



UNIVERSITATEA TEHNICĂ

DIN CLUJ-NAPOCA

**FACULTATEA DE AUTOMATICĂ ȘI 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 reseaua 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

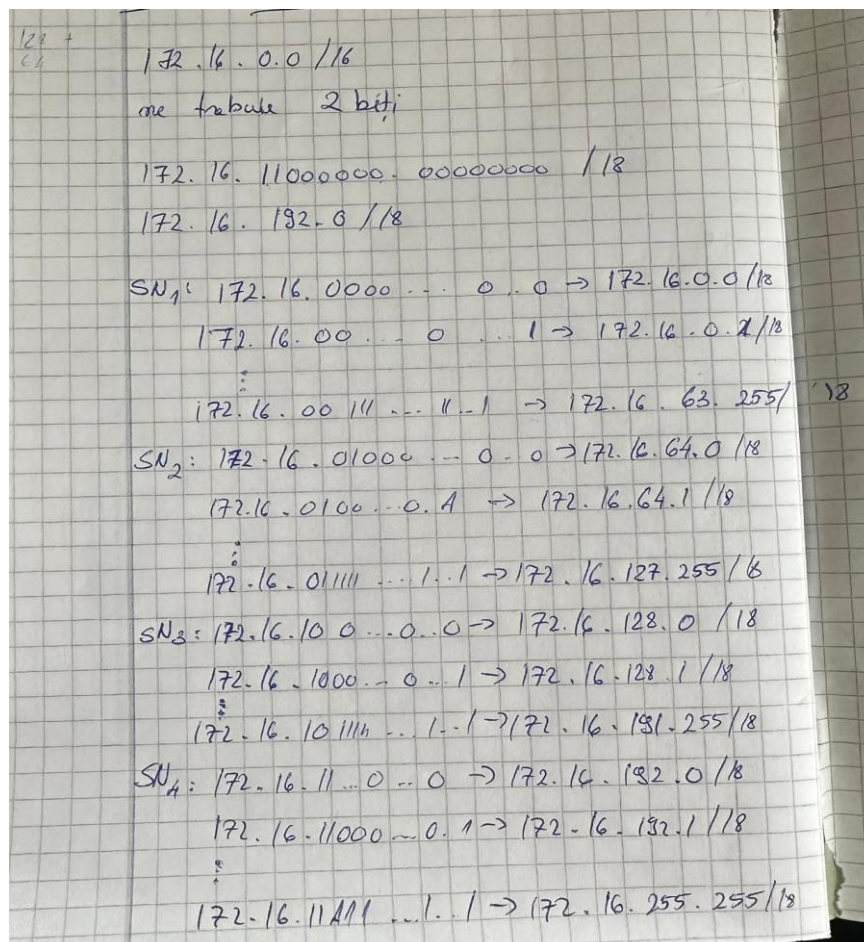
Cuprins

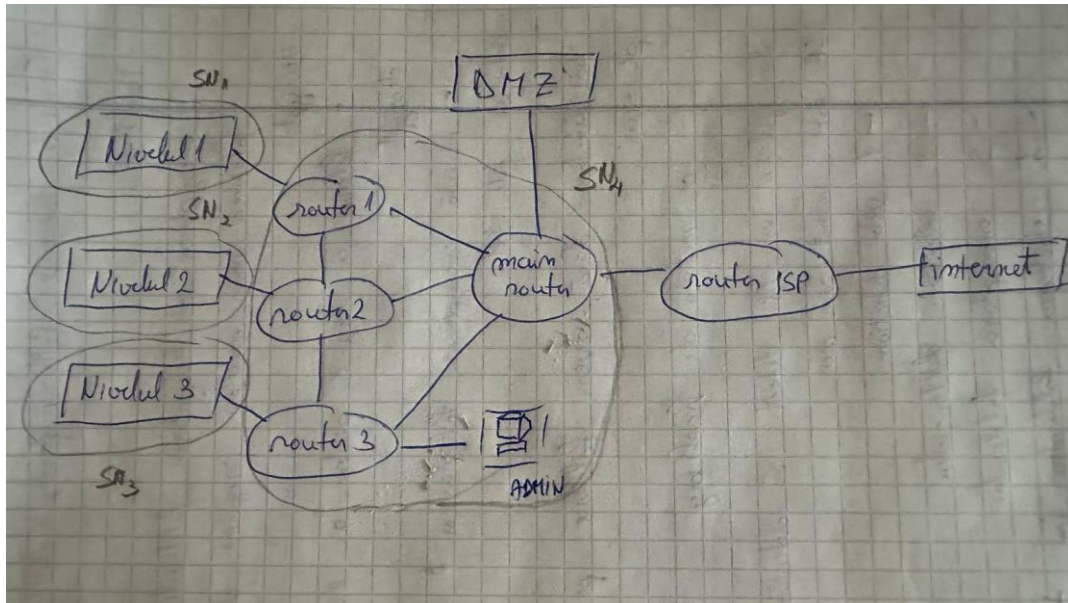
Cerinta:.....	2
Topologia retelei:	4
Subnetare:	4
Configurare VLAN/VTP:	5
Configurare Subretele	8
Configurare DHCP.....	9
Configurare NAT	12
Configurare DMZ	14
Serverul DNS:	15
Pagina de HTTP:.....	16
Serverul de FTP	17
Serverul EMAIL	18
Securitate.....	19
Securitate SHH.....	20
Admin/Management	21
Reteaua externa (Internet).....	22

Topologia rețelei:

Avem o topologie de tip stea extinsă, cu multiple conexiuni redundante, asigurând astfel ca, în cazul unei defecțiuni a unei legături, există rute alternative de backup pentru menținerea conectivității. Rețeaua este o rețea de switch-uri, iar ieșirea spre internet este asigurată 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

```
Switch#show vtp status
VTP Version                : 1
Configuration Revision      : 0
Maximum VLANs supported locally : 255
Number of existing VLANs    : 9
VTP Operating Mode          : Server
VTP Domain Name             : szekely_gergo
VTP Pruning Mode            : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation        : Disabled
MD5 digest                  : 0xC4 0x77 0x6F 0xA8 0x26 0x33 0x58 0x27
Configuration last modified by 0.0.0.0 at 3-1-93 03:53:15
Local updater ID is 0.0.0.0 (no valid interface found)
```

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

```
Switch#show vtp status
VTP Version                : 1
Configuration Revision      : 4
Maximum VLANs supported locally : 255
Number of existing VLANs    : 9
VTP Operating Mode          : Client
VTP Domain Name             : szekely_gergo
VTP Pruning Mode            : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation        : Disabled
MD5 digest                  : 0xEE 0x75 0xE1 0xCF 0x1E 0x99 0x55 0xDA
Configuration last modified by 0.0.0.0 at 3-1-93 04:08:58
```

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

configure terminal

#vlan 9

#name nivel1

#exit

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

```
VTP_switch>en
Password:
VTP_switch#show vlan brief

VLAN Name                Status    Ports
-----
1    default                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
9    nivel1                  active
19   nivel2                  active
29   nivel3                  active
999  management               active
1002 fddi-default             active
1003 token-ring-default      active
1004 fddinet-default         active
1005 trnet-default           active
VTP_switch#
```

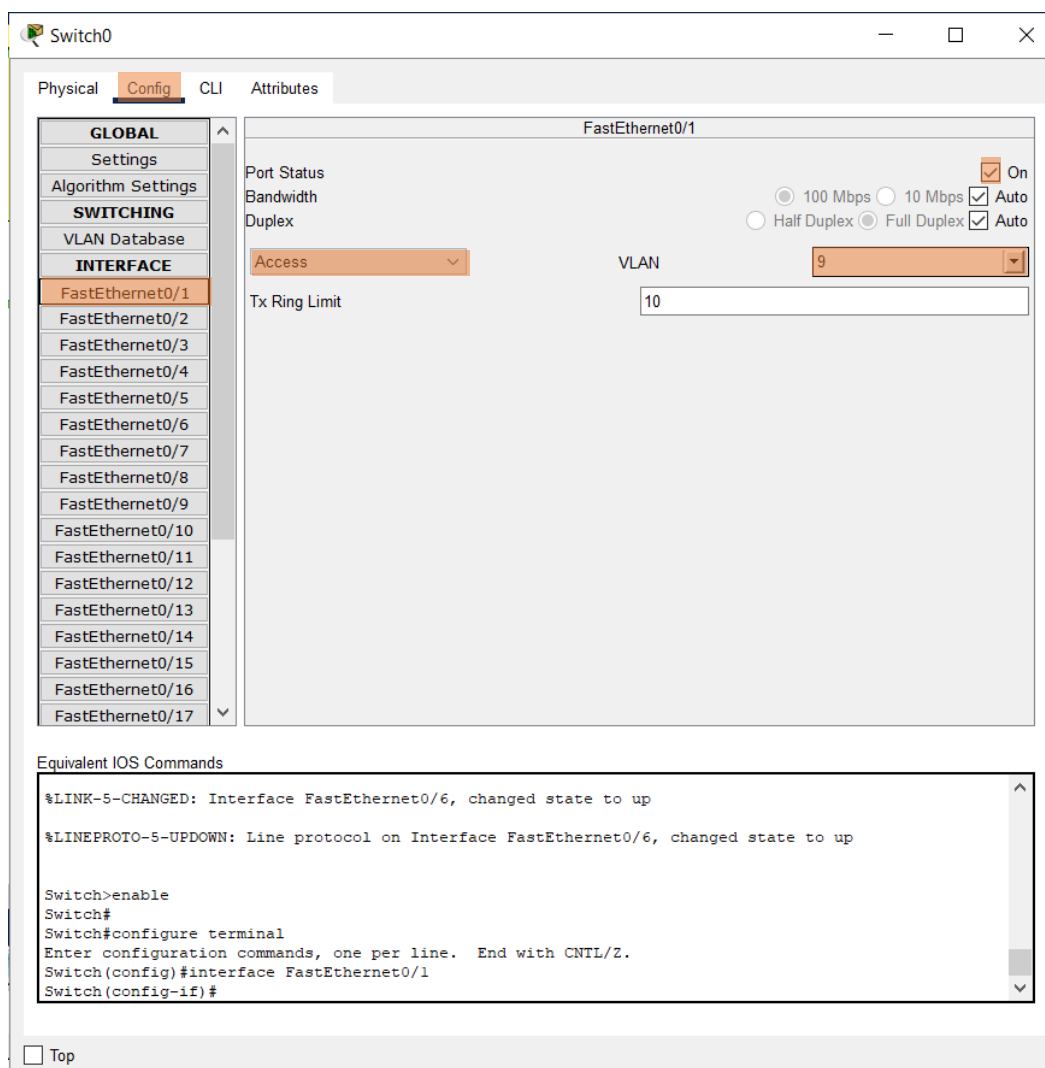
Am setat VLAN-urile potrivite pentru switch-uri, am dat click pe switch, am selectat config, apoi am ales portul la care doream sa fac asignarea. L-am pus in modul acces si am selectat VLAN-ul corespunzator. Aceste setari pot fi realizate si din cod, si din terminal, folosind urmatoarele comenzi:

- 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:

```
VTP_switch#show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     on        802.1q         trunking    1
Fa0/2     on        802.1q         trunking    1
Fa0/3     on        802.1q         trunking    1
Fa0/4     on        802.1q         trunking    1

Port      Vlans allowed on trunk
Fa0/1     1-1005
Fa0/2     1-1005
Fa0/3     1-1005
Fa0/4     1-1005

Port      Vlans allowed and active in management domain
Fa0/1     1,9,19,29,999
Fa0/2     1,9,19,29,999
Fa0/3     1,9,19,29,999
Fa0/4     1,9,19,29,999
```

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.

```
Device Name: MainLAN
Device Model: Router-PT
Hostname: main_router
```

Port	Link	IP Address	IPv6 Address	MAC Address
FastEthernet0/0	Up	<not set>	<not set>	00E0.F968.C20E
FastEthernet0/0.9	Up	172.16.0.1/18	<not set>	00E0.F968.C20E
FastEthernet0/0.19	Up	172.16.64.1/18	<not set>	00E0.F968.C20E
FastEthernet0/0.29	Up	172.16.128.1/18	<not set>	00E0.F968.C20E
FastEthernet0/0.999	Up	172.16.192.1/18	<not set>	00E0.F968.C20E
FastEthernet1/0	Up	210.1.1.65/27	<not set>	00E0.F9D7.8CC1
Serial2/0	Down	<not set>	<not set>	<not set>
Serial3/0	Down	<not set>	<not set>	<not set>
FastEthernet4/0	Down	<not set>	<not set>	000B.BE0E.C72C
FastEthernet5/0	Down	<not set>	<not set>	000D.BD86.9280
GigabitEthernet6/0	Up	210.1.1.34/27	<not set>	0060.7030.0672
GigabitEthernet7/0	Down	<not set>	<not set>	000A.418B.80BA
GigabitEthernet8/0	Down	<not set>	<not set>	0007.EC74.418E

```
Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > MainLAN
```

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 *172.16.0.2* este serverul si DNS serverul 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.

Physical Config Services **Desktop** Programming Attributes

IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 172.16.0.2

Subnet Mask: 255.255.192.0

Default Gateway: 172.16.0.1

DNS Server: 210.1.1.66

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address: /

Link Local Address: FE80::2E0:B0FF:FE96:3380

Default Gateway:

DNS Server:

802.1X

☐ Use 802.1X Security

Authentication: MD5

Username:

Password:

☐ Top

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP**
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DHCP

Interface: FastEthernet0 Service: ☒ On ☐ Off

Pool Name: serverPool

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

Start IP Address: 172.16.0.16

Subnet Mask: 255.255.192.0

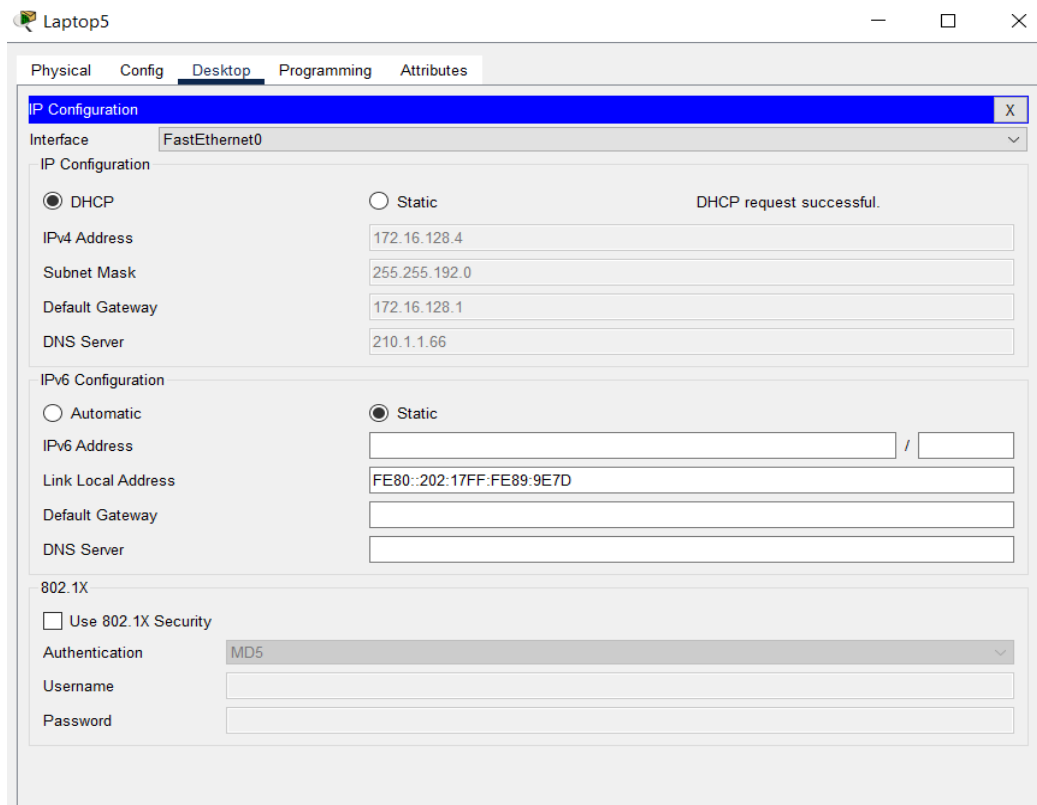
Maximum Number of Users: 512

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
pool_gergo_dhcp_9	172.16.0.1	210.1.1.66	172.16.0.3	255.255.192.0	200	0.0.0.0	0.0.0.0
pool_gergo_dhcp_19	172.16.64.1	210.1.1.66	172.16.64.3	255.255.192.0	200	0.0.0.0	0.0.0.0
pool_gergo_dhcp_29	172.16.128.1	210.1.1.66	172.16.128.3	255.255.192.0	200	0.0.0.0	0.0.0.0
pool_gergo_dhcp_999	172.16.192.1	210.1.1.66	172.16.192.3	255.255.192.0	200	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	172.16.0.0	255.255.192.0	512	0.0.0.0	0.0.0.0

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:

PC1

Physical Config Desktop Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

☒ DHCP ☐ Static DHCP request successful.

IPv4 Address 172.16.64.4

Subnet Mask 255.255.192.0

Default Gateway 172.16.64.1

DNS Server 210.1.1.66

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80::2E0:8FFF:FE22:536E

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication MD5

Username

Password

Admin

Physical Config Desktop Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

☒ DHCP ☐ Static DHCP request successful.

IPv4 Address 172.16.192.3

Subnet Mask 255.255.192.0

Default Gateway 172.16.192.1

DNS Server 210.1.1.66

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80::201:63FF:FE62:4473

Default Gateway

DNS Server

802.1X

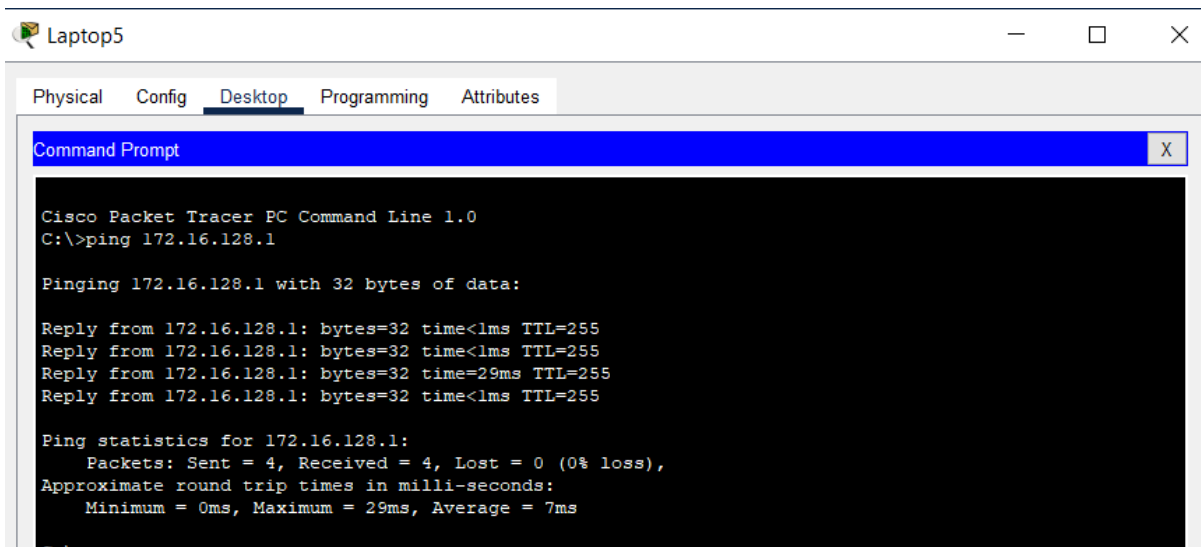
☐ Use 802.1X Security

Authentication MD5

Username

Password

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



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.16.128.1

Pinging 172.16.128.1 with 32 bytes of data:

Reply from 172.16.128.1: bytes=32 time<1ms TTL=255
Reply from 172.16.128.1: bytes=32 time<1ms TTL=255
Reply from 172.16.128.1: bytes=32 time=29ms TTL=255
Reply from 172.16.128.1: bytes=32 time<1ms TTL=255

Ping statistics for 172.16.128.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 29ms, Average = 7ms
```

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 reseaua.

```
main_router>en
Password:
main_router#config t
Enter configuration commands, one per line. End with CNTL/Z.
main_router(config)#access-list 1 permit 172.16.0.0 0.0.63.255
main_router(config)#access-list 1 permit 172.16.64.0 0.0.63.255
main_router(config)#access-list 1 permit 172.16.128.0 0.0.63.255
main_router(config)#access-list 1 permit 172.16.192.0 0.0.63.255
main_router(config)#ip nat pool gergo_nat_pool 210.1.1.35 210.1.1.62 netmask 255.255.255.224
main_router(config)#ip nat inside source list 1 pool gergo_nat_pool overload
main_router(config)#interface gig6/0
main_router(config-if)#ip nat outside
main_router(config-if)#exit
main_router(config)#interface fa0/0.9
main_router(config-subif)#ip nat inside
main_router(config-subif)#exit
main_router(config)#interface fa0/0.19
main_router(config-subif)#ip nat inside
main_router(config-subif)#exit
main_router(config)#interface fa0/0.29
main_router(config-subif)#ip nat inside
main_router(config-subif)#exit
main_router(config)#interface fa0/0.999
main_router(config-subif)#ip nat inside
main_router(config-subif)#exit
main_router(config)#exit
main_router#
%SYS-5-CONFIG_I: Configured from console by console
```

Pentru verificare am folsoit comanda:

#show ip route

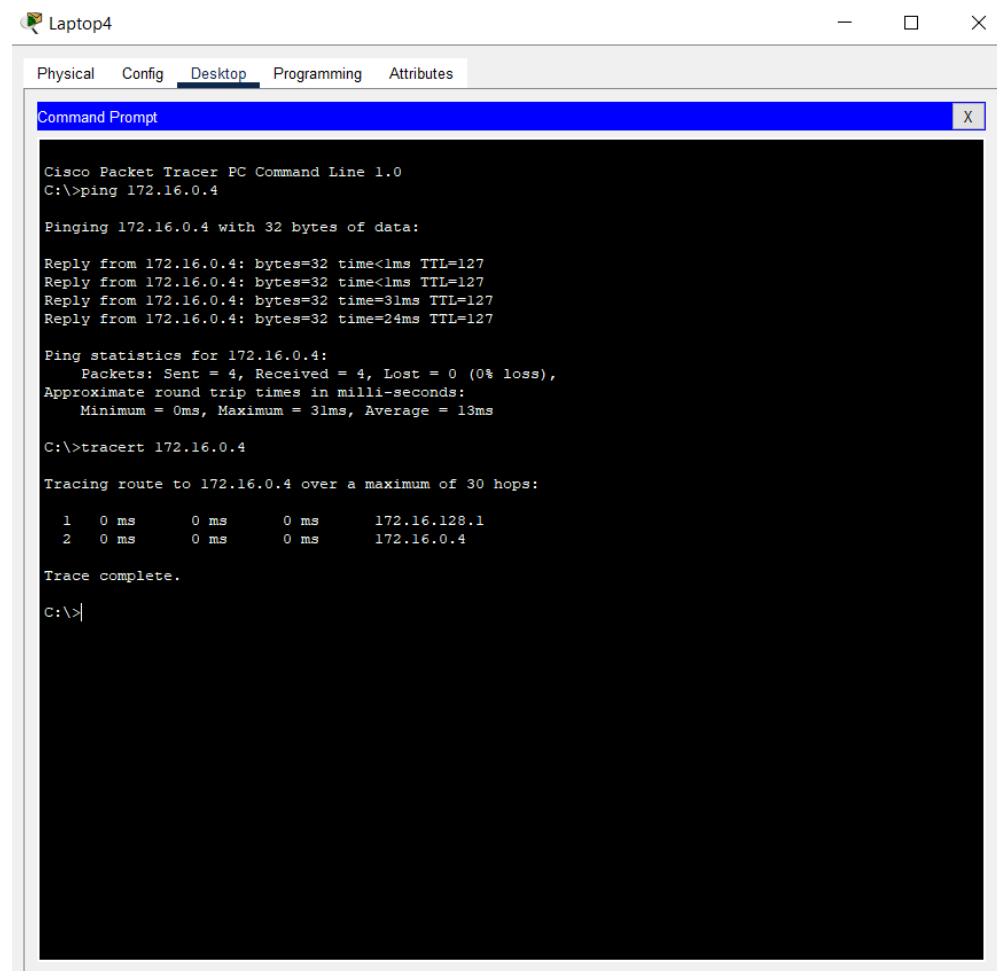
```
Router>enable
Router#show ip nat translations
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF 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 210.1.1.34 to network 0.0.0.0

    172.16.0.0/18 is subnetted, 4 subnets
C       172.16.0.0 is directly connected, FastEthernet0/0.9
C       172.16.64.0 is directly connected, FastEthernet0/0.19
C       172.16.128.0 is directly connected, FastEthernet0/0.29
C       172.16.192.0 is directly connected, FastEthernet0/0.999
    210.1.1.0/27 is subnetted, 2 subnets
C       210.1.1.32 is directly connected, GigabitEthernet6/0
C       210.1.1.64 is directly connected, FastEthernet1/0
S*    0.0.0.0/0 [1/0] via 210.1.1.34

Router#
```

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



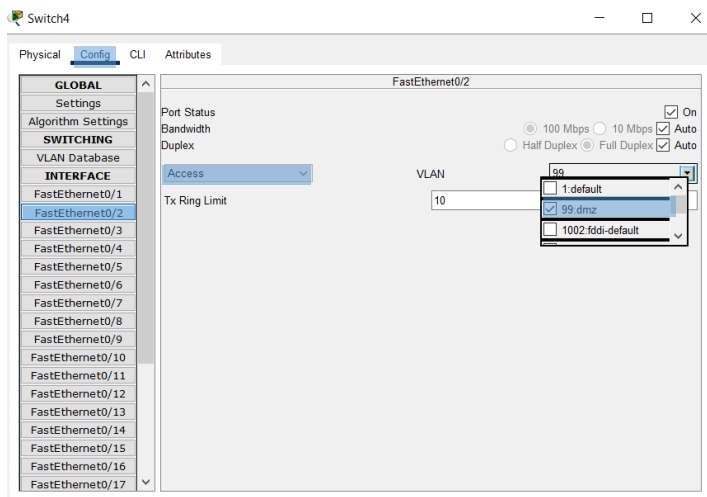
Configurare DMZ

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 terminalul CLI in urmatoarul fel:

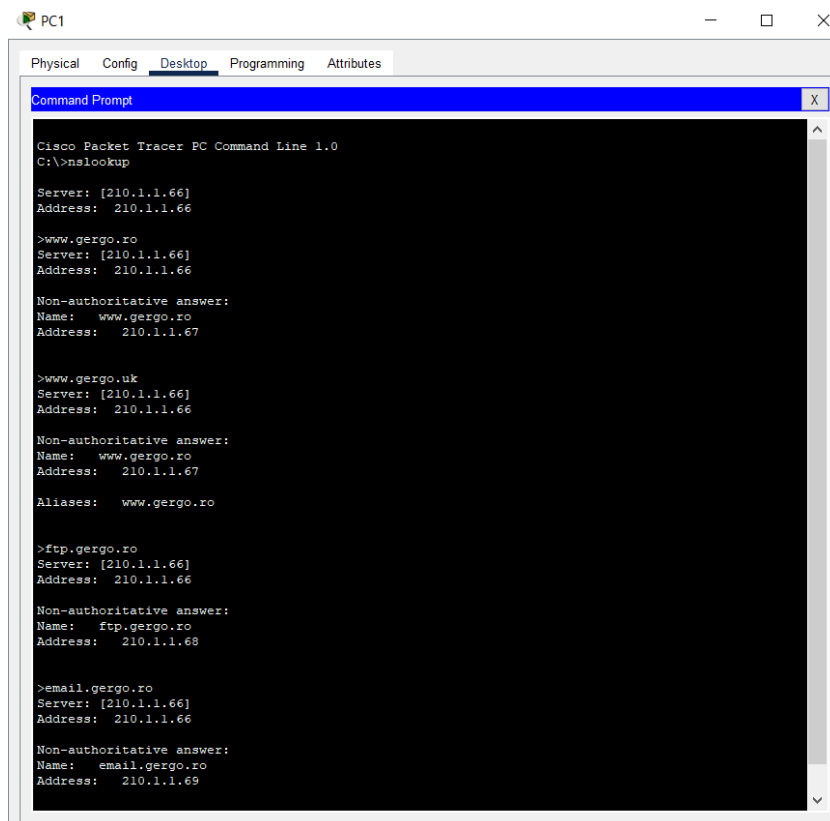
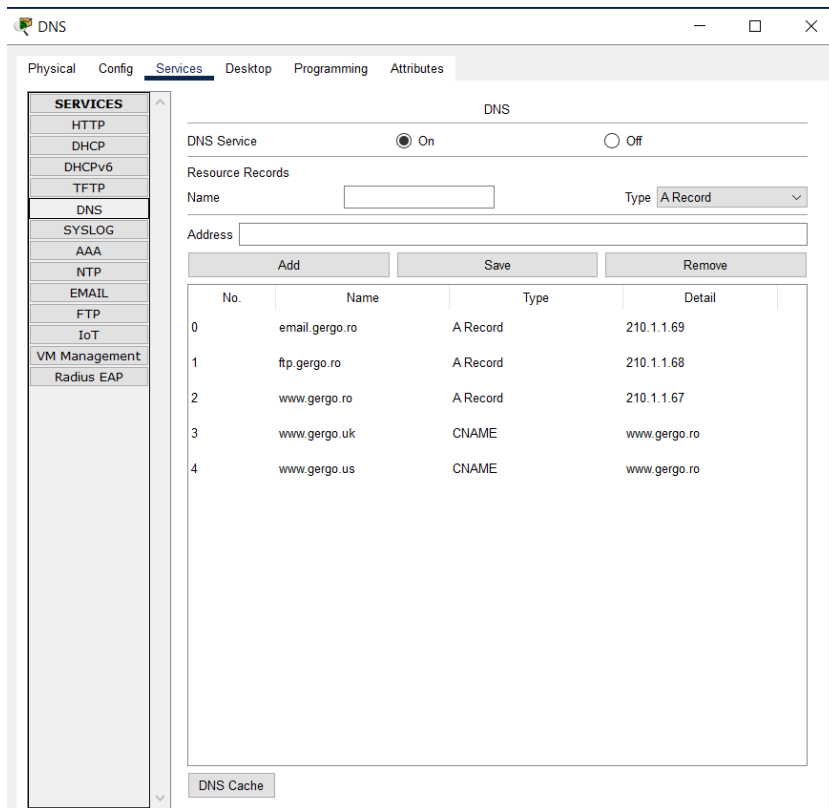
```
#enable
#config terminal
#interface Fa 0/1
# switchport mode access
# switchport access vlan 99
#exit
#interface range Gig 0/1-2
#switchport mode access
#switchport access vlan 99
```

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
```

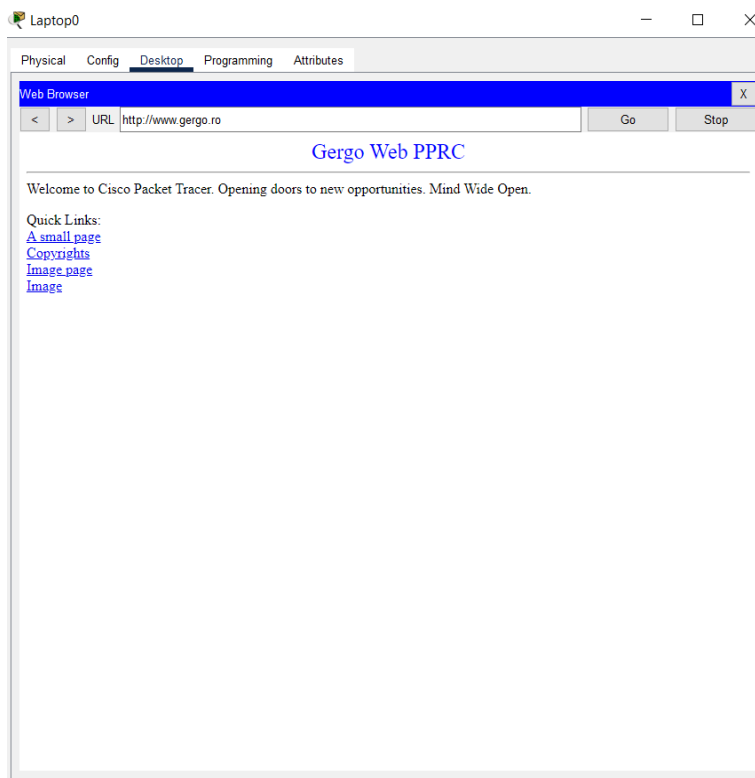
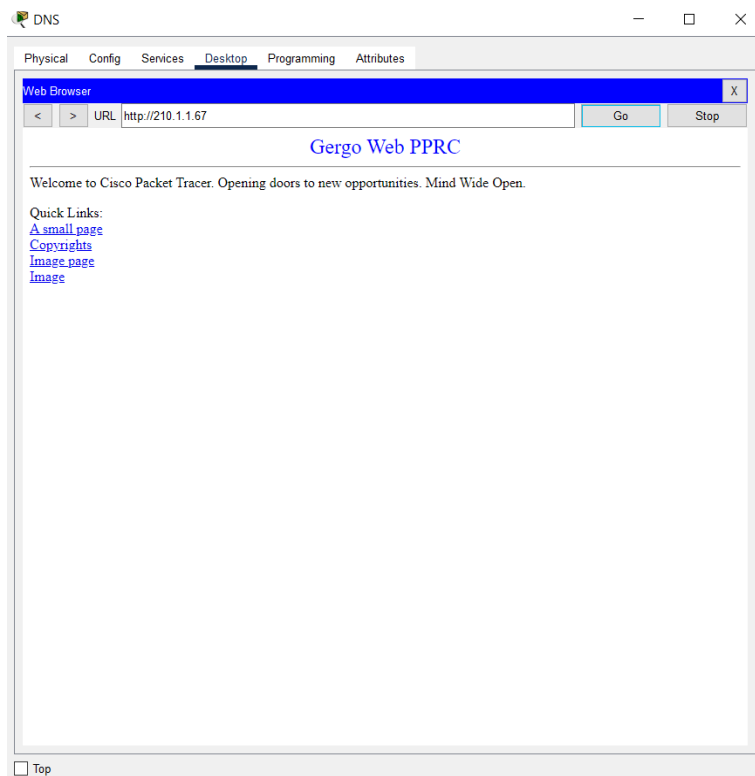
Serverul DNS:

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



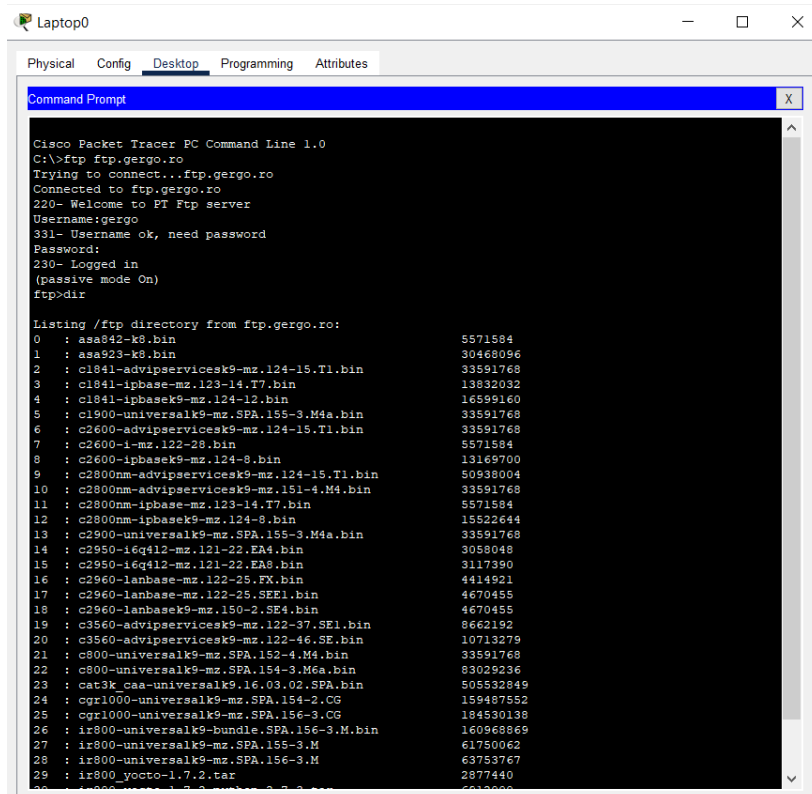
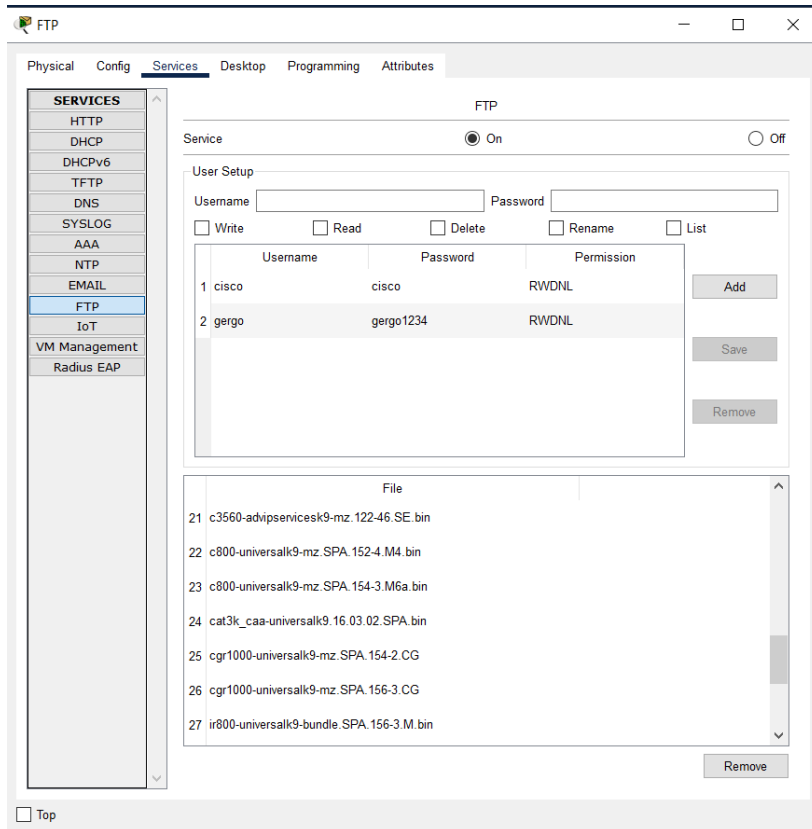
Pagina de HTTP:

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 afiseze toate fisierele.



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:

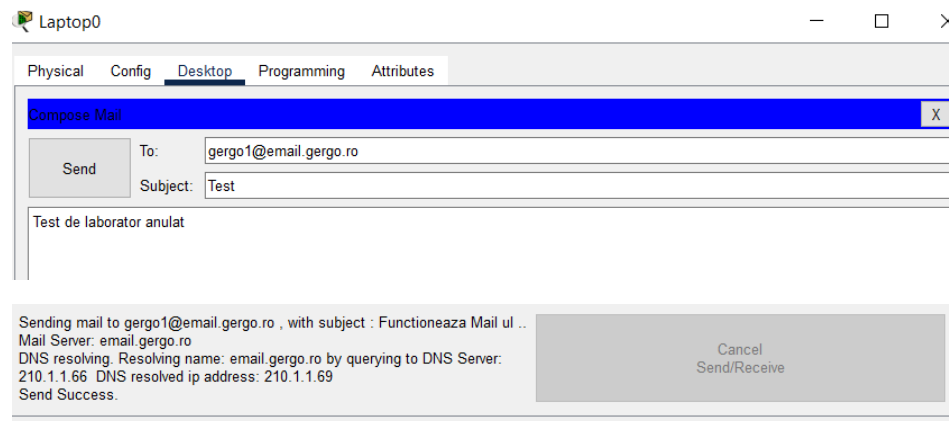
Pasul 1:

The screenshot shows the 'MAIL' configuration window with the 'Services' tab selected. On the left, a 'SERVICES' list includes HTTP, DHCP, DHCPv6, TFTP, DNS, SYSLOG, AAA, NTP, EMAIL (highlighted), FTP, IoT, VM Management, and Radius EAP. The main area is titled 'EMAIL' and contains two service toggle buttons: 'SMTP Service' (ON) and 'POP3 Service' (ON). Below these is a 'Domain Name' field with the value 'email.gergo.ro' and a 'Set' button. A 'User Setup' section includes a 'User' field with 'gergo1' and a 'Password' field. To the right of the password field are buttons for '+', '-', 'Change', and 'Password'.

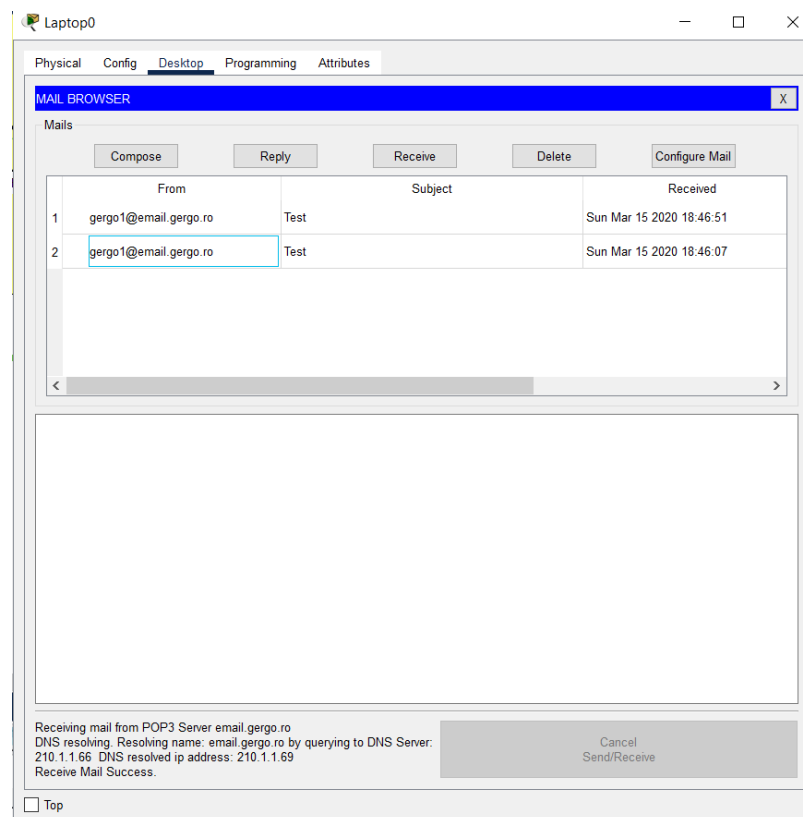
Pasul 2:

The screenshot shows the 'Configure Mail' dialog box with the 'Desktop' tab selected. The dialog is divided into three sections: 'User Information' with fields for 'Your Name' (Szekely Gergo) and 'Email Address' (gergo1@email.gergo.ro); 'Server Information' with fields for 'Incoming Mail Server' and 'Outgoing Mail Server' (both email.gergo.ro); and 'Logon Information' with fields for 'User Name' (gergo1) and 'Password' (masked with dots). At the bottom are buttons for 'Save', 'Remove', 'Clear', and 'Reset'.

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-uriei 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 switch-urile 3 si 4, si la main router:

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

Prin adaugarea cuvantului cheie *secret* parolele utilizatorilor 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 folosim *secret* atunci cu parole cryptate:

```
Switch#show run
Building configuration...

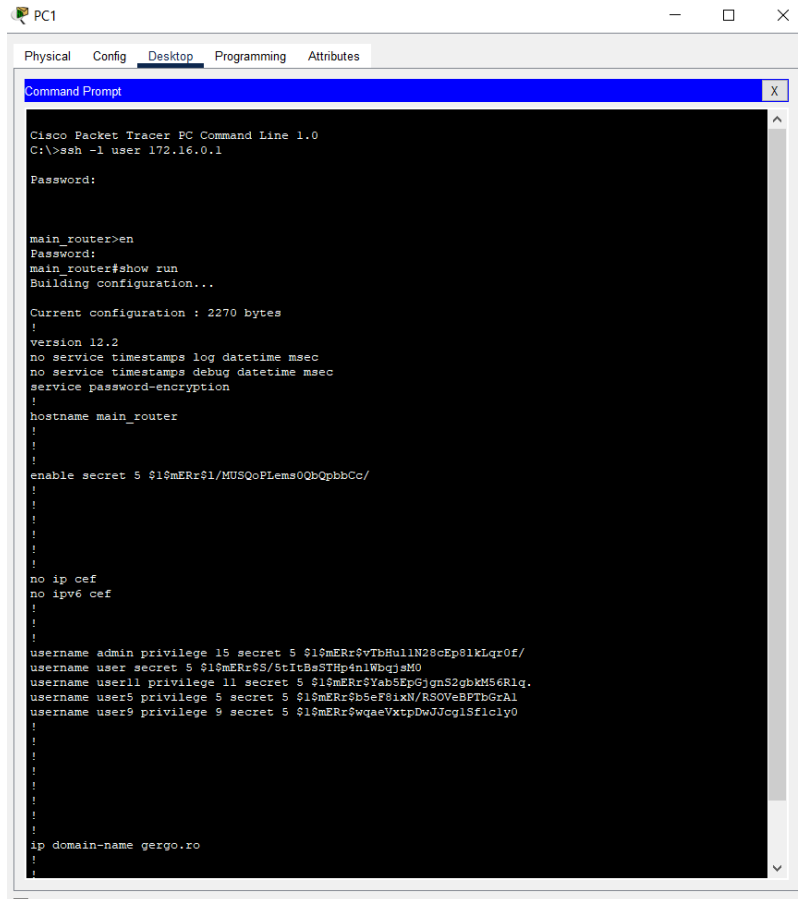
Current configuration : 1475 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
enable secret 5 $1$mERr$1/MUSQoPLems0QbQpbbCc/
!
!
!
!
username admin secret 5 $1$mERr$vTbHullN28cEp8lkLqr0f/
username user privilege 1 password 0 user
username user11 secret 5 $1$mERr$Yab5EpGjgnS2gbkM56Rlq.
username user5 privilege 5 password 0 user5
username user9 secret 5 $1$mERr$WqaeVxtpDwJcglSflcly0
!
```

Securitate SSH

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.



```

Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l user 172.16.0.1

Password:

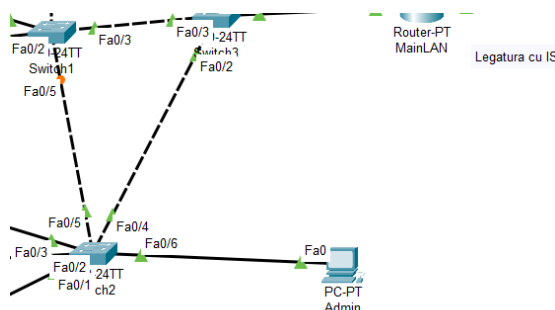
main_router>en
Password:
main_router#show run
Building configuration...

Current configuration : 2270 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname main_router
!
!
enable secret 5 $1$mERr$1/MU5QoPLems0bQpbhCc/
!
!
!
no ip cef
no ipv6 cef
!
!
username admin privilege 15 secret 5 $1$mERr$VtBhullN28cEp$1kLqrOf/
username user secret 5 $1$mERr$S/6tItBeSTHp4nlWbqjeM0
username user11 privilege 11 secret 5 $1$mERr$Yab5EpGjgmS2gbkM56Rlq.
username user5 privilege 5 secret 5 $1$mERr$B5eF8ixN/R50VeBPTbGzhl
username user9 privilege 9 secret 5 $1$mERr$WqaeVxtpDwJJCglsfclcy0
!
!
!
!
ip domain-name gergo.ro
!
!

```

Admin/Management

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

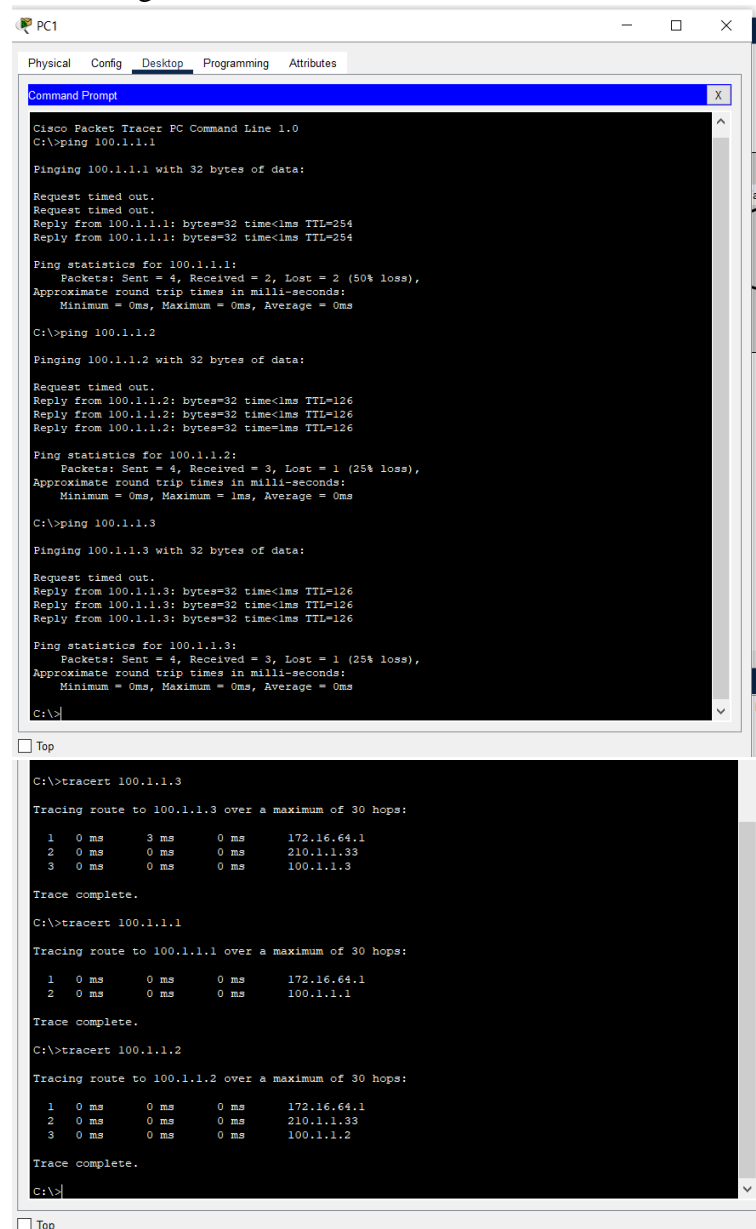


Am setat adrese publice pentru routerul ISP, switch, PC si serverul din INTERNET. Pe routerul SPI am folosit urmatoarele comenzi:

```
#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 reseaua interna (PC1) si o adresa din reseaua externa (o adresa IP publica), folosind comanda *#ping <adresaIP>*. Cu comanda *#tracert <adresaIP>* verificam daca conexiunea este stabilita corect si gaseste interfetele necesare.



```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 100.1.1.1

Pinging 100.1.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 100.1.1.1: bytes=32 time<1ms TTL=254
Reply from 100.1.1.1: bytes=32 time<1ms TTL=254

Ping statistics for 100.1.1.1:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 100.1.1.2

Pinging 100.1.1.2 with 32 bytes of data:

Request timed out.
Reply from 100.1.1.2: bytes=32 time<1ms TTL=126
Reply from 100.1.1.2: bytes=32 time<1ms TTL=126
Reply from 100.1.1.2: bytes=32 time<1ms TTL=126

Ping statistics for 100.1.1.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 100.1.1.3

Pinging 100.1.1.3 with 32 bytes of data:

Request timed out.
Reply from 100.1.1.3: bytes=32 time<1ms TTL=126
Reply from 100.1.1.3: bytes=32 time<1ms TTL=126
Reply from 100.1.1.3: bytes=32 time<1ms TTL=126

Ping statistics for 100.1.1.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>

C:\>tracert 100.1.1.3

Tracing route to 100.1.1.3 over a maximum of 30 hops:

  0  0 ms    3 ms    0 ms    172.16.64.1
  1  0 ms    0 ms    0 ms    210.1.1.33
  2  0 ms    0 ms    0 ms    100.1.1.3

Trace complete.

C:\>tracert 100.1.1.1

Tracing route to 100.1.1.1 over a maximum of 30 hops:

  0  0 ms    0 ms    0 ms    172.16.64.1
  1  0 ms    0 ms    0 ms    100.1.1.1

Trace complete.

C:\>tracert 100.1.1.2

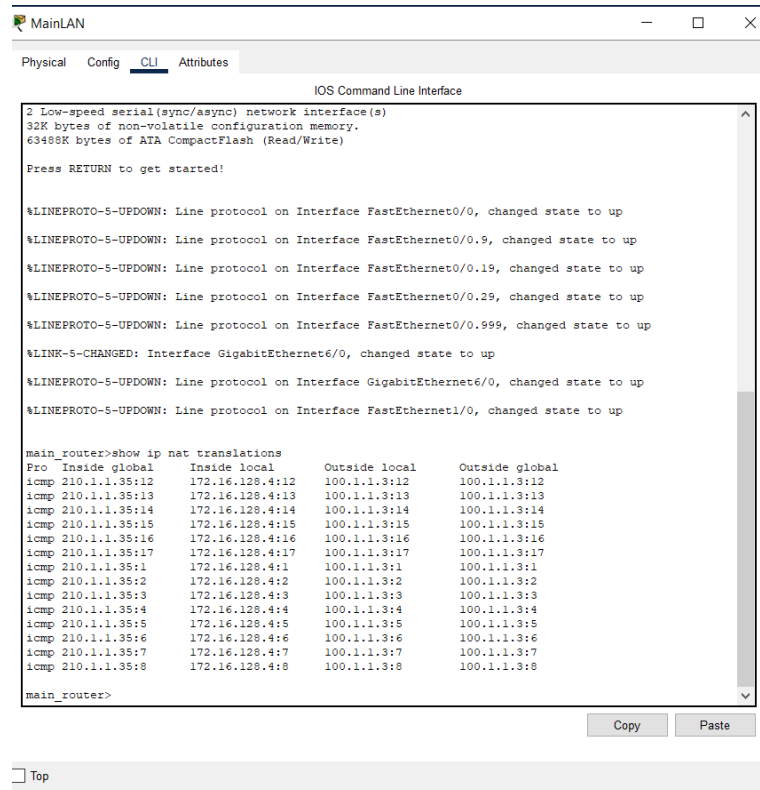
Tracing route to 100.1.1.2 over a maximum of 30 hops:

  0  0 ms    0 ms    0 ms    172.16.64.1
  1  0 ms    0 ms    0 ms    210.1.1.33
  2  0 ms    0 ms    0 ms    100.1.1.2

Trace complete.

C:\>
```

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



The screenshot shows the MainLAN web interface with the CLI tab selected. The CLI output displays the status of various network interfaces and the results of the `show ip nat translations` command.

```
2 Low-speed serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
63498K bytes of ATA CompactFlash (Read/Write)

Press RETURN to get started!

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.9, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.19, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.29, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.999, changed state to up
%LINK-5-CHANGED: Interface GigabitEthernet6/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet6/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up

main_router>show ip nat translations
Pro  Inside global      Inside local      Outside local      Outside global
icmp 210.1.1.35:12       172.16.128.4:12  100.1.1.3:12      100.1.1.3:12
icmp 210.1.1.35:13       172.16.128.4:13  100.1.1.3:13      100.1.1.3:13
icmp 210.1.1.35:14       172.16.128.4:14  100.1.1.3:14      100.1.1.3:14
icmp 210.1.1.35:15       172.16.128.4:15  100.1.1.3:15      100.1.1.3:15
icmp 210.1.1.35:16       172.16.128.4:16  100.1.1.3:16      100.1.1.3:16
icmp 210.1.1.35:17       172.16.128.4:17  100.1.1.3:17      100.1.1.3:17
icmp 210.1.1.35:1       172.16.128.4:1  100.1.1.3:1       100.1.1.3:1
icmp 210.1.1.35:2       172.16.128.4:2  100.1.1.3:2       100.1.1.3:2
icmp 210.1.1.35:3       172.16.128.4:3  100.1.1.3:3       100.1.1.3:3
icmp 210.1.1.35:4       172.16.128.4:4  100.1.1.3:4       100.1.1.3:4
icmp 210.1.1.35:5       172.16.128.4:5  100.1.1.3:5       100.1.1.3:5
icmp 210.1.1.35:6       172.16.128.4:6  100.1.1.3:6       100.1.1.3:6
icmp 210.1.1.35:7       172.16.128.4:7  100.1.1.3:7       100.1.1.3:7
icmp 210.1.1.35:8       172.16.128.4:8  100.1.1.3:8       100.1.1.3:8

main_router>
```