresc să setez ceva (de exemplu o imprimantă), să o pot face static.

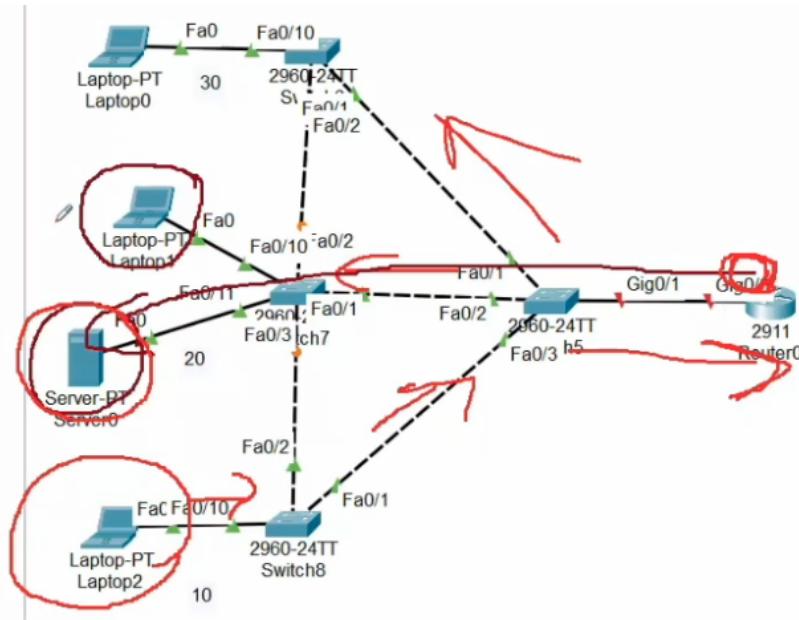


Figura 16: Cazul în care o stație din afara VLAN-ului serverului de DHCP cere o adresă IP

VLAN-ul 20 (implicit serverul de DHCP) este marcat cu maro. Oricărei stații din VLAN 20 îi este ușor să obțină o adresă IP, fiind tot acolo. Dar, în momentul în care stația din VLAN 10 (deci diferit) (marcată cu roșu) lansează un DHCP discover request<sup>6</sup> care se împărtășie în toată rețea, dar doar în VLAN 10.

Pentru a adresa această problemă, fie pui câte un DHCP server în fiecare VLAN<sup>7</sup>, fie se folosește următoarea tehnică: în momentul în care DHCP discover loveste gateway-ul, el este redirectat către serverul respectiv. Redirectarea se face cu adresa de gateway din VLAN-ul meu, în care vreau să

<sup>5</sup>în cazul unui DHCP discover, stația care a lansat requestul va vedea această adresă din partea serverului de DHCP

<sup>6</sup>marcat de săgețile roșii

<sup>7</sup>e posibil să definești 4000 de VLAN-uri, ceea ce ar însemna costuri ridicate

obțin adresele (VLAN 10), așa încât serverul de DHCP să înțeleagă că trebuie să dea adrese din *pool*-ul de adrese aferente VLAN-ului 10.

```
172.16.10.0/24
172.16.10.1 gw
redirectare spre 172.16.20.2 spre DHCP
```

Figura 17: Rezumat

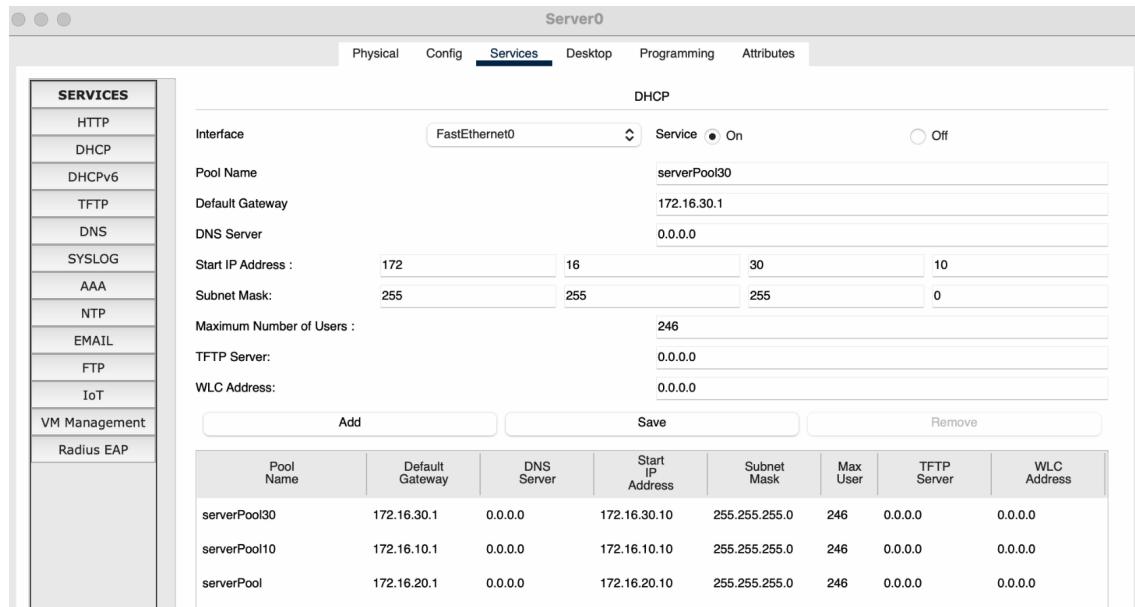


Figura 18: Cele trei pool-uri de adrese ale DHCP server, pentru VLAN 10, VLAN 20 și VLAN 30

Această configurare se face pe routerul principal. Se definește adițional un `ip address-helper` 172.16.20.2, adică adresa serverului de DHCP, pentru fiecare interfață, așa încât la orice DHCP Discover request să știe routerul unde să reruteze cererea (8).

## 2 Etapa 2 - Adăugarea zonei demilitarizate (DMZ)

### 2.1 Layout

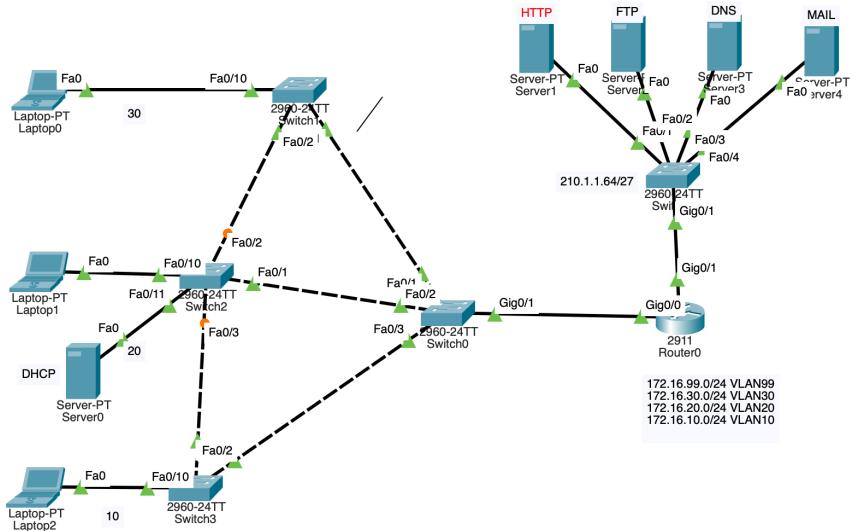


Figura 19: La finalul configurărilor, fiecare stație poate vorbi cu orice altă stație, fie că e din rețeaua locală, fie că e din DMZ

### 2.2 Comenzi

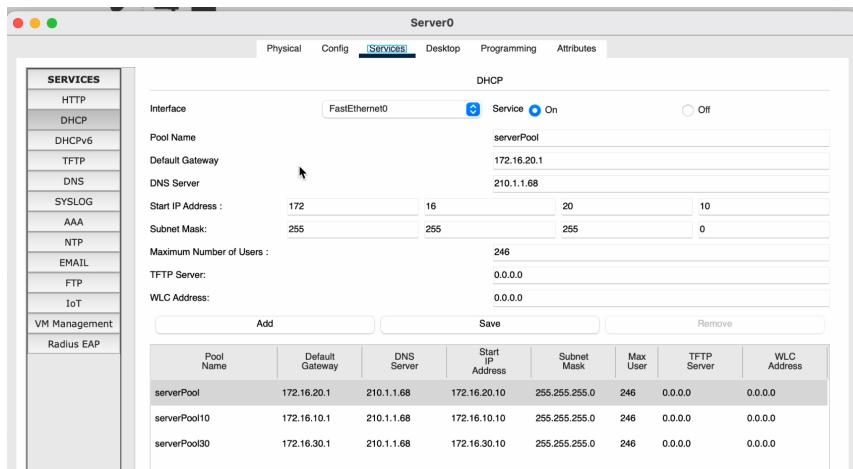


Figura 20: Configurarea switch-ului din DMZ

```

DMZ(config)#int ra gi 0/1-2
DMZ(config-if-range)#sw mo acc
DMZ(config-if-range)#sw acc vlan 2
DMZ(config-if-range)#do show vlan

VLAN Name          Status    Ports
----- 
1     default      active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
2     DMZ          active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                           Fa0/9, Fa0/10, Fa0/11, Fa0/12
                           Fa0/13, Fa0/14, Fa0/15, Fa0/16
                           Fa0/17, Fa0/18, Fa0/19, Fa0/20
                           Fa0/21, Fa0/22, Fa0/23, Fa0/24
                           Gig0/1, Gig0/2
1002 fddi-default   active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default   active

```

Figura 21: Efectul 20: toate interfețele selectate se mută în VLAN-ul DMZ

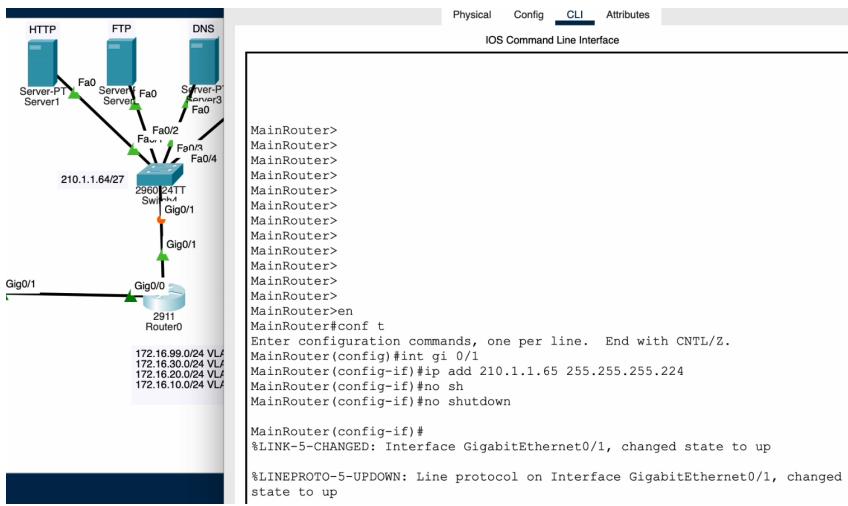


Figura 22: Enter Caption

## 2.3 Memoriu tehnic

### 2.3.1 Hop-by-hop routing

Spre deosebire de rutarea de la sursă<sup>8</sup>, hop-by-hop routing este un procedeu de rutare ad-hoc. Fiecare router are propria sa tabelă de rutare și decide către ce router să dea mai departe pachetul transmis, până când IP-ul destinație match-uește cu stația la care a ajuns.

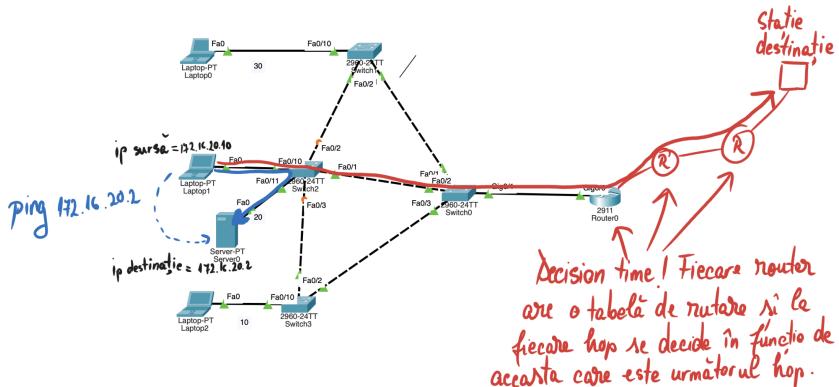


Figura 23: Rutare hop-by-hop

```

MainRouter#sh ip route
Codes: L - local, C - connected, 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, E - EGP
i - IS-IS, 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

Gateway of last resort is not set

172.16.0.0/16 is variably subnetted, 8 subnets, 2 masks
C   172.16.10.0/24 is directly connected, GigabitEthernet0/0.10
L   172.16.10.1/32 is directly connected, GigabitEthernet0/0.10
C   172.16.20.0/24 is directly connected, GigabitEthernet0/0.20
L   172.16.20.1/32 is directly connected, GigabitEthernet0/0.20
C   172.16.30.0/24 is directly connected, GigabitEthernet0/0.30
L   172.16.30.1/32 is directly connected, GigabitEthernet0/0.30
C   172.16.99.0/24 is directly connected, GigabitEthernet0/0.99
L   172.16.99.1/32 is directly connected, GigabitEthernet0/0.99

```

Figura 24: Tabela de rutare pentru MainSwitch, cu `sh ip route`

<sup>8</sup>Exemplul clasic este cel al GPS-urilor care de la sursă configurează un traseu complet către destinație

### 2.3.2 Zona demilitarizată - DMZ

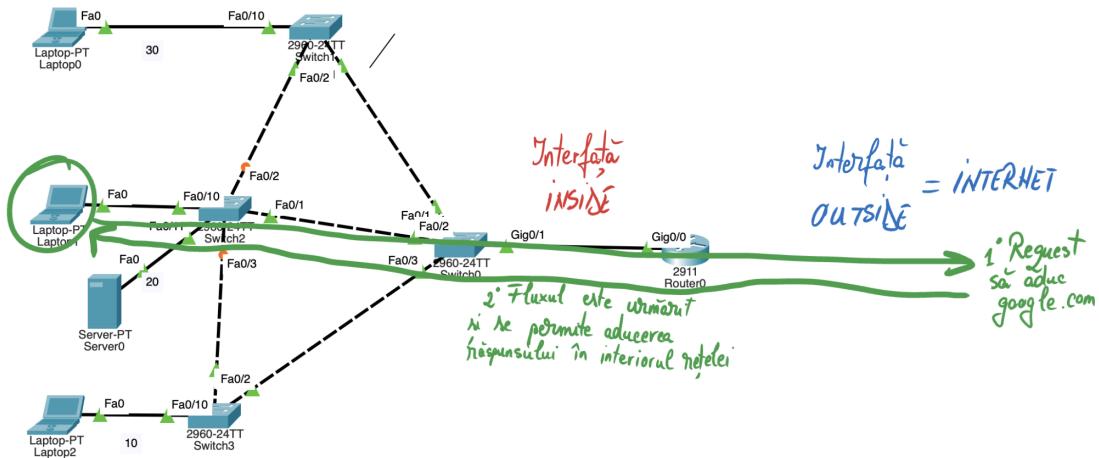


Figura 25: O stație încearcă să acceseze din interior internetul

Situația se schimbă în cazul unui request inițiat din exterior. Pe principala poartă de acces în rețea, adică pe gateway, se configurează un **firewall**. Acest gen de protecție este foarte bun pentru securitate, însă foarte prost pentru business<sup>9</sup>. Astfel apare necesitatea existenței unei zone demilitarizate - DMZ.

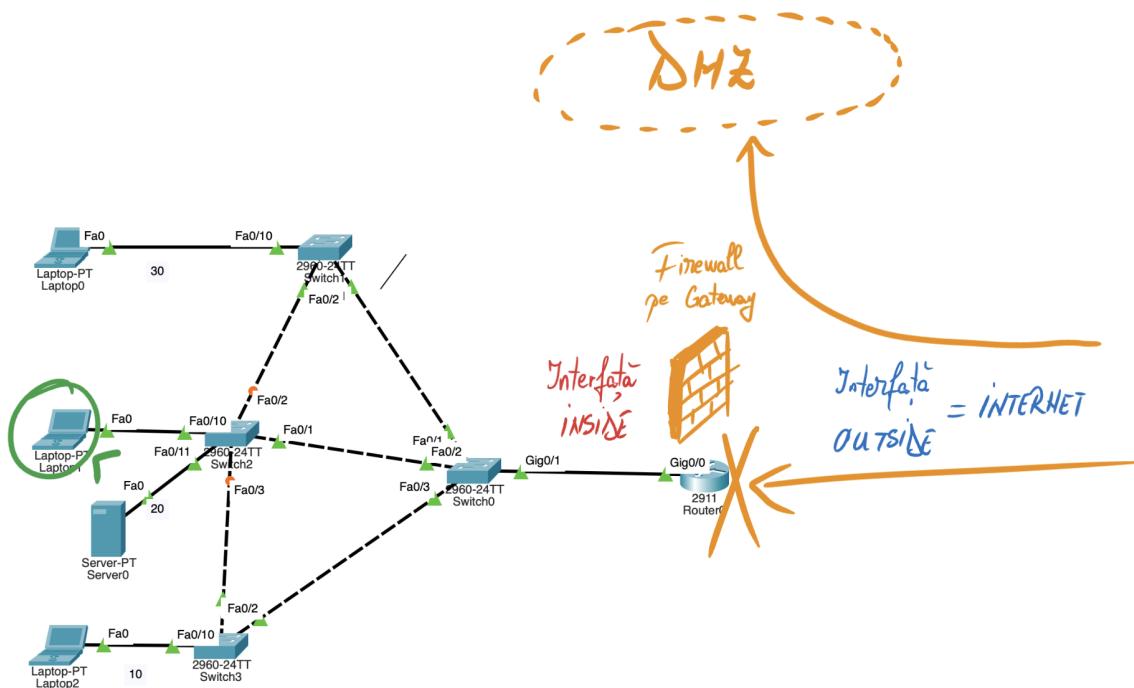


Figura 26: Requestul inițiat din exterior este blocat de către firewall-ul rețelei

<sup>9</sup>De exemplu un server de mail poate exista aici, aşa încât atunci când angajatul este acasă (home office), să poată să citească

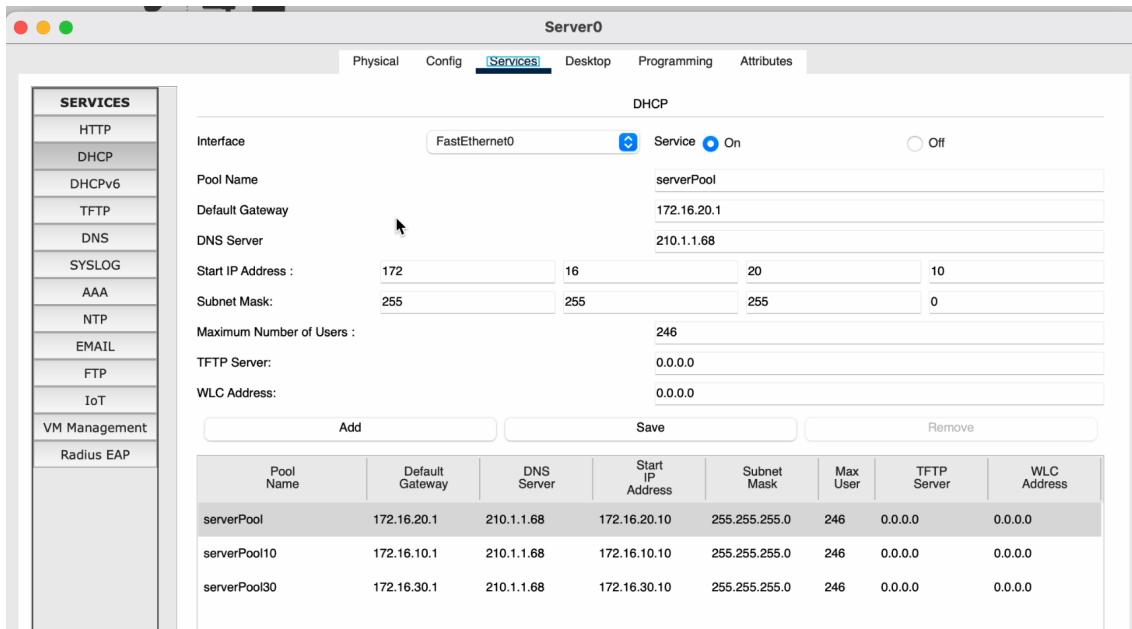


Figura 27: Pe serverul de DHCP se actualizează adresa DNS server pentru fiecare pool, acum fiind cunoscută

### 3 Etapa 3 - Configurarea serviciilor din zona demilitarizată. Conectarea remote prin SSH

#### 3.1 Layout

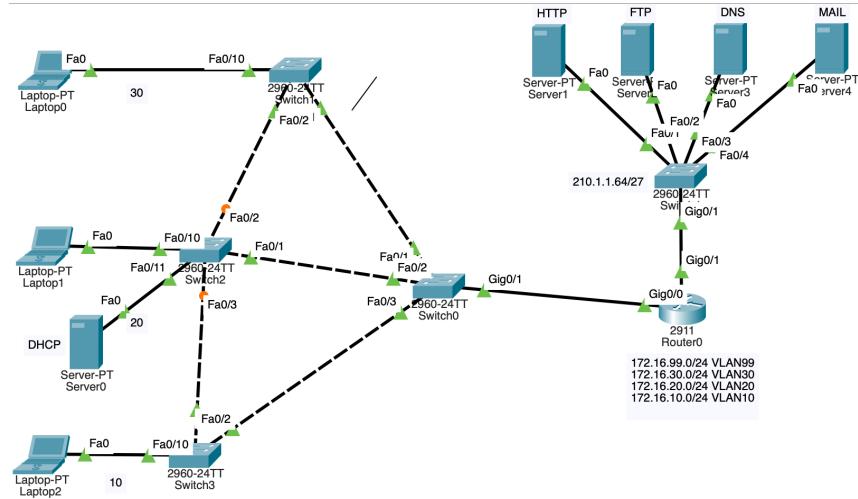


Figura 28: La finalul configurațiilor, serverele sunt mapate în servicii de DNS și accesibile prin numele de domeniu.

#### 3.2 Comenzi

##### FTP

Pentru a crea un nou fișier pe o mașină locală și a-l urca pe FTP server, procedura este următoarea:

1. se accesează Laptop1, Desktop, Text editor

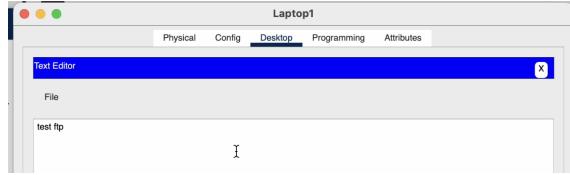


Figura 29: Editorul de text de pe Laptopul aferent primului etaj

2. Serverul de FTP este configurat aşa încât să poată fi accesat de la distanţă, în serverul DNS fiind făcută maparea între domeniul și adresa IP alocată. Laptop1, Desktop, Command Prompt
3. C:\> `ftp <numele_domeniului>`, comandă care va cere un username și o parolă.

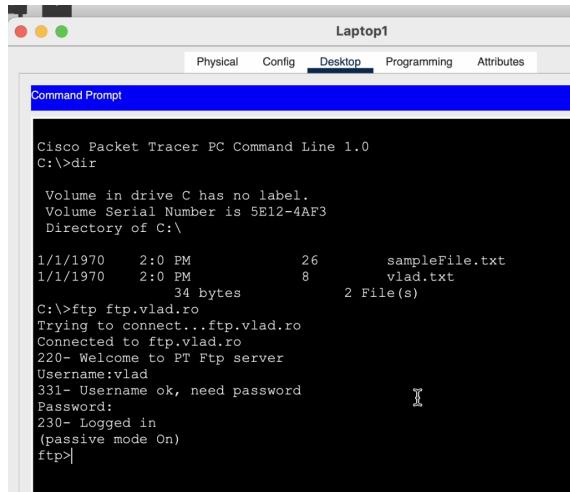


Figura 30: Autentificarea pe serverul de FTP pentru domeniul ftp.vlad.ro

4. `ftp> put <file.extension>`, ex: `ftp> put vlad.txt`

În același timp, pentru a obține un fișier de pe server pe mașina locală, comanda este:

```
ftp>get some_file.bin.
```

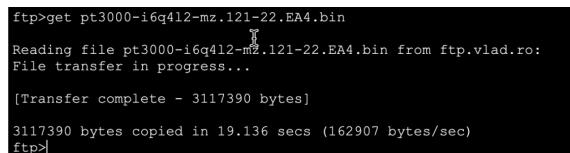


Figura 31: Obținerea unui fișier de pe serverul FTP

**Mail** Având userii creați pe serverul de mail (44), putem să testăm funcționalitatea transmiterii și primirii de mesaje tip email, respectând următorii pași:

1. accesarea mailului: Laptop, Desktop, Mail Browser (sau Email)
2. autentificarea cu credențiale la Mail server

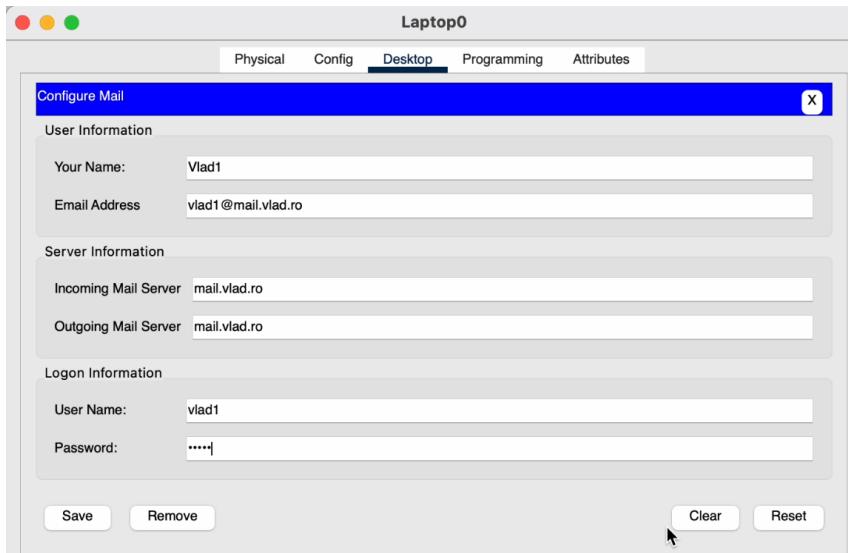


Figura 32: Laptopul 0 de pe etajul 2 se va loga folosind credențialele **vlad1**, parolă **vlad1**. A se remarcă formatul adresei de email, compus din user name, simbolul @ și adresa de domeniu

Pe laptopul 1 de pe etajul 1 se va efectua același procedeu, cu credențialele **vladbartolomei**, parolă **vladbartolomei**.

### 3. testarea serviciului prin trimiterea de mesaje de test

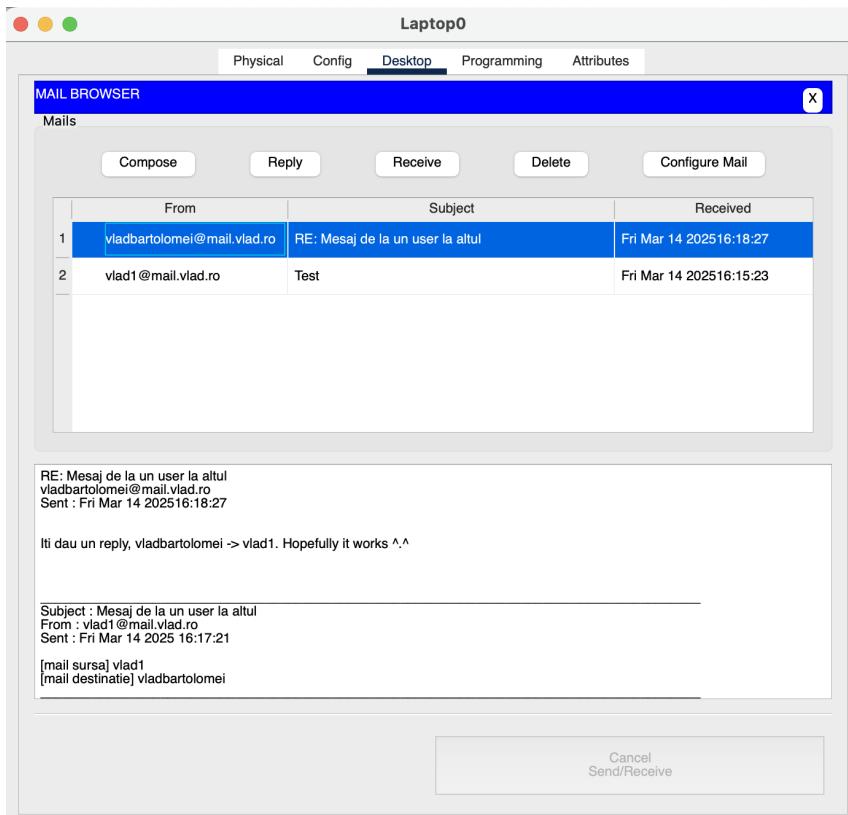


Figura 33: Schimb de mesaje între Laptop0 și Laptop1. În Packet Tracer, trebuie apăsat explicit butonul **Receive** pentru a aduce mesajele

```

Sending mail to adrian1@mail.adrian.ro , with subject : test .. Mail Server:
mail.adrian.ro
DNS resolving. Resolving name: mail.adrian.ro by querying to DNS Server:
210.1.1.68 DNS resolved ip address: 210.1.1.69
Send Success.

```

Figura 34: Un exemplu de mesaj din Packet Tracer când un mail este trimis la o anumită adresă

## SSH

```

SecondFloor>en
SecondFloor#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SecondFloor(config)#ip domain-name vlad.ro
SecondFloor(config)#crypto key generate rsa
The name for the keys will be: SecondFloor.vlad.ro
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 4096
% Generating 4096 bit RSA keys, keys will be non-exportable...[OK]

SecondFloor(config)#do show run

```

Figura 35: Comenzi pentru configurarea protocolului SSH (1)

Numele pentru cheie va fi: SecondFloor.vlad.ro

```

SecondFloor(config)#line vty 0 4
SecondFloor(config-line)#transport input ssh
SecondFloor(config-line)#login local

```

Figura 36: Comenzi pentru configurarea protocolului SSH (2)

Comanda `line vty 0 4` specifică câți useri se pot conecta deodată. În acest caz 5 useri. Un alt exemplu este `line vty 0 15`, care permite conectarea a 16 useri deodată.

```

SecondFloor(config)#enable ?
      password Assign the privileged level password
      secret   Assign the privileged level secret
SecondFloor(config)#enable secret vlad15

```

Figura 37: Setarea parolei secrete **vlad15**

## SSH cu AAA

Comenzi:

1. FirstFloor(config)#aaa new-model
2. FirstFloor(config)#aaa authentication login default group radius none
3. FirstFloor(config)#radius server Vlad - comandă pentru ca switch-ul să ştie de serverul Radius
4. FirstFloor(config-radius-server)#address ipv4 172.16.20.2 - adresa serverului DHCP
5. FirstFloor(config-radius-server)#key vlad15 - cheia de autentificare
6. FirstFloor(config-radius-server)#exit
7. FirstFloor(config)#line vty 0 4
8. FirstFloor(config)#transport input ssh - accept sesiuni ssh
9. FirstFloor(config)#login authentication default - autentificarea este default (nu mai e locală), cu serverul de radius de mai sus, a cărui adresă și cheie le-am specificat mai sus (pașii 3 și 4)

### 3.3 Memoriu tehnic

#### 3.3.1 Rezolvarea adresării serverelor prin DNS

Serviciile din DMZ (HTTP, FTP, DNS, Mail) sunt funcționale în acest stagiul. Ele pot fi accesate cunoscând **adresa IP** asignată, însă acest procedeu este neintuitiv pentru utilizator. Astfel că serverul de DNS va fi responsabil să mapeze adresele IP la domenii.

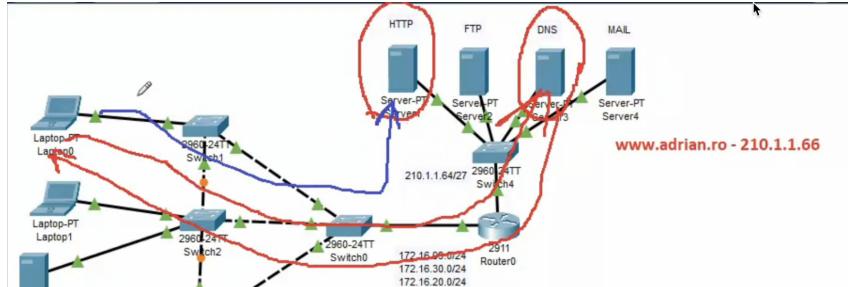


Figura 38: În cazul unui request de la laptop către serverul de HTTP, prima oară este apelat DNS server pentru a afla adresa serverului HTTP, este returnată către laptop (roșu); ulterior laptopul face requestul către adresa acum cunoscută (albastru).

În tabelul de mai jos notăm adresele IP și numele de domeniu echivalente care au fost decise. Domeniul comun pentru această infrastructură IT este **vlad.ro**, iar fiecare serviciu este referit prin adăugarea unui prefix (http, ftp, mail).

Serviciu	Numele de domeniu	Adresa IP
HTTP	www.vlad.ro	210.1.1.66
FTP	ftp.vlad.ro	210.1.1.67
MAIL	mail.vlad.ro	210.1.1.69
DNS	-	210.1.1.68

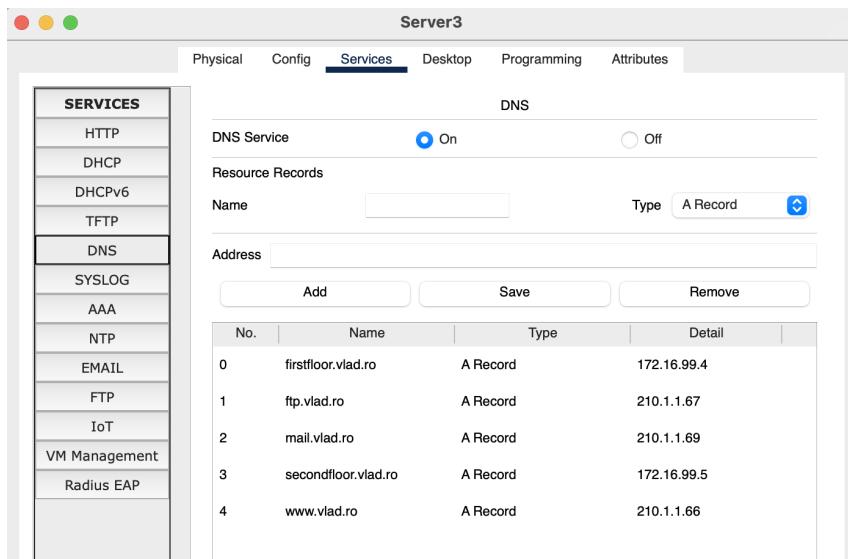


Figura 39: Tabela de mapare a serverului de DNS, asignată manual

După această configurare, toate serviciile sunt accesibile prin ping.

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping ftp.vlad.ro

Pinging 210.1.1.67 with 32 bytes of data:

Request timed out.
Reply from 210.1.1.67: bytes=32 time<1ms TTL=127
Reply from 210.1.1.67: bytes=32 time<1ms TTL=127
Reply from 210.1.1.67: bytes=32 time<1ms TTL=127

Ping statistics for 210.1.1.67:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>

```

Figura 40: Testarea mapării domeniilor din DNS prin ping la serverul de FTP

### HTTP

După ce ne-am asigurat că HTTP server este accesibil din terminal, vrem să testăm de pe client dacă putem să și vizualizăm pagina. Cisco Packet Tracer a configurat o pagină web default, care este accesibilă acum la [www.vlad.ro](http://www.vlad.ro).

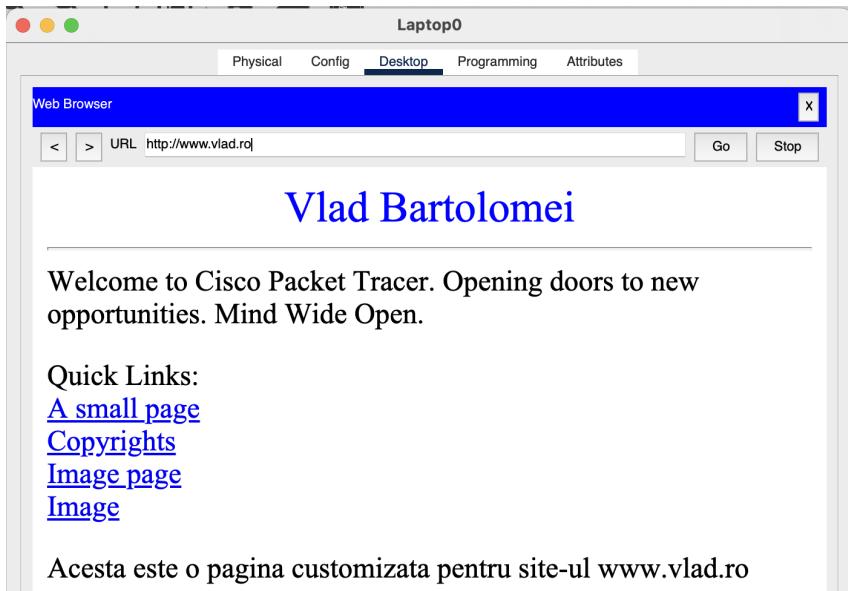


Figura 41: www.vlad.ro

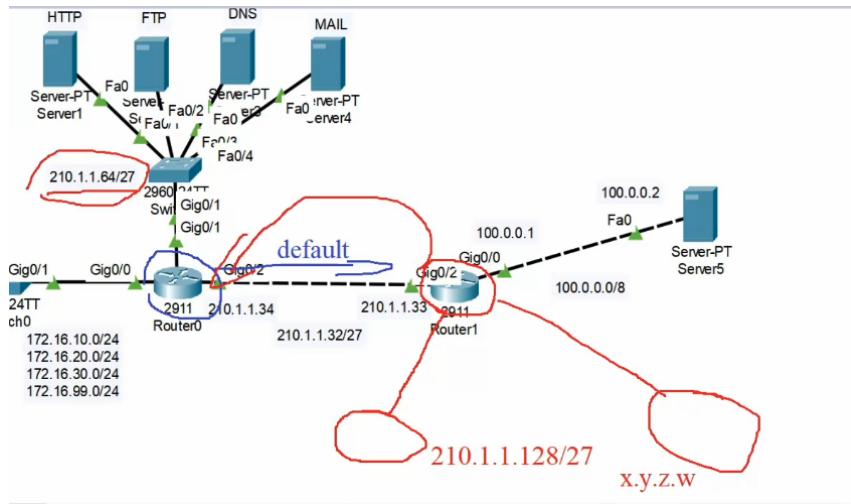


Figura 42: Serverul de HTTP ține fișierele necesare site-ului accesat. Butonul de edit permite configurarea aparenței site-ului

### FTP

Pe serverul de DNS configurăm un nou user *Vlad* cu toate permisiunile.

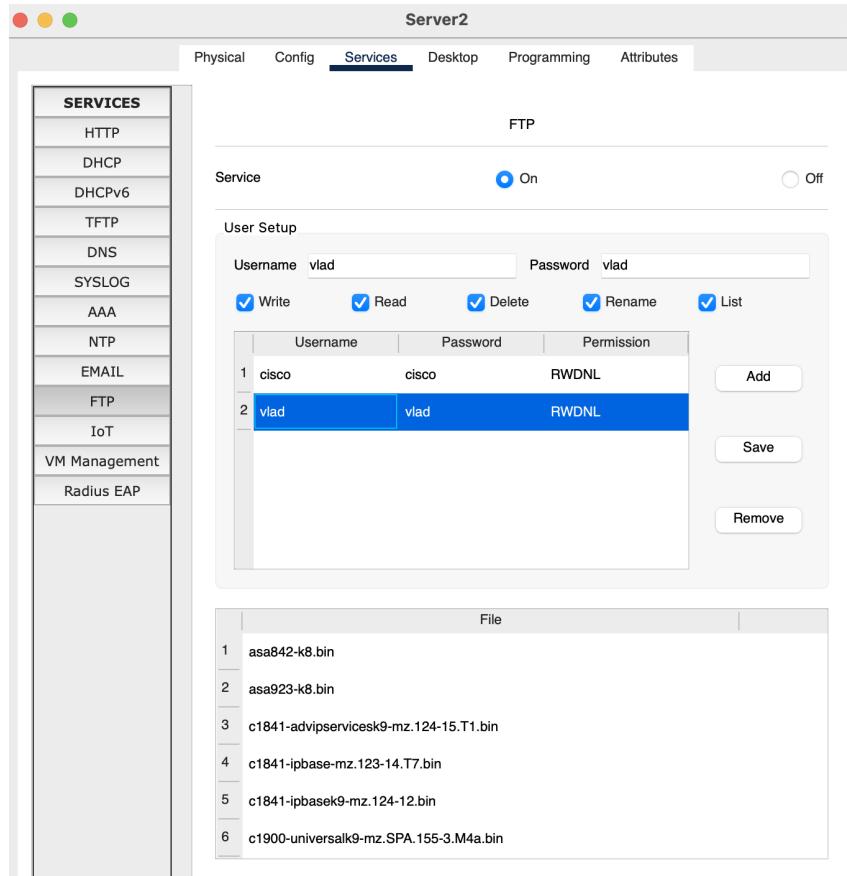


Figura 43: FTP server are deja niște fișiere by default (tab-ul de File). Sunt imagini pentru sistemul de operare

### Mail

Protocoloale care pot asigura un serviciu de mail sunt:

- perechea POP și IMAP - se ocupă de citirea mesajului:
  - IMAP aduce mesajul, lăsând o copie și pe server

- POP descarcă mesajul de pe server, ținând doar originalul pe mașina locală
  - SMTP - când eu transmit mesajul, se asigură că ajunge până în inboxul destinație.
- După ce am făcut mailul accesibil pe serviciul de DNS, creăm un utilizator nou pe Mail server:

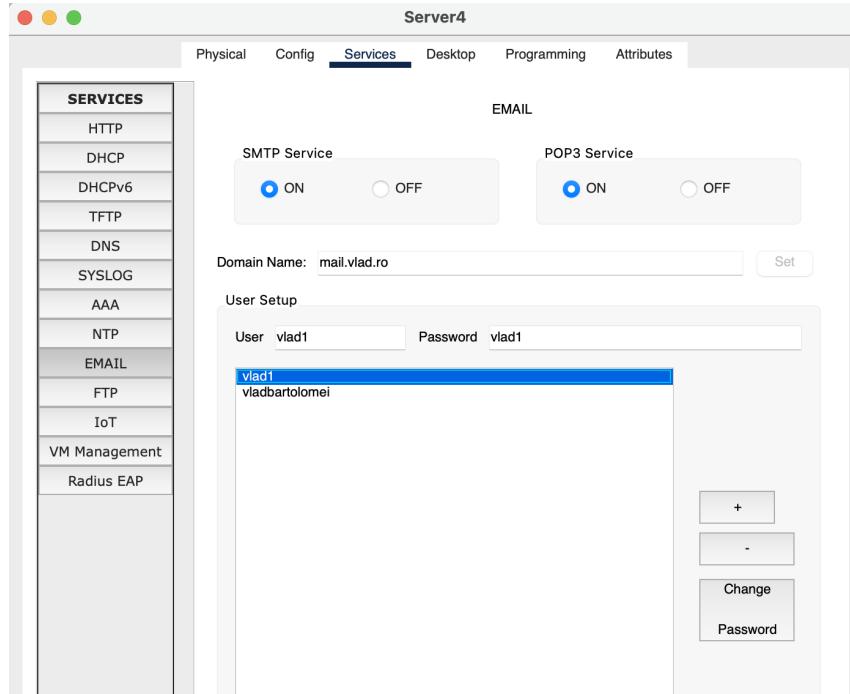


Figura 44: Serviciul de Mail pe serverul de Mail, cu cei doi utilizatori care vor exista la final, fiecare aferent câte unui laptop

### 3.3.2 Conectarea remote la switch-uri

Fiecare switch are integrat un aşa numit **port de consolă**, la care administratorul de retea se poate conecta cablat. Însă nu este o metodă foarte flexibilă. De aceea, una dintre cerințele proiectului este facilitarea conectării la distanță pe switch-uri, pentru configurare și menținere.

Pentru conectare remote se pot folosi două protocoale:

- telnet - este nesigur;
- ssh - protocol secured de conectare.

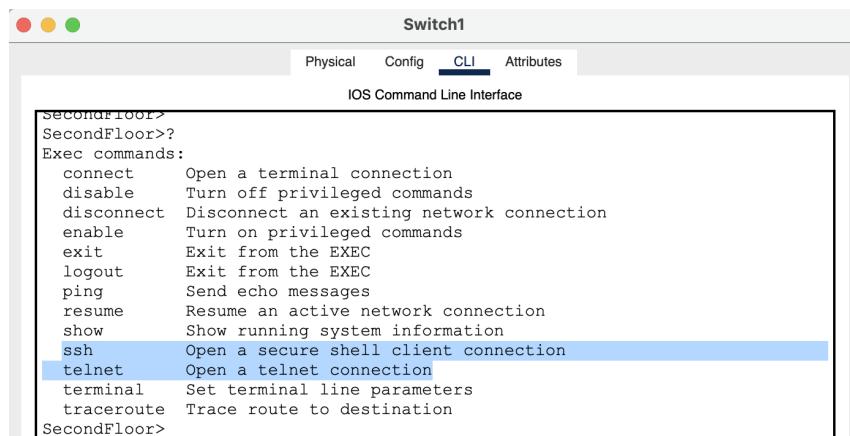


Figura 45: Rezultatul comenzi >? pusă pe terminalul unui switch prezintă cele două protocoale de conectare

Folosirea unei console de switch se face pe anumite *nivele* de acces. Depinzând de cât de mult a accesat utilizatorul, se acordă un nivel de privilegiu. Unele comenzi sau chiar unele parametri nu sunt accesibile la unele nivele.

```

SecondFloor>sh privilege
Current privilege level is 1

```

Figura 46: Nivelul de privilegiu 1 este foarte restrâns. Nu poți face multe nici ca user, nici ca admin. Prin activarea comenții >enable, privilege level crește la 15

Nu întotdeauna dorim ca cine accesează switch-ul să aibă drepturi deplinide de administrator. Un caz ar fi când o autoritate solicită un audit, iar noi ca administratori de sistem îi vom furniza niște credențiale de conectare de la distanță **cu drepturi restrânse**.

```

SecondFloor(config)#username vlad2 privilege 2 password vlad2
SecondFloor(config)#username vlad8 privilege 8 password vlad8

```

Figura 47: Crearea a două tipuri de useri cu privilegii diferite

## SSH

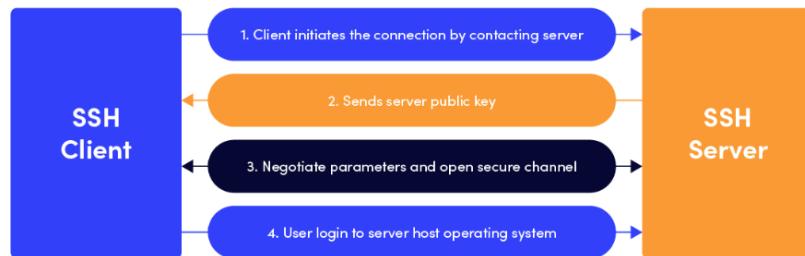


Figura 48: Funcționarea protocolului SSH. Sursă: [2]

Protocolul SSH implică negocierea unor parametri, și anume cheia secretă. SSH folosește o cheie pre-shared, prin urmare o criptare simetrică. La fiecare timeout bine determinat (de obicei la fiecare 3600 de secunde) are loc un schimb de mesaje între cele două stații – numere foarte mari – în urma căruia fiecare parte compune aceeași cheie secretă. Chiar dacă mesajele sunt interceptate, este prea puțin pentru a sparge cheia. Acest procedeu se numește Diffie-Hellman [1].

După configurări (vezi 35 și 36) un administrator se poate autentifica pe switch de la distanță folosind comanda

```

ssh -l <username> <desired_switch_address>,
unde switch-ul va fi mapat în serverul de DNS (vezi 40)
Exemplu: ssh -l vlad2 secondfloor.vlad.ro

```

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping www.vlad.ro

Pinging 210.1.1.66 with 32 bytes of data:

Request timed out.
Reply from 210.1.1.66: bytes=32 time=36ms TTL=127
Reply from 210.1.1.66: bytes=32 time<1ms TTL=127
Reply from 210.1.1.66: bytes=32 time<1ms TTL=127

Ping statistics for 210.1.1.66:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 36ms, Average = 12ms

C:\>ssh -l vlad2 secondfloor.vlad.ro

Trying 172.16.99.5 ...
Password:

SecondFloor#sh priv
Current privilege level is 2
SecondFloor#sh user
  Line      User      Host(s)          Idle      Location
  0 con 0    vlad2      idle           00:00:56
* 2 vty 0    vlad2      idle           00:00:00

  Interface   User          Mode      Idle      Peer Address
SecondFloor#enable
% No password set.
SecondFloor#enable
Password:
SecondFloor#sh priv
Current privilege level is 15

```

Figura 49: Conectarea cu user prin ssh îmi cere și o parolă. Comanda `show user` îmi listează toti userii, marcând cu \* userul logat

```

SecondFloor#enable
% No password set.
SecondFloor#

```

Figura 50: În acest moment parola nu este setată. Pentru configurare se vor urma comenziile din [37](#)

```

SecondFloor#enable
Password:
SecondFloor#sh priv
Current privilege level is 15

```

Figura 51: O nouă încercare de autentificare, de această dată cu parola setată

Până acum am definit un model de conectare prin SSH **local**. Însă autoritatea care solicită auditul din exemplul nostru nu se va autentifica local, ci de la distanță. Rezultă că pentru acest user este nevoie de un nou model de autentificare numit **AAA - Authentication, Authorization și Accounting**

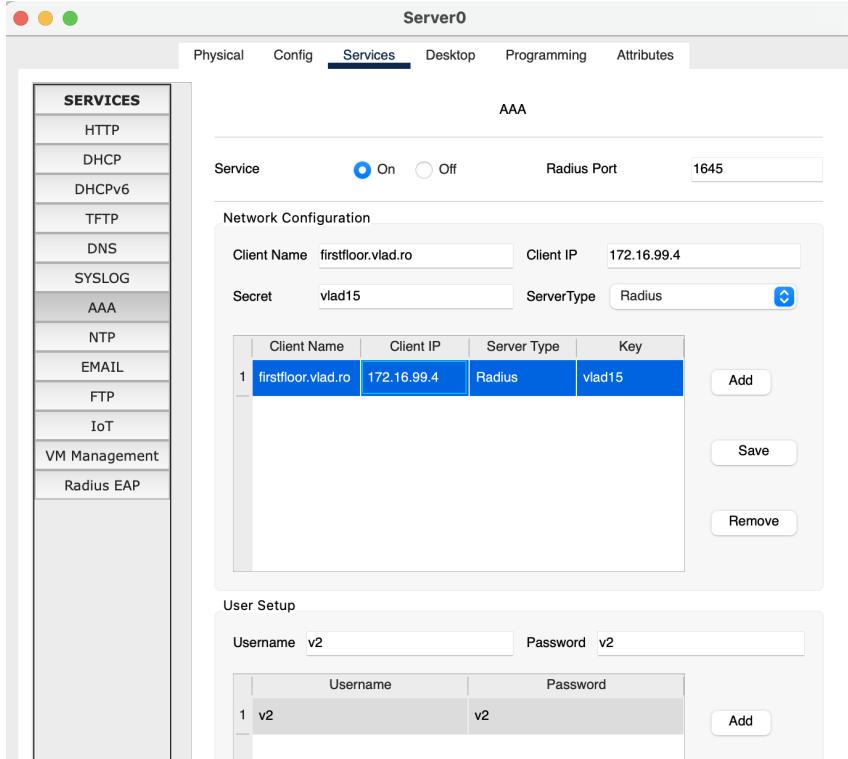


Figura 52: În urma configurațiilor (vezi Comenzi), serverul DHCP va juca și rol de server Radius; comanda de creare a unei conexiuni va fi `ssl -l v2 firstfloor.vlad.ro`

## 4 Etapa 4 - Ieșirea în Internet prin Network Address Translation (NAT)

### 4.1 Layout

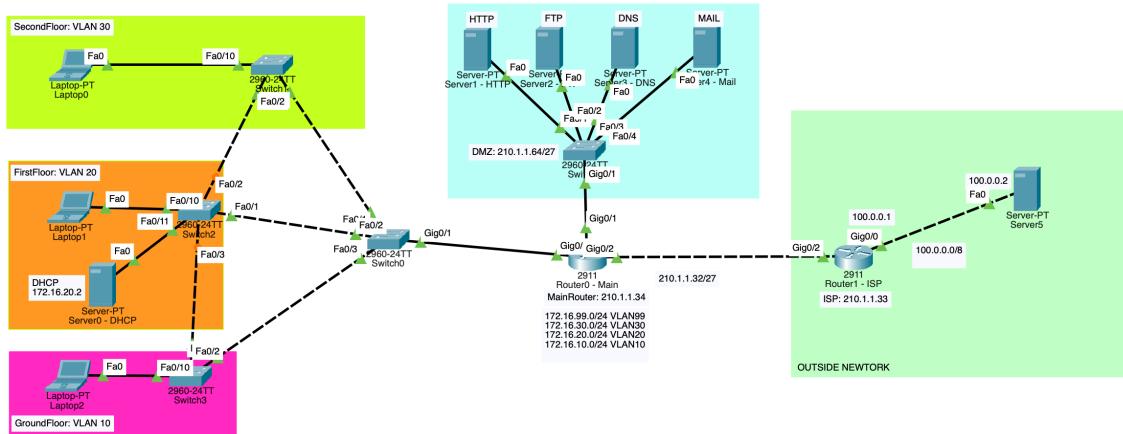


Figura 53: Configurarea infrastructurii rețelelor pentru clădirea pe trei etaje cu rețea privată, servicii publice în zona demilitarizată și acces la internet

## 4.2 Comenzi

### 4.2.1 Legătura punct-la-punct MainRouter-ISP

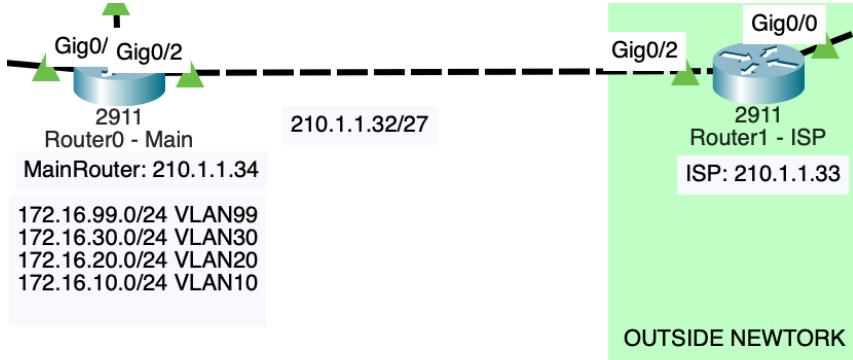


Figura 54: Ideea: cablarea routerului principal la routerul ISP pe interfețele corespunzătoare prin legătură **punct-la-punct** cu cablu cross-over, la adresele IP specificate în cerință

Pentru Routerul principal:

- MainRouter(config)# int gi 0/2
- MainRouter(config-if)# ip address 210.1.1.34 255.255.255.224
- MainRouter(config-if)# no shutdown

Pentru ISP:

- Router(config)#hostname ISP
- ISP(config)#int gi 0/2
- ISP(config-if)# ip add 210.1.1.33 255.255.255.224
- ISP(config-if)#no shutdown

Testarea se va face prin ping-uri la adresele ante-menționate.

### 4.2.2 Listele de acces

Sunt folosite pentru a identifica traficul

- MainRouter(config)#access-list ?  
<1-99> IP standard access list - necesară nouă, identifică traficul după adresa sursă  
<100-199> IP extended acecss list - se uită la IP sursă, IP dest, port sursă, port dest, și aproape orice câmp din headere  
O listă de acces este identificată ca o variabilă referită de un număr aflat într-unul dintre variabilele specificate
- MainRouter(config-if)#access-list 10 ?  
deny Specify packets to reject  
permit Specify packets to forward  
remark Access list entry comment
- MainRouter(config-if)#access-list 10 permit 172.16.0.0 0.0.255.255  
Permit orice pachet care are 172.16 la început de adresă. Aceasta comandă are nevoie de wildcard bits, adică masca inversată.
- MainRouter (config-if)#ip nat pool vlad 210.1.1.35 210.1.1.62 netmask 255.255.255.224
- MainRouter (config-if)#ip nat inside source list 10 pool vlad - translateaza adresele care încep cu 172.16.0.0 (potrivesc criteriilor din lista de acces 10) la adrese din pool-ul definit în comanda anterioară

#### 4.2.3 Translatarea interior-exterior

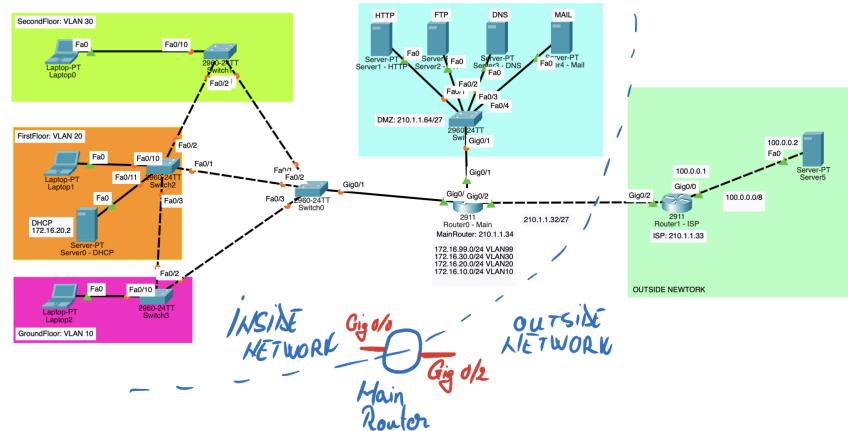


Figura 55: Translatarea adreselor se va face doar dacă ieșim din interior în exterior. În poză: interfețele corespunzătoare Inside și Outside

```

MainRouter(config)#int gi 0/0.10
MainRouter(config-subif)#ip nat inside
MainRouter(config-subif)#exit
MainRouter(config)#int gi 0/0.20
MainRouter(config-subif)#ip nat inside
MainRouter(config-subif)#exit
MainRouter(config)#int gi 0/0.30
MainRouter(config-subif)#ip nat inside
MainRouter(config-subif)#exit
MainRouter(config)#int gi 0/0.99
MainRouter(config-subif)#ip nat inside
MainRouter(config-subif)#exit
MainRouter(config)#int gi 0/2
MainRouter(config-if)#ip nat outside
MainRouter(config-if)#end
MainRouter#
%SYS-5-CONFIG_I: Configured from console by console

MainRouter#show ip nat tra
MainRouter#show ip nat translations
Pro Inside global      Inside local        Outside local        Outside
global
icmp 210.1.1.35:1    172.16.30.10:1    210.1.1.33:1    210.1.1.33:1
icmp 210.1.1.35:2    172.16.30.10:2    210.1.1.33:2    210.1.1.33:2
icmp 210.1.1.35:3    172.16.30.10:3    210.1.1.33:3    210.1.1.33:3
icmp 210.1.1.35:4    172.16.30.10:4    210.1.1.33:4    210.1.1.33:4

MainRouter#

```

Figura 56: Comenzile corespunzătoare translatării interior-exterior

#### 4.2.4 Configurarea rețelei Outside

Având routerul ISP adăugat, îi atașăm un server pe interfața Gig0/0 pentru a simula existența unei resurse accesibile public online.

```

ISP(config)#int gi 0/0
ISP(config-if)#ip add
ISP(config-if)#ip address 100.0.0.1 255.0.0.0
ISP(config-if)#no shut

ISP(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up

```

Figura 57: Adresa 100.0.0.1 pe Gig 0/0

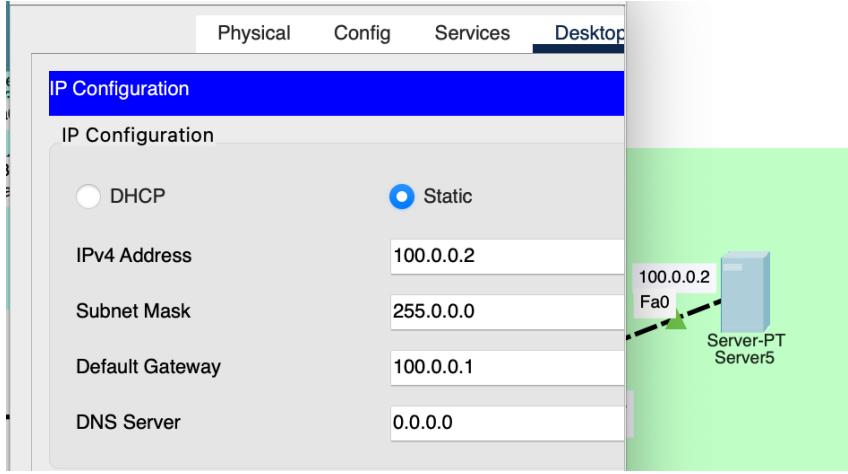


Figura 58: Așezare de adresă statică pentru server

#### 4.2.5 Rutarea de la Interior la Exterior

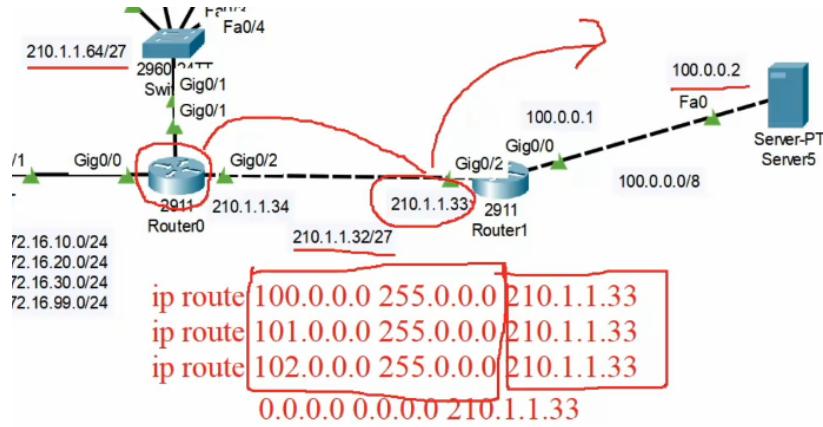


Figura 59: Internetul are mai multe rețele publice dorite, nu doar 100.0.0.0/8; de aceea comanda `route` care s-ar scrie pentru o rețea specifică e adaptată ca să meargă per general, punând placeholderul 0.0.0.0 (calculatorul făcând o potrivire/matching de adrese cu SI-logic)

Comandă: `ip route 0.0.0.0 0.0.0.0 - rută default.`

În celălalt sens al flow-ului de date, din exterior spre interior, situația stă diferit.

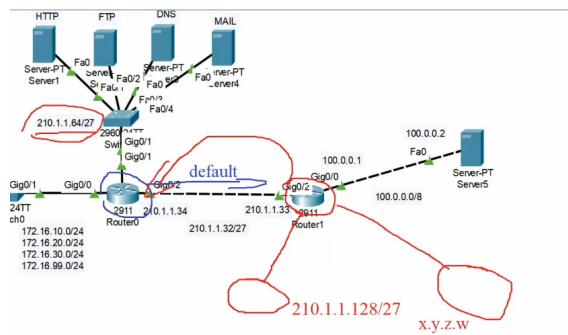


Figura 60: Un client exterior accesează serverul de mail al companiei mele (îi trimite un mail) în rețeaua 210.1.1.64. Asta înseamnă că, având această adresă destinație, routerul ISP trebuie să știe să ruteze datele către MainRouter (săgeata roșie) care știe ce să facă mai departe.

Comandă: `ip route 210.1.1.64 255.255.255.224 210.1.1.34 - rută default.`

```
MainRouter#sh ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
tcp 210.1.1.35:1025    172.16.30.10:1025  100.0.0.2:80      100.0.0.2:80
```

Figura 61: Testarea translatărilor se poate face folosind această comandă. Rapid, cât timp fluxul este încă în viață, comanda va afișa fluxurile existente

#### 4.2.6 Mapare statică NAT

Comandă: MainRouter (config)#ip nat inside source static tcp 172.16.20.2 80 210.1.1.34 80 - rutează orice request din exterior la adresa 172.16.20.2:80 dacă se lovește adresa routerului 210.1.1.34:80. Comandă ca să meargă și https: schimb portul 80 cu portul 443.

### 4.3 Memoriu tehnic

#### 4.3.1 NAT - Network Access Translation

Adresele folosite în internet sunt **publice** și **unice** pentru fiecare stație în parte. Însă spațiul de adrese al IPv4 este insuficient pentru a bifa aceste caracteristici.

Class	Activity Type	Activity Name
A	10.0.0.0 – 10.255.255.255	10.0.0.0/8
B	172.16.0.0 – 172.31.255.255	172.16.0.0/12
C	192.168.0.0 – 192.168.255.255	192.168.0.0/16

Figura 62: Fiecare clasă de adrese are un range de adrese private (cele afișate în rubrica Activity Type), pe care le folosim și acasă

Ieșirea în Internet a unei stații cu adresă IP privată se poate face în două feluri

- proxy
- NAT

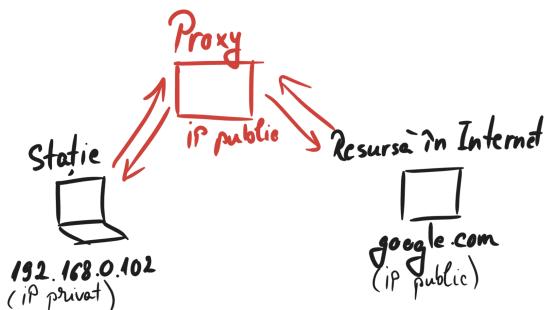


Figura 63: Prințipiul de funcționare al unui Proxy

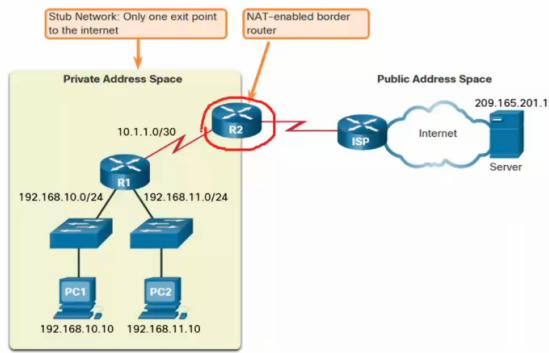


Figura 64: Ideea de la NAT: tehnologie folosită pe routerul de la granița retelei

Un tabel NAT conține 4 câmpuri, referitoare la adrese IP:

- inside local - adresa stației, privată
- inside global - adresa stației, publică, primită de la router prin NAT
- outside local - adresa stației/resursei din rețea externă (outside). Notă: poate avea doar adresă publică, deci coincide cu outside global
- outside global - adresa stației/resursei, publică

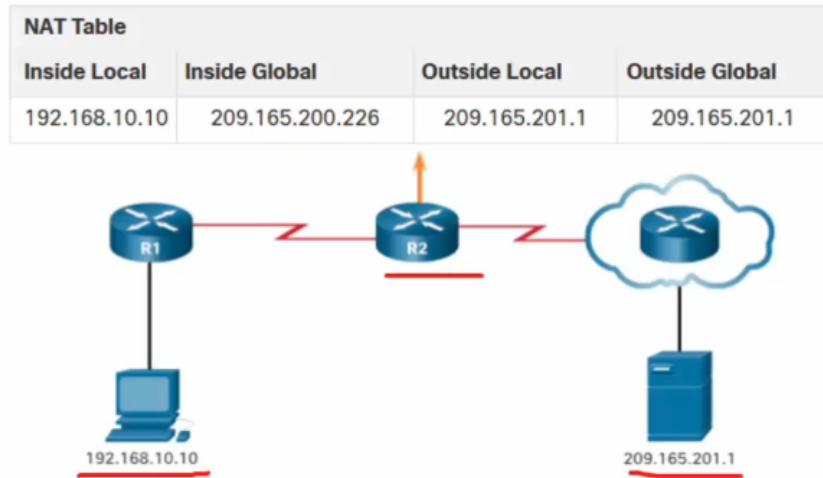


Figura 65: Un exemplu de translatare NAT

### Tipuri de NAT

- Static NAT
- Dynamic NAT

#### 4.1: Static NAT

- Use case: când se dorește accesarea din exterior a unei resurse din interior cunoscută doar ca adresă locală

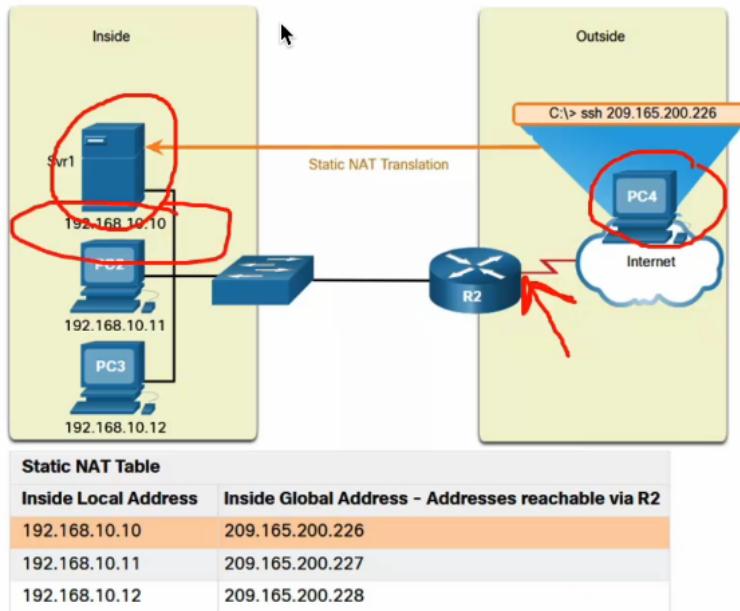


Figura 66: Situație de utilizare a Static NAT

- PC4 dorește să acceseze Server1, fără adresă publică. PC4 nu poate referenția din afara rețelei adresa 192.168.10.10 - locală
- Atunci va folosi o adresă publică din pool-ul de adrese, care rămâne constantă
- Sau chiar adresa routerului.
- Se face o mapare: în momentul în care adresa routerului este lovită, cu un port anume setat, se redirectează requestul către Server4, cel dorit. **Port forwarding**
- Nu mai vorbim de fluxuri, deoarece resursa trebuie să fie mereu available. Prin urmare, asignare statică

## 4.2: Dynamic NAT

- Folosește un pool de adrese publice și le asignează pe principiul Primul venit, primul servit.

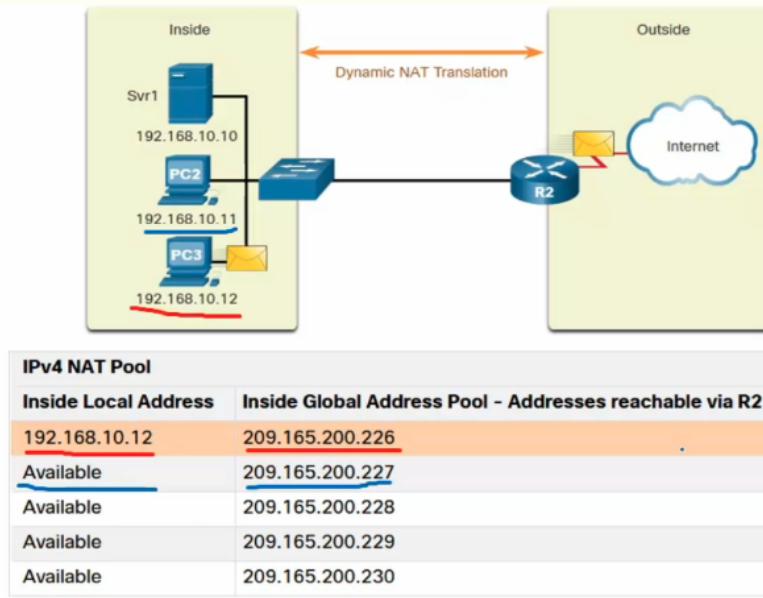


Figura 67: Device-urile primesc adrese pentru o perioadă limitată de timp

- Fluxul definește operațiile: se stabilește conexiunea, se transferă, se desființează conexiunea
- După o perioadă de inactivitate de la închiderea fluxului, slot-ul device-ului este eliberat și disponibil pentru a fi luat de un altul.
- **Problema:** trebuie să am suficiente fluxuri publice pentru a acoperi la un moment dat accesul spre Internet

NAT este înlocuit de PAT.

### 4.3.2 PAT - Port Address Translation

Scopul său este de a crește economia de adrese. Este cunoscut ca și *NAT overload* și reduce problema la nivel de porturi.

Pentru ca două stații să facă schimb de pachete (să comunice), ele folosesc un flux unic identificat de câmpurile:

- IP sursă
- IP destinație
- Port sursă
- Port destinație
- **Protocolul de nivel transport** - TCP, UDP

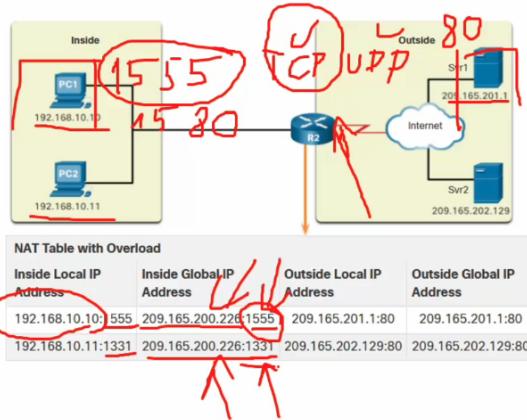


Figura 68: PAT explicitat. Două stații diferite comunică în internet. Pentru o economie mai mare de adrese, ele primesc același IP (care poate fi fix **gateway-ului**). Sansa ca cele două stații să primească același port la un moment este foarte mică (din intervalul 1025-aproximativ 65000)

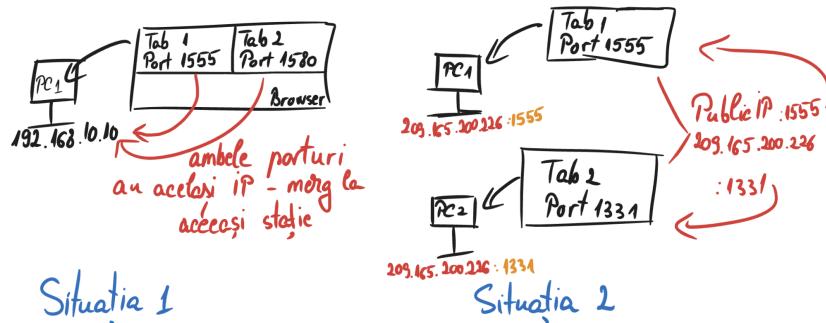


Figura 69: Situația 1: o statie cu două procese pornite; Situația 2: două stații cu câte un proces pornit primesc același IP. Portul determină IP-ul local către se face translatarea

#### 4.3: Next Available Port

Situația în care două stații aleg același port nu este absolut exclusă. Prin PAT se însearcă menținerea portului original sursă. Dacă portul original este deja folosit (principiul primul venit, primul servit), se va aloca următorul port disponibil. Dacă nu mai sunt porturi disponibile, dar mai există adrese publice libere în pool, se merge pe următoarea adresă.

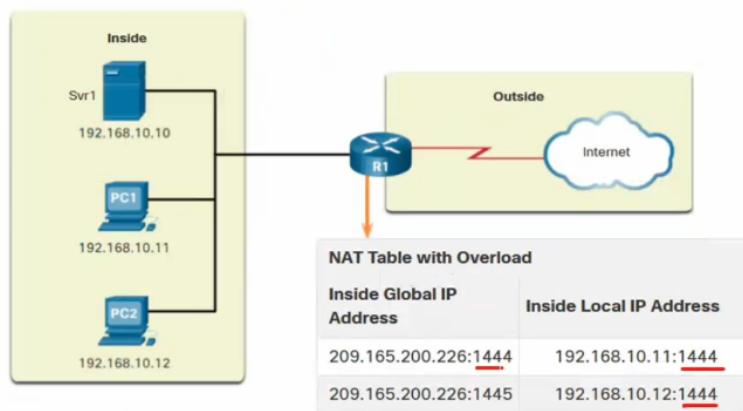


Figura 70: Next Available Address

## 5 Etapa 5 - Securizarea suplimentară a echipamentelor

### 5.1 Memoriu tehnic

#### 5.1.1 Protejarea Switch-urilor

##### Cum funcționează un switch

Un switch este un dispozitiv de rețea care operează la nivelul 2 (data link) al modelului OSI. Funcționarea sa de bază include:

- Tabelul MAC (MAC Address Table) - Switch-ul memorează adresele MAC ale dispozitivelor conectate la fiecare port în acest tabel
- Învățare (Learning) - Când un pachet sosește pe un port, switch-ul înregistrează adresa MAC sursă și portul asociat
- Înaintare (Forwarding) - Switch-ul trimite pachetele doar către portul specific unde este conectat destinatarul, nu către toate porturile
- Filtrare (Filtering) - Pachetele sunt trimise doar către portul destinație corect, reducând traficul inutl

##### Atacul MAC Overflow

Un atac MAC overflow (sau MAC flooding) funcționează astfel:

1. Atacatorul trimite rapid un mare număr de pachete cu adrese MAC sursă falsificate, rapid schimbate către switch. Pentru aceasta se poate folosi un tool de genul **MacOF**
2. Switch-ul este obligat să învețe toate adresele MAC care vin pe portul atacat (Fa0/10 în figura 71). Astfel că tabelul MAC al switch-ului se umple complet cu aceste adrese false
3. Când tabelul atinge capacitatea maximă, switch-ul poate:
  - Să eliminate cele mai vechi înregistrări pentru a face loc celor noi
  - Să intre în modul "fail-open" - se comportă ca un hub, trimițând traficul pe toate porturile

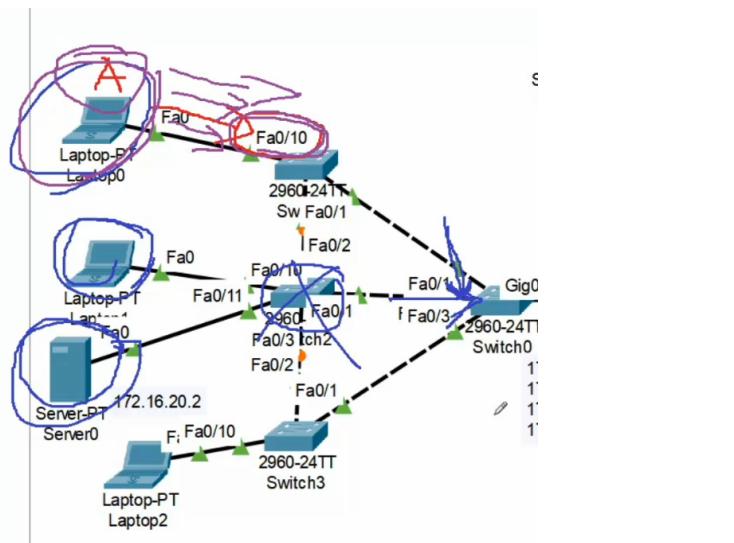


Figura 71: Atac MACOF

Modul Fail-open se traduce prin faptul că switch-ul nu mai știe cui să trimită pachetele, și atunci le aruncă în toate direcțiile, rezultând un atac de tip Denial of Service în primă fază. Însă ulterior, cadrele care ajung de la celelalte stații la switch-ul afectat sunt rearuncate în rețea și ajung și la atacator. De aici atacatorul poate porni un sniffer și recunoaște traficul (atac de recunoaștere), ceea ce poate conduce la un atac de tip acces.

Pe scurt, consecințele includ:

- Switch-ul devine inefficient (asemenea unui Hub)
- Traficul poate fi interceptat de atacator (sniffing)
- Posibile intreruperi de serviciu

**Rezolvare** Switch-ul care trebuie protejat ar trebui să poată învăța un număr limitat de comenzi, peste care să închidă conexiunea. Așadar, vom presupune că un singur calculator (deci un singur MAC) se poate conecta la switch pe interfața Fa0/10<sup>10</sup>.

### 5.1: Comenzi

1. GroundFloor>enable
2. GroundFloor#configure terminal
3. GroundFloor(config)#interface FastEthernet 0/10<sup>a</sup>
4. GroundFloor(config-if)#switchport port-security - activează securitatea pe port
5. GroundFloor(config-if)#switchport port-security maximum 1 - permite învățarea unei singure adrese MAC
6. GroundFloor(config-if)#switchport port-security violation shutdown - în caz de încărcare a politicii switch-ul se oprește (shutdown) și nu mai funcționează în rețea
7. save la fisierul de packet tracer

<sup>a</sup>Important: această interfață trebuie să fie configurată să ruleze în VLAN (în cazul de față VLAN 10) conform cerințelor proiectului. Altfel nu va funcționa în rețea

O simplă testare a eficacității acestei comenzi este schimbarea adresei MAC a laptopului în mod curent conectat pe Fa0/10:

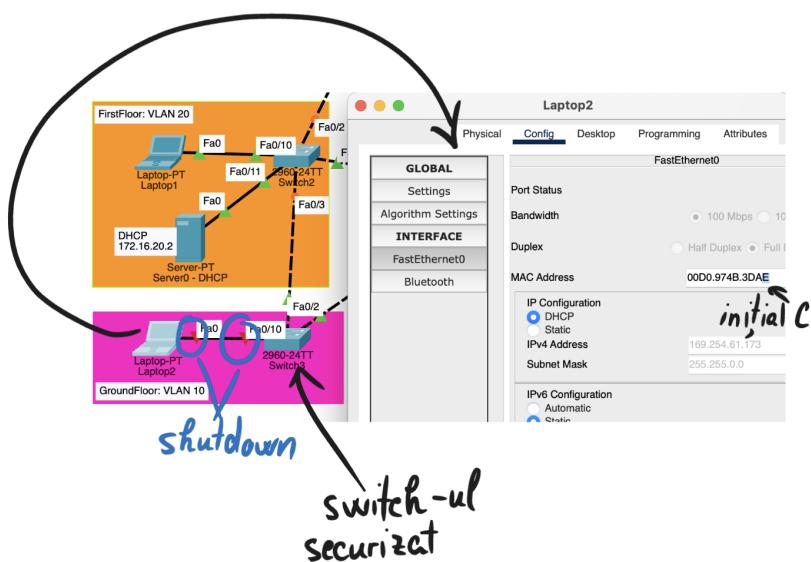


Figura 72: Un singur Bit este suficient să fie alterat, pentru a se activa politica de protecție

#### 5.1.2 Liste de acces extinse pe routerul principal

Zona DMZ a companiei trebuie să fie accesibilă diferiților utilizatori, însă transparența nu ar trebui să fie totală. Un atacator nu ar trebui să afle rețeaua printr-un singur ping.

Astfel că se impune filtrarea traficului. Metoda la care vom apela este Lista de acces extinsă (Extended ACL), configurată pe MainRouter. Această ACL poate permite, refuza sau remarca

<sup>10</sup>Switch-urile se protejează separat pe interfețe

traficul de la o anumită adresă sursă la o anumită adresă destinație<sup>11</sup> în mod standard, iar în mod extended putem adăuga detalii pe filtrare: Port sursă, port destinație, protocol folosit.

Ne dorim următoarele:

- a. Accesul la site-ul companiei - acces la serverul HTTP (210.1.1.66) pe protocolele HTTP și HTTPS
- b. Acces la serverul de FTP (210.1.1.67)
- c. Acces la serviciul de Mail (210.1.1.69), pentru a putea trimite și recepta mailuri la și de la companie
- d. Acces la serverul de DNS (210.1.1.68), pentru a putea rezolva mapările nume de domeniu – adresă ip.

Procesul de securizare prin ACL constă în două etape:

1. Definirea Extended ACL pe MainRouter, în modul *configure terminal*
2. Activarea listei de acces pe interfața dorită. Ne dorim să protejăm zona DMZ, așa că ne vom referi la interfața GigabitEthernet 0/1, cu sensul OUT<sup>12</sup>

Semnătura comenzii este: `access-list <identifier> <permit/deny/remark> <protocol> <ip sursă> <ip destinație> <wildcard bits> <eq (portul este)> <număr port>`.

## 5.2: Comenzi

1. `MainRouter>enable`
2. `MainRouter#configure terminal`
3. HTTP Server:  
`MainRouter(config)#access-list 101 permit tcp any 210.1.1.66 0.0.0.0 eq 80`  
`MainRouter(config)#access-list 101 permit tcp any 210.1.1.66 0.0.0.0 eq 443`
4. FTP Server:  
`MainRouter(config)#access-list 101 permit tcp any 210.1.1.67 0.0.0.0 eq ftp`
5. Mail:  
`MainRouter(config)#access-list 101 permit tcp any 210.1.1.69 0.0.0.0 eq smtp`  
`MainRouter(config)#access-list 101 permit tcp any 210.1.1.69 0.0.0.0 eq pop3`  
`MainRouter(config)#access-list 101 permit tcp any 210.1.1.69 0.0.0.0 eq 143 - portul pentru IMAP`
6. DNS Resolver:  
`MainRouter(config)#access-list 101 permit udp any 210.1.1.68 0.0.0.0 eq 53`
7. `MainRouter(config)#interface GigabitEthernet 0/1`
8. `MainRouter(config-if)#ip access-group 101 out`
9. save la fișierul de packet tracer

Notă: comanda `access-list` dă by default deny la celelalte adrese (deny ip any any).

<sup>11</sup>putem vorbi de range-uri de adrese

<sup>12</sup>Sensurile IN și OUT ale traficului trebuie privite din punctul de vedere al routerului. Pachetele pot intra/ieși din router

```

! interface GigabitEthernet0/1
  ip address 210.1.1.65 255.255.255.224
  ip access-group 101 out
  duplex auto
  speed auto
!
```

Figura 73: Comanda do show running-config confirmă că pe interfața Gi0/1 este activ access-group-ul identificat de id-ul 101

```

MainRouter(config)#do sh acc
Standard IP access list 10
  10 permit 172.16.0.0 0.0.255.255
Extended IP access list 101
  10 permit icmp any any
  20 permit tcp any host 210.1.1.69 eq smtp
  30 permit tcp any host 210.1.1.69 eq pop3
  40 permit tcp any host 210.1.1.69 eq 143
  50 permit tcp any host 210.1.1.66 eq www (6 match(es))
  60 permit udp any host 210.1.1.68 eq domain (4 match(es))
  70 permit tcp any host 210.1.1.66 eq 443 (7 match(es))
  80 permit tcp any host 210.1.1.67 eq ftp (8 match(es))
```

Figura 74: Comanda do show access-list listează toate ACL definite

Pentru testare se va accesa de pe orice mașină domeniul www.vlad.ro sau 210.1.1.66 cu Http(s), se va încerca transmisia (SMTP) și receptia (POP3) de mailuri și se va încerca conectarea prin command prompt la serverul de ftp cu comanda ftp 210.1.1.67.

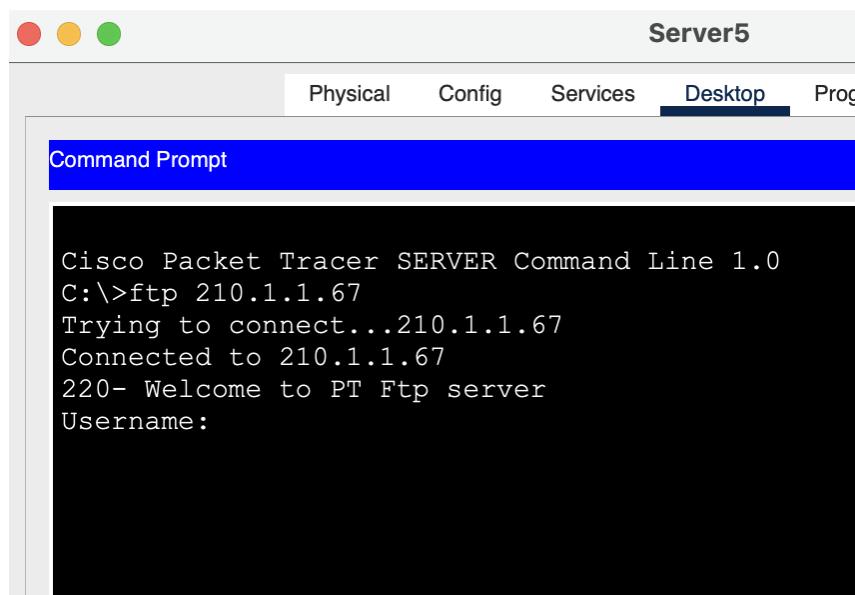


Figura 75: Conectarea cu ftp 210.1.1.67