**FACULTATEA DE AUTOMATICĂ ŞI CALCULATOARE**

**DEPARTAMENTUL CALCULATOARE**

****

**Proiect protocoale si retele de comunicatii**

**Student:** Szekely Gergo

**Grupa:** 30244

**Specializarea:** Calculatoare

**Profesor:** Prof. Bogdan Iancu

# Cerinta:

Se considera o cladire comerciala cu 3 nivele. Se va folosi adresa de retea 172.16.0.0/16 pentru reteaua intranet, adresa de retea 210.1.1.64/27 pentru DMZ si adresa de retea 210.1.1.32/27 pentru accesul in exterior. Se vor proiecta 4 VLAN-uri (unul pentru fiecare etaj si unul pentru traficul de management). Pentru configurarea VLAN-urilor se va folosi protocolul VTP. Prin cablarea si configurarea retelei se va asigura redundanta. Adresele hosturilor vor fi alocate dinamic folosind un singur server de DHCP aflat in VLAN-ul corespunzator primului etaj. Numarul minim de utilizatori deserviti de catre fiecare VLAN este 200. Serverele de HTTP, FTP, DNS si MAIL vor fi plasate in DMZ si vor avea adrese publice. Numele domeniului web va include numele studentului. Pentru asigurarea conectivitatii se vor configura rute statice. Accesul in exterior se va realiza folosind NAT pe routerul care controleaza DMZ, pe urmatorul interval de adrese publice: 210.1.1.35-210.1.1.62.

Conectarea la ISP se va realiza printr-o interfata de tip Ethernet avand adresa 210.1.1.34/27. Adresa ISP-ului este 210.1.1.33/27. Reteaua Internet se va simula prin intermediul unui server si a unui calculator.

Pentru securizarea echipamentelor de retea se vor realiza urmatoarele configurari: 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 si implementa doua masuri suplimentare de securizare a retelei.

Nu am facut *prezentarea si implementarea a doua masuri suplimentare de securizare a retelei*

Cuprins

[Cerinta: 2](#_Toc195171049)

[Topologia retelei: 4](#_Toc195171050)

[Subnetare: 4](#_Toc195171051)

[Configurare VLAN/VTP: 5](#_Toc195171052)

[Configurare Subretele 8](#_Toc195171053)

[Configurare DHCP 9](#_Toc195171054)

[Configurare NAT 12](#_Toc195171055)

[Configurare DMZ 14](#_Toc195171056)

[Serverul DNS: 15](#_Toc195171057)

[Pagina de HTTP: 16](#_Toc195171058)

[Serverul de FTP 17](#_Toc195171059)

[Serverul EMAIL 18](#_Toc195171060)

[Securitate 19](#_Toc195171061)

[Securitate SHH 20](#_Toc195171062)

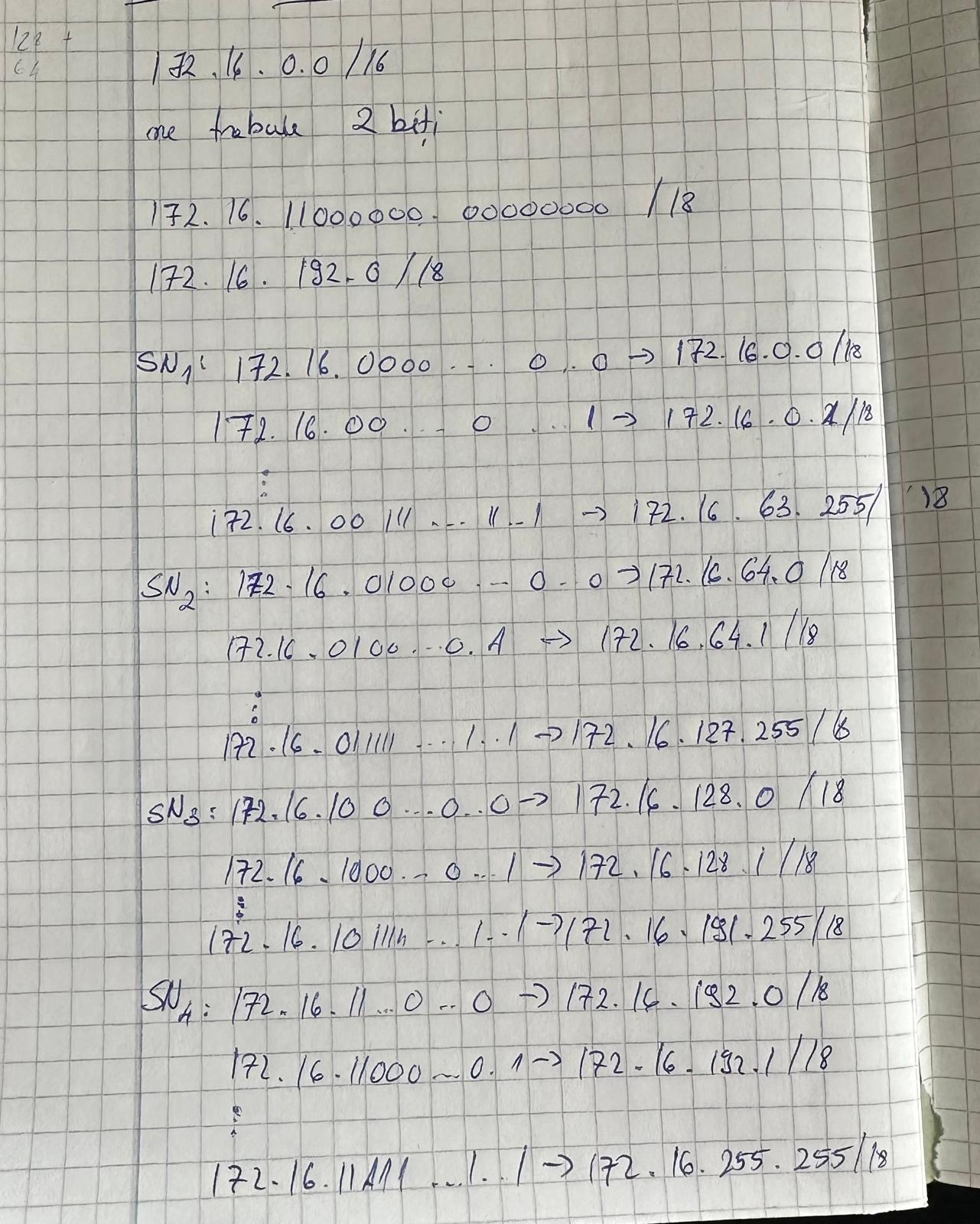
[Admin/Management 21](#_Toc195171063)

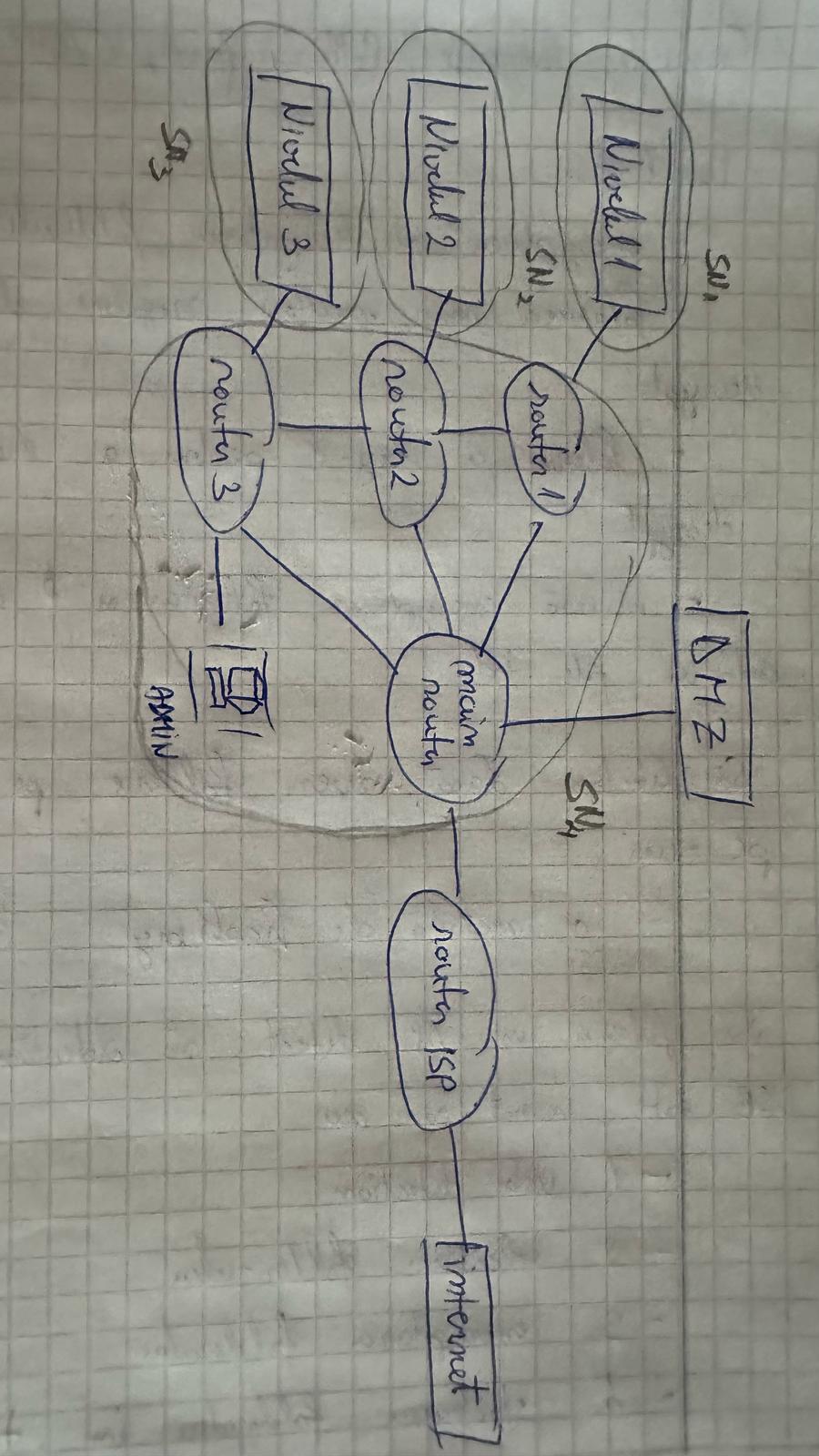
[Reteaua externa (Internet) 22](#_Toc195171064)

## Topologia retelei:

Avem o topologie de tip stea extinsa, cu multiple conexiuni redundante, asigurand astfel ca, in cazul unei defectiuni a unei legaturi, exista rute alternative de backup pentru mentinerea conectivitatii. Reteaua este o retea de switch-uri, iar iesirea spre internet este asigurata printr-un router

## Subnetare:





| **VLAN** | **Subnet (/18)** | **Interval IP utilizabile** |
| --- | --- | --- |

|  |  |  |
| --- | --- | --- |
| *VLAN 1 (Etaj 1)* | *172.16.0.0/18* | *172.16.0.1 - 172.16.63.254* |

|  |  |  |
| --- | --- | --- |
| *VLAN 2 (Etaj 2)* | *172.16.64.0/18* | *172.16.64.1 - 172.16.127.254* |

|  |  |  |
| --- | --- | --- |
| *VLAN 3 (Etaj 3)* | *172.16.128.0/18* | *172.16.128.1 - 172.16.191.254* |

|  |  |  |
| --- | --- | --- |
| *VLAN 4 (Management)* | *172.16.192.0/18* | *172.16.192.1 - 172.16.255.254* |

*DMZ 210.1.1.64/27 210.1.1.65 - 210.1.1.94  
SPI 210.1.1.32/27 210.1.1.33 -* *210.1.1.34  
NAT 210.1.1.35 -* *210.1.1.62*

## Configurare VLAN/VTP:

Exista trei VLAN-uri pentru utilizatori (VLAN 9, VLAN 19, VLAN 29) si un VLAN dedicat traficului de management (VLAN 999), pentru a separa traficul de management si monitorizare de traficul utilizatorilor. Am configurat porturile de tip trunk intre switch-uri si intre switch si router, pentru a permite transportul tuturor VLAN-urilor necesare.

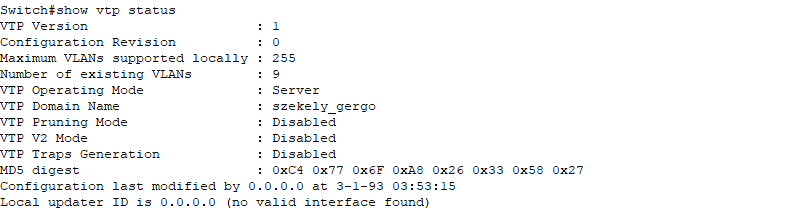
Am configurat VLAN-urile folosind protocolul VTP (Vlan Trunking Protocol), stabilind un domeniu comun pentru toate switch-urile și o parolă unică pentru autentificarea acestora între ele. Astfel, proiectul nostru poate fi extins cu usurinta, daca este necesar.  
Dintre cele patru switch-uri, am ales switch-ul 3 sa functioneze ca server, unde am definit cele patru VLAN-uri mentionate mai sus, folosind urmatoarele comenzi prezentate mai jos:

*#vtp domain szekely\_gergo*

*#vtp mode server*

*#vtp password alma1234*

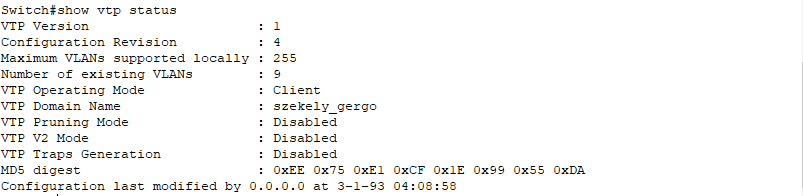
pentru a ma asigura am folosit comanda:  
# *show vtp status*



Am executat aceleasi comenzi si pentru switch-urile 0, 1 si 2, doar ca acum ele se comporta ca si clienti:

*#vtp domain szekely\_gergo*

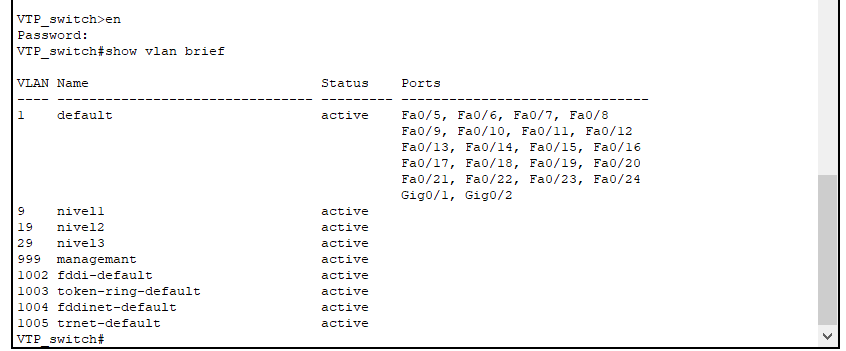
*#vtp password alma1234*

*#vtp mode client*  


Pentru crearea vlan-urilor vlan 9(nivel1), vlan 19(nivel2), vlan 29(nivel3) si vlan 999(management) am folosit urmatorele comenzi:

*# configure terminal  
#vlan 9  
#name nivel1  
#exit*

Cu comanda *#show vlan brief* putem vedea vlan-urile create pe switch:

  
Am setat VLAN-urile potrivite pentru switch-uri, am dat click pe switch, am selectat config, apoi am ales portul la care doream sa fac asignarea. L-am pus in modul acces si am selectat VLAN-ul corespunzator. Aceste setari pot fi realizate si din cod, si din terminal, folosind urmatoarele comenzi:

* Pentru *switch0*:

*#configure terminal*

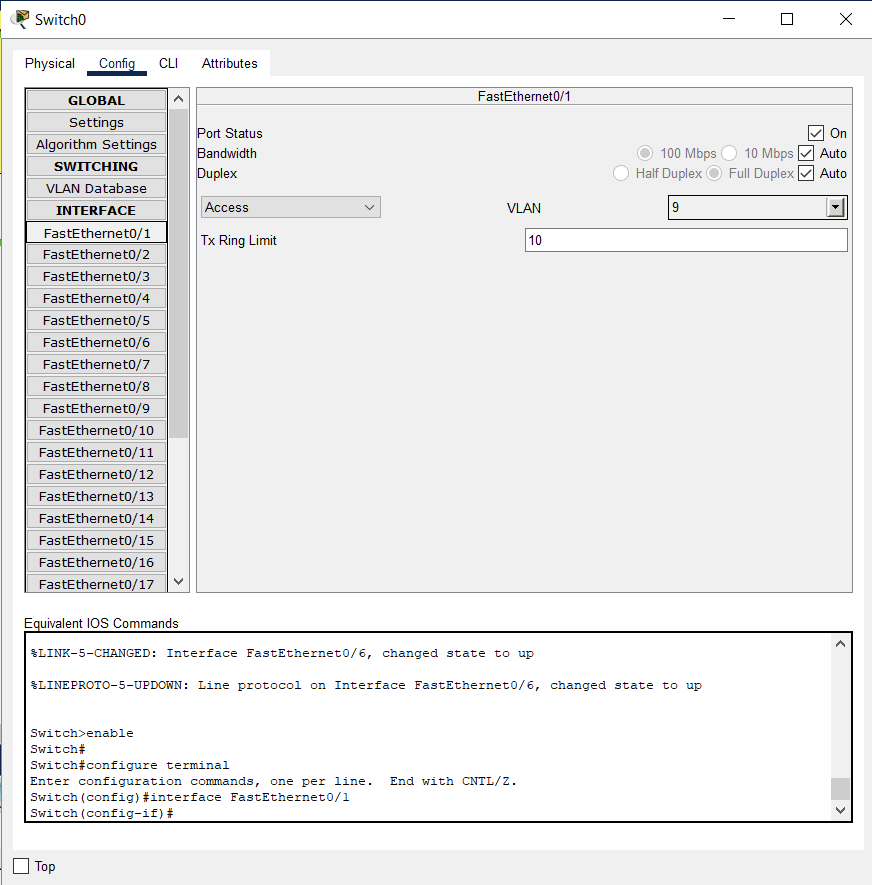
*#interface range fastEthernet 0/1*

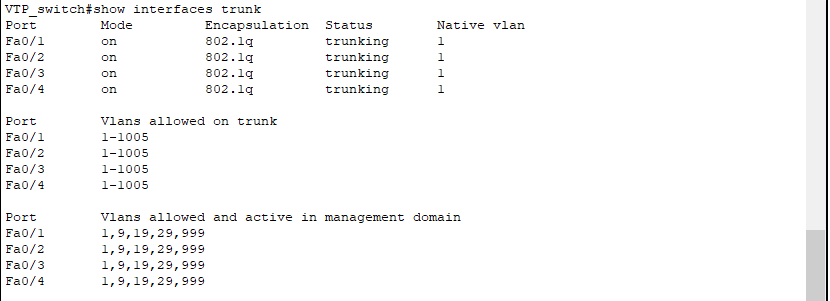
*#switchport mode access*

*#switchport access vlan 9*

Asa am facut pentru switch-ul 0,1,2.

Din Config panel:



Pentru testare si verificare am folosit comanda #*show interfaces trunk* si mi-a aratat urmatoarea informatii:  


## Configurare Subretele

Pe routerul principal, am activat interfata Fa0/0 cu comanda no shutdown si am creat patru subinterfete pentru VLAN-uri. Am configurat adresele gateway pentru fiecare VLAN folosind urmatoarele comenzi. Aceeasi procedura a fost aplicata pentru interfetele 0.9, 0.19, 0.29 si 0.999:

*#enable*

*#configure terminal*

*#interface Fa0/0*

*#no shutdown*

*#exit*

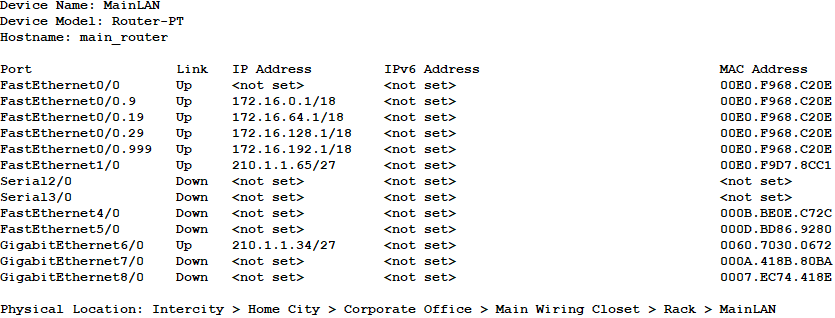
*#interface Fa0/0.9*

*#encapsulation dot1q 9*

*#ip address 172.16.0.1 255.255.192.0*

#exit

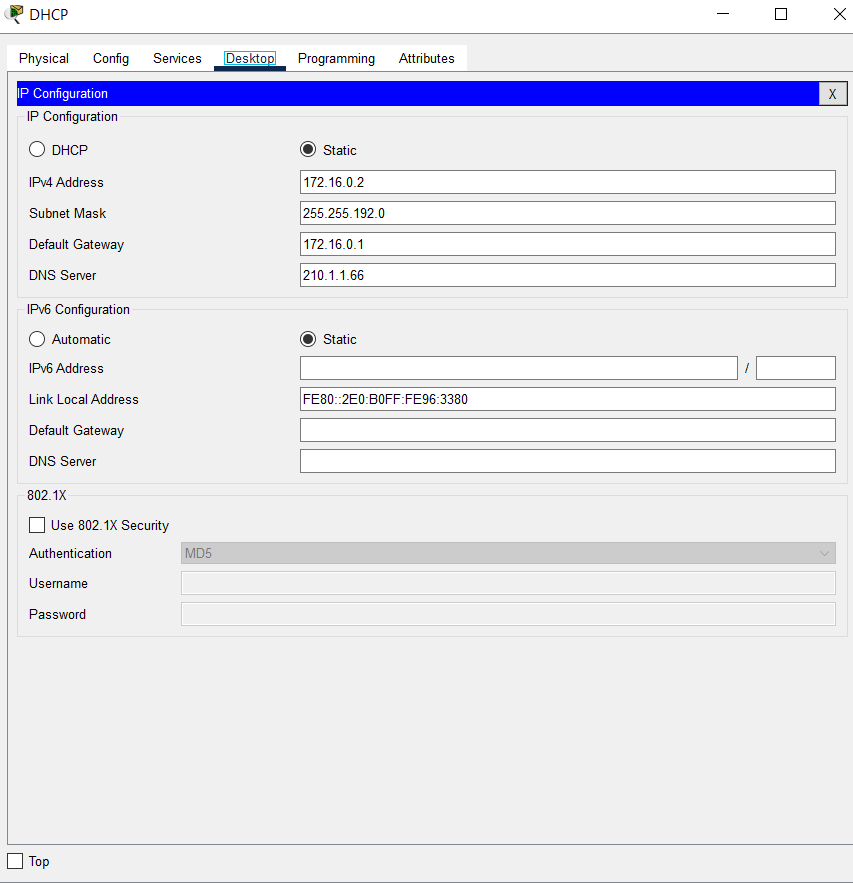
Asadar putem vedea interfetele si IP-urile lor.

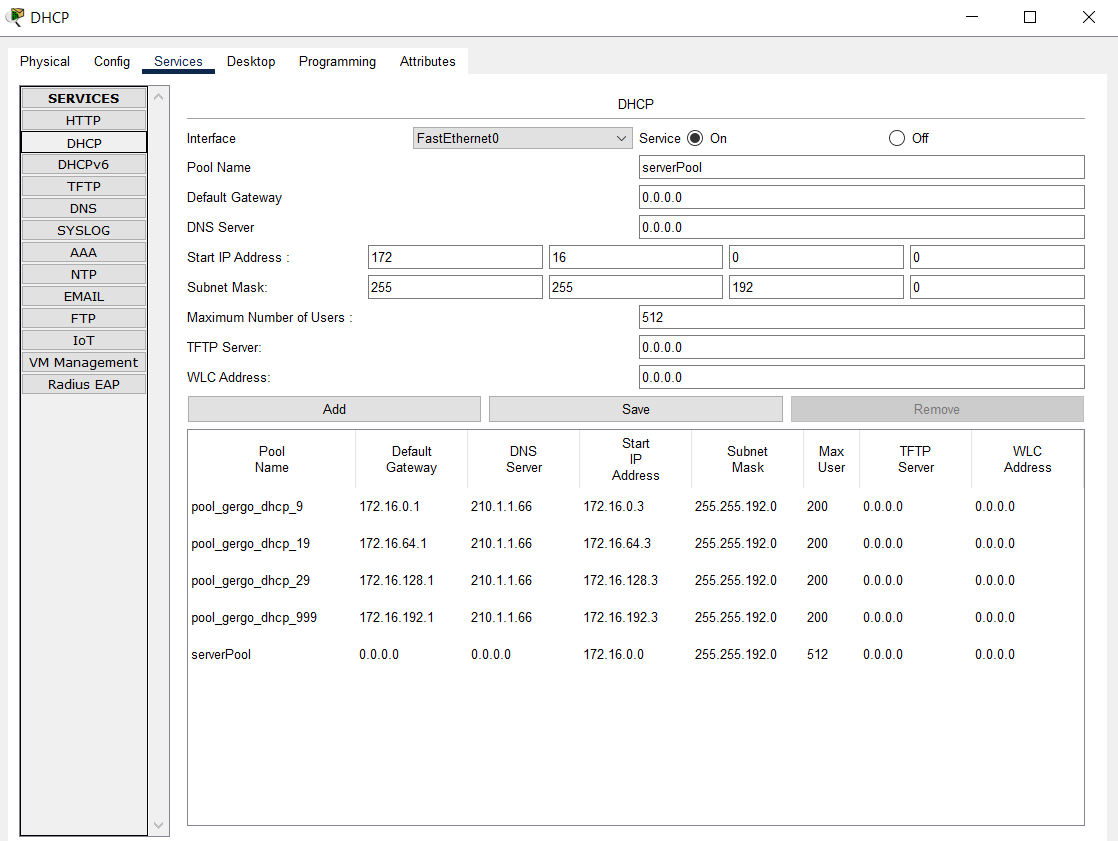


Am adaugat rutarea default static cu comanda urmatoarea in router-ul main:  
*#ip route 0.0.0.0 0.0.0.0 210.1.1.33*

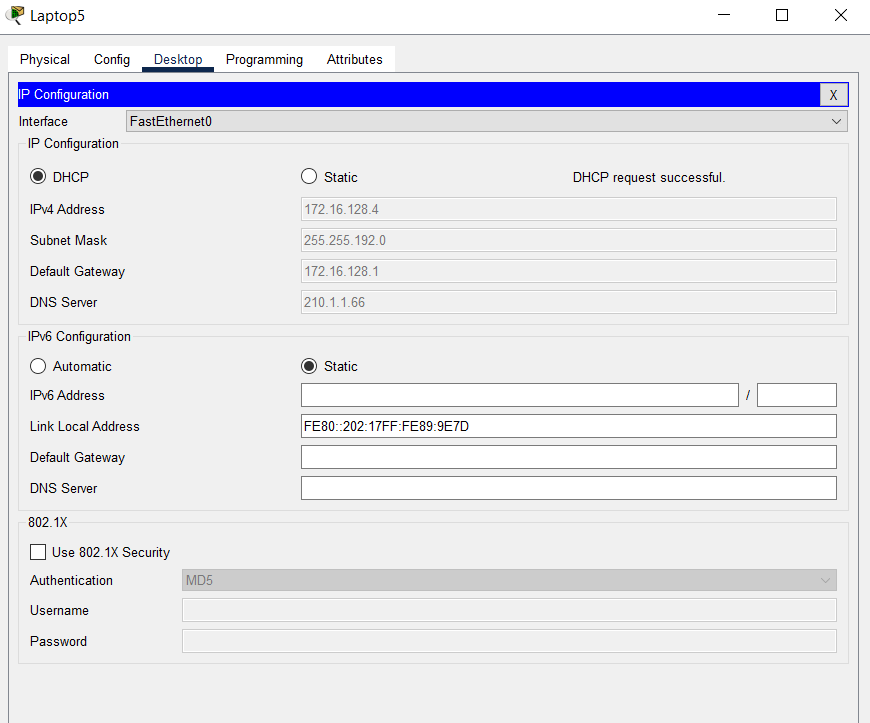
## Configurare DHCP

Din VLAN 9 (primul etaj), Server0 a fost configurat ca server DHCP, iar pentru a verifica distribuirea adreselor IP dinamice, s-a accesat optiunea IP Configuration unde se observa ca adresa IP de start este *172.16.0.3*, deoarece *172.16.0.1* este gateway-ul, iar *172.16.00.2* este serverul si DNS several are *210.1.1.66*. De asemenea, s-au alocat adrese IP pentru 200 de utilizatori, iar serverul DHCP a fost activat (Service On). Dupa asta am creat pool-urile pentru vlan-uri cu gateway-urile potrivite.



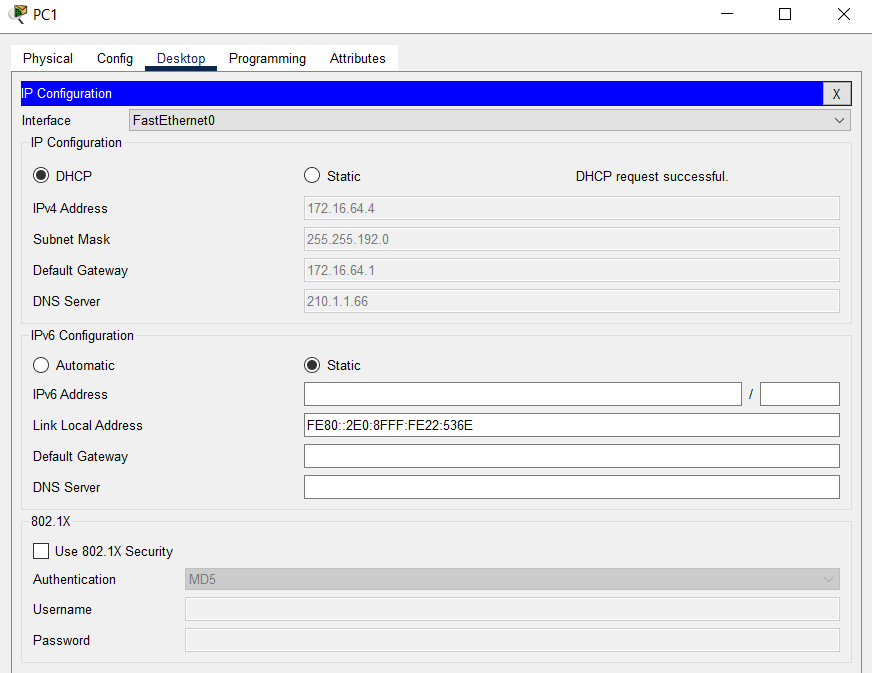


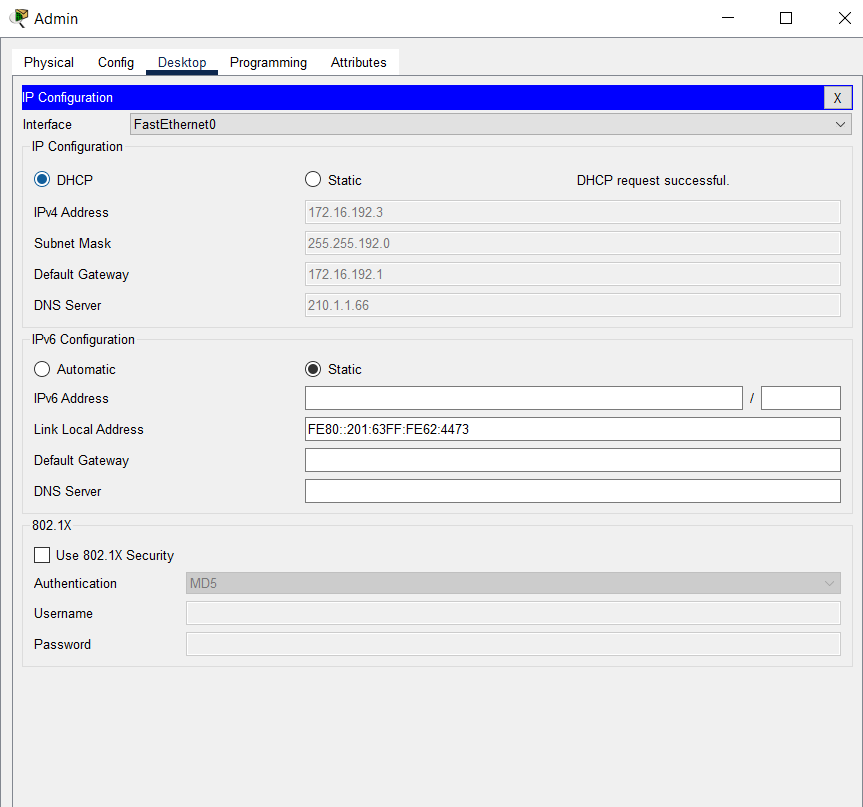
In imaginea de mai jos se vede cum un laptop se conecteaza prin DHCP:



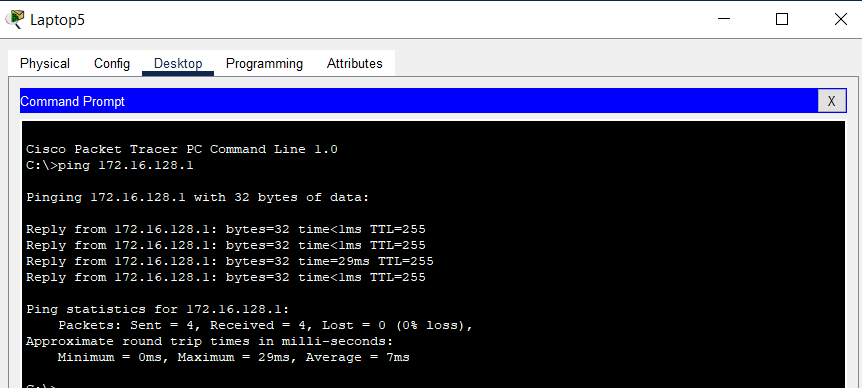
Prin folosirea unei comenzi fac legatura intre router si DHCP:

*#enable  
#configure terminal  
#interface Fa0/0.9  
#ip helper-address 172.16.0.2  
#interface Fa0/0.19  
#ip helper-address 172.16.0.2  
#interface Fa0/0.29  
#ip helper-address 172.16.0.2  
#interface Fa0/0.999  
#ip helper-address 172.16.0.2*

Asadar daca intram pe un device, pe IP Configuration si selectam DHCP adresarea se face dynamic pe vlan-uri:

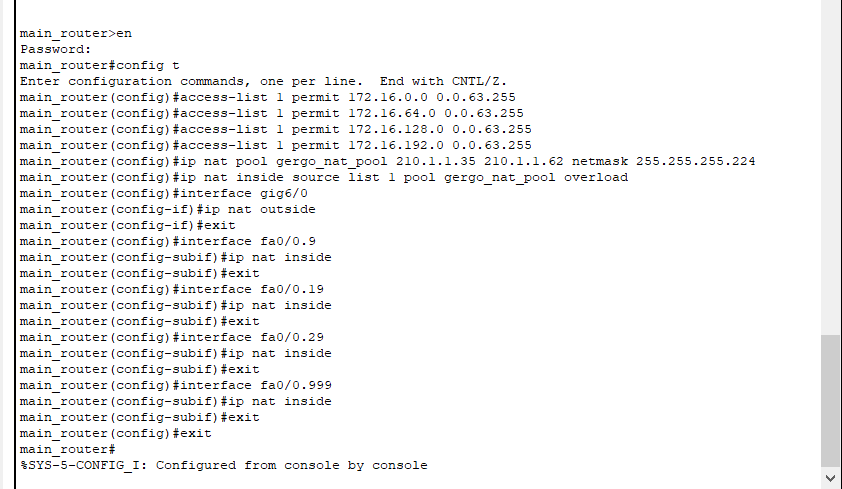


Verificarea conectivitatii putem testa dintr-un device (de exemplu laptop5) cu urmatoarea comanda *#ping 172.16.128.1*

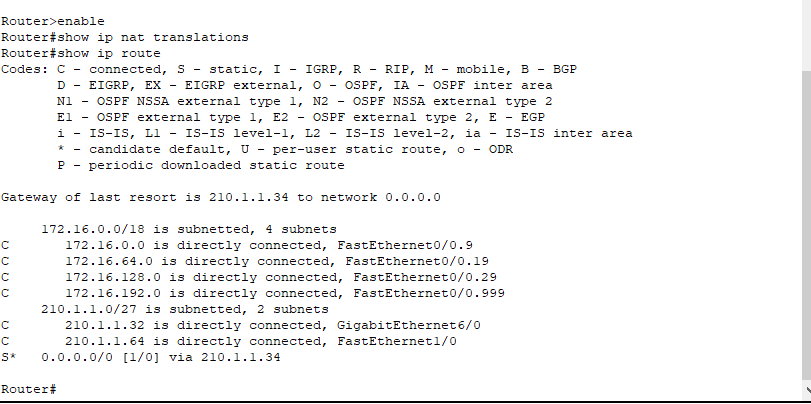


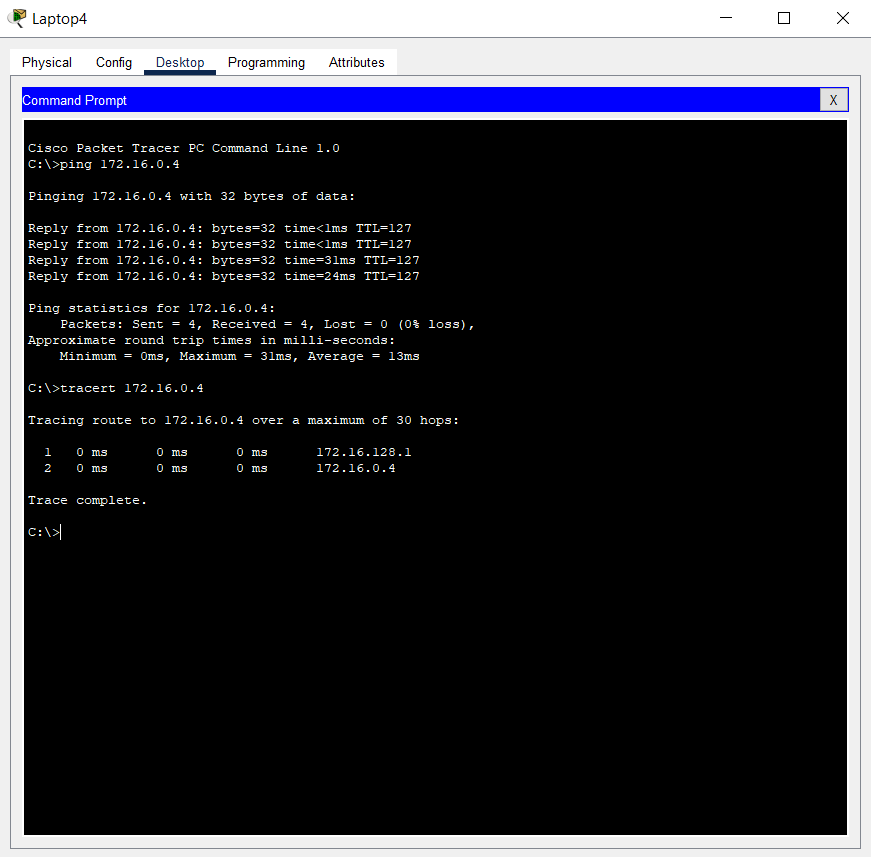
## Configurare NAT

In cadrul retelei interne, se utilizeaza adrese IP din intervalul 172.16.0.0, care sunt adrese private. Pentru a permite iesirea in exterior, aceste adrese private trebuie sa fie traduse in adrese publice. Aceasta translatare se face prin NAT (Network Address Translation), un proces care functioneaza la nivelul stratului 3 al modelului OSI, adica la nivelul adreselor IP. Routerul mentine o tabela de translatare in care leaga fiecare adresa IP privata de adresa publica echivalenta, pentru a gestiona traficul care paraseste reteaua.



Pentru verificare am folsoit comanda:  
*#show ip route*

  
  
Pentru verificare folosim comanda *#tracert <target>*:



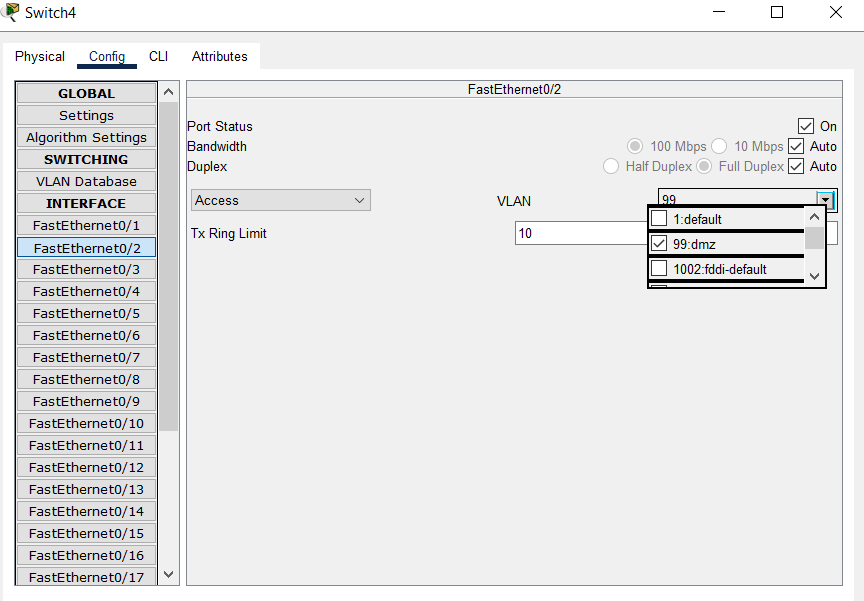
## Configurare DMZ

Din motive de securitate, in switch-ul din DMZ nu ma voi conecta la VLAN-ul 1, voi crea un nou VLAN, **VLAN 99**, denumit **DMZ**. In acest switch, voi conecta serverele DNS, HTTP, FTP si MAIL in **mod acces**.

Adresele IP alocate pentru servere sunt urmatoarele:

* **DNS**: 210.1.1.66
* **HTTP**: 210.1.1.67
* **FTP**: 210.1.1.68
* **MAIL**: 210.1.1.69

Descidand switch-ul 4, din config panel selectam Fa0/2, Fa0/3, Fa0/4, Fa0/5 alegem modul acces si selectam din lista de vlan-uri, vlan-ul *dmz.*



Sau se poate si din treminalul CLI in urmatorul fel:  
*#enable  
#config terminal  
#interface Fa 0/1  
# switchport mode access  
# switchport access vlan 99  
#exit*

*#interface range Gig 0/1-2*

*#switchport mode access*

*#switchport access vlan 99*

Si asa primeste vlan-ul un IP din IP-urile assignate DMZ-ului:

*#interface vlan 99*

*#ip address 210.2.2.70 255.255.255.224*

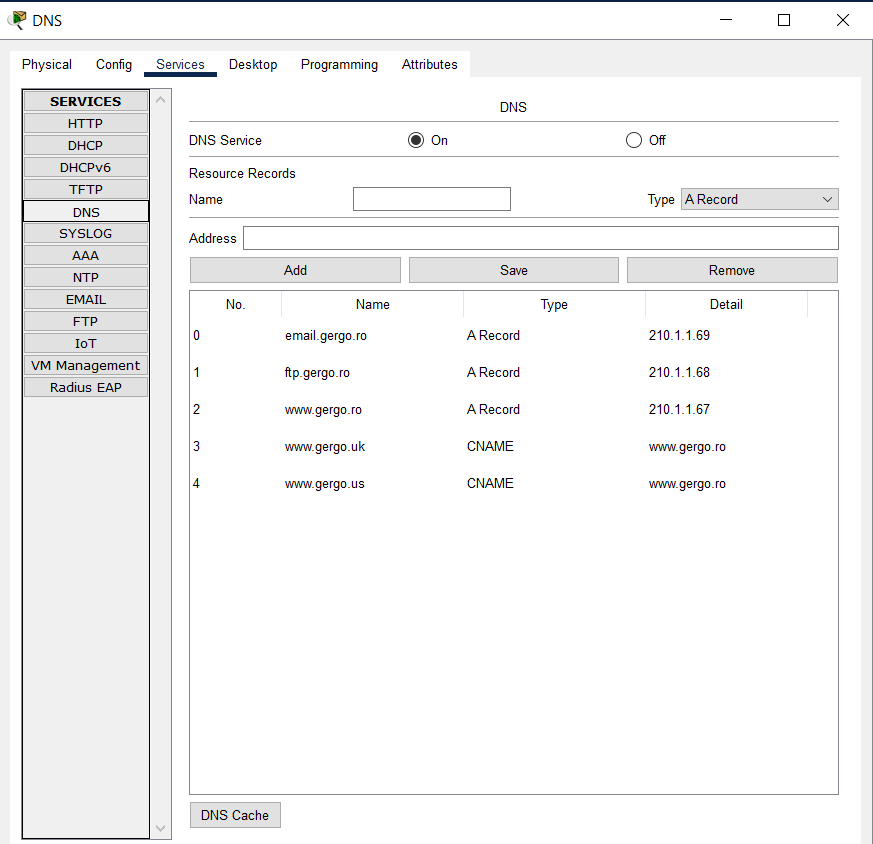
*#no shutdown*

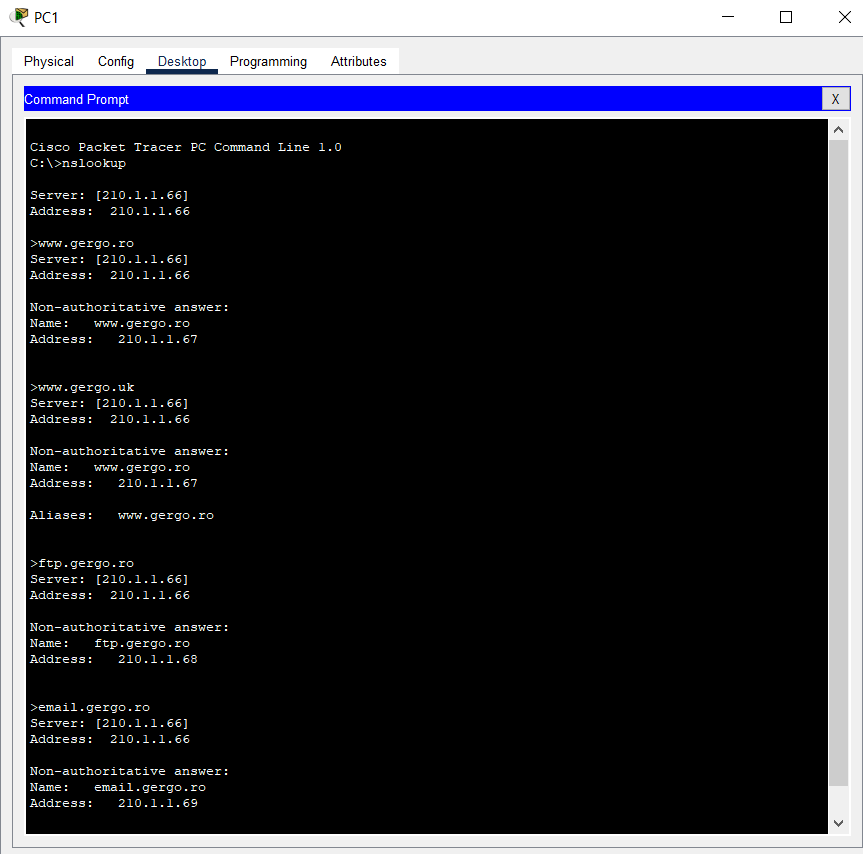
*#exit*

*#ip default-gateway 210.2.2.65*

### Serverul DNS:

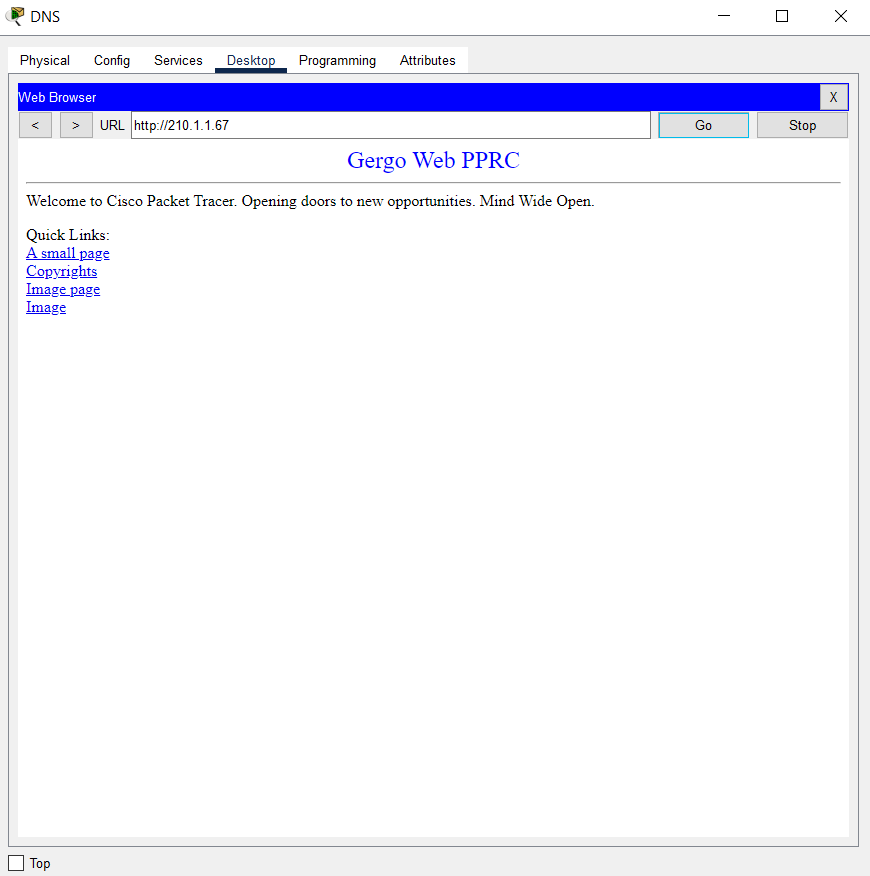
Folosind comanda *nolookup* in terminal, putem verifica functionarea serverului DNS.

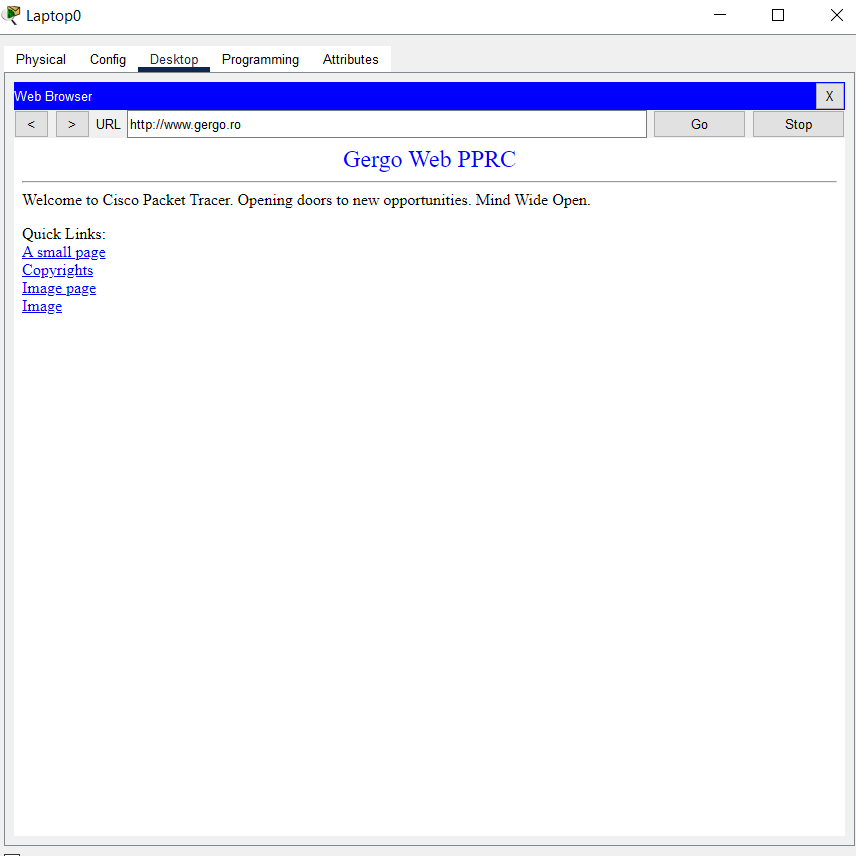




### Pagina de HTTP:

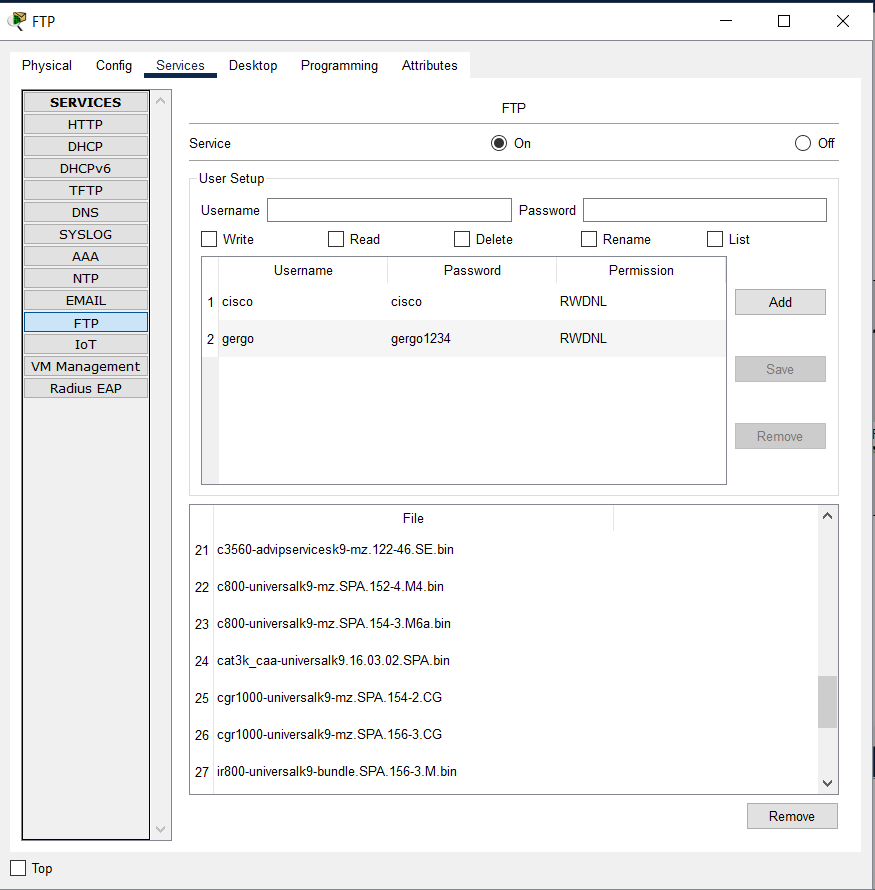
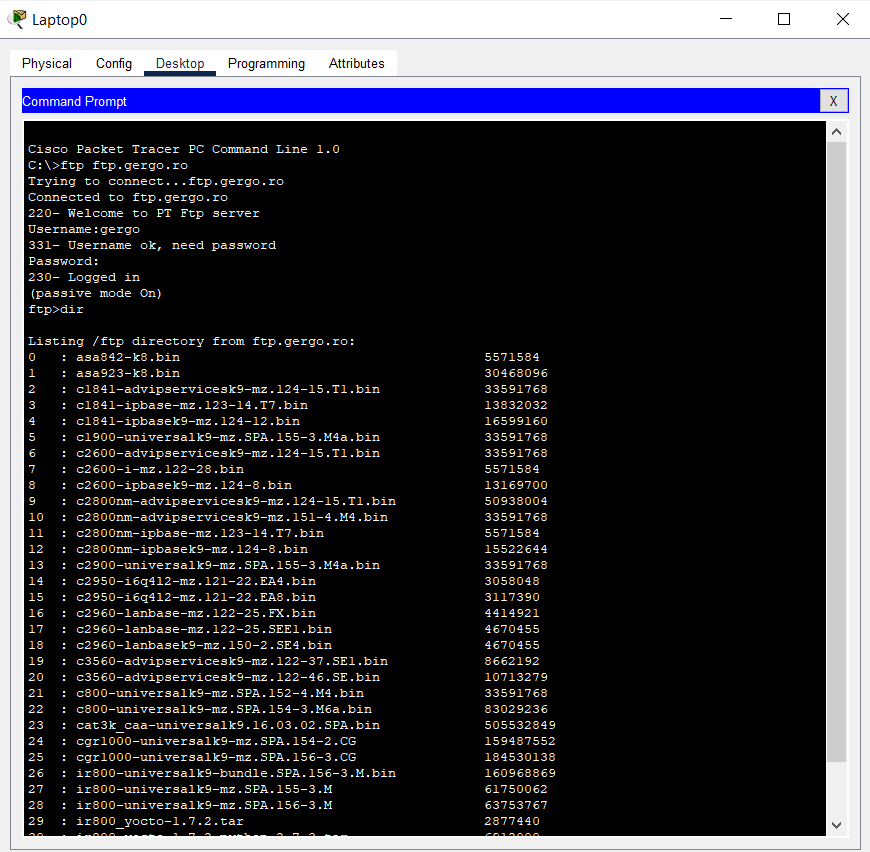
Verificarea serverului HTTPS se face din desktop-ul unui dispozitiv din retea, folosind optiunea ***Web Browser*** si introducand numele atribuit serverului HTTP prin DNS.





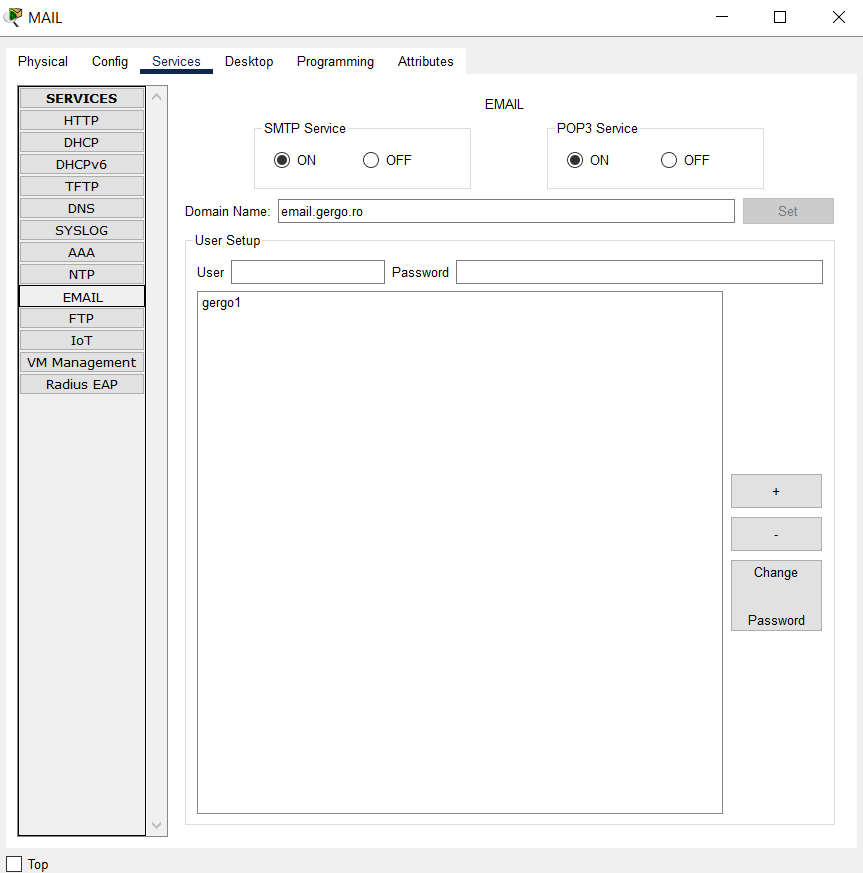
Serverul de FTP:

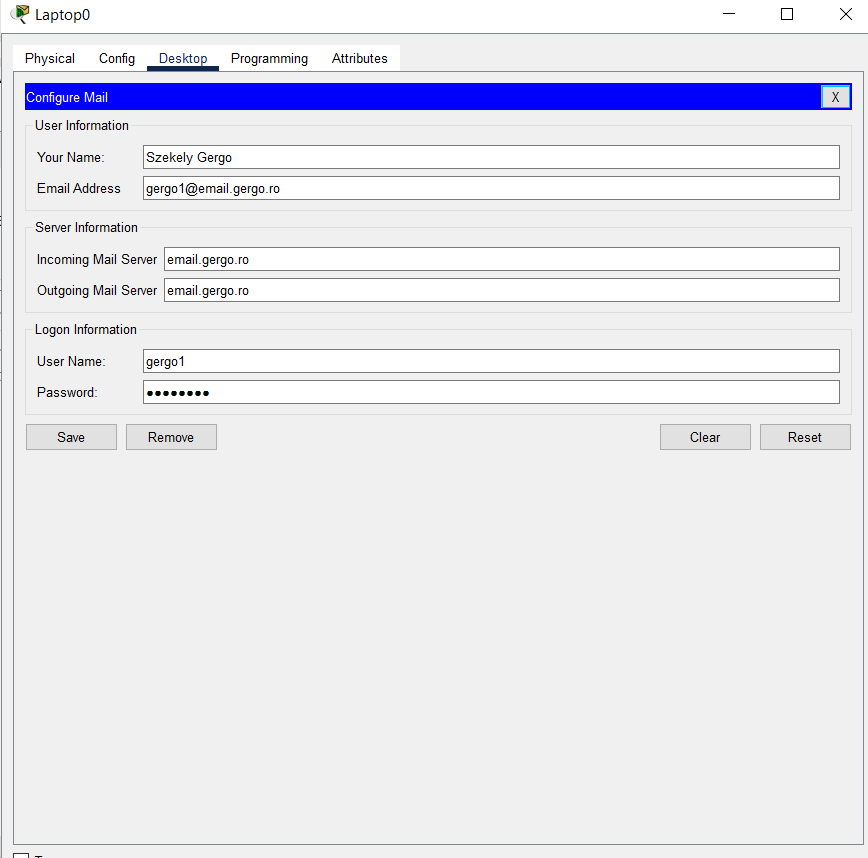
Folosind comanda ***ftp ftp.gergo.ro***, putem verifica serverul FTP din terminalul unui dispozitiv din retea, dupa ce am introdus numele de utilizator si parola am folosit comanda *dir* ca sa mi afisez toate fisiierele.

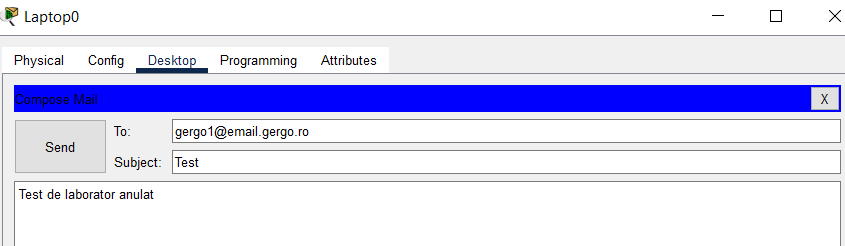


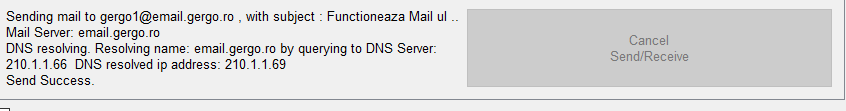
### Serverul EMAIL

De la fereastra de email a unui device, configurez informatiile legate de adresa de email existenta. Dupa configurare, compun un email si il trimit. In final, apas pe optiunea **Receive** pentru a primi email-ul. Am facut urmatorii pasi prezentat mai jos:

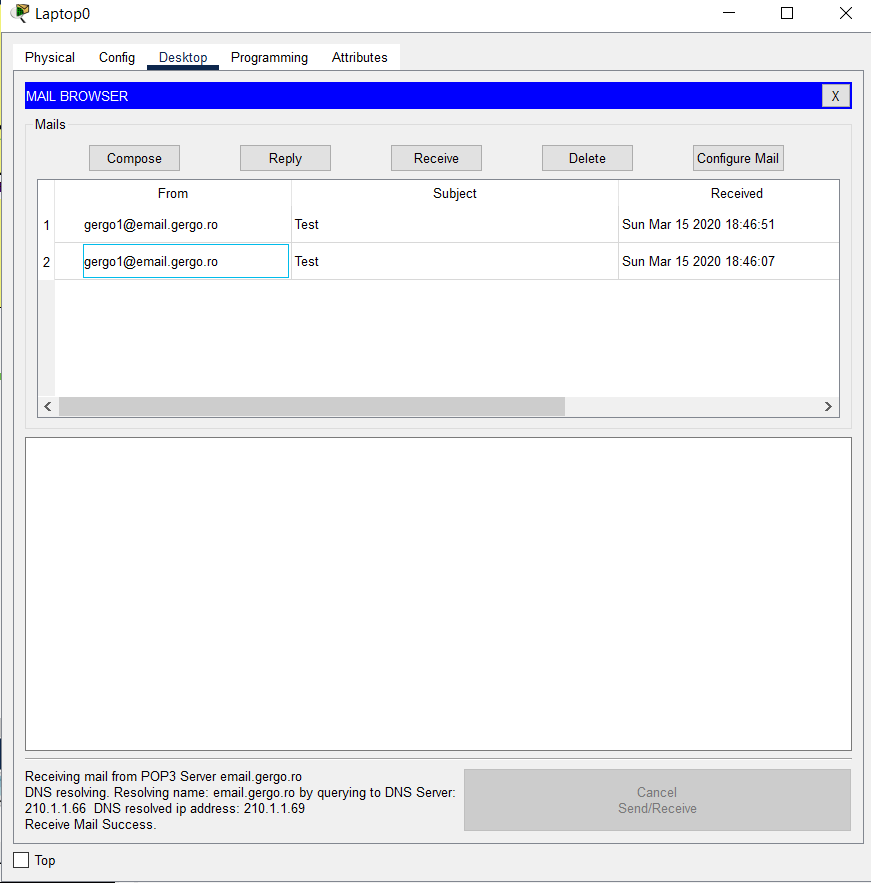
Pasul 1:  


Pasul 2:

Pasul 3:  




Pasul 4:



## Securitate

Pentru securitatea switch-urilor si a routerului am adaugat passwordul securizat (*secret* ne ajuta prin encryptarea complexa a parolei) cu urmatoarea comanda la switcu-uriel 3 si 4, si la main router:

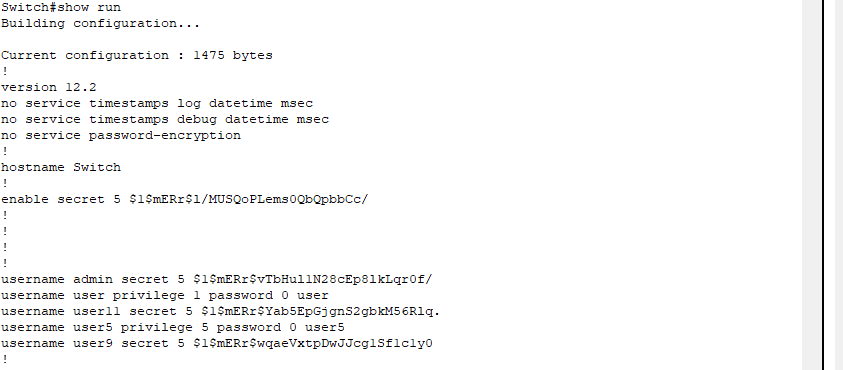
*# enable secret gergo*

Exista 15 nivele de privilegiu pentru utilizatori, unde **User EXEC mode** corespunde nivelului 1 (guest), iar **Privileged EXEC mode** corespunde nivelului 15, care este cel mai ridicat. Am realizat urmatoarele comenzi la switcu-uriel 3 si 4, si la main router:

*# username user privilege 1 password user   
# username user5 privilege 5 password user5*

Prin adaugarea cuvantulaui cheie *secret* parolele utilizatoriilor o sa fie cryptate:

# username user9 privilege 9 secret user9   
# username user11 privilege 11 secret user11   
# username admin privilege 15 secret admin   
  
Pentru verificare putem rula comanda *show running-configuration* unde o sa vedem utilizatorii cu parola si daca folsoim *secret* atunci cu parole cryptate:

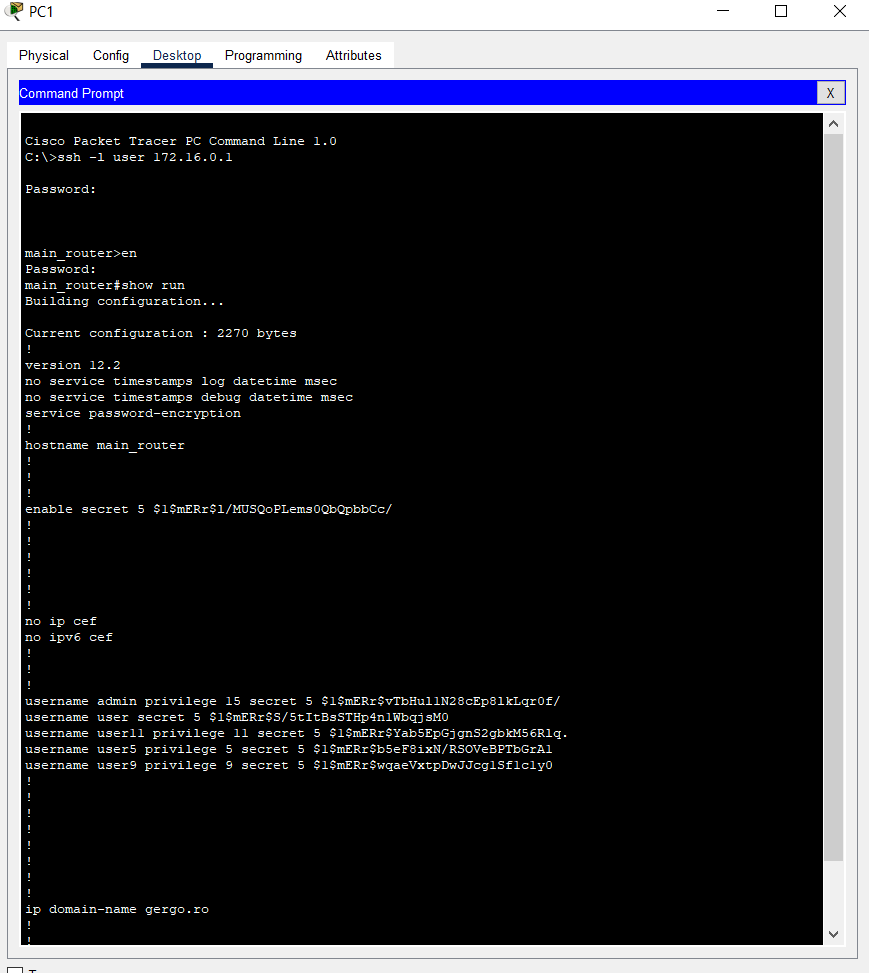


## Securitate SHH

SSH este un protocol de conectare securizata care permite stabilirea unei conexiuni intre doua calculatoare, asigurand ca informatiile schimbate raman confidentiale. Prin criptare, SSH protejeaza atat confidentialitatea, cat si integritatea datelor, si ajuta la autentificarea corecta a celor implicati in comunicare. Pentru a face totul sa functioneze, am folosit algoritmul RSA. Am facut urmatoarele comenzi pe mainrouter, switchul 3 si 4.

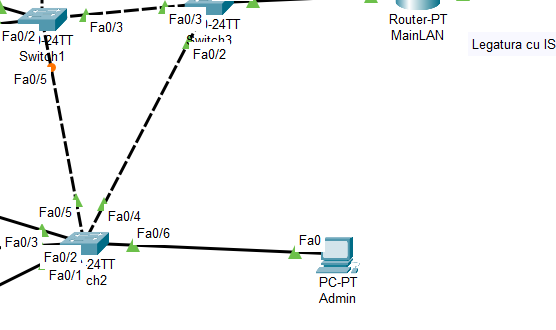
*#hostname <numele>  
#ip domain-name gergo.ro  
#crypto key generate rsa  
#line vty 0 4  
#transport input ssh  
#login local*

Testarea se poate realiza astfel: intram pe un dispozitiv (de exemplu, PC0), accesam terminalul din Desktop si introducem comanda ssh -l <username> <target\_device\_IP>. Dupa ce rulam comanda, vom introduce parola utilizatorului pentru a stabili conexiunea SSH. Apoi, va trebui sa introducem a doua parola pentru a ne conecta la routerul principal. Dupa ce autentificarea este completa, putem efectua diverse operatiuni pe routerul principal.



## Admin/Management

Am adaugat un nou PC denumit **PCAdmin**, dedicat VLAN-ului 999 de administrare, care se ocupa de managementul retelei. Acesta a primit automat adresa IP prin intermediul DHCP.



Am setat adrese publice pentru routerul ISP, switch, PC si serverul din INTERNET. Pe router-ul SPI am folosit urmatoarele comenzi:

*#enable*

*#configure terminal*

*#interface Fa0/0*

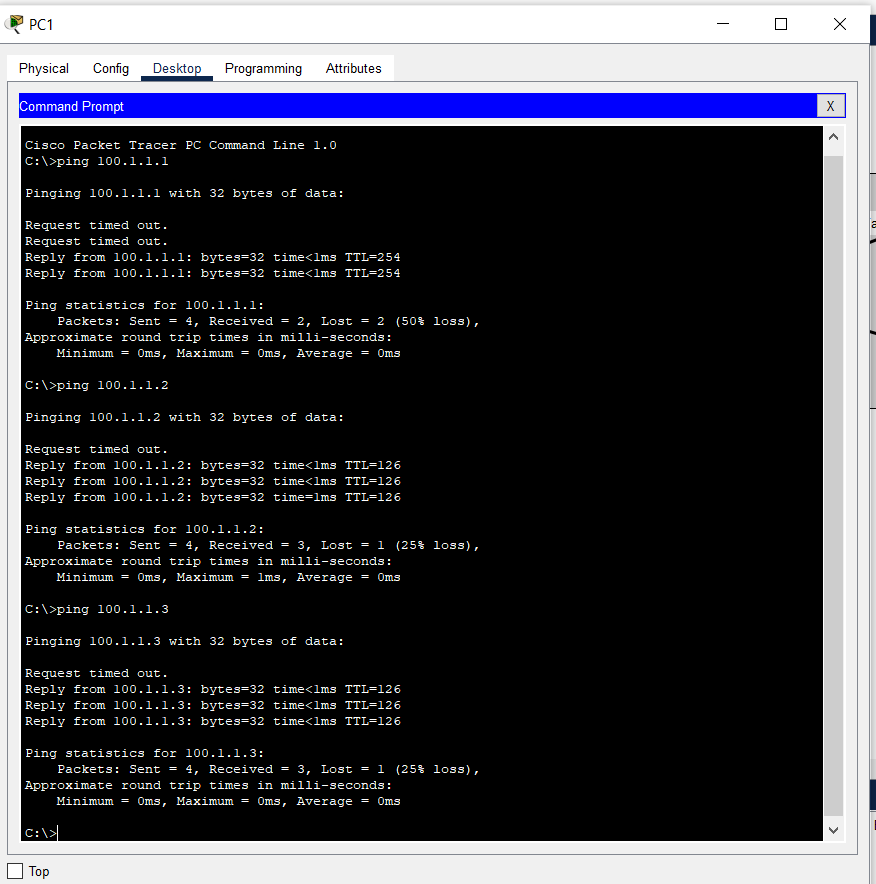
*#ip address 100.1.1.1 255.0.0.0*

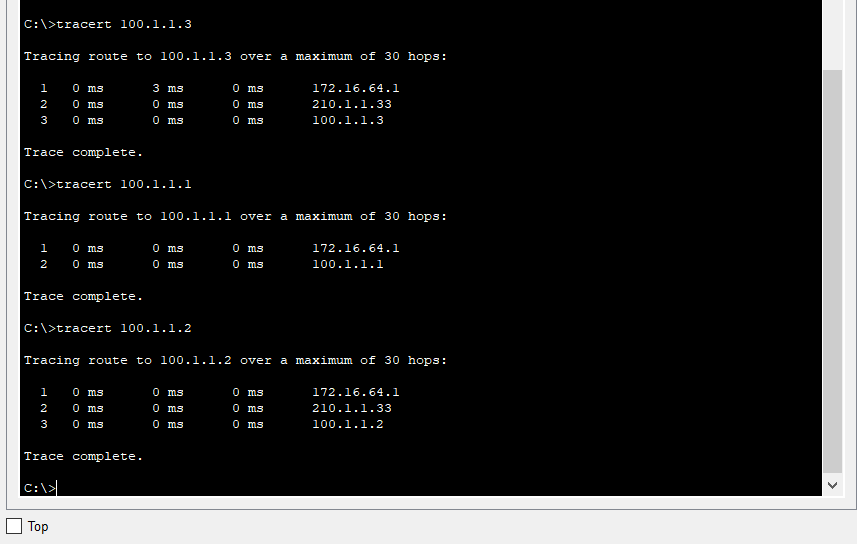
*#no shutdown*

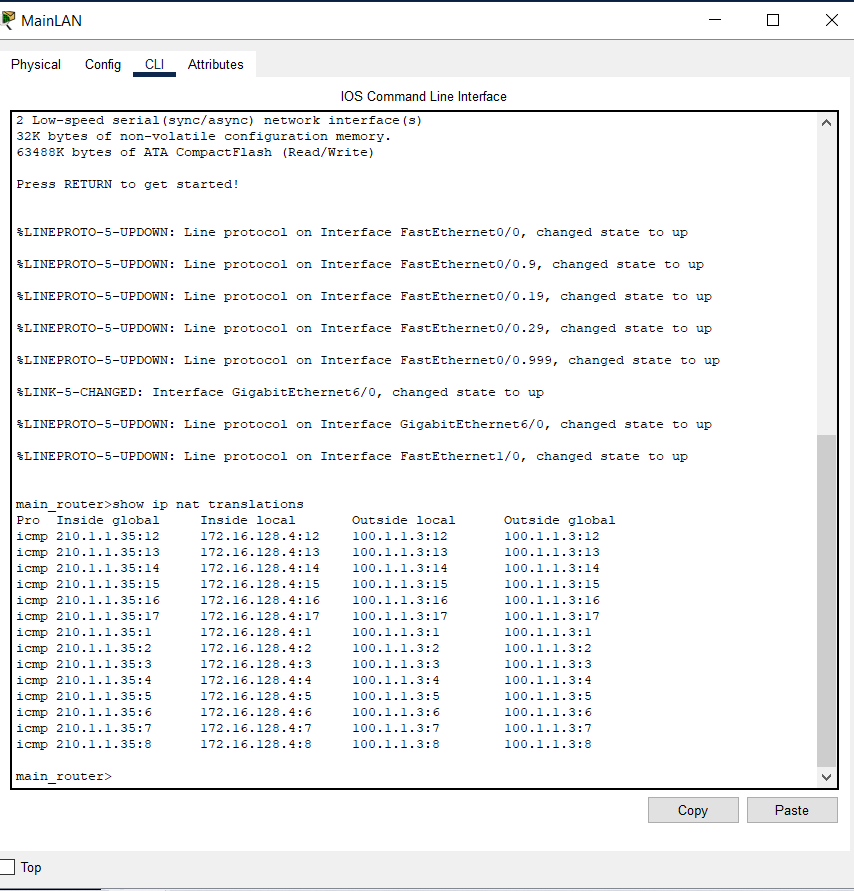
*#exit*

## Reteaua externa (Internet)

Am procedat la fel, doar ca de data aceasta pe switch-ul 5, unde am setat adresele IP pentru server si calculator. Serverul a primit adresa IP 100.1.1.2, iar calculatorul a primit adresa IP 100.1.1.3. La final, am testat conexiunea catre acestea alegand un dispozitiv din reteaua interna (PC1) si o adresa din reteaua externa (o adresa IP publica), folosind comanda #*ping <adresaIP>.* Cu comanda *#tracert <adresaIP>* verificam daca conexiunea este estabilita correct si gaseste interfetele necesare.





Asadar, folosind comanda *#show ip nat translations*, ne-am asigurat ca s-a realizat conexiunea intre reteaua interna si cea externa, confirmand astfel ca NAT-ul functioneaza corect.