



UNIVERSITATEA TEHNICA DIN CLUJ-NAPOCA

**FACULTATEA DE AUTOMATICA SI CALCULATOARE
TEHNOLOGIA INFORMATIEI**

**Proiectarea Retelelor de Calculatoare
PROIECT**

Tema 2 - proiect cladire comerciala cu 3 niveluri

Student:

Claudiu-Andrei BIRLUTIU

Indrumator:

Conf.dr.ing. Peculea Adrian

An academic:

2022/2023

Cuprins

1	Problema	1
2	Sedinta 1	2
2.1	Arhitectura	2
2.2	Mode Trunk	4
2.3	Definire VLAN-uri	5
2.3.1	Definire protocol VTP	5
2.3.2	Creare VLAN-uri	6
2.4	Spanning Tree	7
2.5	Adrese IP	8
2.5.1	Subnetare	8
2.5.2	Configurare Main Router	9
2.5.3	Conifgurare server DHCP	9
3	Sedinta 2	14
3.1	Extindere retea server: http, ftp, dns, mail	14
3.2	Configurare gigabit interface pentru DMZ	15
3.3	Configurare Swtich DMZ	15
3.4	Adrese servere	16
3.5	Interfata virtuala switch DMZ	17
3.6	DNS server	18
3.7	Server http	18
3.8	Server ftp	18
3.9	Mail Server	19
4	Sedinta 3	21
4.1	Router ISP	21
4.2	Configurarea translatarei adreselor - NAT	22
4.3	Extindere retea in exterior	24
4.4	Mail din exterior	25
4.5	Http page	26
5	Sedinta 4	27
5.1	Conectare ssh MainRouter	27
5.2	Conexiune ssh MainSwitch (switch 0)	29
6	Securitate	31
6.1	Conectare ssh MainRouter restrictionata doar la vlan 10	31
6.2	Conectare cu AAA local si remote ISP router	34

Capitolul 1

Problema

Se considera o cladire comerciala cu **3** niveluri. Se va folosi:

- adresa de retea $172.27.0.0/16$ pentru reseaua **intranet**
- adresa de retea $210.2.2.64/27$ pentru **DMZ**
- adresa de retea $210.2.2.32/27$ 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: $210.2.2.35-210.2.2.62$.

Conectarea la ISP se va realiza printr-o interfata de tip Ethernet avand adresa $210.2.2.34/27$. Adresa ISP-ului este $210.2.2.33/27$. 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 niveluri de privilegii, criptarea parolelor, configurarea remote se va face doar prin ssh, se va securiza protocolul VTP.

Capitolul 2

Sedinta 1

2.1 Arhitectura

Pentru proiectarea, simularea si testarea rețelei ne-am folosit de tool-ul Packet Tracer, un software de simulare a rețelelor de calculatoare dezvoltat de către Cisco Systems. Pentru crearea rețelei clădirii cu 3 nivele avem nevoie initial de un Router(2911) la care legam un Switch(2950) din care se pot conecta prin cablu inversor cate un switch la fiecare nivel al clădirii. De asemenea, se leaga prin cabluri inversoare switchul de la nivelul 1 cu cel de la nivelul 2 si switch-ul de la nivelul 3 cu cel de la nivelul 2. La adaugarea cablurilor am pastrat o regula de legare a acestora pentru fi mai usor de configurat, astfel:

- Fa0/1 de la Switch1 cu Fa0/1 de la Switch0 principal
- Fa0/1 de la Switch2 cu Fa0/2 de la Switch0
- Fa0/1 de la Switch3 cu Fa0/3 de la Switch0
- Fa0/2 de la Switch3 cu Fa0/2 de la Switch2 (urmatoarele disponibile)
- Fa0/2 de la Switch1 cu Fa0/3 de la Switch2 (urmatoarele disponibile)
- Gig0/1 de la Switch0(main) la Router1 cu cablu drept

Vom avea modelul de stea extinsa.

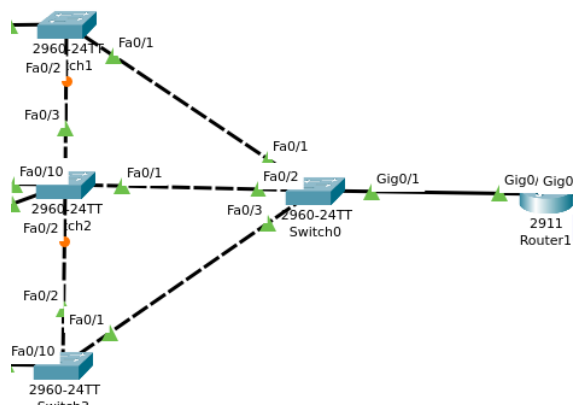


Figura 2.1: Arhitectura pe cele 3 nivele ale clădirii

În continuare am pus la fiecare nivel câte un host (pentru testarea rețelei, în realitate vor fi mai multe hosturi). În cerința se specifică faptul că adresele host-urilor vor fi alocate prin folosirea unui singur server DHCP, un server ce va oferi configurații IP automate și dinamic pentru dispozitivele care se conectează la o rețea. În momentul în care se va lansa o cerere spre serverul DHCP de alocare adresă IP, serverul DHCP va lua această cerere și va alocă o adresă IP disponibilă dintr-un pool de adrese IP care sunt predefinite și o va atribui acelui dispozitiv.

Pentru a ușura procesul de configurare s-a ales legarea hosturilor la switch-uri la portul Fa0/10, iar serverul la portul Fa0/11 cum se observă în figura următoare. Legarea s-a făcut cu cablu drept.

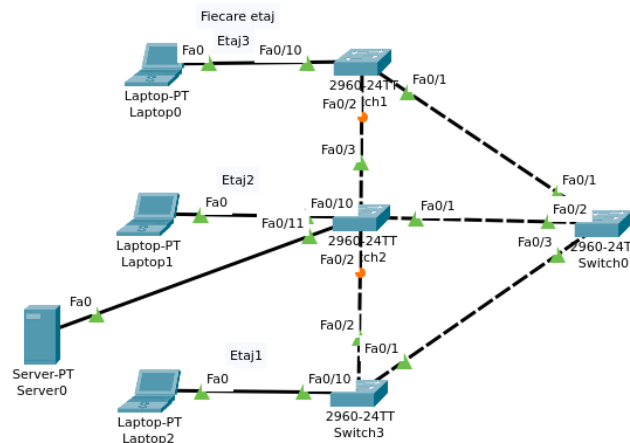


Figura 2.2: Legare hosturi

La nivelul fiecărui etaj vom avea un VLAN, o rețea virtuală care permite gruparea și separarea dispozitivelor dintr-o rețea fizică în grupuri logice distincte - se permite astfel gruparea dispozitivelor în funcție de nevoile specifice ale organizației sau rețelei. Vor fi definite 3 VLAN-uri la nivelul fiecărui etaj și de asemenea va fi definit un VLAN de management, utilizat pentru gestionarea și controlul echipamentelor de rețea. Pentru configurări avem 2 tipuri de linii: de acces și trunk. Liniile de acces vor lega utilizatorii la rețea (laptop-switch), iar trunk vom folosi pentru legăturile switch-switch și switch-router. Vom configura astfel Router1 care reprezintă router-ul principal și vom rula comenzile următoare:

```
#pentru a intra in modul admin/root
$ enable
#pentru a intra in modul configurare
$ configure terminal
#pentru a seta numele la MainRouter
$ hostname MainRouter
#punem porturile 1, 2, si 3 in modul trunc
```

```

#vom intra in modul configurare range
$ interface range fastEthernet 0/1-3
#definim porturile ca trunk
$ switchport mode trunk
#dam un pas in spate si configuram calea gigabit
$ interface gigabitEthernet 0/1
# definim modul trunk pentru cale
$ switchport mode trunk

```

2.2 Mode Trunk

Vom continua sa configuram switch-urile de la cele 3 nivele si vom pune porturile lor pe mode-ul trunk in afara de Fa0/10 care e mode acces (leaga utilizatorii). Exemplu pentru Switch3 (FirstFloor)

```

#pentru a intra in modul admin/root
$ enable
#pentru a intra in modul configurare
$ configure terminal
#pentru a seta numele la FirstFloor
$ hostname FirstFloor
#punem porturile 1, 2, si 3 in modul trunc
#vom intra in modul configurare range
$ interface range fastEthernet 0/1-2
#definim porturile ca trunk
$ switchport mode trunk

```

```

.
hostname FirstFloor
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
    switchport mode trunk
!
interface FastEthernet0/2
    switchport mode trunk
!

```

Figura 2.3: Verificare configurare porturi trunk SwitchPort3

<pre>FirstFloor#show interfaces trunk Port Mode Encapsulation Status Native vlan Fa0/1 on 802.1q trunking 1 Fa0/2 on 802.1q trunking 1 Port Vlans allowed on trunk Fa0/1 1-1005 Fa0/2 1-1005 Port Vlans allowed and active in management domain Fa0/1 1,10,20,30,99 Fa0/2 1,10,20,30,99 Port Vlans in spanning tree forwarding state and not pruned Fa0/1 1,10,20,30,99 Fa0/2 1,10,20,30,99 FirstFloor#</pre>	<pre>SecondFloor#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 Port Vlans allowed on trunk Fa0/1 1-1005 Fa0/2 1-1005 Fa0/3 1-1005 Port Vlans allowed and active in management domain Fa0/1 1,10,20,30,99 Fa0/2 1,10,20,30,99 Fa0/3 1,10,20,30,99 Port Vlans in spanning tree forwarding state and not pruned Fa0/1 1,10,20,30,99 Fa0/2 none Fa0/3 1,10,20,30,99 SecondFloor#</pre>
(a) FirstFloor	(b) SecondFloor
<pre>ThirdFloor#show interfaces trunk Port Mode Encapsulation Status Native vlan Fa0/1 on 802.1q trunking 1 Fa0/2 on 802.1q trunking 1 Port Vlans allowed on trunk Fa0/1 1-1005 Fa0/2 1-1005 Port Vlans allowed and active in management domain Fa0/1 1,10,20,30,99 Fa0/2 1,10,20,30,99 Port Vlans in spanning tree forwarding state and not pruned Fa0/1 1,10,20,30,99 Fa0/2 none ThirdFloor#</pre>	
(c) ThirdFloor	

Figura 2.4: Verificare setare porturi trunk

S-au aplicat comenzi similare pentru celelalte 2 switch-uri pentru a le configura. Vom rula comanda *show interfaces trunk* pentru fiecare switch pentru a vedea daca s-au setat interfetele corespunzator. Se observa in figura 2.4.

2.3 Definire VLAN-uri

2.3.1 Definire protocol VTP

Plecand de la premisa ca fiecare switch care transporta un VLAN, trebuie sa aiba definit acel VLAN atunci toate VLAN-urile definite trebuie definite pe toate switch-urile noastre. Pentru acest lucru ne vom folosi de protocolul **VTP**. Folosind acest protocol, vom putea face modificarile ce tin de VLAN-uri la nivelul unui switch principal-server (MainSwitch in cazul nostru), iar modificarile de VLAN vor fi cunoscute de celelalte switch-uri de care se leaga - clientii. Configurarea protocol VTP pe MainSwitch 2.5:

```
#pentru a intra in modul admin/root
$ enable
#pentru a intra in modul configurare
$ configure terminal
#definire domeniu VTP
$ vtp domain claudiuBirlutiu
#definire parola
$ vtp password Claudiu
```



```
#setare MainSwitch to server
$ vtp mode server
```

Ne vom duce pe celelalte 3 switch-uri de la fiecare nivel si le configuram ca fiind clienti vtp cu acelasi domeniu si parola definite pentru MainSwitch. Exemplu configurare:

```
#pentru a intra in modul admin/root
$ enable
#pentru a intra in modul configurare
$ configure terminal
#definire domeniu VTP
$ vtp domain claudiuBirlutiu
#definire parola
$ vtp password Claudiu
#setare switch ca client
$ vtp mode client
```

```
MainSwitch#show vtp status
VTP Version capable      : 1 to 2
VTP version running      : 1
VTP Domain Name          : claudiuBirlutiu
VTP Pruning Mode         : Disabled
VTP Traps Generation     : Disabled
Device ID                 : 0001.9779.5400
Configuration last modified by 0.0.0.0 at 3-1-93 00:50:18
Local updater ID is 172.27.99.2 on interface V199 (lowest numbered VLAN interface found)

Feature VLAN :
-----
VTP Operating Mode      : Server
Maximum VLANs supported locally : 255
Number of existing VLANs : 9
Configuration Revision  : 8
MD5 digest              : 0xFD 0xA6 0xFF 0xA0 0x14 0xB7 0x47 0x84
                        | 0xE0 0xF4 0xB8 0x38 0x30 0xE5 0xE7 0xF5
```

Figura 2.5: Vizualizare VTP MainSwitch-Server

2.3.2 Creare VLAN-uri

In mod normal, exista un VLAN default pe MainSwitch, dar acesta din motive de securitate nu se foloseste. Vom defini 4 VLAN-uri:

- VLAN-10: nivel 1
- VLAN-20: nivel 2
- VLAN-30: nivel 3
- VLAN-99: trafic de management

Mergem pe MainSwitch si executam:

```
#pentru a intra in modul admin/root
$ enable
#pentru a intra in modul configurare
$ configure terminal
```

```

# definire vlan 10
$ vlan 10
#definire nume
$ nam Vlan10
#inapoi un pas
$ exit
# definire vlan 20
$ vlan 20
#definire nume
$ nam Vlan20
#inapoi un pas
$ exit
# definire vlan 30
$ vlan 30
#definire nume
$ nam Vlan30
#inapoi un pas
$ exit
# definire vlan 99
$ vlan 99
#definire nume
$ nam Vlan99
#inapoi un pas
$ exit

```

```

MainSwitch>sh vlan

```

VLAN Name	Status	Ports
1 default	active	Fa0/4, 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, Gig0/2
10 Vlan10	active	
20 Vlan20	active	
30 Vlan30	active	
99 Vlan99	active	
1002 fddi-default	active	
1003 token-ring-default	active	

(a) Main

```

FirstFloor>sh vlan

```

VLAN Name	Status	Ports
1 default	active	Fa0/3, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, 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 Fa0/10
10 Vlan10	active	
20 Vlan20	active	
30 Vlan30	active	
99 Vlan99	active	
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddi-default	active	

(b) FirstFloor

```

SecondFloor>sh vlan

```

VLAN Name	Status	Ports
1 default	active	Fa0/4, Fa0/5, Fa0/6, Fa0/7 Fa0/8, Fa0/9, 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
10 Vlan10	active	
20 Vlan20	active	Fa0/10, Fa0/11
30 Vlan30	active	
99 Vlan99	active	

(c) SecondFloor

```

ThirdFloor>sh vlan

```

VLAN Name	Status	Ports
1 default	active	Fa0/3, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, 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
10 Vlan10	active	
20 Vlan20	active	
30 Vlan30	active	Fa0/10
99 Vlan99	active	
1002 fddi-default	active	

(d) ThirdFloor

Figura 2.6: Verificare vlan-uri

2.4 Spanning Tree

O alta problema ce a fost rezolvata este Spanning Tree. Facem MainSwitch radacina (**root bridge**), ii da prioritatea cea mai mare (numar mic) 2.7 Pe

MainSwitch vom rula:

```
#pentru a intra in modul admin/root
$ enable
#pentru a intra in modul configurare
$ configure terminal
#setam prioritatea cea mai mare
$ spanning-tree vlan 1, 10, 20 ,30, 99 priority 0
```

```
MainSwitch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    1
             Address     0001.C94C.64EE
             This bridge is the root
             Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 s

  Bridge ID  Priority    1 (priority 0 sys-id-ext 1)
```

Figura 2.7: Root bridge

2.5 Adrese IP

La routere, servere vom da adrese statice, pe cand utilizatorilor le vom oferi adrese dinamice. Protocolul pentru adrese dinamice este DHCP.

DHCP este un protocol de rețea care permite dispozitivelor să obțină automat o adresă IP și alte informații de rețea necesare pentru a se conecta la rețea. Când un dispozitiv se conectează la o rețea care utilizează un server DHCP, dispozitivul trimite o cerere de configurare a rețelei la serverul DHCP. Serverul va răspunde cu o adresă IP disponibilă, precum și alte informații, cum ar fi adresa gateway-ului sau a serverului DNS.

2.5.1 Subnetare

Vom porni de la adresa de rețea **172.27.0.0/16**. Vom subneta aceasta adresa pentru a respecta cerinta problemei (minim 200 de accesari/utilizatori) => vom lasa un numar minim de 8 biti pentru partea de host => 8 biti pentru partea de subnet.

Pentru simplitate vom acorda subnet 10 pentru Vlan10, subnet 20 pentru vlan20, subnet 30 pentru Vlan30, subnet 99 pentru Vlan 99.

Exemplu configurare subretea pentru Vlan 20:

- 172.27.20.0/24 - subretea
- 172.27.20.1 - gateway

- 172.27.20.2 - DHCP
- 172.27.20.10 - 172.27.20.254 - hosturile (peste 200)

2.5.2 Configurare Main Router

In prima faza se va activa interfata gigabit:

```
#pentru a intra in modul admin/root
$ enable
#pentru a intra in modul configurare
$ configure terminal
# configuram interfata
$ interface gigabitEthernet 0/0
# activam interfata
$ no shutdown
# un pas inapoi
$ exit
# definim subinterfata pentru Vlan 20
$ interface gigabitEthernet 0/0.20
# incapsualare si sa ramana in vlan 20
$ encapsulation dot1Q 20
# definire subretea 20
$ ip address 172.27.20.1 255.255.255.0
```

2.5.3 Conifgurare server DHCP

In prima faza trebuie configurate interfetele Fa0/10 si Fa0/11 ale switchurilor de pe cele 3 nivele in modul access. Exemplu configurare Switch 2:

```
#pentru a intra in modul admin/root
$ enable
#pentru a intra in modul configurare
$ configure terminal
# configuram interfatele
$ interface range fastEthernet 0/10-11
# setam modul
$ switchport mode access
# asociem vlan-ul
$ switchport access vlan 20
```

Se repeta pasii pentru fiecare Switch de la cele 3 nivele si se asociaza VLAN-ul corespunzator.

In continuare se va defini serviciul de DHCP pentru server-ul 0. Se va defini pentru fiecare VLAN un server pool in care se vor seta informatiile de gateway, host-uri valide, subnet etc. Se observa in figura 2.10

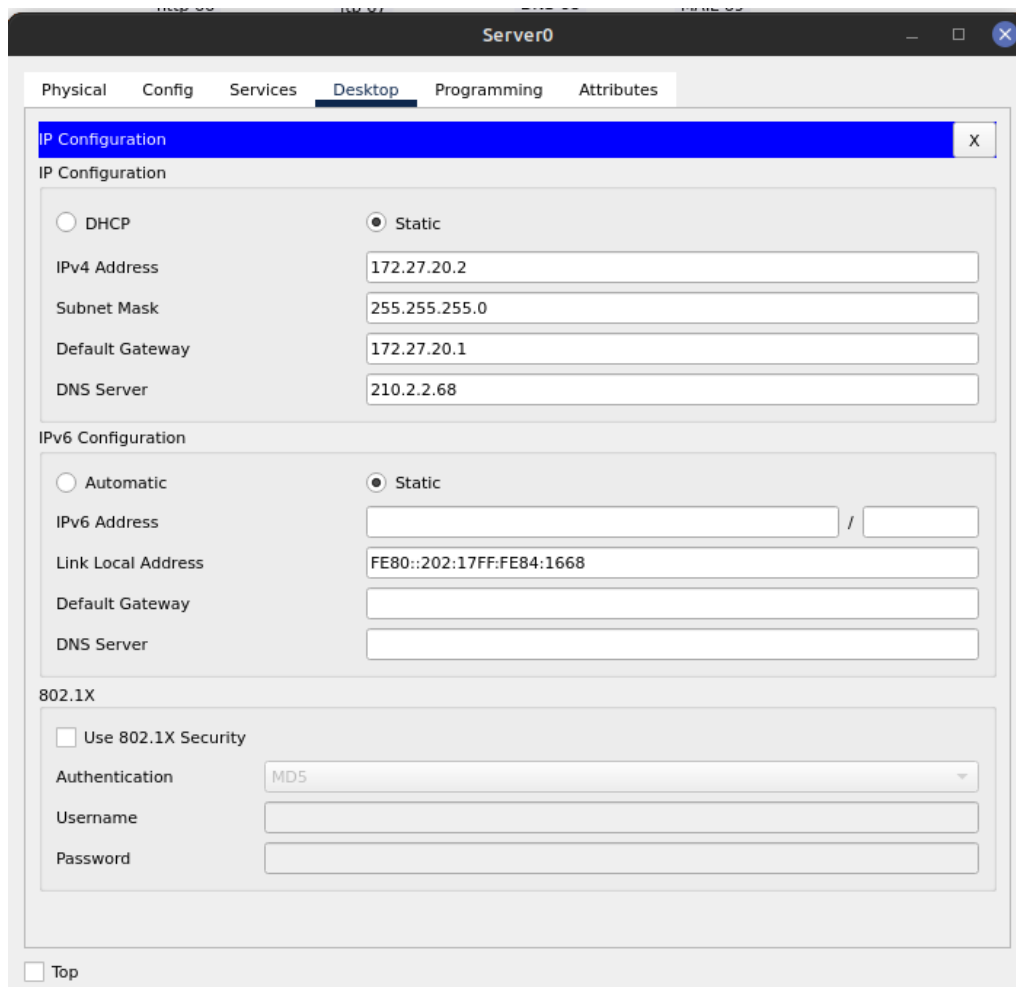


Figura 2.8: Configurarea DHCP Server

Pentru fiecare statie (laptopuri) vom se in cadrul ip-configuration optiunea DHCP - si i se va da automat o adresa IP. Se poate observa in 2.12

Remark. In cazul definiri celorlalte interfete pentru vlan-urile 30, 10 si 99(aici nu helper address) se va pune un help-address care va face trimitere catre serverul de DHCP.

`$ ip helper-address 172.27.20.2`

Remark. Se va pune default gateway in MainRouter configuration

`$ ip default-gateway 172.27.99.1`

Remark. Pentru cele 3 switch-uri se va configura interfata pentru vlan99

`$ int vlan 99`

`$ ip address 172.27.99.3 255.255.255.0`

`$ no shutdown`

`$ exit`

`$ ip default-gateway 172.27.99.1`

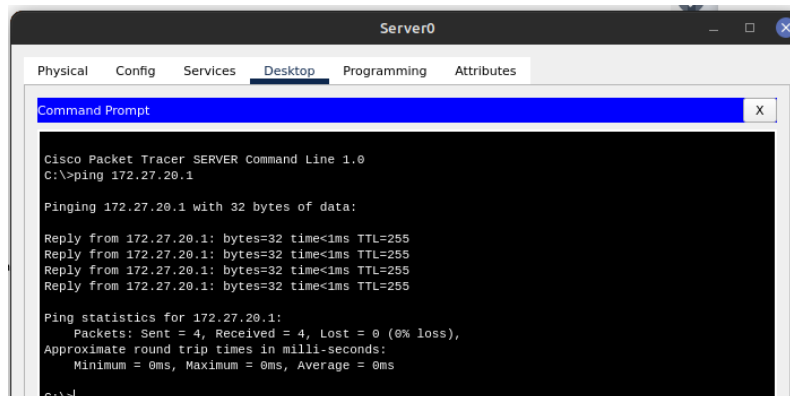


Figura 2.9: Testare ping din server DHCP

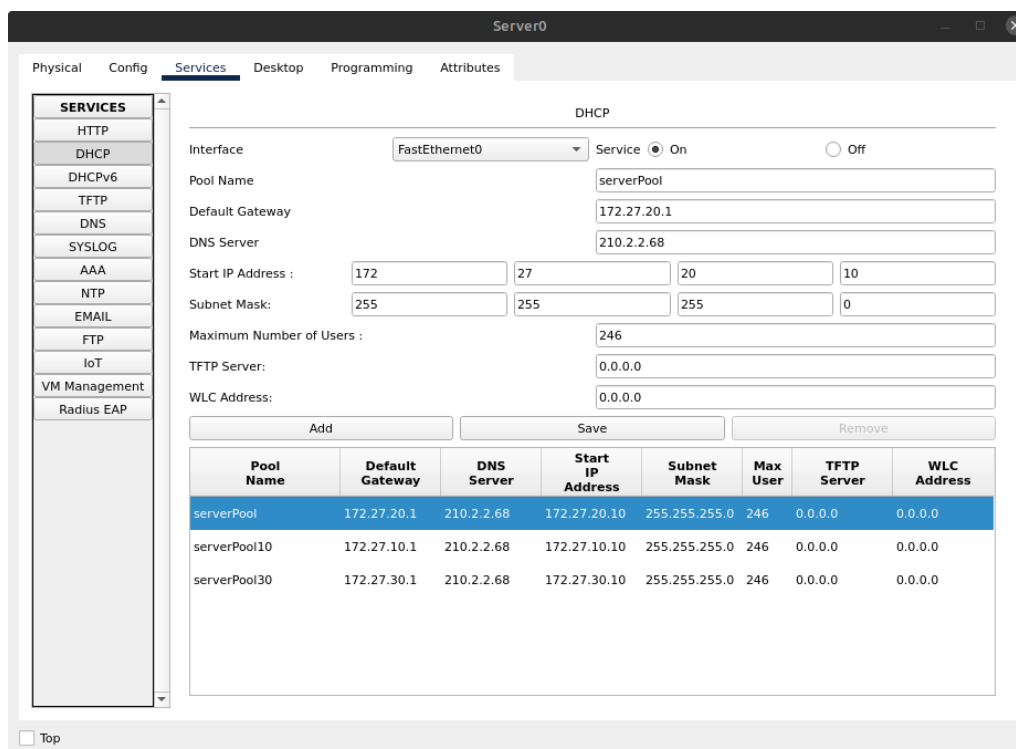


Figura 2.10: Configurare DHP service

Laptop1

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

☒ DHCP ☐ Static

IPv4 Address 172.27.20.10

Subnet Mask 255.255.255.0

Default Gateway 172.27.20.1

DNS Server 210.2.2.68

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80::290:CFF:FE95:6C87

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication MD5

Username

Password

☐ Top

Figura 2.11: Setare optiune DHCP pentru statii

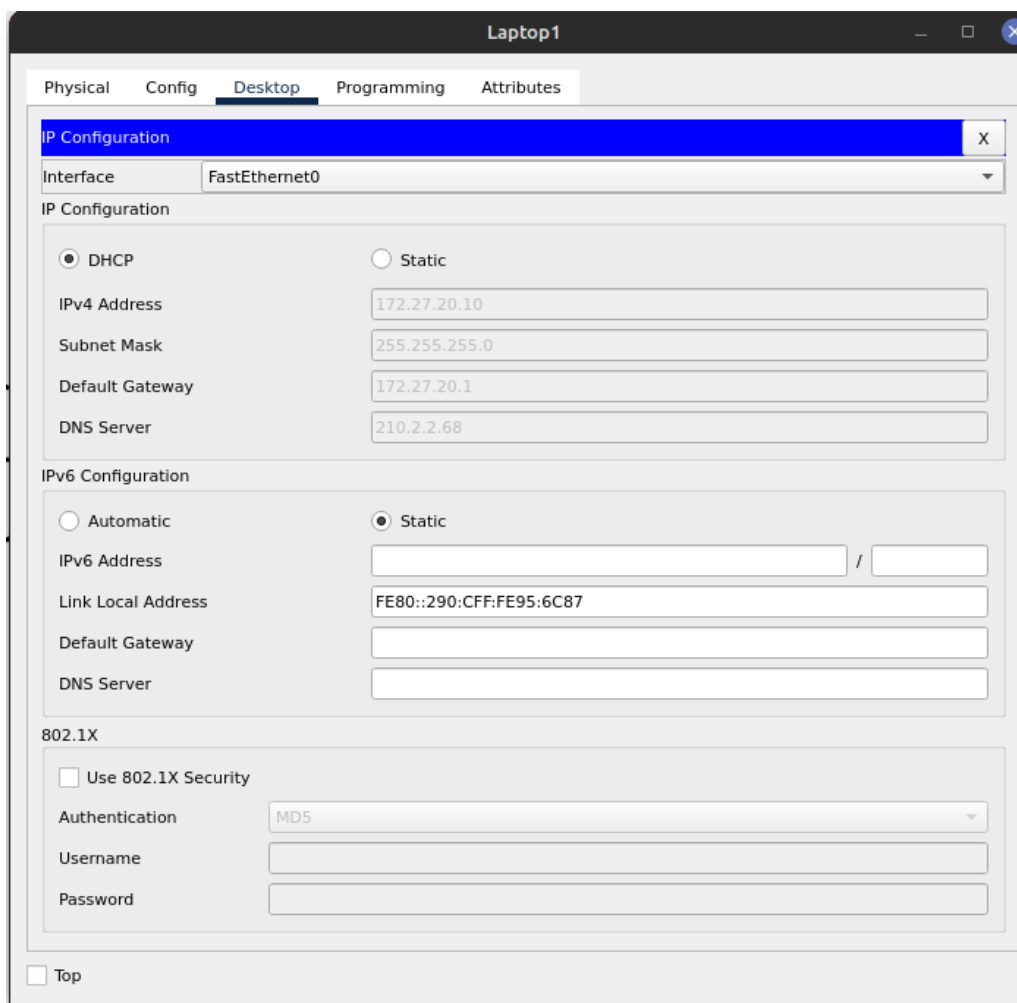


Figura 2.12: Setare optiune DHCP pentru statii

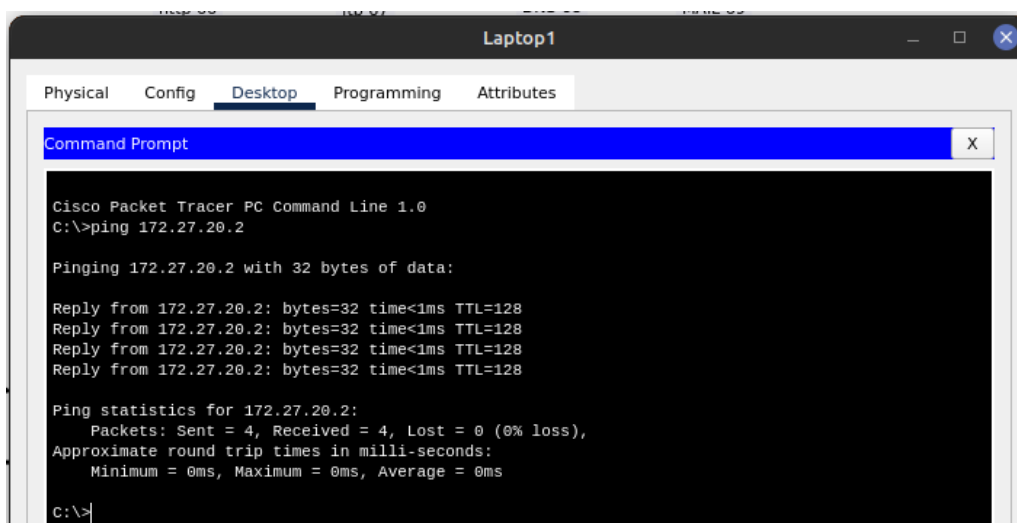


Figura 2.13: Testare ping

Capitolul 3

Sedinta 2

În cadrul acestei sedințe s-au adăugat serverele de HTTP, FTP, DNS și MAIL ce vor fi plasate în DMZ și vor avea adrese publice. Numele domeniului web va include numele meu. Pentru asigurarea conectivității se vor configura rute statice. Prin DMZ se înțelege o zonă demilitarizată, o sub-rețea fizică sau logică care separă o rețea locală (LAN) de alte rețele necunoscute - de obicei, internetul public. DMZ-urile sunt cunoscute și sub denumirea de rețele perimetrice sau subrețele monitorizate.[1]

3.1 Extindere rețea server: http, ftp, dns, mail

S-a adăugat un nou Switch-2960 (4) pe care l-am denumit DMZ și am legat 4 servere (tipul Server-PT) la acest switch printr-un cablu drept pe porturile Fa0/1, Fa0/2, Fa0/3 și respectiv Fa0/4. Tot printr-un cablu drept a fost legat switchul nou la Router1 pe interfața Gig0/1. Arhitectura nouă se poate observa în figura 3.1

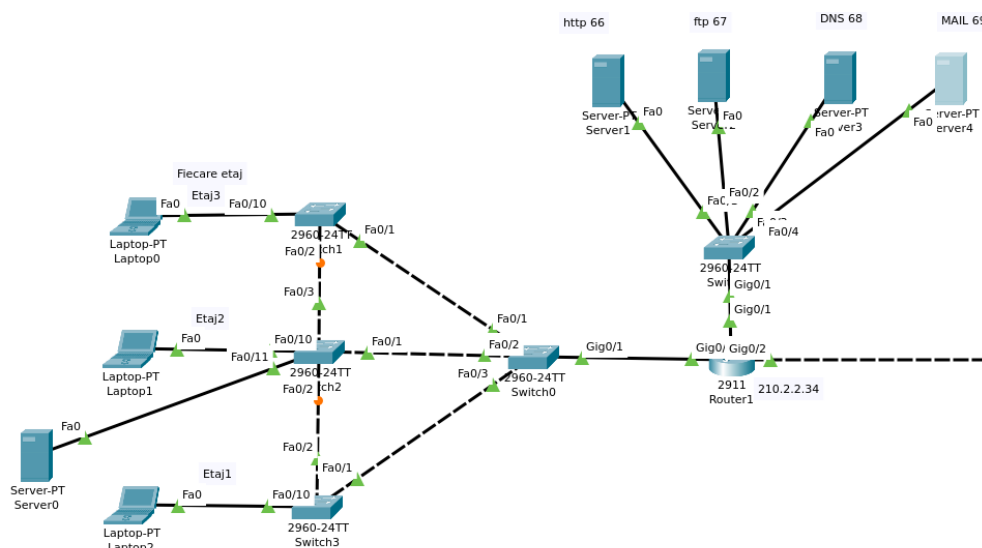


Figura 3.1: Legare servere: http, ftp, dns, mail

Fiecare din cele 4 servere vor fi configurate servicii pentru http, ftp, DNS și mail.

3.2 Configurare gigabit interface pentru DMZ

Configurarea interfeței gigabit Ethernet 0/1 al main Routerului și adăugarea adresei de gateway din subrețeaua DMZ.

```
#pentru a intra in modul admin/root
$ enable
#pentru a intra in modul configurare
$ configure terminal
#intrare in modul configurare interfata Gi 0/1
$ interface gigabitEthernet 0/1
# adauagarea adresei gateway-ului
$ ip address 210.2.2.65 255.255.255.224
# activam interfata
$ no shutdown
```

3.3 Configurare Swtich DMZ

În continuare se regăsesc comenzile de configurare ale Switch-ului 4 pe care îl vom denumi DMZ.

```
#pentru a intra in modul admin/root
$ enable
#pentru a intra in modul configurare
$ configure terminal
# setare hostname
$ hostname DMZ
# creare vlan 2
$ vlan 2
#se da un nume
$ name DMZ
#un pas inapoi
$ exit
#intrarea in modul de configurare al interfetelor Fa0/1-24
$ interface range fastEthernet 0/1-24
# setam modul acces ca tip de acces pentru aceste interfete
# in aces mod interfața este utilizată pentru a
# conecta un dispozitiv final de rețea sau stație
$ switchport mode access
# atribuim vlan 2 interfetelor: toate pachetele care intră
# și ies prin această interfață sunt atribuite VLAN-ului 2
$ switchport access vlan 2
# dam un pas inapoi si intram in modul configurare a
# interfetelor Gigabit
$ exit
```

```
$ interface range gigabitEthernet 0/1-2
# setam cele 2 interfete ca fiind de tip access si
# atribuim vlan-ul 2
$ switchport mode access
$ switchport access vlan 2
```

3.4 Adrese servere

Adrese din **subnetul**: 210.2.2.64/27, **masca**: 255.255.255.224. Default gateway -ul va fi astfel: 210.2.2.65. DNS serverul va fi cel de la adresa ip 210.2.2.68. Pentru cele 4 servere s-au adaugat ip-uri static astfel:

- server http: 210.2.2.66 masca: 255.255.255.224; DNS server: 210.2.2.68
- server ftp: 210.2.2.67 masca: 255.255.255.224; DNS server: 210.2.2.68
- server DNS: 210.2.2.68 masca: 255.255.255.224; DNS server: 210.2.2.68
- server mail: 210.2.2.69 masca: 255.255.255.224; DNS server: 210.2.2.68

Se poate observa in figura 3.2 cum au fost atribuite aceste valori pentru serverul 1. S-a testat de asemenea ping-ul spre gateway si adres 127.27.20.2 3.3

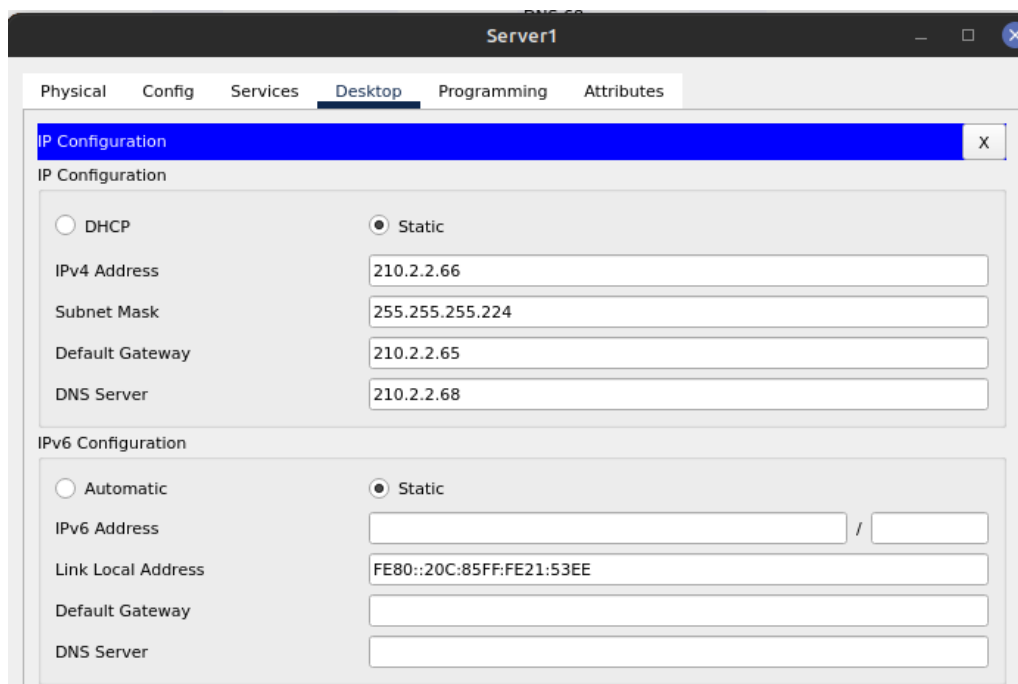


Figura 3.2: Ip configuration server 1

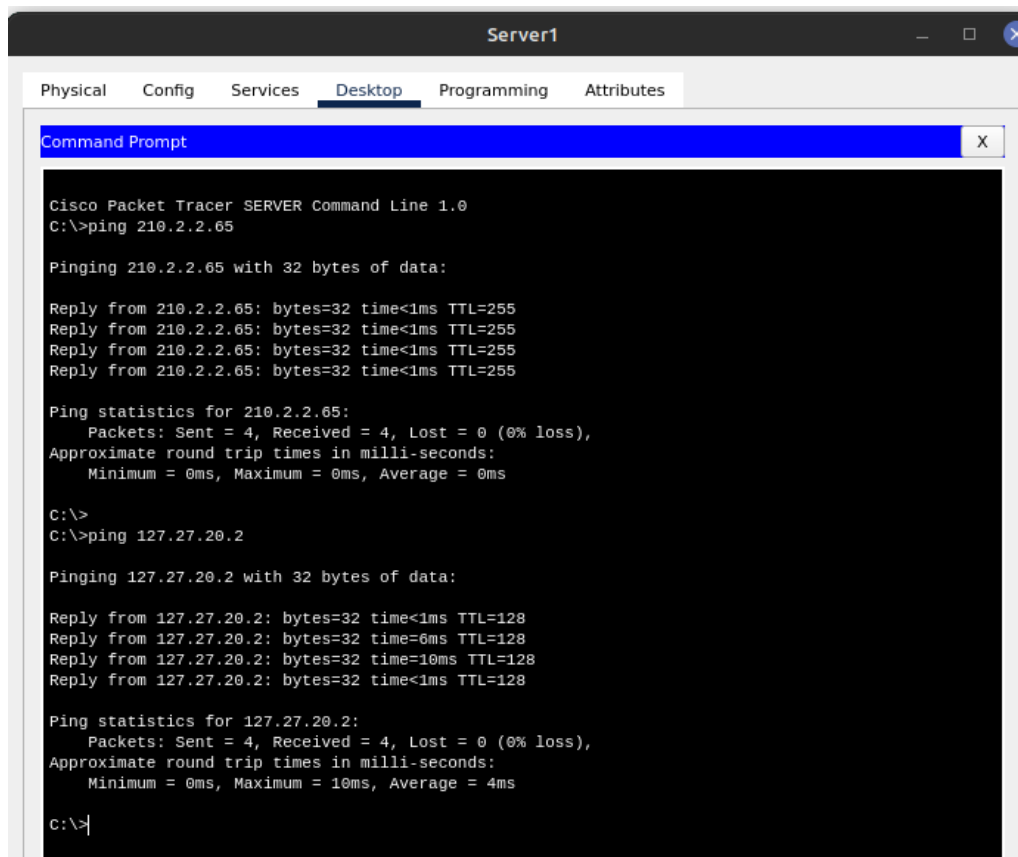


Figura 3.3: Testare ping server 1

3.5 Interfata virtuala switch DMZ

Am adaugat o interfata virtuala pe switch DMZ la care i-am atribuit o adresa IP (210.2.2.70/24), o interfata VLAN fiind o metodă de a crea mai multe rețele logice separate pe un singur switch.

```
#pentru a intra in modul admin/root
$ enable
#pentru a intra in modul configurare
$ configure terminal
#intrare in modul configurare interfata vlan 2
$ interface vlan 2
# setare adresa ip
$ ip address 210.2.2.70 255.255.255.224
# activam interfata
$ no shutdown
# dam un pas insapoi
$ exit
# declararea default gateway
$ ip default-gateway 210.2.2.65
```

3.6 DNS server

În prima fază vom seta pentru Serverul DHCP DNS-ul ca fiind adresa 210.2.2.68. De asemenea pentru fiecare server pool (10, 30, 20) s-a adăuga DNS-server-ul. Se poate observa acest lucru în figura 3.4

The screenshot shows the configuration interface for a DHCP server. The 'Interface' is set to 'FastEthernet0' and the 'Service' is 'On'. The 'Pool Name' is 'serverPool10'. The 'Default Gateway' is '172.27.10.1'. The 'DNS Server' is '210.2.2.68'. The 'Start IP Address' is '172.27.10.10' and the 'Subnet Mask' is '255.255.255.0'. The 'Maximum Number of Users' is '246'. The 'TFTP Server' and 'WLC Address' are both '0.0.0.0'. Below the configuration fields are buttons for 'Add', 'Save', and 'Remove'. At the bottom is a table showing the configuration for three server pools: 'serverPool', 'serverPool10', and 'serverPool30'.

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	172.27....	210.2.2...	172.27....	255.25...	246	0.0.0.0	0.0.0.0
serverPool10	172.27....	210.2.2...	172.27....	255.25...	246	0.0.0.0	0.0.0.0
serverPool30	172.27....	210.2.2...	172.27....	255.25...	246	0.0.0.0	0.0.0.0

Figura 3.4: Setare DNS server pentru serverul DHCP

Vom rula apoi la nivelul fiecărei stații/ host (laptop0 - laptop 2) în command prompt următoarea instrucțiune pentru a vedea dacă și-a luat adresa serverului DNS, adică 210.2.2.68:

```
C:\> ipconfig /renew
```

3.7 Server http

Se va configura serviciul de http pentru a afișa numele meu (Birlutiu Claudiu-Andrei), iar în server-ul 3 (210.2.2.68) se va adăuga în DNS un domain name `www.claudiu.ro`, de tipul record și care sta pentru adresa ip: 210.2.2.66 (adresa serverului 1 caruia i-am configurat pagina http). Vom deschide din laptop 0 un web browser și vom căuta pagina: **www.claudiu.ro** și se poate observa rezultatul în figura 3.5

3.8 Server ftp

Pentru configurarea serviciului de ftp pe serverul 2(210.2.2.67) s-a creat un user cu **username: claudiu** și **parola: claudiu** și cu permisiunile de write, read, delete, rename și list. În serverul de DNS s-a adăugat un nou domeniu:



Figura 3.5: HTTP service

ftp.claudiu.ro cu adresa 210.2.2.67 . Cadrul de testare: pe laptop 0 s-a creat un fisier text denumit **ftp_claudiu.txt**. M-am conecta la serverul ftp cu user si parola, se observa in figura cum incarc si fisierul 3.6

```
C:\>ftp ftp.claudiu.ro
Trying to connect...ftp.claudiu.ro
Connected to ftp.claudiu.ro
220- Welcome to PT Ftp server
Username:claudiu
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>put ftp_claudiu.txt

writing file ftp_claudiu.txt to ftp.claudiu.ro:
File transfer in progress...

[Transfer complete - 18 bytes]

18 bytes copied in 0.153 secs (117 bytes/sec)
ftp>
```

Figura 3.6: Ftp connection

3.9 Mail Server

Am adaugat domeniul **mail.cladiu.ro** in DNS server la adresa 210.2.2.69. In serviciul de EMAIL din serverul 210.2.2.69 am adaugat domaeniul mail.claudiu.ro si am adaugat 2 useri claudiu1 si claudiu2 cu aceeasi parola ca username-ul. In figura 3.7 se pot observa mail-urile trimise de pe o adresa de email pe alta.

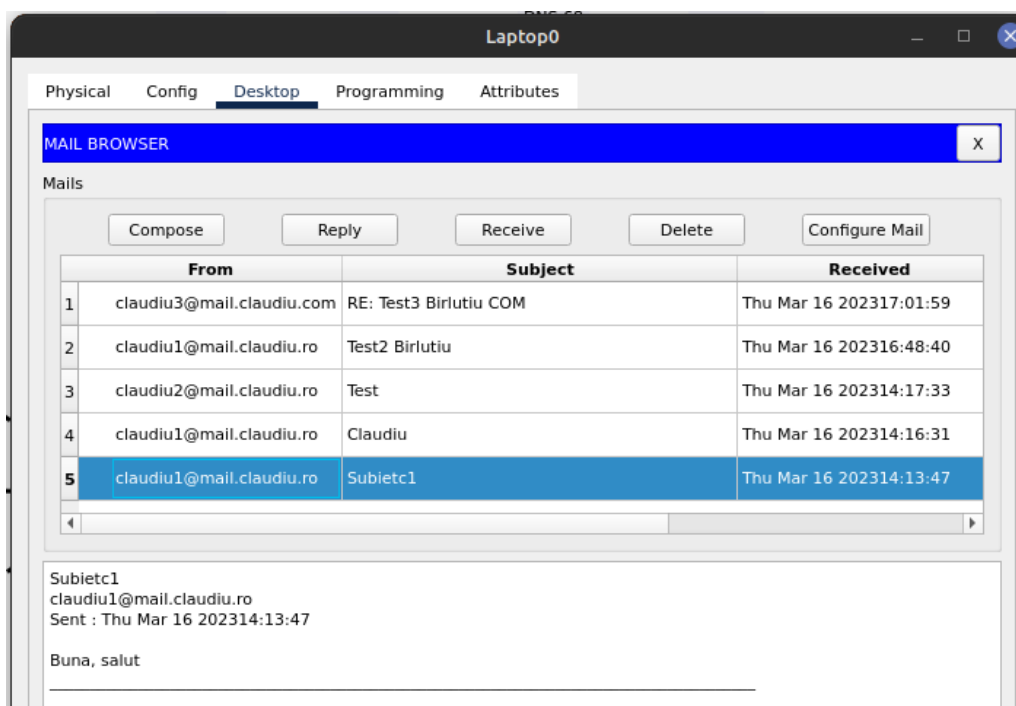


Figura 3.7: Mails

Capitolul 4

Sedinta 3

In cadrul acestei sedinte se va face sccesul in exterior folosind NAT pe routerul care controleaza DMZ, pe urmatorul interval de adrese publice: 210.2.2.35-210.2.2.62. De asemenea, conectarea la ISP se va realiza printr-o interfata de tip Ethernet avand adresa 210.2.2.34/27. Adresa ISP-ului este 210.2.2.33/27. Reteaua Internet se va simula prin intermediul unui server si a unui calculator. se va face conectarea la ISP printr-o interfata de tip Ethernet avand adresa **210.2.2.34/27**. Adresa ISP-ului este 210.2.2.33/27, iar Reteaua Internet se va simula prin intermediul unui server si a unui calculator.

4.1 Router ISP

Se va adauga un router nou in arhitectura si il legam printr-un cablu drept de mainRouter intre interfetele Gi0/2. Acest router nou adaugat va juca rolul unui dispozitiv utilizat de un furnizor de servicii de internet (ISP) pentru a furniza conectivitate la internet a cladirii noastre fig 4.1.

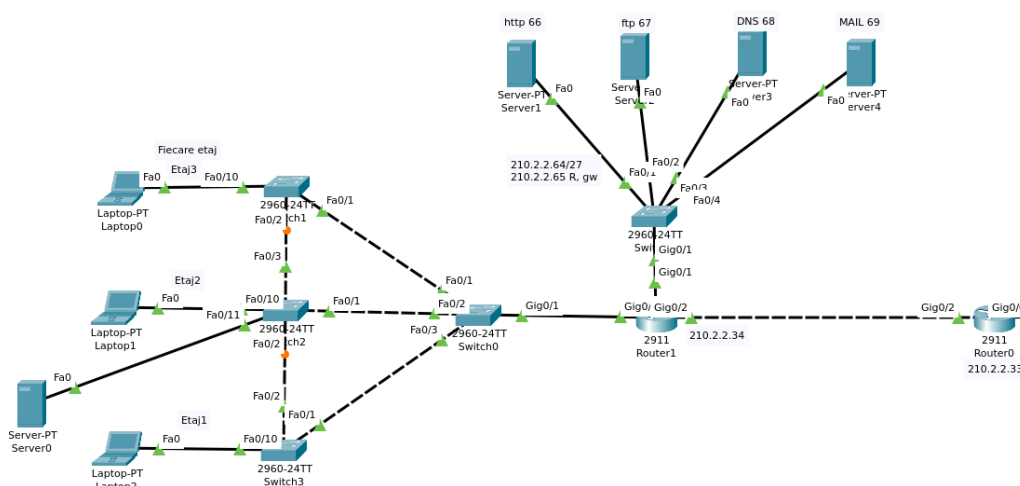


Figura 4.1: Arhitectura noua cu router ISP

Subreteaua data de acest router va fi 210.2.2.32/27. Astfel adresa IP a router-ului ISP pe interfata Gi0/2 va fi 210.2.2.33, iar pe int Gi0/2 a mainRouter-ului este 210.2.2.34. Pentru NAT vom avea adrese ip intre 210.2.2.35-210.2.2.62.

Vom configura mainRouter pentru a activa interfata Gi0/2 astfel:

```
#pentru a intra in modul admin/root
$ enable
#pentru a intra in modul configurare
$ configure terminal
#intrare in modul configurare interfata Gi0/2
$ interface gigabitEthernet 0/2
# setare adresa ip
$ ip address 210.2.2.34 255.255.255.224
# activam interfata
$ no shutdown
```

Vom configura in continuare router-ul adaugat pentru ISP astfel:

```
#pentru a intra in modul admin/root
$ enable
#pentru a intra in modul configurare
$ configure terminal
# setam un host name
$ hostname ISP
#intrare in modul configurare interfataa Gi0/2
$ interface gigabitEthernet 0/2
# setare adresa ip
$ ip address 210.2.2.33 255.255.255.224
# activam interfata
$ no shutdown
```

Am testat daca functioneaza ping-ul la 210.2.2.34 din ISP fig4.2.

```
ISP(config)#do ping 210.2.2.34

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 210.2.2.34, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

ISP(config)#
```

Figura 4.2: Ping ISP la 210.2.2.34

4.2 Configurarea translatarei adreselor - NAT

Pentru a permite accesul la Internet sa va folosi tehnica NAT(Network Address Translation) care va fi schimba adresa/adrese IP private ce sunt utilizate in interiorul cladirii noastre intr-o adresa publica (sau mai multe) si invers.

Scopul nostru este de a crea cadrul prin care din retea interna putem comunica in Internet. Astfel in mainRouter vom face urmatoarele configurari:

```
#pentru a intra in modul admin/root
```

```

$ enable
#pentru a intra in modul configurare
$ configure terminal
#se va defini lista de acces pentru IP-urile private care vor
#putea face NAT
$ access-list 15 permit 172.27.0.0 0.0.255.255
#definesc lista de adrese publice ce vor fi utilizate
#pentru NAT
$ ip nat pool claudiu 210.2.2.35 210.2.2.62 netmask 255.255.255.224
#realizez legatura intre IP-urile private si cele publice
$ ip nat inside source list 15 pool claudiu
#folosim comanda nat inside pe interfata Gi 0/0 private
#a mainRouter-ului avand in vedere VLAN-urile definite
$ interface gigabitEthernet 0/0.10
$ ip nat inside
$ exit
$ interface gigabitEthernet 0/0.20
$ ip nat inside
$ exit
$ interface gigabitEthernet 0/0.30
$ ip nat inside
$ exit
#interfata Gi 0/2 va fi config outside pentru ca realizeaza
#legatura cu ISP
$ interface gigabitEthernet 0/2
$ ip nat outside
$ exit

```

Dupa un ping de la laptopul 0 la 210.2.2.33 vom verifica apoi lista de translatari NAT fig4.3

```

mainRouter#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
icmp 210.2.2.35:1      172.27.30.10:1    210.2.2.33:1       210.2.2.33:1
icmp 210.2.2.35:2      172.27.30.10:2    210.2.2.33:2       210.2.2.33:2
icmp 210.2.2.35:3      172.27.30.10:3    210.2.2.33:3       210.2.2.33:3
icmp 210.2.2.35:4      172.27.30.10:4    210.2.2.33:4       210.2.2.33:4
icmp 210.2.2.35:5      172.27.30.10:5    210.2.2.33:5       210.2.2.33:5
icmp 210.2.2.35:6      172.27.30.10:6    210.2.2.33:6       210.2.2.33:6
icmp 210.2.2.35:7      172.27.30.10:7    210.2.2.33:7       210.2.2.33:7
icmp 210.2.2.35:8      172.27.30.10:8    210.2.2.33:8       210.2.2.33:8
mainRouter#

```

Figura 4.3: Verificare ip nat translations

4.3 Extindere retea in exterior

Se vor adauga un switch, un server si un laptop in reteaua 100.0.0.0/8. Noua arhitectura va arata astfel ca in fig 4.4. Vom configura in continuare interfata

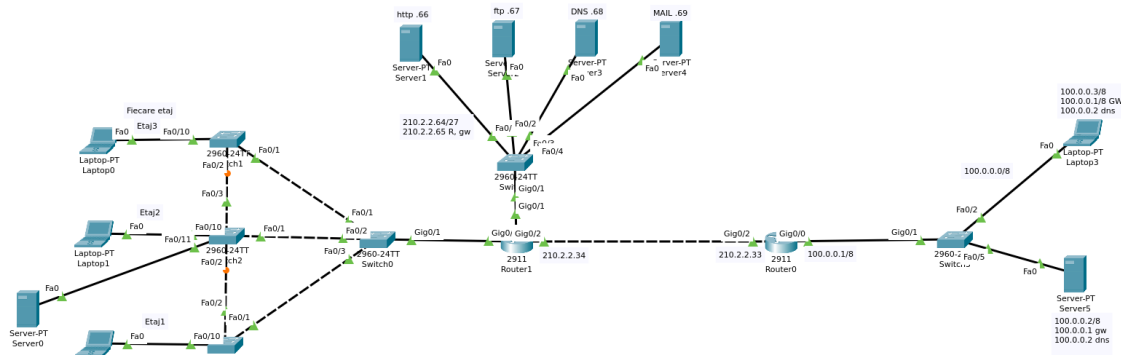
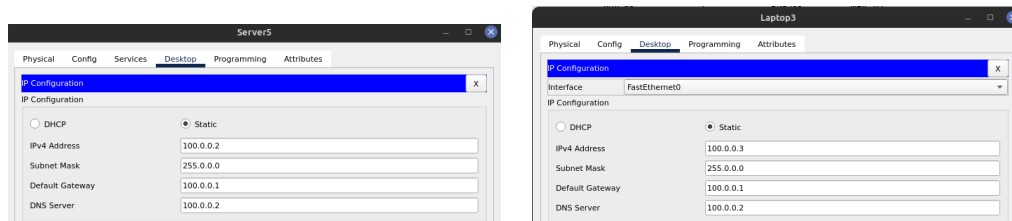


Figura 4.4: Retea finala

Gi0/0 a router-ului ISP

```
#pentru a intra in modul admin/root
$ enable
#pentru a intra in modul configurare
$ configure terminal
#intrare in modul configurare interfata Gi0/2
$ interface gigabitEthernet 0/0
# setare adresa ip
$ ip address 100.0.0.0.1 255.0.0.0
# activam interfata
$ no shutdown
```

Vom intra in IP configuration pentru server-ul nou adaugat si in IP configuration al laptopului. Serverul va oferi serviciul de DNS in exterior fig4.5.



(a) Server

(b) Laptop

Figura 4.5: IP configuration

In mainRouter vom configura o ruta statica default cu adresa de next hop -> adresa routerului ISP:

```
#pentru a intra in modul admin/root
```

```
$ enable
#pentru a intra in modul configurare
$ configure terminal
# toate pachetele care nu sunt directionate catre o ruta mai specifica
#trebuie sa fie directionate catre adresa IP 210.2.2.33.
$ ip route 0.0.0.0 0.0.0.0 210.2.2.33
```

Efectul comenzii de mai sus este ilustrata in fig 4.7

In ISP router vom seta ip route astfel:

```
#comanda specifica ca pachetele care sunt directionate catre adresa
#de retea 210.2.2.64 cu masca 255.255.255.224 trebuie sa fie directionate
#catre adresa IP 210.2.2.34
$ ip route 210.2.2.64 255.255.255.224 210.2.2.34
```

```

172.27.0.0/16 is variably subnetted, 8 subnets, 2 masks
C    172.27.10.0/24 is directly connected, GigabitEthernet0/0.10
L    172.27.10.1/32 is directly connected, GigabitEthernet0/0.10
C    172.27.20.0/24 is directly connected, GigabitEthernet0/0.20
L    172.27.20.1/32 is directly connected, GigabitEthernet0/0.20
C    172.27.30.0/24 is directly connected, GigabitEthernet0/0.30
L    172.27.30.1/32 is directly connected, GigabitEthernet0/0.30
C    172.27.99.0/24 is directly connected, GigabitEthernet0/0.99
L    172.27.99.1/32 is directly connected, GigabitEthernet0/0.99
210.2.2.0/24 is variably subnetted, 4 subnets, 2 masks
C    210.2.2.32/27 is directly connected, GigabitEthernet0/2
L    210.2.2.34/32 is directly connected, GigabitEthernet0/2
C    210.2.2.64/27 is directly connected, GigabitEthernet0/1
L    210.2.2.65/32 is directly connected, GigabitEthernet0/1
S*  0.0.0.0/0 [1/0] via 210.2.2.33
mainRouter#
```

Figura 4.6: IP routes mainRouter

4.4 Mail din exterior

In urmatoarea etapa dorim sa adaugam un domeniu **mail.claudiu.com** in serverul 5 (100.0.0.2), setat ca server de DNS. Acest domeniu va fi pentru adresa 100.0.0.2 (chiar adresa server-ului 5). Configuram in cadrul acestui server un serviciu de email unde adaugam un user nou claudiu3 cu parola claudiu3 si domeniul mail.claudiu.com ??

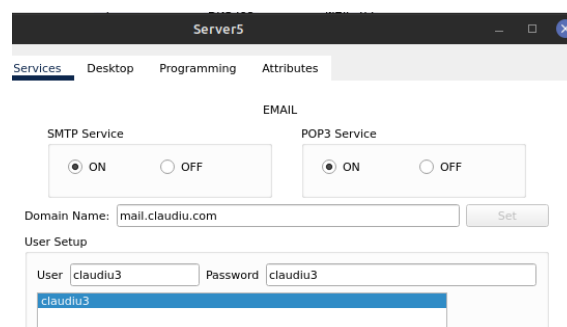


Figura 4.7: Adaugare cont email

Remark. Vom configura mail-ul creat pe laptopul 3 (100.0.0.3). Vom adauga domeniul **mail.claudiu.com** in serverul de DNS 210.2.2.68 la adresa 100.0.0.2.

Remark. In server 5 (100.0.0.2) vom adauga in serviciul de DNS domeniul **mail.claudiu.ro** la adresa 210.2.2.69 (serverul de mail din reseaua internă).

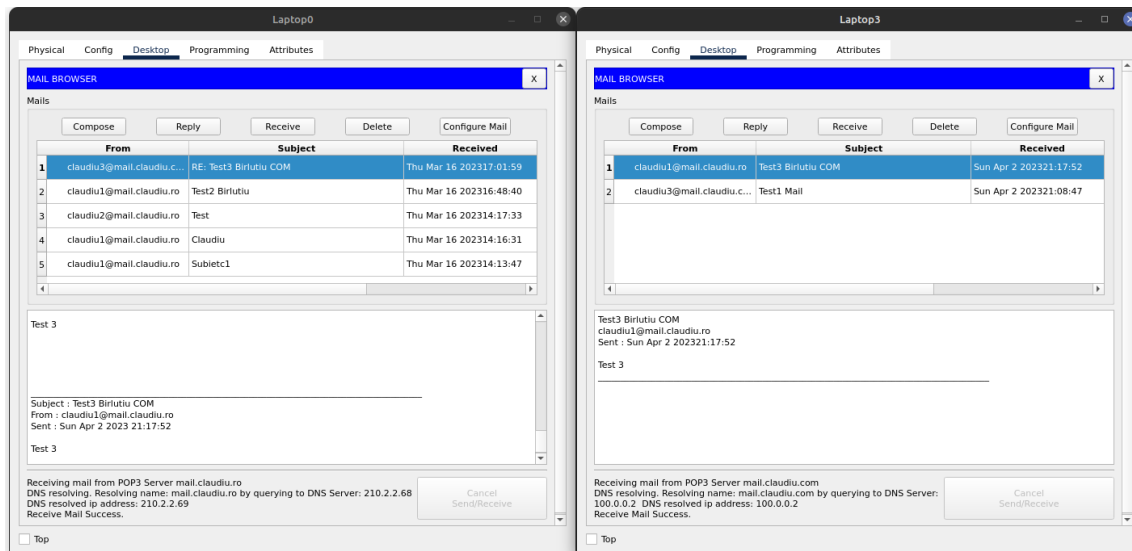


Figura 4.8: Testare email

4.5 Http page

S-a configurat serviciu http pe server 5 (100.0.0.2) si am adaugat numele meu paginii fig4.9.

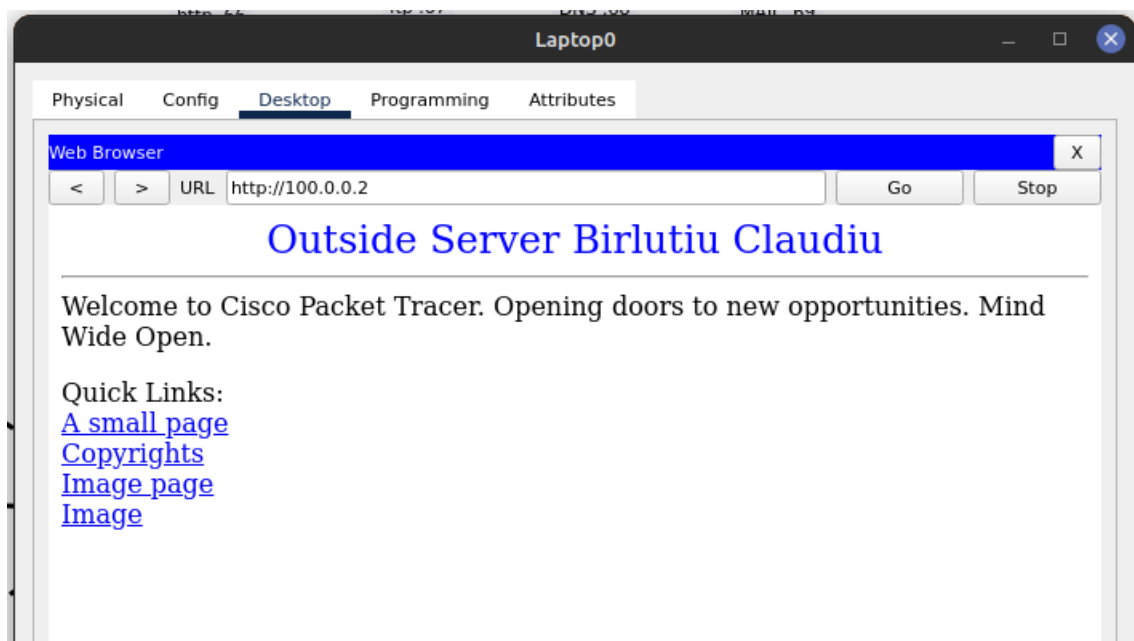


Figura 4.9: Testare http

Capitolul 5

Sedinta 4

In aceasta sedinta s-au atins aspecte legate de securitate. Am creat useri la nivelul mainRouter-uului cu diferite privilegii si m-am conecta de la distanta prin ssh. Am repetat acesti pasi si pentru switch-ul 0. Pentru securizarea parolelor s-a folosit crypto (hash pe parola).

Nivelul de privilegii:

- privilege level 1 - user exec mode; putine comenzi; parametri putini
- ...
- privilege level 15 - privileged exec mode (root) - se poate face orice

Tipul de encriptare disponibile:

- tipul 0 - fara encriptare
- tipul 7 - simple encryption
- tipul 5 - complex encryption

5.1 Conectare ssh MainRouter

In continuare se va configura conectarea remote la mainRouter. Se vor adauga urmatorii useri in felul urmator:

```
#pentru a intra in modul admin/root
$ enable
#pentru a intra in modul configurare
$ configure terminal
# adaugare username si parola
# primii 2 useri au parola clear text
$ username claudiu1 privilege 1 password claudiu1
$ username claudiu7 privilege 7 password claudiu7
# adaugarea unui user cu privilegii depline si cheia encriptata
$ username claudiu15 privilege 15 secret claudiu15
# definim un domeniu - necesar pentru certificare
$ ip domain-name claudiu.ro
# vom genera cheile pentru acest domeniu
# rsa este un algoritm destul de vechi si folosit
# dam 2048 de biti
```

```

$ crypto key generate rsa
# configurma terminalul virtual cu care ne legam
# in acest caz vor fi disponibile doar 2 conexiuni simultan acceptate
$ line vty 0 1
# setam sa fie acceptate sesiunile ssh
$ transport input ssh
# configuram verificare locala a user-ului in db
$ login local
# un pas in spate
$ exit
# setare parola pentru a intra in modul root/privilegiat
$ enable secret claudiu15

```

In urmatoarea imagine se observa cum ne putem conecta remote de pe laptopul 0 la mainRouter fig5.1. Am testat de asemenea daca ma pot conecta de pe 3 dispozitive (cele 3 laptopuri) simultan, dar nu s-a putut realiza cea de-a treia conexiune din cauza ca am pus vty pentru maxim 2 canale de conexiune.

```

C:\>ssh -l claudiu1 210.2.2.65

Password:

mainRouter>show privilege
Current privilege level is 1
mainRouter>enable
Password:
mainRouter#show privilege
Current privilege level is 15
mainRouter#exit

[Connection to 210.2.2.65 closed by foreign host]
C:\>ssh -l claudiu7 210.2.2.65

Password:

mainRouter#show privilege
Current privilege level is 7
mainRouter#enable
Password:
mainRouter#show privilege
Current privilege level is 15
mainRouter#exit

[Connection to 210.2.2.65 closed by foreign host]
C:\>ssh -l claudiu15 210.2.2.65

Password:

mainRouter#show privilege
Current privilege level is 15
mainRouter#

```

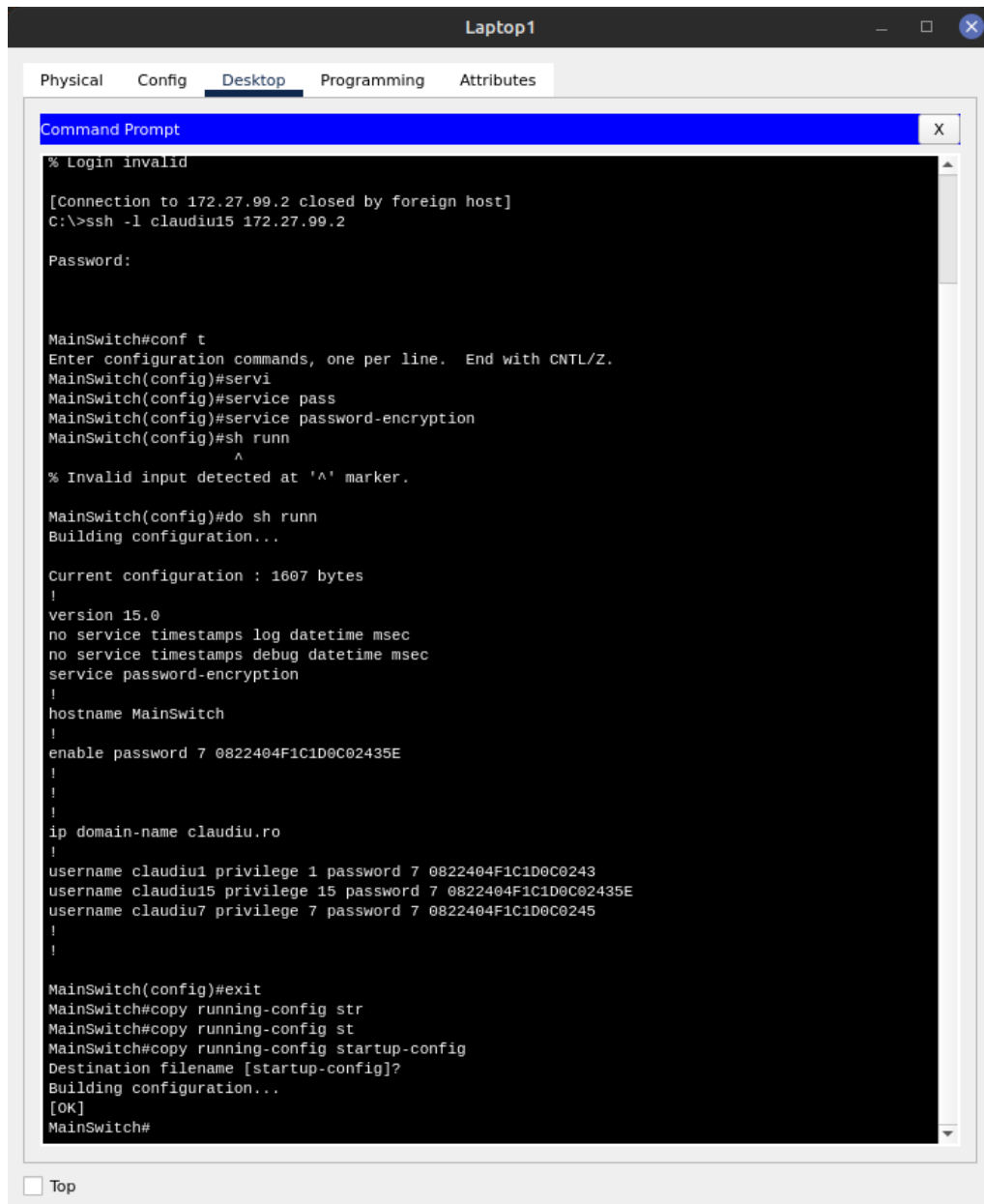
Figura 5.1: Verificare conexiune ssh

5.2 Conexiune ssh MainSwitch (switch 0)

Pentru a configura MainSwitch sa accepte conexiuni remote se poate proceda la fel ca in cazul MainRouter-ului. In prima faza se vor adauga useri in db local cu parola clear text iar apoi se vor encripta aceste parole. Traficul de management este pe **vlan-ul 99**, iar adresa ip est **172.27.99.2**. Se va configura astfel:

```
#pentru a intra in modul admin/root
$ enable
#pentru a intra in modul configurare
$ configure terminal
# adaugare username si parola
$ username claudiu1 privilege 1 password claudiu1
$ username claudiu7 privilege 7 password claudiu7
$ username claudiu15 privilege 15 password claudiu15
# definim un domeniu - necesar pentru certificare
$ ip domain-name claudiu.ro
# vom genera cheile pentru acest domeniu
# rsa este un algoritm destul de vechi si folosit
# dam 2048 de biti
$ crypto key generate rsa
# configuram terminalul virtual cu care ne legam
# in acest caz vor fi disponibile doar 2 conexiuni simultan acceptate
$ line vty 0 1
# setam sa fie acceptate sesiunile ssh
$ transport input ssh
# configuram verificare locala a user-ului in db
$ login local
# un pas in spate
$ exit
# setare parola pentru a intra in modul root/privilegiat
$ enable secret claudiu15
```


În continuare s-a folosit conexiunea ssh la MainSwitch și s-au encriptat parolele pentru MainSwitch. Se va face encriptarea cu un algoritm de encriptare. Procesul presupune parsarea fișierului de configurare și encriptarea parolilor găsite. fig5.2



```
Command Prompt
% Login invalid

[Connection to 172.27.99.2 closed by foreign host]
C:\>ssh -l claudiu15 172.27.99.2

Password:

MainSwitch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MainSwitch(config)#servi
MainSwitch(config)#service pass
MainSwitch(config)#service password-encryption
MainSwitch(config)#sh runn
MainSwitch(config)#sh runn
^
% Invalid input detected at '^' marker.

MainSwitch(config)#do sh runn
Building configuration...

Current configuration : 1607 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname MainSwitch
!
enable password 7 0822404F1C1D0C02435E
!
!
!
ip domain-name claudiu.ro
!
username claudiu1 privilege 1 password 7 0822404F1C1D0C0243
username claudiu15 privilege 15 password 7 0822404F1C1D0C02435E
username claudiu7 privilege 7 password 7 0822404F1C1D0C0245
!
!
MainSwitch(config)#exit
MainSwitch#copy running-config str
MainSwitch#copy running-config st
MainSwitch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
MainSwitch#
```

Figura 5.2: Verificare conexiune ssh

Useri parole:

- username: **claudiu1** password: **claudiu1** privilege: **1**
- username: **claudiu7** password: **claudiu7** privilege: **7**
- username: **claudiu15** password: **claudiu15** privilege: **15**

Parola enable: claudiu15

Capitolul 6

Securitate

În acest capitol sunt prezentate câteva metode de securitate aplicate rețelei create anterior. Ca metode de securitate așea voi aminti restricționarea prin access list a conexiunii ssh la VLAN-ul de management, și conexiune AAA local la routerul ISP.

6.1 Conectare ssh MainRouter restricționată doar la vlan 10

Considerăm ca accesul remote prin ssh la router-ul MainRouter să fie disponibilă doar pentru subrețeaua de vlan 10 (presupunem ca aceasta este folosită de către echipa de IT/ administratorul de rețea). Pentru a realiza acest lucru mă voi folosi de un access list prin care să creez regula enunțată anterior. Access list-urile sunt utilizate pentru a permite, restricționa sau filtra traficul pe baza unor criterii precum adrese IP, porturi de protocol, adrese MAC sau alte atribute specifice pachetelor de rețea.

Eu voi folosi un access list **standard** careia îi voi adăuga un remark pentru traficul din vlan 10 ca fiind permis. Voi permite pentru toate adresele ip din vlan10 să se conecteze la switch și pentru asta voi adăuga permisiunea în access list. Voi adăuga aceste reguli la linia virtuală(VTY) care e folosită pentru accesul la dispozitivul mainSwitch prin intermediul protocolului Telnet sau SSH.

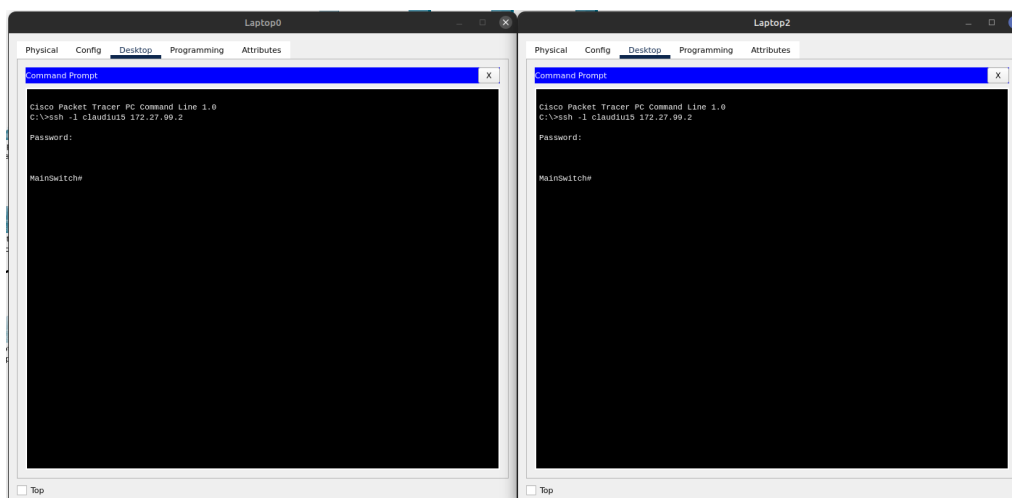


Figura 6.1: Verificare conexiune ssh vlan30-laptop0 și vlan10-laptop2 - înainte de regula

In figura 6.1 se pot observa 2 conexiuni spre main router din vlan 10 (laptop-2) si vlan 30(laptop-0) respectiv inainte de a impune regula. Comenziile aplicate pe switch-ul mainSwitch:

```
#conectare mainSwitch
$ enable
$ password: claudiu15
#intrare in mod configurare
$ configure terminal
# definire access list standard cu numarul 99 care permite trafic vlan10
$ access-list 99 remark vlan 10 traffic
# impunere regula de permisiune pentru toate adresele din vlan10
$ access-list 99 permit 172.27.10.0 0.0.0.255
# deny pentru toate celelate tipuri de conexiuni
$ access-list 99 deny any
# deschidere mod configurare terminal virtual
$ line vty 0 15
# adaugare access list acestui terminal virtual pentru aplicare restrictii
$ access-class 99 in
```

Se observa ca in cadrul regulei definite specificam faptul ca permitem traficul venit de la vlan 10 pentru orice adresa din cadrul acestuia. Comanda *line vty 0 15* face referire la linia virtuală (VTY) de la 0 la 15, care este folosită pentru accesul la dispozitiv prin intermediul protocolului Telnet sau SSH. Se va intra in modul de configurare al acestui terminal si ii atasam restrictia creata anterior. In figura 6.2 se pot observa 2 conexiuni spre main router din vlan 10 si vlan 30 respectiv inainte de a impune regula.

```
access-list 99 remark vlan 10 traffic
access-list 99 permit 172.27.10.0 0.0.0.255
access-list 99 deny any
line con 0
!
line vty 0 1
  access-class 99 in
  login local
  transport input ssh
line vty 2 4
  access-class 99 in
  login
line vty 5 15
  access-class 99 in
  login
!
```

Figura 6.2: Verificare aplicare restrictie in running config

Se vor incerca din nou conexiunile de pe laptop 0(vlan30), laptop 1 (vlan 20) si laptop 0(vlan 10) la main switch (switch 0) prin ssh. Se observa ca doar in cazul conexiunii de pe laptopul 2 (vlan 10) s-a putut realiza conectarea prin ssh la mainSwitch.

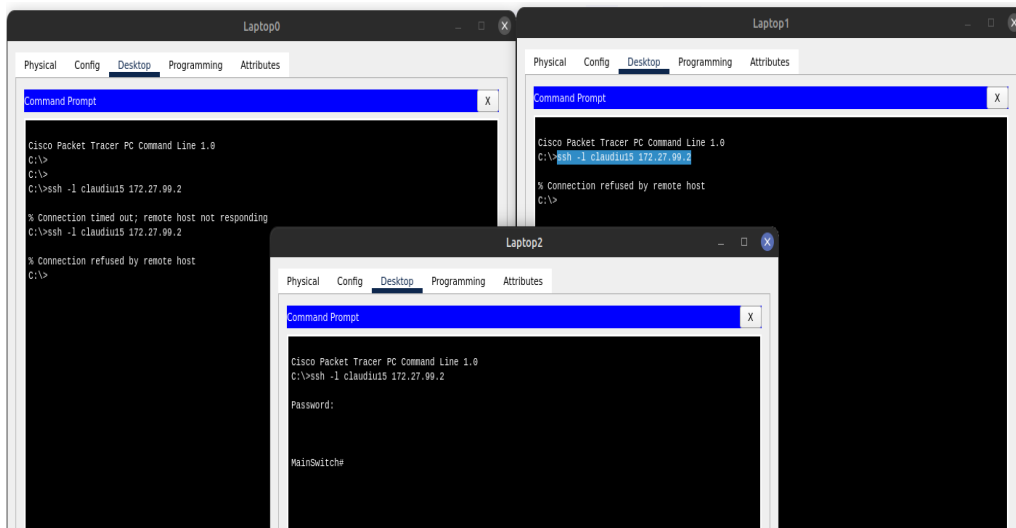


Figura 6.3: Verificare conexiune ssh dupa aplicare reguli

REZULTATE: Doar utilizatorii de la etaj 1 al caror vlan este 10 vor avea access ssh la main switch.

6.2 Conectare cu AAA local si remote ISP router

Voi realiza autentificare locala prin AAA pentru routerul ISP. Voi configura pentru acest serviciu serverul cu numarul 5 (100.0.0.2/8) unde voi defini un utilizator care se poate loga intr-o conexiune ssh, primind astfel acces la configurariile routerului. In prima faza voi configura serverul, iar apoi voi activa conexiunea de tip ssh pe routerul ISP asociind posibilitatea autentificarii de tip AAA. AAA authentication oferă o abordare centralizată și flexibilă pentru administrarea autentificării în rețelele de calculatoare.

AAA asigură framework-ul principal pentru a seta controlul accesului pe un echipament de rețea. Implementarea acestei parti de securitate s-a realizat consultand un exemplu publicat pe un canal de youtube [2]

Am configurat serviciul AAA pe serverul **100.0.0.2/8** unde am definit un user (claudiuAAA) si o parola pentru acesta (claudiuAAA) si am configurat rețeaua in care doresc sa fac aceasta configurare (detaliile despre router). Am selectat tipul de server ca fiind RADIUS, radius fiind un protocol și un tip de server utilizat pentru autentificarea, autorizarea și contabilitatea utilizatorilor care accesează o rețea. Serverul va juca rolul in acest caz de punct centralizat de autentificare și autorizare pentru utilizatori, precum si monitorizare. In figura de mai jos 6.4 se observa configurarea serviului AAA.

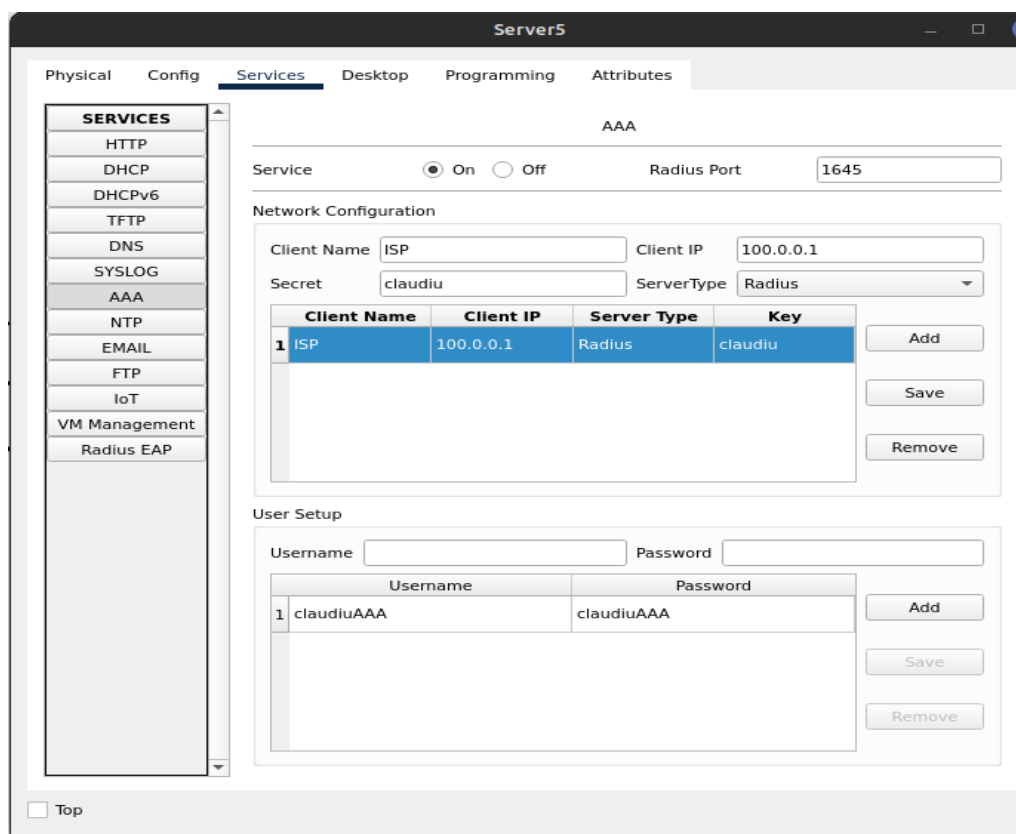
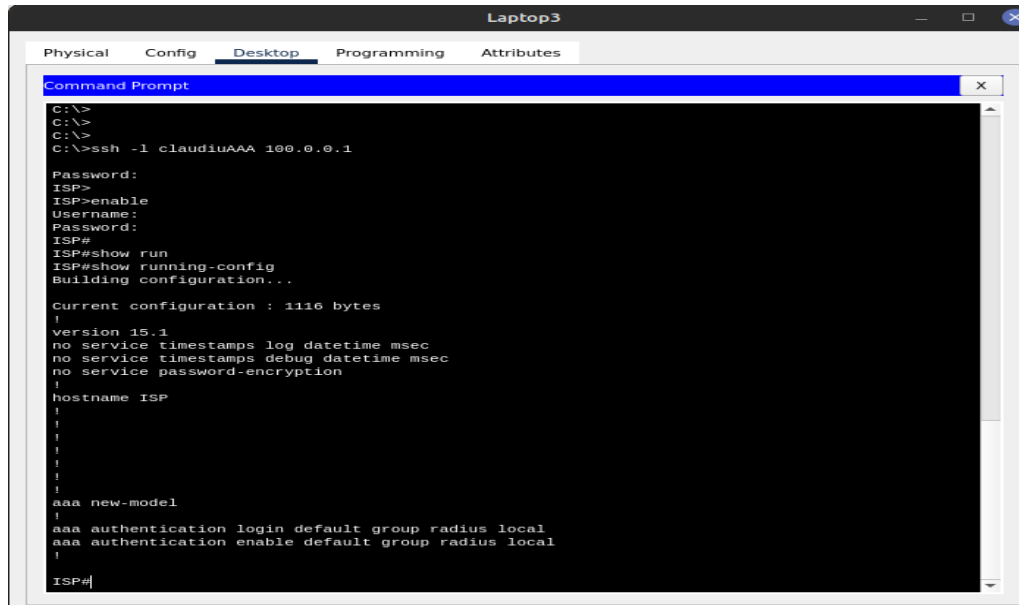


Figura 6.4: Configurare serviciu AAA pe server 100.0.0.2/8

In continuare voi configura routerul ISP pentru conexiune ssh si asociem serverul de autentificare AAA.

```
#pentru a intra in modul admin/root
$ enable
#pentru a intra in modul configurare
$ configure terminal
# adaugare username si parola; parola encriptata
$ username claudiuISP secret claudiuISP
# se activează și se aduce în funcțiune funcționalitatea AAA pe router
$ aaa new-model
# definim metoda de logare implicita ca fiind prin serverul radius
$ aaa authentication login default group radius local
# definim metoda de logare implicita la nivelul modului enable
# ca fiind prin serverul radius
$ aaa authentication enable default group radius local
# configuram informatiile despre serverul radius
# key-ul este cel pe care l-am setat in pe server
$ radius-server host 100.0.0.2 key claudiu
# definim un domeniu - necesar pentru certificare
$ ip domain name claudiu.com
# setam versiunea ip ssh la 2, routerul va folosi doar versiunea 2
$ ip ssh version 2
# vom genera cheile pentru acest domeniu
# rsa este un algoritm destul de vechi si folosit
# dam 1024 de biti
$ crypto key generate rsa
# configuram terminalul virtual cu care ne legam
# in acest caz vor fi disponibile doar 5 conexiuni simultan acceptate
$ line vty 0 4
# setam sa fie acceptate sesiunile ssh
$ transport input ssh
# setam autentificare default (cea pe care am setat-o inainte)
# prima data server radius
$ login authentication default
# un pas in spate
$ exit
```

Pentru testarea conexiunii ssh prin intermediul serviciului AAA de logare am accesat commnad line-ul laptopului 100.0.0.3/8 si am incercat sa ma conectez prin ssh cu utilizatorul claudiuAAA pe care l-am inscris in serverul radius. Observam in figura fig6.5 cum ne logam intial cu privilegiu 1 la routerul ISP (100.0.0.1/8) si apoi ne logam la nivelul enable (privilegiu 15) tot cu credentialele pe care le-am setat in serviul AAA. Am setat default login ca fiind serverul radius (AAA) si nu se mai tine cont de baza de date locala.



```
C:\>
C:\>
C:\>ssh -l claudiuAAA 100.0.0.1

Password:
ISP>
ISP>enable
Username:
Password:
ISP#
ISP#show run
ISP#show running-config
Building configuration...

Current configuration : 1116 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname ISP
!
!
!
!
!
!
aaa new-model
!
aaa authentication login default group radius local
aaa authentication enable default group radius local
!
ISP#
```

Figura 6.5: Verificare conexiune ssh cu username AAA

Useri parole:

- AAA: username: **claudiuAAA** password: **claudiuAAA**

Bibliografia

- [1] Ben Lutkevich, „DMZ in networking”, în (), URL: <https://www.techtarget.com/searchsecurity/definition/DMZ> (cit. în p. 14).
- [2] TechWithMi, *Radius Server, AAA Local and Server based Authentication Configuration with packet Tracer*. <https://www.youtube.com/watch?v=S9RBZTDIfIo>, 17.05.2023, 2022 (cit. în p. 34).