

Pași Laborator

Contents

Laboratorul 1 (4 Octombrie).....	2
Laboratorul 2 (11 Octombrie).....	6
Laboratorul 3 (18 Octombrie).....	11
Laboratorul 4 (25 Octombrie).....	22
Laboratorul 6 (7 Noiembrie)	28
Laboratorul 7 (14 Noiembrie)	40
Laboratorul 8 (21 Noiembrie)	43
Laboratorul 9 (28 Noiembrie)	46
Laboratorul 10 (5 Decembrie)	48
Laboratorul 11 (12 Decembrie).....	50
Laboratorul 12 (19 Decembrie).....	52
Laboratorul 13 (9 Ianuarie)	54

Laboratorul 1 (4 Octombrie)

- Link Calcul IP-uri: <https://jodies.de/ipcalc>

- **Puterile lui 2:**

2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7
1	2	4	8	16	32	64	128

Un număr va fi reprezentat astfel: $172 = 128 + 32 + 8 + 4 = 1 \times 2^7 + 0 \times 2^6 + 1 \times 2^5 + 0 \times 2^4 + 1 \times 2^3 + 1 \times 2^2 + 0 \times 2^1 + 0 \times 2^0 = 1010.1100$

Suma totală: $128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 255$

- Network Address (**NA**), Broadcast Address (**BA**), Range Addresses (**RA**), Subnet Mask (**SM**), **Wildcard**, Default Gateway (**DGW**), **DNS**:

IP: 192.168.10.13 /25 = 1100.0000/1010.1000/0000.1010/0000.1101 /25

$192 = 128 + 64$; $168 = 128 + 32 + 8$; $10 = 8 + 2$; $13 = 8 + 4 + 1$

NA: Am pus 25 de 1. Facem operație de **SI** între primele 2 rânduri → vom obține **primele /25** de caractere din **IP** și **restul până la 32** (7 caractere) vor fi **0**.

IP	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	1	1	0	1
/25	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0
NA	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0

NA: 192.168.10.0 /25

BA: Copiem **primii /25 de biți din NA** și **restul până la 32 sunt 1**.

NA	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	1	1	0	1
/25	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
BA	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	1	0	1	0	0	1	1	1	1	1	1	1

BA: 192.168.10.127 /25

RA: $NA+1 - BA-1 \rightarrow 192.168.10.1 - 192.168.10.126$ /25

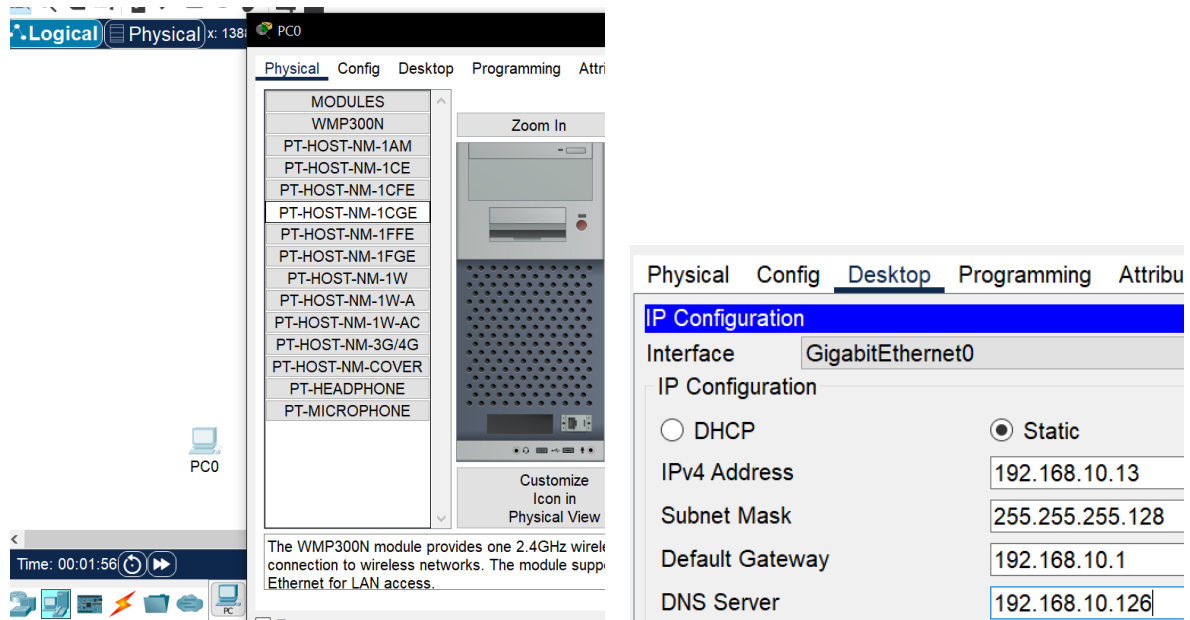
SM: /25 de 1 → 255.255.255.128 /25

Wildcard: /25 de 0 și **restul până la 32** (7 biți) de 1 → 0.0.0.127 /25

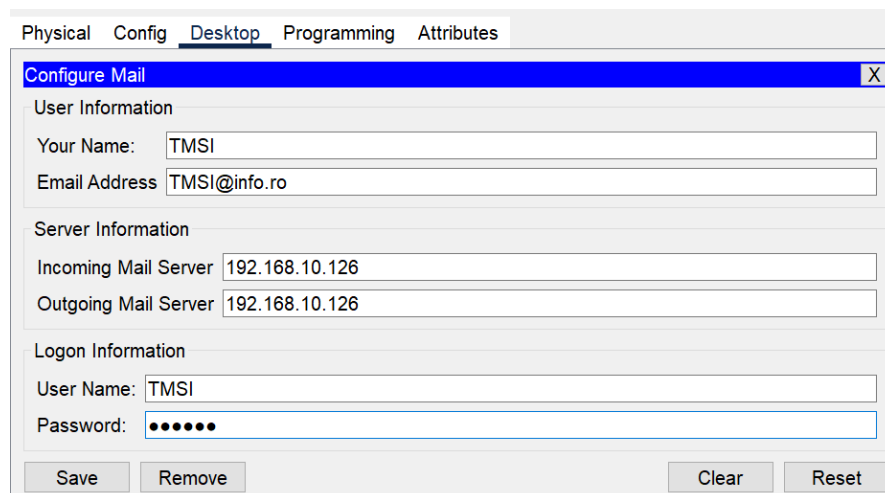
DGW: Cel mai **MIC IP din RA** → 192.168.10.1 /25

DNS: Cel mai **MARE IP din RA** → 192.168.10.126 /25

- Topologiile le construim de la *stânga la dreapta* și de *jos în sus*.
- Pentru **PC**: Turn OFF power, scoatem placa veche și o punem pe cea nouă **PT-HOST-NM-1CGE**; după power ON. **Desktop** → **IP Configuration** și introducem ce am calculat.

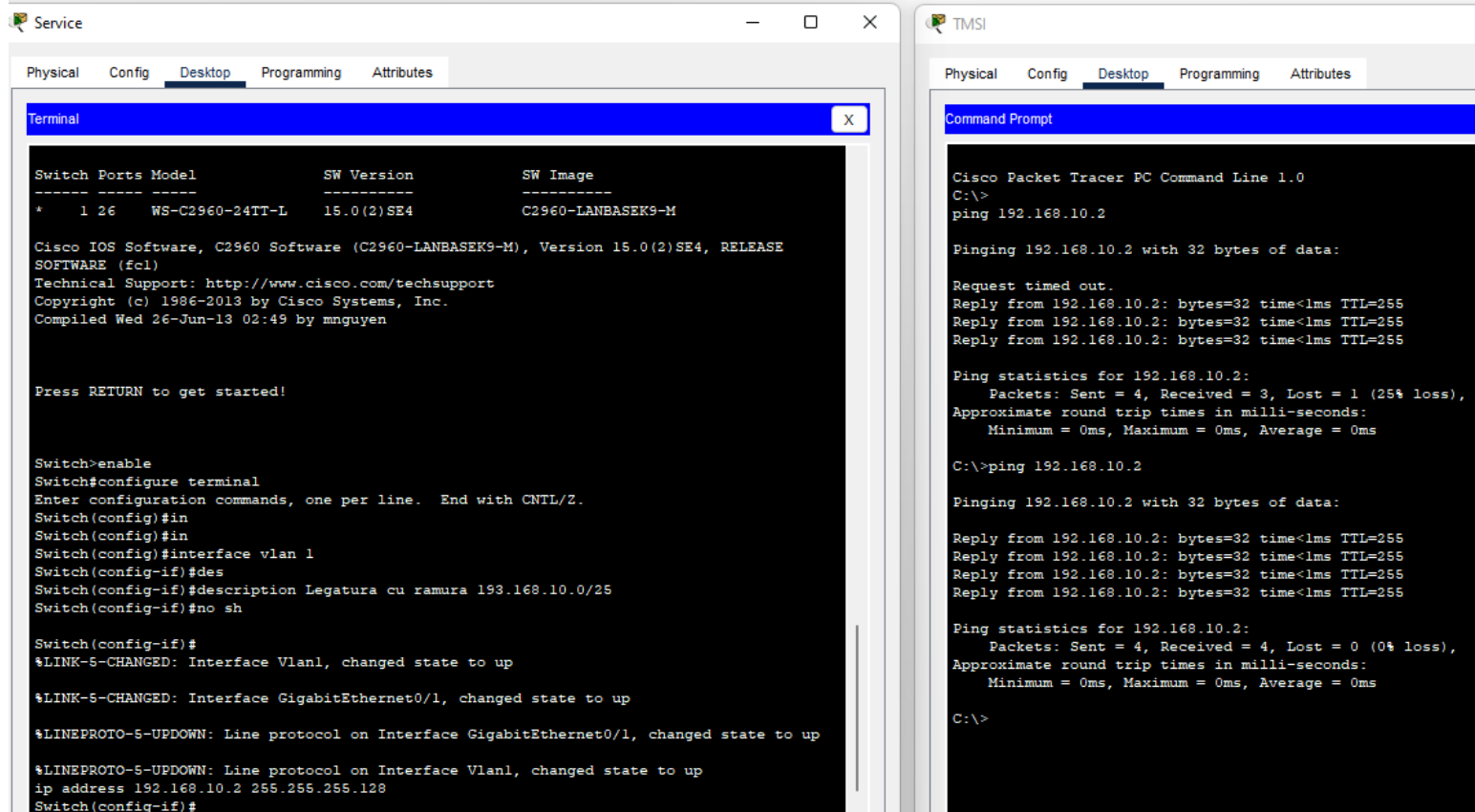


Desktop → **Email**: *Incoming/Outgoing mail* este *DNS-ul* și *parola* de mail este *123456*. SAVE. (Numele este numele PC-ului)



- Pentru **SWITCH**: Folosim *switch 2960*. Avem nevoie și de un *laptop* pe care îl vom numi *SERVICE* și îl vom conecta la toate echipamentele pe care dorim să le configurăm, folosind *firul consolă* (cel *albastru*; capăt *RS232 în laptop* și capăt *consolă în echipament*). **Laptop** → **Desktop** → **Terminal** → **Ok**: și aici vom introduce comenzile din laboratoarele viitoare.

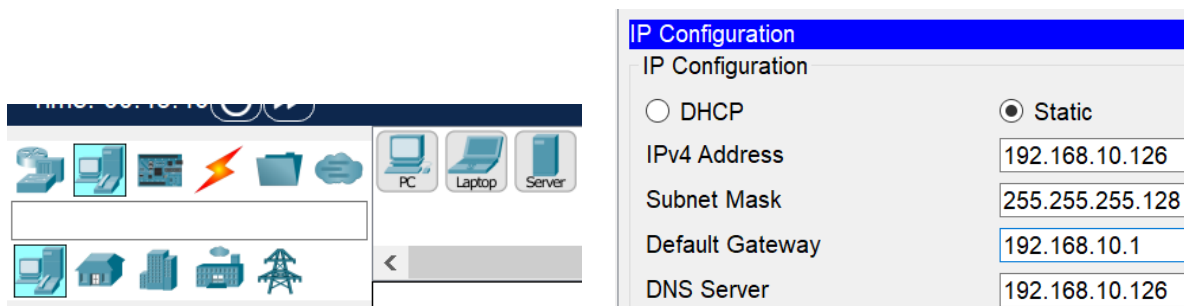




- Pentru **ROUTER**: Folosim **router 2911**. Vom folosi tot laptopul SERVICE pentru configurare (comenzile în laboratoarele viitoare).



- Pentru **SERVER**: Turn OFF power, scoatem placa veche și o punem pe cea nouă **PT-HOST-NM-1CGE**; după power ON. **Desktop** → **IP Configuration** și introducem ce am calculat: **IPv4 = DNS**, SM și GDW ca mai sus.



Desktop → **Email**: *Incoming/Outgoing mail* este *DNS-ul* și *parola* de mail este *123456*. SAVE. (Numele este numele serverului)

Configure Mail

User Information

Your Name:

Email Address:

Server Information

Incoming Mail Server:

Outgoing Mail Server:

Logon Information

User Name:

Password:

Services → **HTTP**: **HTTP** punem **OFF**.

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6

HTTP

HTTP ☐ On ☒ Off

HTTPS ☒ On ☐ Off

Services → **DNS**: **Address** este **DNS**. Și add.

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS**
- SYSLOG
- AAA
- NTP
- EMAIL

DNS

DNS Service ☒ On ☐ Off

Resource Records

Name: Type:

Address:

No.	Name	Type	Detail
-----	------	------	--------

Services → **EMAIL**: ...

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL**

EMAIL

SMTP Service ☒ ON ☐ OFF

POP3 Service ☒ ON ☐ OFF

Domain Name:

User Setup

User: Password:

Laboratorul 2 (11 Octombrie)

- Pasi Configurare Host PC:**

End Devices → PC:

Pas1: Nume **ARAD** (majuscule neapărat)

Pas2: Click pe PC; Power OFF; Scoatem placa de rețea; Punem placa **PT-HOST-NM-1CGE**, Power ON

Pas3: **Desktop → IP Configuration**

(Ipv4: **192.168.100.164**

S.M.: **255.255.255.224**

D.Gw.: **192.168.100.161** (cel mai mic IP din RA)

DNS: **209.165.201.254** (cel mai mare IP din RA))

Pas4: **Desktop → Email**

(Name: **ARAD**

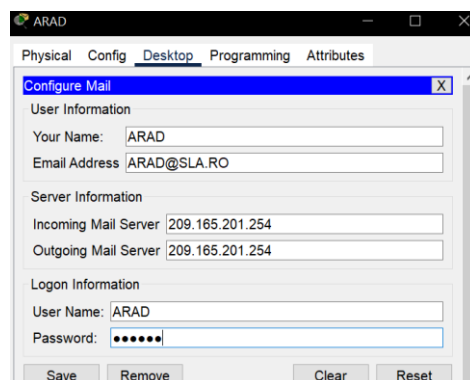
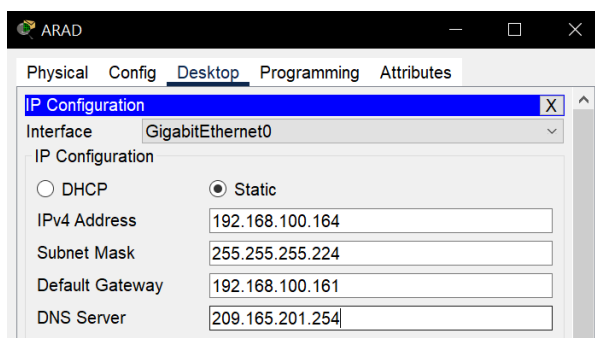
Email: **ARAD@SLA.RO**

Incoming/Outcoming Mail Server: **209.165.201.254** (DNS)

User: **ARAD**

Password: **123456**

SAVE)

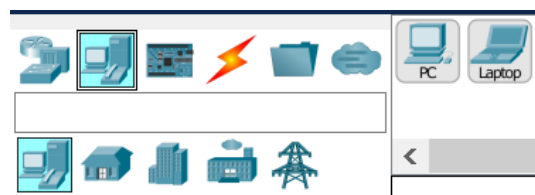


- Pasi Configurare Laptop SERVICE:**

End Devices → Laptop:

Pas1: Nume **SERVICE** (majuscule neapărat)

Connections → Console (firul albastru):



Pas1: Capăt **RS232** în laptop **SERVICE** și capăt **Console** în echipamentul pe care dorim să îl configurăm.

Pas2: **Laptop** → **Desktop** → **Terminal** → **Ok** și de aici vom introduce sintaxa de configurare a echipamentelor.



!!! Atentie: Vom refolosi laptopul și firul pentru toate echipamentele pe care dorim să le configurăm (nu vom lua/defini unele noi).

- **Pași Configurare Switch 2960:**

Pas1: Nume **SWARAD**

Pas2: Trebuie să cunoaștem **IP-ul switch-ului** (luăm **D.Gw. + 1** – sau cea mai apropiată adresă liberă de D.Gw.) și **S.M.** de la **PC**.

Pas3: Introducem următoarea sintaxă din laptopul **SERVICE**, după ce ne conectăm la **SWARAD**.

Sintaxă Switch (ce este după // sau ---, sunt comentarii):

Enter

```
SWARAD> enable // mod user
SWARAD# configure terminal // mod privilegiat
SWARAD (config)# no ip domain-lookup // ca să nu se blocheze echipamentul când greșim
SWARAD (config)# hostname SWARAD
SWARAD (config)# no cdp run
SWARAD (config)# service password-encryption // criptare parole
SWARAD (config)# enable secret ciscosecpa55 // parola puternică
SWARAD (config)# enable password ciscoenapa55 // back-up parolă pt. cea de sus
SWARAD (config)# banner motd #Vineri, la 14.00, serverul va fi oprit!#
----- (conexiune locală, prin cablul Consolă/Rollover)
SWARAD (config)# line console 0
SWARAD (config-line)# password ciscoconpa55
SWARAD (config-line)# login // cere parolă la logare
SWARAD (config-line)# logging synchronous // ne întoarcem de unde am rămas în caz update
SWARAD (config-line)# exec-timeout 25 25 // în stand-by după 25 min și 25 sec
SWARAD (config-line)# exit
```

----- (conexiune virtuală, de la distanță)

```
SWARAD (config)# line vty 0 15
SWARAD (config-line)# password ciscovtpa55
SWARAD (config-line)# login
SWARAD (config-line)# logging synchronous
SWARAD (config-line)# exec-timeout 10 10
SWARAD (config-line)# end
```

----- (dată și oră)

```
SWARAD# copy running-config startup-config // SAVE (de câte ori vrem)
SWARAD# clock set 20:05:32 11 Oct 2022
SWARAD# configure terminal
```

----- (configurare SSH)

```
SWARAD (config)# ip domain name SLA.RO
SWARAD (config)# username Admin01 privilege 15 secret Admin01pa55 // admin SSH cu toate drepturile
SWARAD (config)# line vty 0 15
SWARAD (config-line)# transport input ssh
SWARAD (config-line)# login local
SWARAD (config-line)# exit
SWARAD (config)# crypto key generate rsa → 2048 (scriem)
```

----- (configurare interfață VLAN)

```
SWARAD (config)# interface vlan 1
SWARAD (config-if)# description Legatura cu LAN 192.168.100.160/27 // N.A.
SWARAD (config-if)# ip address 192.168.100.162 255.255.255.224 // IP_SWARAD S.M.
SWARAD (config-if)# no shutdown // activare interfață
```

----- (dacă greșim IP)

```
SWARAD (config-if)# no ip address // și revenim de la ip address...
```

Pas4: **Connections** → **Copper Straigh-Through** (firul negru, drept; al 3-lea) și legăm **SWARAD** la **ARAD**.

Pas5: **PC (ARAD) → Desktop → Command Prompt** (ca să verificăm că există conexiune:

ping **192.168.100.162**

ssh -l **Admin01 192.168.100.162** → parola: **Admin01pa55**)

- **Pași Configurare Router 2911:**

Pas1: Nume **RARAD**

Pas2: Trebuie să cunoaștem **IP-ul router-ului** (luăm **D.Gw.**) și **S.M.**

Pas3: Introducem următoarea sintaxă din laptopul **SERVICE**, după ce ne conectăm la **RARAD**.

Sintaxă Router (similar cu ce avem la Switch, ce este diferit, va fi marcat cu roșu și !):

Enter

RARAD> enable // mod user

RARAD# configure terminal // mod privilegiat

RARAD (config)# no ip domain-lookup // ca să nu se blocheze echipamentul când greșim

RARAD (config)# hostname **RARAD**

RARAD (config)# no cdp run

RARAD (config)# service password-encryption // criptare parole

!RARAD (config)# security passwords min-length 10

!RARAD (config)# login block-for60 attempts 3 within 15

RARAD (config)# enable secret **ciscosecpa55** // parola puternică

RARAD (config)# enable password **ciscoenapa55** // back-up parolă pt. cea de sus

RARAD (config)# banner motd **#Vineri, la 14.00, serverul va fi oprit!#**

!RARAD (config)# banner login #Accesul persoanelor neautorizate complet interzis!#

----- (conexiune locală, prin cablul Consolă/Rollover)

RARAD (config)# line console 0

RARAD (config-line)# password **ciscoconpa55**

RARAD (config-line)# login // cere parolă la logare

RARAD (config-line)# logging synchronous // ne întoarcem de unde am rămas în caz update

RARAD (config-line)# exec-timeout 25 25 // în stand-by după 25 min și 25 sec

RARAD (config-line)# exit

----- (conexiune virtuală, de la distanță)

```
RARAD (config)# line vty 0 15
RARAD (config-line)# password ciscovtypa55
RARAD (config-line)# login
RARAD (config-line)# logging synchronous
RARAD (config-line)# exec-timeout 10 10
RARAD (config-line)# end
```

----- (dată și oră)

```
RARAD# copy running-config startup-config // SAVE (de câte ori vrem)
RARAD# clock set 20:05:32 11 Oct 2022
RARAD# configure terminal
```

----- (configurare SSH)

```
RARAD (config)# ip domain name SLA.RO
RARAD (config)# username Admin01 privilege 15 secret Admin01pa55 // admin SSH cu toate drepturile
RARAD (config)# line vty 0 15
RARAD (config-line)# transport input ssh
RARAD (config-line)# login local
RARAD (config-line)# exit
RARAD (config)# crypto key generate rsa → 2048 (scriem)
```

----- (configurare interfață VLAN) → NU AVEM LA ROUTER

```
RARAD (config)# interface vlan 1
RARAD (config-if)# description Legatura cu LAN 192.168.100.160/27 // N.A.
RARAD (config-if)# ip address 192.168.100.162 255.255.255.224 // IP_RARAD S.M.
RARAD (config-if)# no shutdown // activare interfață
```

----- (configurare interfață Gigabit)

```
!RARAD (config)# interface GigabitEthernet 0/0
!RARAD (config-if)# description Legatura cu LAN 192.168.100.161/27 // D.Gw.
!RARAD (config-if)# ip address 192.168.100.161 255.255.255.224 // IP_RARAD S.M.
!RARAD (config-if)# no shutdown // activare interfață
```

Pas4: **Connections** → **Copper Straigh-Through** (firul negru, drept; al 3-lea) și legăm **RARAD** la **SWARAD**.

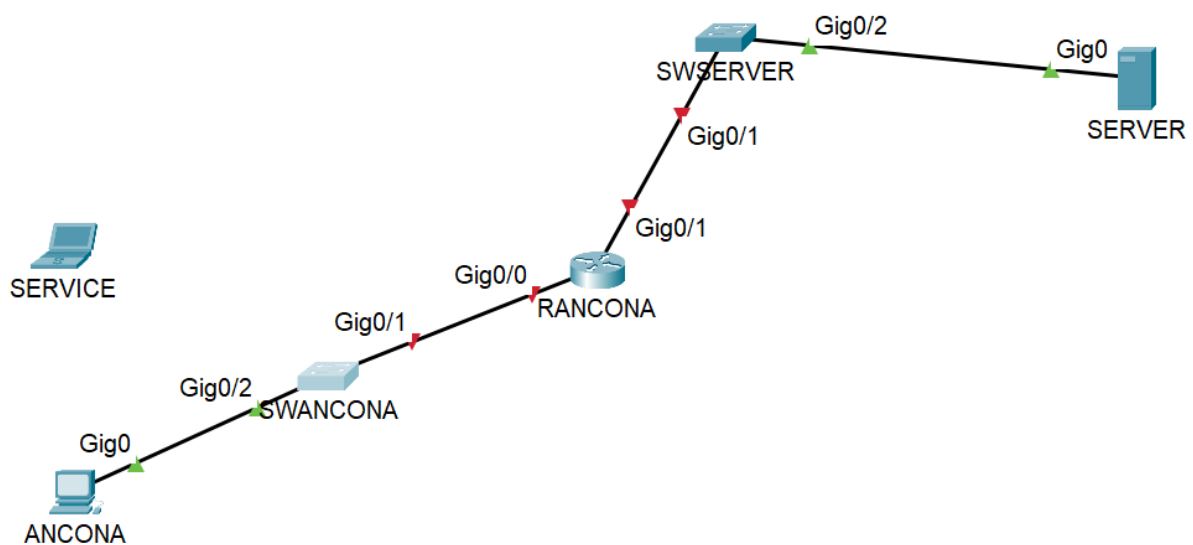
Pas5: **PC (ARAD)** → **Desktop** → **Command Prompt** (ca să verificăm că există conexiune:

ping **192.168.100.161**

ssh -l **Admin01 192.168.100.161** → parola: **Admin01pa55**)

!!! Atenție: Între echipamente de același fel, folosim **cablul cross-over** (linie dreaptă, neagră, întretăiată), iar pentru cele diferite, cu diferență de layere = 1 (OSI), folosim **cablul straight-through** (linie dreaptă, neagră).

Laboratorul 3 (18 Octombrie)



Vom încerca să configurăm următoarea topologie. Datele pe care le cunoaștem:

- **192.168.10.160/27** pentru **LAN ANCONA**;
- **DNS: 209.165.201.174/28**;
- **209.165.201.160/28** pentru **LAN SERVER**;

Pentru **LAN ANCONA (192.168.10.160/27)** împărțim astfel IP-urile:

- N.A.: 192.168.10.160 / 27
- B.A.: 192.168.10.191 / 27
- R.A.: 192.168.10.161 – 192.168.10.190 / 27
- S.M.: 192.168.10.224
- D.Gw.: 192.168.10.161

- **D.Gw.** este asignat **router-ului** (192.168.10.161). Cele mai apropiate adrese sunt pentru switch-uri: **D.Gw.+1** (192.168.10.162) și **D.Gw.+2** (192.168.10.163) sunt pentru **switch-uri** și după avem 30 de adrese IP pentru celelalte dispozitive, deci **PC-ul** va primi **D.Gw.+3** (192.168.10.164).

!!! Cum calculăm numărul de switch-uri?

Ex1: 192.168.10.160/27 → 32 – 27 = 5 (masca maximă de rețea) → $2^5=32$ (numărul total de IPs) → 32 – 2 = 30 (numărul de IPs asignabile) → $[30 / 26] = 1$ (împărțim la **numărul de porturi ale unui switch**), deci avem nevoie de 2 (1 + 1) switch-uri pentru a acoperi necesarul de porturi (numărul de porturi trebuie să depășească numărul de IPs).

Ex2: 192.168.10.0/26 → 32 – 26 = 6 → $2^6 = 64$ → 64 – 2 = 62 → $[62 / 26] = 2$ → 3 Switches

(În mod similar gândim și pentru **LAN SERVER**). IP-urile pentru LAN SERVER (**209.165.201.160/28**):

- **N.A.**: 209.165.201.160 / 28
- **B.A.**: 209.165.201.175 / 28
- **R.A.**: 209.165.201.161 – 209.165.201.174 / 28
- **S.M.**: 255.255.255.240
- **D.Gw.**: 209.165.201.161
- Router: 209.165.201.161; Switch1: 209.165.201.162; Switch2: 209.165.201.163; PC: 209.165.201.164; SERVER: va avea adresa DNS-ului.

• Pasi Configurare Host PC:

End Devices → PC:

Pas1: Nume **ANCONA** (majuscule neapărat)

Pas2: Click pe PC; Power OFF; Scoatem placa de rețea; Punem placa **PT-HOST-NM-1CGE**, Power ON

Pas3: Desktop → IP Configuration

(Ipv4: **192.168.10.164**

S.M.: **255.255.255.224**

D.Gw.: **192.168.10.161** (cel mai mic IP din RA)

DNS: **209.165.201.174**)

Pas4: Desktop → Email

(Name: **ANCONA**

Email: **ANCONA@SLA.RO**

Incoming/Outcoming Mail Server: **209.165.201.174** (DNS)

User: **ANCONA**

Password: **123456**

SAVE)

- **Pasi Configurare Switch SWANCONA 2960:**

Pas1: Nume **SWANCONA**

Pas2: **IP-ul switch-ului:** 192.168.10.162; **S.M.:** 255.255.255.224

Pas3: Introducem următoarea sintaxă din laptopul **SERVICE**, după ce ne conectăm la **SWANCONA**.

Sintaxă Switch (adăugiri cu roșu):

Enter

```
SWANCONA> enable
```

```
SWANCONA# configure terminal
```

```
SWANCONA (config)# no ip domain-lookup
```

```
SWANCONA (config)# hostname SWANCONA
```

```
SWANCONA (config)# no cdp run
```

```
SWANCONA (config)# service password-encryption
```

```
SWANCONA (config)# enable secret ciscosecpa55
```

```
SWANCONA (config)# enable password ciscoenapa55
```

```
SWANCONA (config)# banner motd #Vineri, la 14.00, serverul va fi oprit!#
```

----- (conexiune locală, prin cablul Consolă/Rollover)

```
SWANCONA (config)# line console 0
```

```
SWANCONA (config-line)# password ciscoconpa55
```

```
SWANCONA (config-line)# login
```

```
SWANCONA (config-line)# logging synchronous
```

```
SWANCONA (config-line)# exec-timeout 25 25
```

```
SWANCONA (config-line)# exit
```

----- (conexiune virtuală, de la distanță)

```
SWANCONA (config)# line vty 0 15
```

```
SWANCONA (config-line)# password ciscovtypa55
```

```
SWANCONA (config-line)# login
```

```
SWANCONA (config-line)# logging synchronous
```

```
SWANCONA (config-line)# exec-timeout 10 10
```

```
SWANCONA (config-line)# end
```

----- (dată și oră)

```
SWANCONA# copy running-config startup-config // SAVE (de câte ori vrem)
```

```
SWANCONA# clock set 20:05:32 11 Oct 2022
```

```
SWANCONA# configure terminal
```

```
----- (configurare SSH)
```

```
SWANCONA (config)# ip domain name SLA.RO
```

```
SWANCONA (config)# username Admin01 privilege 15 secret Admin01pa55
```

```
SWANCONA (config)# line vty 0 15
```

```
SWANCONA (config-line)# transport input ssh
```

```
SWANCONA (config-line)# login local
```

```
SWANCONA (config-line)# exit
```

```
SWANCONA (config)# crypto key generate rsa → 2048 (scriem)
```

```
----- (configurare interfață VLAN)
```

```
SWANCONA (config)# interface vlan 1
```

```
SWANCONA (config-if)# description Legatura cu LAN 192.168.10.160/27
```

```
SWANCONA (config-if)# ip address 192.168.10.162 255.255.255.224
```

```
SWANCONA (config-if)# no shutdown
```

```
----- (închidem interfețele nefolosite și setăm D.Gw.)
```

```
!SWANCONA (config)# interface range fa 0/1-24
```

```
!SWANCONA (config-if-range)# shutdown
```

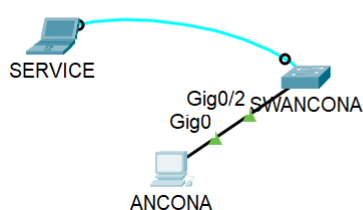
```
!SWANCONA (config)# ip default-gateway 192.168.10.161
```

Pas4: Connections → Copper Straigh-Through (firul negru, drept; al 3-lea) și legăm **SWANCONA** la **ANCONA**.

Pas5: PC (ANCONA) → Desktop → Command Prompt (ca să verificăm că există conexiune:

```
ping 192.168.10.162
```

```
ssh -l Admin01 192.168.10.162 → parola: Admin01pa55)
```



```
Packets: Sent = 4, Received = 3, Lost = 1 (100% loss),
C:\>ping 192.168.10.162
Pinging 192.168.10.162 with 32 bytes of data:
Request timed out.
Reply from 192.168.10.162: bytes=32 time<1ms TTL=255
Reply from 192.168.10.162: bytes=32 time<1ms TTL=255
Reply from 192.168.10.162: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.10.162:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

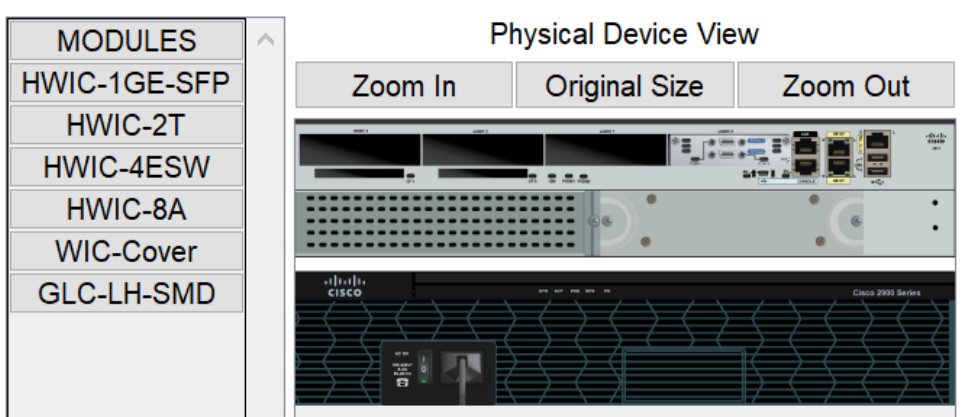
C:\>ssh -l Admin01 192.168.10.162
Password:
Vineri, la 12, serverul va fi oprit!
SWANCONA#
```

- **Pasi Configurare Router RANCONA 2911:**

Pas1: Nume **RANCONA**

Pas2: **IP-ul router-ului:** 192.168.10.161 și **S.M.:** 255.255.255.224

Pas3: Click pe router; Power OFF; Punem placa **HWIC-2T** (o punem în slot-ul cel mai din dreapta → pentru a putea avea serial 0/0/0 și să putem lega mai multe routere între ele), Power ON



Pas4: Introducem următoarea sintaxă din laptopul **SERVICE**, după ce ne conectăm la **RANCONA**.

Sintaxă Router (similar cu Laboratorul 2, nimic nou adăugat momentan, dar configurăm în același timp ambele interfețe – gigabit0/0, unde avem 192.168.10.161, și gigabit 0/1, unde avem 209.165.201.161)

Pas5: **Connections** → **Copper Straigh-Through** (firul negru, drept; al 3-lea) și legăm **RANCONA** la **SWANCONA**.

Pas6: **PC (ANCONA)** → **Desktop** → **Command Prompt** (ca să verificăm că există conexiune:

ping **192.168.10.161**

ssh -l **Admin01 192.168.10.161** → parola: **Admin01pa55**) (nu va merge să dăm ping și ssh în 209.165.201.161 până nu vom conecta și SWSERVER)

```
Pinging 192.168.10.161 with 32 bytes of data:
Request timed out.
Reply from 192.168.10.161: bytes=32 time<1ms TTL=255
Reply from 192.168.10.161: bytes=32 time<1ms TTL=255
Reply from 192.168.10.161: bytes=32 time=10ms TTL=255

Ping statistics for 192.168.10.161:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 3ms

C:\>ssh -l Admin01 192.168.10.161
Password:
Vineri, 1a 12, serverul va fi restartat!
RANCONA#exit

[Connection to 192.168.10.161 closed by foreign host]
C:\>ping 209.165.201.161

Pinging 209.165.201.161 with 32 bytes of data:
Reply from 192.168.10.161: Destination host unreachable.
Reply from 192.168.10.161: Destination host unreachable.
```

- **Pasi Configurare Switch SWANCONA 2960:**

Pas1: Nume **SWSERVER**

Pas2: **IP-ul switch-ului:** 209.165.201.162; **S.M.:** 255.255.255.240

Pas3: Introducem următoarea sintaxă din laptopul **SERVICE**, după ce ne conectăm la **SWSERVER**.

Sintaxă Switch (sintaxă similară cu ce avem mai sus)

Pas4: **Connections → Copper Straigh-Through** (firul negru, drept; al 3-lea) și legăm **SWSERVER** la **RANCONA**.

Pas5: **PC (ANCONA) → Desktop → Command Prompt** (ca să verificăm că există conexiune:

```
ping 209.165.201.162 /.161
```

```
ssh -l Admin01 209.165.201.162 /.161 → parola: Admin01pa55)
```

- **Pasi Configurare Server:**

Pas1: Nume **SERVER**

Pas2: Click pe PC; Power OFF; Scoatem placa de rețea; Punem placa **PT-HOST-NM-1CGE**, Power ON



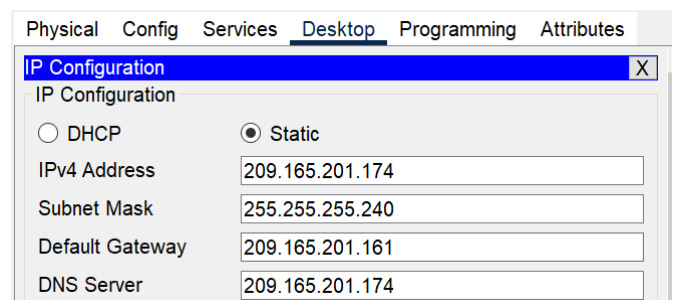
Pas3: **Desktop → IP Configuration**

(Ipv4: 209.165.201.174 **!!!PT SERVERE, IP = DNS**

S.M.: 255.255.255.240

D.Gw.: 209.165.201.161 (cel mai mic IP din RA)

DNS: 209.165.201.174)



Pas4: **Desktop → Email**

(Name: **SERVER**

Email: **SERVER@SLA.RO**

Incoming/Outcoming Mail Server: 209.165.201.174 (DNS)

User: **SERVER**

Password: **123456**

SAVE)

Pas4.1: Services → HTTP (HTTP → **OFF**; HTTPS → **ON**)

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6

HTTP

HTTP ☐ On ☒ Off

HTTPS ☒ On ☐ Off

Pas4.2: Services → DNS(DNS Service → **ON**)Name: **SLA.RO**Address: **209.165.201.174** (DNS)**ADD**)

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS**
- SYSLOG
- AAA
- NTP
- EMAIL

DNS

DNS Service ☒ On ☐ Off

Resource Records

Name Type **A Record**

Address

No.	Name	Type	Detail
0	sla.ro	A Record	209.165.201.174

Pas4.3: Services → EMAIL(Domain Name: **SLA.RO**)**SET** (să devină gri căsuța)

User: **ANCONA** **!!!PT SERVERE, userii sunt echipamentele de la periferie (PC, SERVERE...; aka acele echipamente la care am setat email-ul)**

Password: **123456**

+

User: **SERVER**Password: **123456**

+)

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL**

EMAIL

SMTP Service ☒ ON ☐ OFF

POP3 Service ☒ ON ☐ OFF

Domain Name:

User Setup

User Password

ANCONA

Domain Name:

User Setup

User ANCONA
SERVER

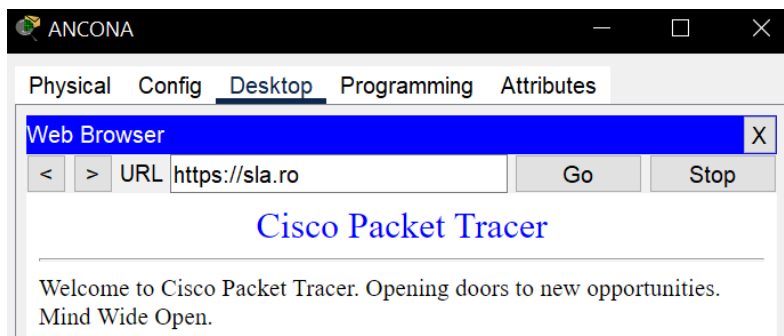
Pas5: Connections → Copper Straigh-Through (firul negru, drept; al 3-lea) și legăm **SWSERVER** la **SERVER**.

Pas6: PC (ANCONA) → Desktop → Command Prompt (ca să verificăm că există conexiune:
ping 209.165.201.174)

!!! Recomandare: De la SERVER la fiecare echipament, inclusiv ANCONA, ar trebui să facem ping și ssh pentru a verifica conexiunea.

- **Verificare:**

Pas1: PC (ANCONA) → Desktop → Web Browser (scriem **sla.ro** și o să avem autocomplete <http://sla.ro>; Go și vom obține Request Timeout. Acum scriem <https://sla.ro> și o să meargă bine.)



Pas2: PC (ANCONA) → Desktop → Email → Compose

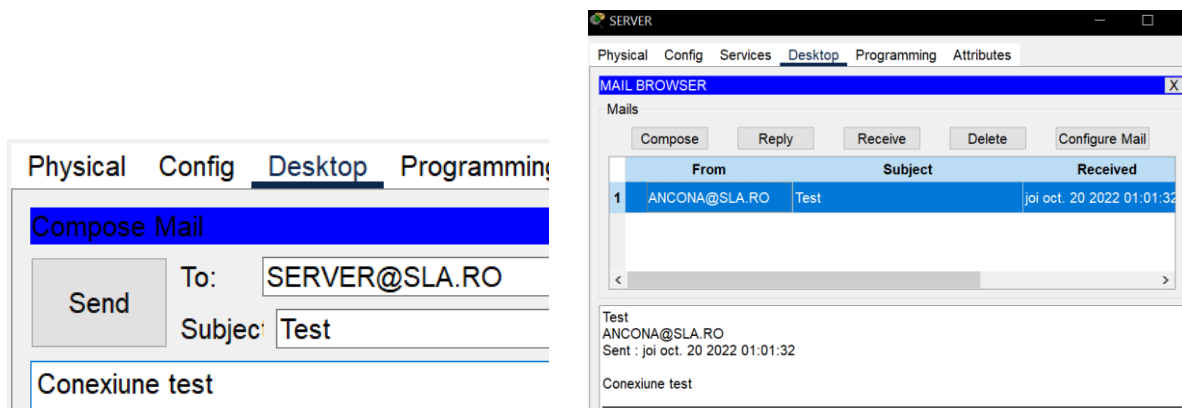
(To: **SERVER@SLA.RO**

Subject: **Test Conexiune**

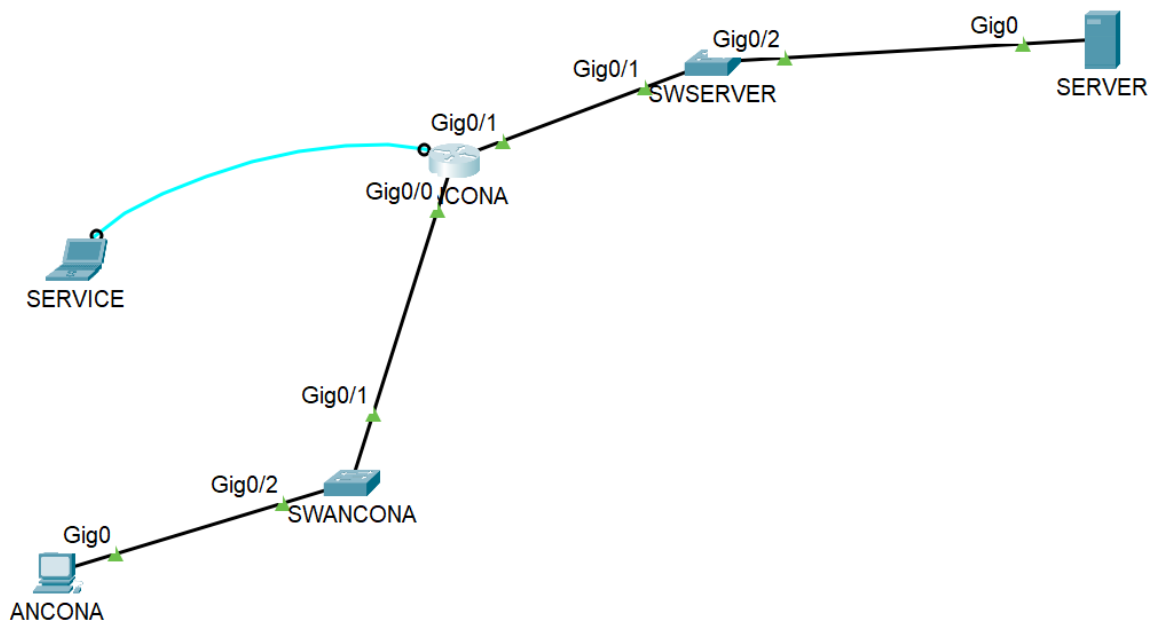
Mesaj: **Test mail**

SEND)

SERVER → Desktop → Email → Receive (Și am primit mail-ul)



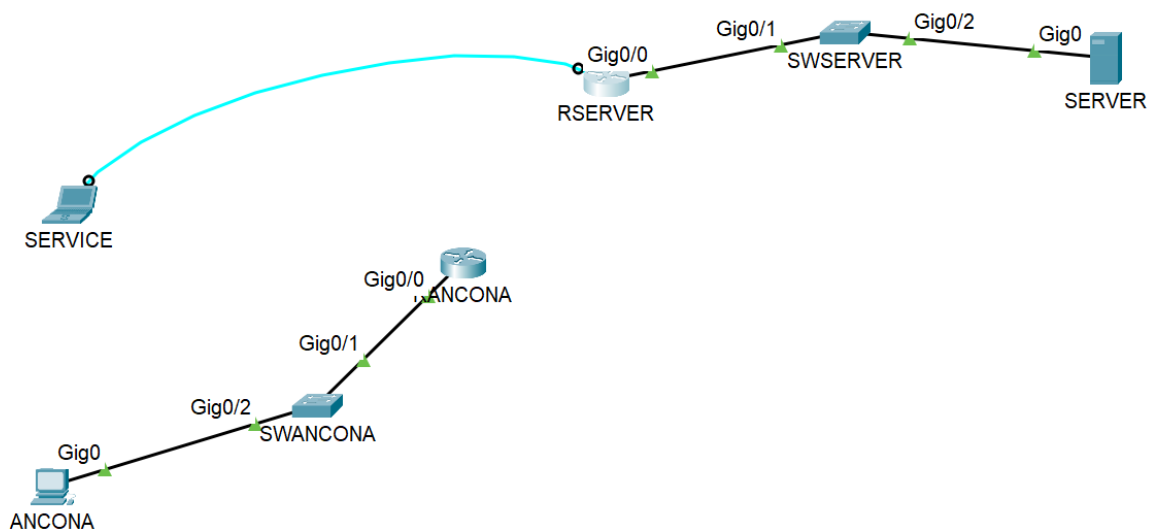
Rezultat:



Acum vom adăuga un nou router, **RSERVER**, și vom încerca să facem legătura dintre **RANCONA** și **RSERVER**. Mai întâi ștergem legătura dintre **RANCONA** și **SWSERVER**. În **RANCONA**, ștergem IP-ul de pe LAN-ul **209.165.201.160/28**:

```
RANCONA(config)#interface g0/1
RANCONA(config-if)#no ip address 209.165.201.161
255.255.255.240
RANCONA(config-if)#sh
```

RSERVER îl configurăm în mod similar (pașii de mai sus), cu IP-ul **209.165.201.161** și testăm conexiunea, ca să fie totul bine. Obținem ceva de genul:



Între 2 routere, vom folosi cablul **Serial DTE** (roșu, fără ceas; al 9-lea). Între cele 2 routere vom folosi **10.10.10.8/30**.

Sintaxă Router RANCONA (OSPF):

RANCONA# configure terminal

----- (setare IP interfață Serial)

RANCONA (config)# interface serial 0/0/0

RANCONA (config-if)# description Legatura cu LAN 10.10.10.8/30

RANCONA (config-if)# ip address 10.10.10.10 255.255.255.252

RANCONA (config-if)# no shutdown

RANCONA (config-if)# exit

----- (OSPF)

RANCONA (config)# router ospf 1

----- (câte LAN-uri sunt)

RANCONA (config)# network 192.168.10.160 0.0.0.31 area 0 // N.A. LAN și Wildcard LAN

RANCONA (config-router)# network 10.10.10.8 0.0.0.3 area 0

RANCONA (config-router)# copy running-config startup-config

Sintaxă Router RSERVER (OSPF):

RSERVER (config)# interface serial 0/0/0

RSERVER (config-if)# description Legatura cu LAN 10.10.10.8/30

RSERVER (config-if)# ip address 10.10.10.10 255.255.255.252

RSERVER (config-if)# no shutdown

RSERVER (config-if)# exit

----- (OSPF)

RSERVER (config)# router ospf 1

----- (câte LAN-uri sunt)

RSERVER (config-router)# network 209.165.201.160 0.0.0.15 area 0

RSERVER (config-router)# network 10.10.10.8 0.0.0.3 area 0

RSERVER (config-router)# copy running-config startup-config

Și testăm conexiunea cu ping și ssh și ar trebui să meargă.

```

Pinging 10.10.10.10 with 32 bytes of data:
Reply from 10.10.10.10: bytes=32 time=1ms TTL=254
Reply from 10.10.10.10: bytes=32 time=1ms TTL=254
Reply from 10.10.10.10: bytes=32 time=16ms TTL=254
Reply from 10.10.10.10: bytes=32 time=9ms TTL=254

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 16ms, Average = 6ms

C:\>ping 209.165.201.174

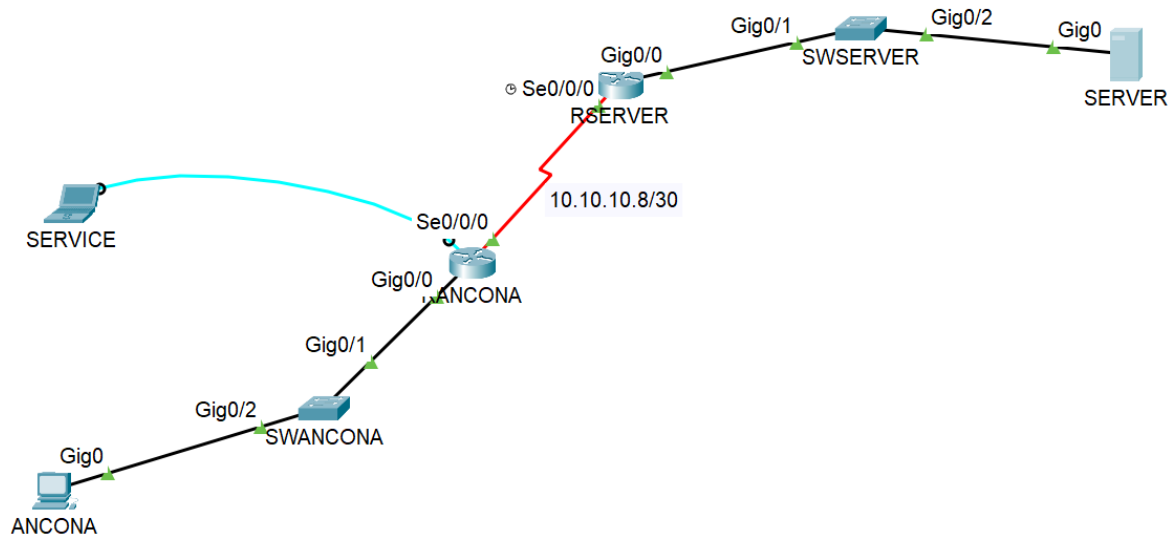
Pinging 209.165.201.174 with 32 bytes of data:

Request timed out.
Reply from 209.165.201.174: bytes=32 time=6ms TTL=126
Reply from 209.165.201.174: bytes=32 time=1ms TTL=126
Reply from 209.165.201.174: bytes=32 time=11ms TTL=126

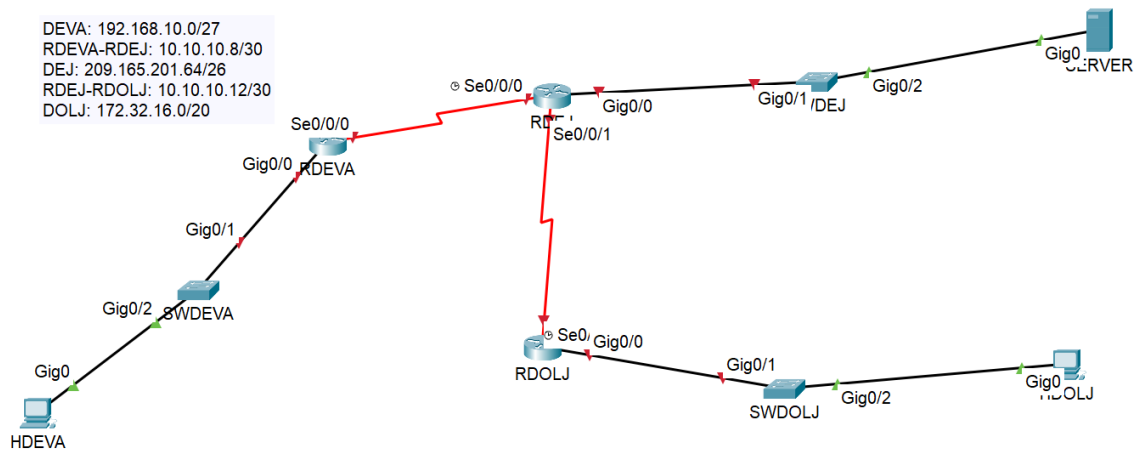
Ping statistics for 209.165.201.174:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:

```

Rezultat:



Laboratorul 4 (25 Octombrie)



Topologia pe care trebuie să o construim.

Sintaxă Switch (Suplimentar, la ce avem deja – Eu, personal, le-am pus după banner):

Switch# configure terminal

----- (înainte de setarea IP-urilor)

Switch (config)# logging host 209.165.201.126 // DNS

Switch (config)# service timestamps log datetime msec

Switch (config)# service timestamps debug datetime msec

Sintaxă Router (Suplimentar, la ce avem deja):

Router# configure terminal

----- (înainte de setarea IP-urilor – Eu, personal, le-am pus după banner)

Router (config)# logging host 209.165.201.126 // DNS

Router (config)# service timestamps log datetime msec

Router (config)# service timestamps debug datetime msec

----- (Rutare OSPF – La final, după setarea IP-urilor)

Router (config)# router ospf 1

Router (config)# network 192.168.10.0 0.0.0.31 area 0 // N.A. LAN; Wildcard

Router (config)# network 10.10.10.8 0.0.0.3 area 0 // N.A. LAN; Wildcard

Router (config)# area 0 authentication message-digest

!!! Dacă avem 2 echipamente de același fel (2 routere), cel din stânga/jos ia IP-ul cel mai MIC, iar cel din dreapta/sus, pe cel mai MARE IP.

!!! ATENȚIE: La porturile în care sunt conectate firele (Drăgan le vrea fix identice). Exemplu: PC are Gigabit0/0 și se conectează cu Switch-ul în Gigabit0/2; Switch-ul se conectează în Gigabit0/1 și Router-ul în Gigabit0/0.

Ordine de configurare: ramura Deva (PC, Switch, Router), ramura Dej (Router, Switch, Server) și ramura Dolj (Router, Switch, PC).

- **Pasi Configurare PC:**

End Devices → PC:

Pas1: Nume **HDEVA/HDOLJ** (majuscule neapărat)

Pas2: Click pe PC; Power OFF; Scoatem placa de rețea; Punem placa **PT-HOST-NM-1CGE**, Power ON

Pas3: **Desktop → IP Configuration**

HDEVA		HDOLJ	
Physical	Config	Physical	Config
Desktop		Desktop	
IP Configuration		IP Configuration	
Interface	GigabitEthernet0	Interface	GigabitEthernet0
IP Configuration		IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static	<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.10.4	IPv4 Address	172.32.16.4
Subnet Mask	255.255.255.224	Subnet Mask	255.255.240.0
Default Gateway	192.168.10.1	Default Gateway	172.32.16.1
DNS Server	209.165.201.126	DNS Server	209.165.201.126

Pas4: **Desktop → Email**

HDEVA		HDOLJ	
Physical	Config	Physical	Config
Desktop		Desktop	
Configure Mail		Configure Mail	
User Information		User Information	
Your Name:	HDEVA	Your Name:	HDOLJ
Email Address	HDEVA@SLA.RO	Email Address	HDOLJ@SLA.RO
Server Information		Server Information	
Incoming Mail Server	209.165.201.126	Incoming Mail Server	209.165.201.126
Outgoing Mail Server	209.165.201.126	Outgoing Mail Server	209.165.201.126
Logon Information		Logon Information	
User Name:	HDEVA	User Name:	HDOLJ
Password:	•••••	Password:	•••••

- **Pasi Configurare Switch [SWDEVA/SWDEJ/SWDOLJ 2960](#)** (Pașii Obișnuiți)
 - [SWDEVA](#): 192.168.10.2
 - [SWDEJ](#): 209.165.201.66
 - [SWDOLJ](#): 172.32.16.2
- **Pasi Configurare Router [RDEVA/RDEJ/RDOLJ 2911](#)** (Pașii Obișnuiți)
 - [RDEVA](#):
 - [Gigabit0/0](#): 192.168.10.1
 - [Serial0/0/0](#): 10.10.10.9
 - [RDEJ](#):
 - [Gigabit0/0](#): 209.165.201.65
 - [Serial0/0/0](#): 10.10.10.10
 - [Serial0/0/1](#): 10.10.10.13
 - [RDOLJ](#):
 - [Gigabit0/0](#): 172.32.16.1
 - [Serial0/0/1](#): 10.10.10.14

- **Pasi Configurare Server:**

Pas1: Nume [SERVER](#)

Pas2: Click pe PC; Power OFF; Scoatem placa de rețea; Punem placa [PT-HOST-NM-1CGE](#), Power ON

Pas3: **Desktop → IP Configuration**

IPv4 Address	209.165.201.126
Subnet Mask	255.255.255.192
Default Gateway	209.165.201.65
DNS Server	209.165.201.126

Pas4: **Desktop → Email**

Configure Mail	
User Information	
Your Name:	SERVER
Email Address	SERVER@SLA.RO
Server Information	
Incoming Mail Server	209.165.201.126
Outgoing Mail Server	209.165.201.126
Logon Information	
User Name:	SERVER
Password:	●●●●●●

Pas4.1: Services → HTTP

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6

HTTP

HTTP ☐ On ☒ Off

HTTPS ☒ On ☐ Off

Pas4.2: Services → DNS

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS**
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP

DNS

DNS Service ☒ On ☐ Off

Resource Records

Name Type **A Record**

Address

Add Save Remove

No.	Name	Type	Detail
0	sla.ro	A Record	209.165.201.126

Pas4.3: Services → EMAIL

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL**
- FTP

EMAIL

SMTP Service ☒ ON ☐ OFF

POP3 Service ☒ ON ☐ OFF

Domain Name: Set

User Setup

User Password

HDEVA
SERVER
HDOLJ

+
-

Pas4.4: Services → FTP(Username: **HDEVA**Password: **123456**

~ Selectăm toate cele 5 căsuțe cu drepturi ~

ADDUsername: **HDOLJ**Password: **123456**

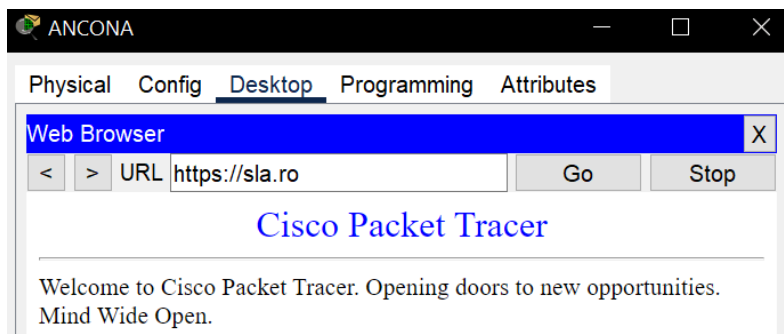
~ Selectăm toate cele 5 căsuțe cu drepturi ~

ADD) !!!NU ADĂUGĂM SERVERUL

SERVICES	FTP												
HTTP DHCP DHCPv6 TFTP DNS SYSLOG AAA NTP EMAIL FTP IoT VM Management	Service <input checked="" type="radio"/> On <input type="radio"/> Off User Setup Username <input type="text" value="HDOLJ"/> Password <input type="text" value="123456"/> <input checked="" type="checkbox"/> Write <input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Delete <input checked="" type="checkbox"/> Rename <input checked="" type="checkbox"/> List <table border="1"> <thead> <tr> <th></th> <th>Username</th> <th>Password</th> <th>Permission</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>cisco</td> <td>cisco</td> <td>RWDNL</td> </tr> <tr> <td>2</td> <td>HDEVA</td> <td>123456</td> <td>RWDNL</td> </tr> </tbody> </table> <div> <input type="button" value="Add"/> <input type="button" value="Save"/> <input type="button" value="Remove"/> </div>		Username	Password	Permission	1	cisco	cisco	RWDNL	2	HDEVA	123456	RWDNL
	Username	Password	Permission										
1	cisco	cisco	RWDNL										
2	HDEVA	123456	RWDNL										

- **Verificare (Și din SERVER către HDEVA/HDOLJ):**

Pas1: PC (HDEVA/HDOLJ) → Desktop → Web Browser (scriem sla.ro și o să avem autocomplete <http://sla.ro>; Go și vom obține Request Timeout. Acum scriem <https://sla.ro> și o să meargă bine.)



Pas2: PC (HDEVA/HDOLJ) → Desktop → Email → Compose

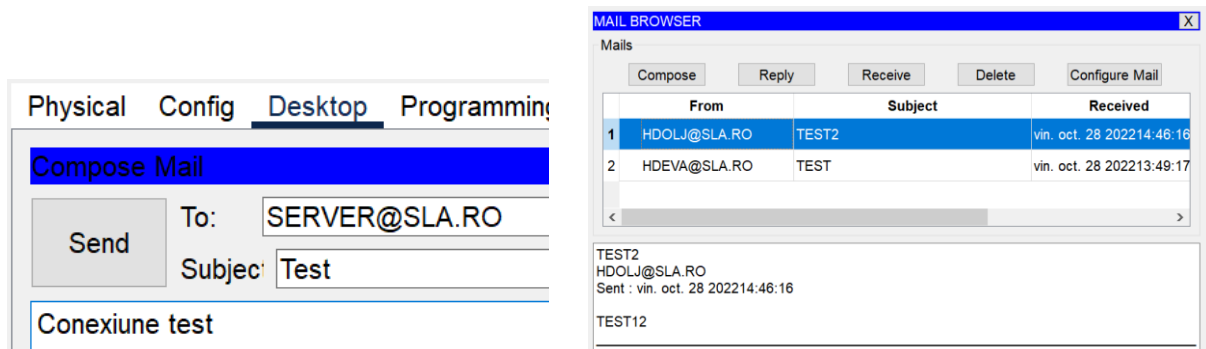
(To: **SERVER@SLA.RO**

Subject: **Test Conexiune**

Mesaj: **Test mail**

SEND)

SERVER → Desktop → Email → Receive (Și am primit mail-ul)



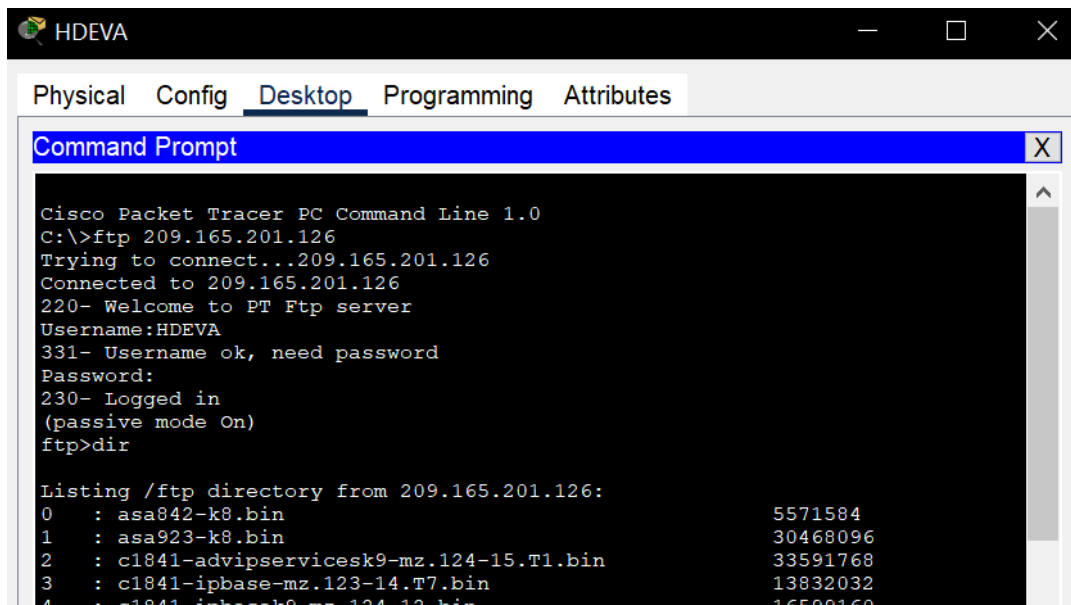
Pas3: **PC (HDEVA/HDOLJ) → Desktop → Command Prompt**

C:\> **ftp 209.165.201.126** // DNS

Username: **HDEVA/HDOLJ**

Password: **123465**

ftp> **dir**



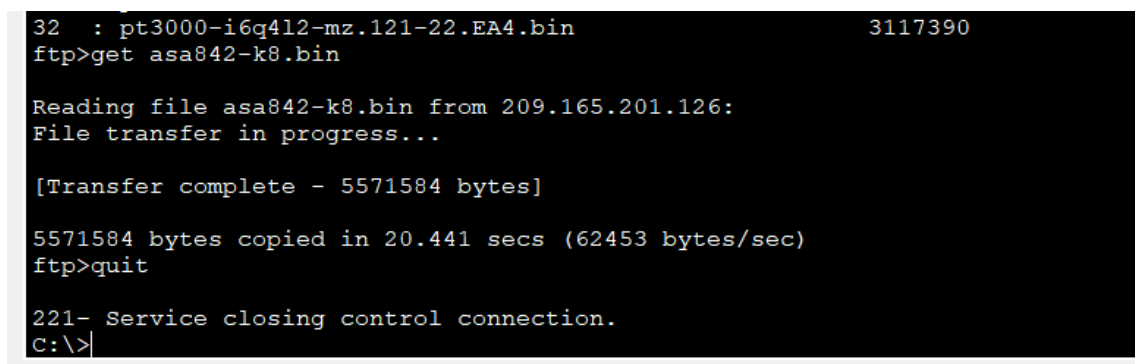
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 209.165.201.126
Trying to connect...209.165.201.126
Connected to 209.165.201.126
220- Welcome to PT Ftp server
Username:HDEVA
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>dir

Listing /ftp directory from 209.165.201.126:
0   : asa842-k8.bin                               5571584
1   : asa923-k8.bin                               30468096
2   : cl841-advipservicesk9-mz.124-15.T1.bin      33591768
3   : cl841-ipbase-mz.123-14.T7.bin               13832032
4   : cl841-ipbasek9-mz.124-12.bin                16599160
```

(Alegem primul pachet: asa842-k8.bin)

ftp>**get asa842-k8.bin** //Descărcăm primul pachet

ftp>**quit**



```
32   : pt3000-i6q412-mz.121-22.EA4.bin           3117390
ftp>get asa842-k8.bin

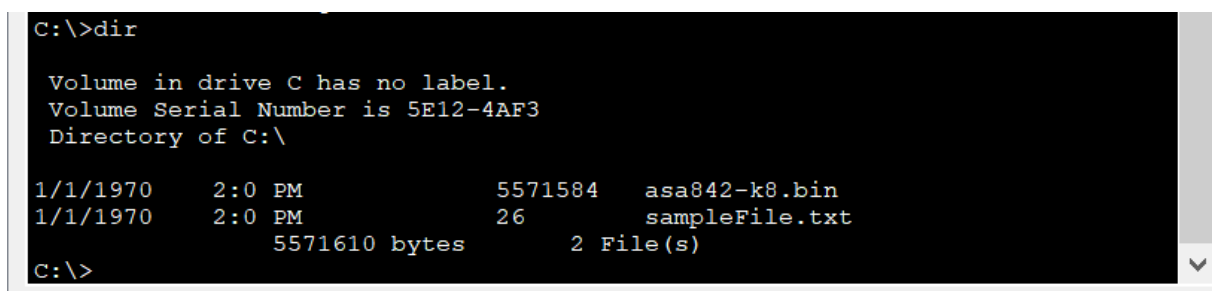
Reading file asa842-k8.bin from 209.165.201.126:
File transfer in progress...

[Transfer complete - 5571584 bytes]

5571584 bytes copied in 20.441 secs (62453 bytes/sec)
ftp>quit

221- Service closing control connection.
C:\>
```

C:\>**dir** //Și aici apare pachetul pe care l-am descărcat



```
C:\>dir

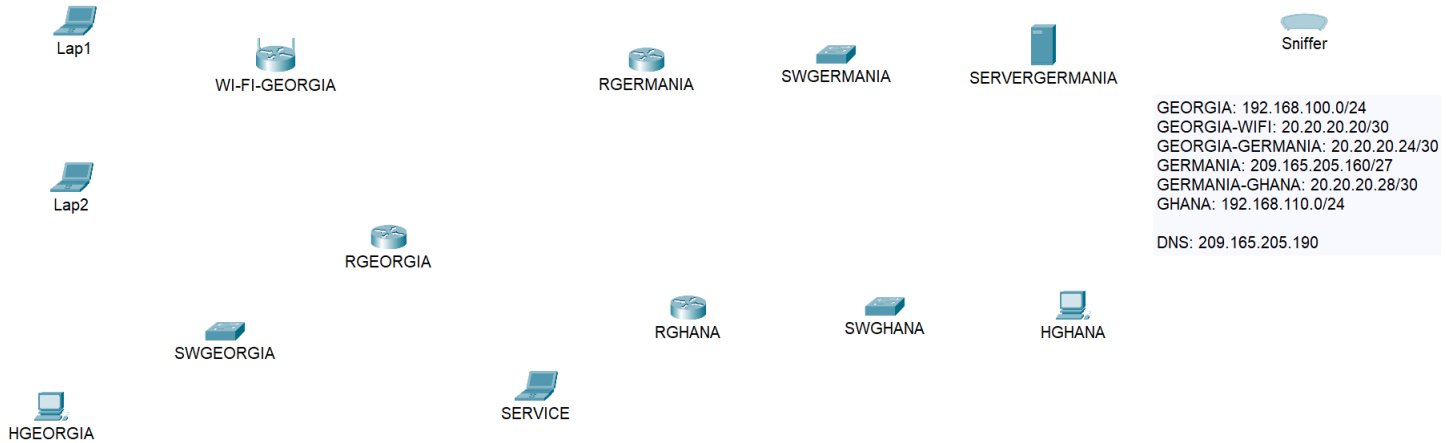
Volume in drive C has no label.
Volume Serial Number is 5E12-4AF3
Directory of C:\

1/1/1970    2:0 PM                5571584    asa842-k8.bin
1/1/1970    2:0 PM                 26         sampleFile.txt
               5571610 bytes          2 File(s)

C:\>
```

Laboratorul 6 (7 Noiembrie)

(Laboratorul 5 e similar cu 6, doar că nu conținea Sniffer-ul. Nu am mai avut timp să scriu și la 5, dar fac totul frumos acum. Laboratorul 6 e similar cu ce am făcut până acum, dar s-a mai schimbat sintaxa și s-au mai adăugat elemente, așa că o să postez toată sintaxa cap-coadă.)



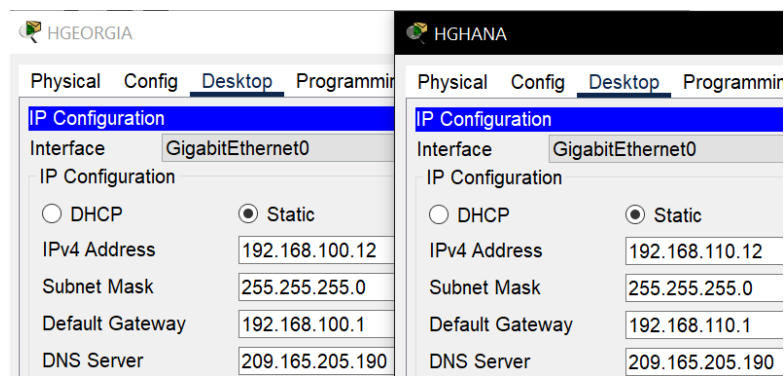
- **Pași Configurare PC:**

End Devices → PC:

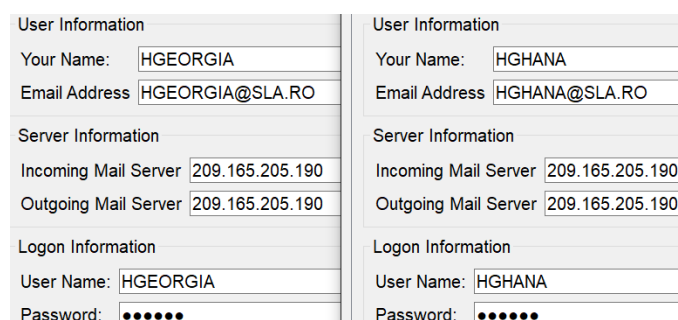
Pas1: Nume **HGEORGIA/HGHANA** (majuscule neapărat)

Pas2: Click pe PC; Power OFF; Scoatem placa de rețea; Punem placa **PT-HOST-NM-1CGE**, Power ON

Pas3: **Desktop → IP Configuration**



Pas4: **Desktop → Email**



- **Pasi Configurare Switch SWGEORGIA/SWGERMANIA/SWGHANA 2960:**

Pas1: Nume **SWGEORGIA/SWGERMANIA/SWGHANA**

Pas2: IP-ul switch-ului: **192.168.100.2 / 209.165.205.162 / 192.168.110.2;**
S.M.: **255.255.255.0 / 255.255.255.224 / 255.255.255.0**

Pas3: Introducem următoarea sintaxă din laptopul **SERVICE**, după ce ne conectăm la **SWGEORGIA/SWGERMANIA/SWGHANA**.

Sintaxă Switch (doar pentru SWGEORGIA, restul sunt similare):

Enter

SW> enable

SW# configure terminal

SW (config)# no ip domain-lookup

SW (config)# hostname **SWGEORGIA**

SW (config)# no cdp run

SW (config)# service password-encryption

SW (config)# enable secret **ciscosecpa55**

SW (config)# enable password **ciscoenapa55**

SW (config)# banner motd **#Vineri, la 12.00, serverul va fi oprit!#**

SW (config)# logging host **209.165.205.190**

SW (config)# service timestamps log datetime msec

SW (config)# service timestamps debug datetime msec

----- (conexiune locală, prin cablul Consolă/Rollover)

SW (config)# line console 0

SW (config-line)# password **ciscoconpa55**

SW (config-line)# login

SW (config-line)# logging synchronous

SW (config-line)# exec-timeout 25 25

SW (config-line)# exit

----- (conexiune virtuală, de la distanță)

SW (config)# line vty 0 15

SW (config-line)# password **ciscovtypa55**

SW (config-line)# login

SW (config-line)# logging synchronous

SW (config-line)# exec-timeout 10 10

SW (config-line)# exit

----- (configurare NTP – nu mai avem nevoie de ceas din cauza asta)

```
SW (config)# ntp server 209.165.205.190
SW (config)# ntp authenticate
SW (config)# ntp trusted-key 1
SW (config)# ntp authentication-key 1 md5 NTPpa55
```

----- (configurare SSH)

```
SW (config)# ip domain name SLA.RO
SW (config)# username Admin01 privilege 15 secret Admin01pa55
SW (config)# line vty 0 15
SW (config-line)# transport input ssh
SW (config-line)# login local
SW (config-line)# exit
SW (config)# crypto key generate rsa → 2048 (scriem)
```

----- (configurare interfață VLAN)

```
SW (config)# interface vlan 1
SW (config-if)# description Legatura cu LAN 192.168.100.0/24
SW (config-if)# ip address 192.168.100.2 255.255.255.0
SW (config-if)# no shutdown
SW (config-if)# exit
```

----- (închidem interfețele nefolosite și setăm D.Gw.)

```
SW (config)# interface range fa 0/1-24
SW (config-if-range)# shutdown
SW (config-if-range)# exit
SW (config)# ip default-gateway 192.168.100.1
```

- **Pași Configurare Router RGEORGIA/RGERMANIA/RGHANA 2911:**

Pas1: Nume **RGEORGIA/RGERMANIA/RGHANA**

Pas2: IP-ul router-ului: **192.168.100.1 / 209.165.205.161 / 192.168.110.1;**
S.M.: **255.255.255.0 / 255.255.255.224 / 255.255.255.0**

Pas3: Click pe router; Power OFF; Punem placa **HWIC-2T** (o punem în slot-ul cel mai din dreapta → pentru a putea avea serial 0/0/0 și să putem lega mai multe routere între ele), Power ON

Pas4: Introducem următoarea sintaxă din laptopul **SERVICE**, după ce ne conectăm la **RGEORGIA/RGERMANIA/RGHANA**.

Sintaxă Router (doar pentru RGEORGIA, restul sunt similare):

Enter

R> enable

R# configure terminal

R (config)# no ip domain-lookup

R (config)# hostname **RGEORGIA**

R (config)# no cdp run

R (config)# service password-encryption

R (config)# security passwords min-length 10

R (config)# login block-for60 attempts 3 within 15

R (config)# enable secret **ciscosecpa55**

R (config)# enable password **ciscoenapa55**

R (config)# banner motd **#Vineri, la 12.00, serverul va fi oprit!#**

!R (config)# banner login **#Accesul persoanelor neautorizate complet interzis!#**

R (config)# logging host **209.165.205.190**

R (config)# service timestamps log datetime msec

R (config)# service timestamps debug datetime msec

----- (conexiune locală, prin cablul Consolă/Rollover)

R (config)# line console 0

R (config-line)# password **ciscoconpa55**

R (config-line)# login

R (config-line)# logging synchronous

R (config-line)# exec-timeout 25 25

R (config-line)# exit

----- (conexiune virtuală, de la distanță)

R (config)# line vty 0 15

R (config-line)# password **ciscovtypa55**

R (config-line)# login

R (config-line)# logging synchronous

R (config-line)# exec-timeout 10 10

R (config-line)# exit

----- (configurare NTP – nu mai avem nevoie de ceas din cauza asta)

R (config)# ntp server **209.165.205.190**

R (config)# ntp authenticate

```
R (config)# ntp trusted-key 1
R (config)# ntp authentication-key 1 md5 NTPpa55
R (config)# ntp update-calendar
----- (configurare SSH)
R (config)# ip domain name SLA.RO
R (config)# username Admin01 privilege 15 secret Admin01pa55
R (config)# line vty 0 15
R (config-line)# transport input ssh
R (config-line)# login local
R (config-line)# exit
R (config)# crypto key generate rsa → 2048 (scream)
----- (configurare interfațe)
R (config)# interface GigabitEthernet 0/0
R (config-if)# description Legatura cu LAN 192.168.100.0/24
R (config-if)# ip address 192.168.100.1 255.255.255.0
R (config-if)# no shutdown
R (config-if)# exit
R (config)# interface GigabitEthernet 0/1
R (config-if)# description Legatura cu 20.20.20.20/30
R (config-if)# ip address 20.20.20.21 255.255.255.252
R (config-if)# no shutdown
R (config-if)# exit
R (config)# interface Serial 0/0/0
R (config-if)# description Legatura cu 20.20.20.24/30
R (config-if)# ip address 20.20.20.25 255.255.255.252
R (config-if)# no shutdown
R (config-if)# exit
----- (rutare OSPF)
R (config)# router ospf 1
R (config-router)# network 192.168.100.0 0.0.0.255 area 0
R (config-router)# network 20.20.20.20 0.0.0.3 area 0
R (config-router)# network 20.20.20.24 0.0.0.3 area 0
R (config-router)# area 0 authentication message-digest
```


- **Pasi Configurare Server:**

Pas1: Nume **SERVERGERMANIA**

Pas2: Click pe PC; Power OFF; Scoatem placa de rețea; Punem placa **PT-HOST-NM-1CGE**, Power ON

Pas3: **Desktop → IP Configuration**

<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	209.165.205.190
Subnet Mask	255.255.255.224
Default Gateway	209.165.205.161
DNS Server	209.165.205.190

Pas4: **Desktop → Email**

User Information	
Your Name:	SERVERGERMANIA
Email Address	SERVERGERMANIA@SLA.RO
Server Information	
Incoming Mail Server	209.165.205.190
Outgoing Mail Server	209.165.205.190
Logon Information	
User Name:	SERVERGERMANIA
Password:	••••••••••

Pas4.1: **Services → HTTP**

SERVICES ↑	HTTP	
	HTTP	
	<input type="radio"/> On	<input checked="" type="radio"/> Off
	HTTPS	
	<input checked="" type="radio"/> On	<input type="radio"/> Off

Pas4.2: **Services → DNS**

SERVICES ↑	DNS			
	DNS Service <input checked="" type="radio"/> On <input type="radio"/> Off			
	Resource Records			
	Name		Type A Record	
	Address			
	Add		Save	
	Remove			
	No.	Name	Type	Detail
	0	sla.ro	A Record	209.165.205.190

Pas4.3: **Services → Syslog**

SERVICES ↑	Syslog		
	Service <input checked="" type="radio"/> On <input type="radio"/> Off		
	Time	HostName	Message

Pas4.4: Services → AAA (La User Setup e tot WI-FI-GEORGIA. Asta m-a ținut 2 ore ca eroare 😞)

La **User Setup**, puteți să puneți alt nume (Ex: WIFI1), dar atunci, mai jos, când creați profilele de utilizatori la laptopuri (pt conexiune wi-fi), trebuie să folosiți noul nume definit de voi.

Pas4.5: Services → NTP (ne asigurăm că data și ceasul se potrivesc)

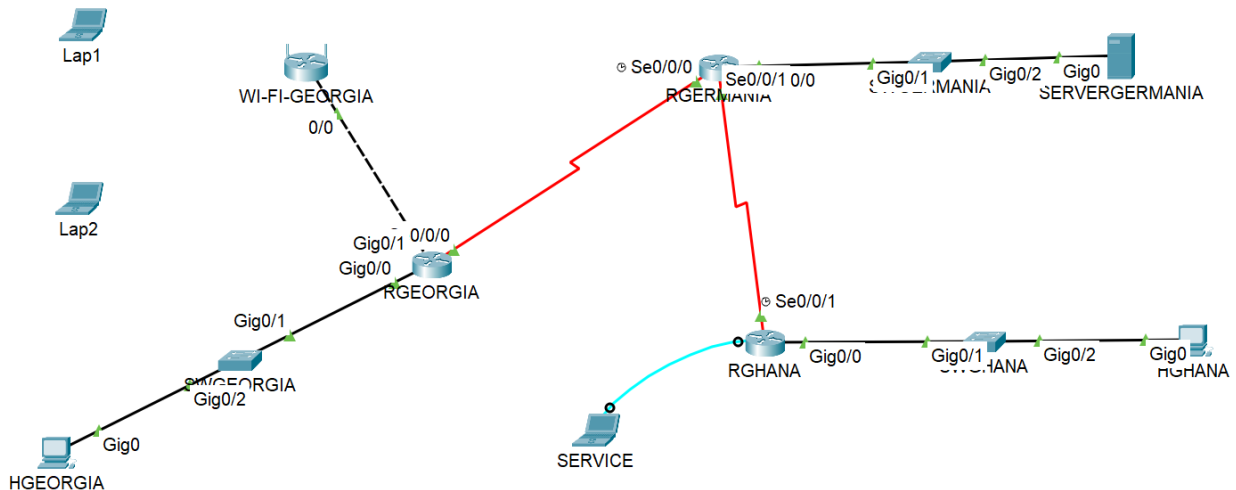
Pas4.5: Services → Email (de adăugat și Lap1 și Lap2)

Pas4.5: Services → FTP (de adăugat și Lap1 și Lap2)

- **Porturi și Legături (!!! Le vrea mereu așa):**

- HGEORGIA/SERVERGERMANIA/HGHANA (*GigabitEthernet0/0*) —
- SWGEORGIA/SWGERMANIA/SWGHANA (*GigabitEthernet0/2*) —
- SWGEORGIA/SWGERMANIA/SWGHANA (*GigabitEthernet0/1*) —
- RGEORGIA/RGERMANIA/RGHANA (*GigabitEthernet0/0*)
- RGEORGIA (*Serial0/0/0*) – RGERMANIA (*Serial0/0/0*)
- RGERMANIA (*Serial0/0/1*) – RGHANA (*Serial0/0/1*)
- RGEORGIA (*GigabitEthernet0/1*) – WI-FI-GEORGIA (*Internet*)

Rezultat:



(Recomandat este să facem toate testele în timp ce lucrăm la topologie. Testele sunt ping, ssh, ftp atunci când avem serverul, web browser și să vedem că http nu merge, dar https funcționează când avem serverul și email-urile)

- **Păși Configurare WI-FI WRT300N (Part I):**

Pas1: Nume **WI-FI-GEORGIA**

Pas2: **Click pe WiFi → GUI → Setup → Basic Setup**

(Internet Connection type: **Static IP**)

Internet IP Address: **20.20.20.22**

Subnet Mask: **255.255.255.252**

Default Gateway: **20.20.20.21**

DNS: **209.165.205.190**

Dăm scroll, dar avem grijă să nu se modifice valorile puse.

Physical Config **GUI** Attributes

Wireless-N Broadband Router

Setup Setup Wireless Security Access Restrictions Applications & Gaming

Basic Setup DDNS MAC Address Clone

Internet Setup

Internet Connection type: Static IP

Internet IP Address: 20 . 20 . 20 . 22

Subnet Mask: 255 . 255 . 255 . 252

Default Gateway: 20 . 20 . 20 . 21

DNS 1: 209 . 165 . 205 . 190

DNS 2 (Optional): 0 . 0 . 0 . 0

DNS 3 (Optional): 0 . 0 . 0 . 0

Optional Settings: Host Name:

Router IP-IP Address: **192.168.15.1** //valoarea poate fi schimbată, dar pe asta ne-a dat-o el

Subnet Mask: **255.255.255.248**

Start IP Address: **192.168.15.2** //după ce dăm save se va face modificarea din 0 în 15

Maximum number of Users: **5**

Scroll, cu grijă să nu modificăm valorile, și Save Settings)

Network Setup

Router IP: IP Address: 192 . 168 . 15 . 1

Subnet Mask: 255.255.255.248

DHCP Server Settings: DHCP Server: ☒ Enabled ☐ Disabled

Start IP Address: 192.168.15. 2

Maximum number of Users: 5

Pas3: GUI → Wireless → Basic Wireless Settings

(SSID: **WI-FI-GEORGIA**

Standard Channel: **6**

Save Settings)

Wireless Setup Wireless Security Access Restrictions Applications & Gaming

Basic Wireless Settings Wireless Security Guest Network Wireless MAC Filter

Basic Wireless Settings

Network Mode: Mixed

Network Name (SSID): WI-FI-GEORGIA

Radio Band: Auto

Wide Channel: Auto

Standard Channel: 6 - 2.437GHz

SSID Broadcast: ☒ Enabled ☐ Disabled

Pas4: GUI → Wireless → Wireless Security(Security Mode: **WPA2 Enterprise**Radius Server: **209.165.205.190** //DNSShared Secret: **RadiusPa55***Save Settings*)

Wireless	Setup	Wireless	Security	Access Restrictions	Applications & Gaming	Wireless MAC Filter
	Basic Wireless Settings		Wireless Security	Guest Network		Wireless MAC Filter
Wireless Security						
Security Mode:		WPA2 Enterprise				
Encryption:		AES				
RADIUS Server:		209	.	165	.	205 . 190
RADIUS Port:		1645				
Shared Secret:		RadiusPa55				
Key Renewal:		3600	seconds			

- Pasi Configurare Lap1 și Lap2 (Ambele trebuie configurate):**

Pas1: Nume **Lap1/Lap2** (Aparent, trebuie să configurăm și adresele de **mail** aici)**Pas2:** POWER OFF. Scoatem placa de rețea și o punem pe **WPC300N**. POWER ON.**Pas3: Desktop → PC Wireless → Profiles***(New*Enter name for new profile: **WI-FI-GEORGIA***Advanced Setup* //colțul dreapta josWireless Network Name: **WI-FI-GEORGIA**DHCP: **ON**Security: **WPA2-Enterprise**Login Name: **WI-FI-GEORGIA**Password: **RadiusPa55***Next, Save, Connect to Network*)**Pas4: Config → Wireless0** (și copiem MAC Address)

Physical	Config	Desktop	Programming	Attributes
GLOBAL		Wireless0		
Settings		Port Status		
Algorithm Settings		Bandwidth		
INTERFACE		11 Mbps		
Wireless0		MAC Address		
Bluetooth		SSID		
		000A.F344.CB68		
		WI-FI-GEORGIA		
		Authentication		

- **Pași Configurare WI-FI WRT300N (Part II):**

Pas1: GUI → Wireless → Wireless MAC Filter

(Enabled)

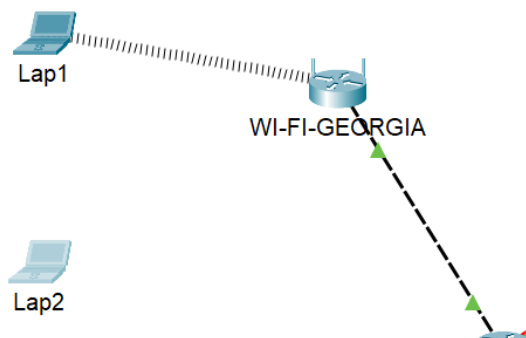
Permit PCs listed below to acces wireless network

MAC01: **00:01:63:67:C0:69** //punem adresa MAC de la un singur laptop, dar le configurăm pe ambele, ca să apară că unul e conectat și altul nu e

Save Settings)

Wireless		Setup	Wireless	Security	Access Restrictions	Applications & Gaming	Wireless-N B
Wireless MAC Filter		Basic Wireless Settings		Wireless Security	Guest Network	Wireless MAC Filter	
Access Resolution		Wireless Port: 2.4G					
MAC Address filter list		<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled <input type="radio"/> Prevent PCs listed below from accessing the wireless network <input checked="" type="radio"/> Permit PCs listed below to access wireless network					
		Wireless Client List					
		MAC 01:	00:0A:F3:44:CB:68	MAC 26:	00:00:00:00:00:00		
		MAC 02:	00:00:00:00:00:00	MAC 27:	00:00:00:00:00:00		

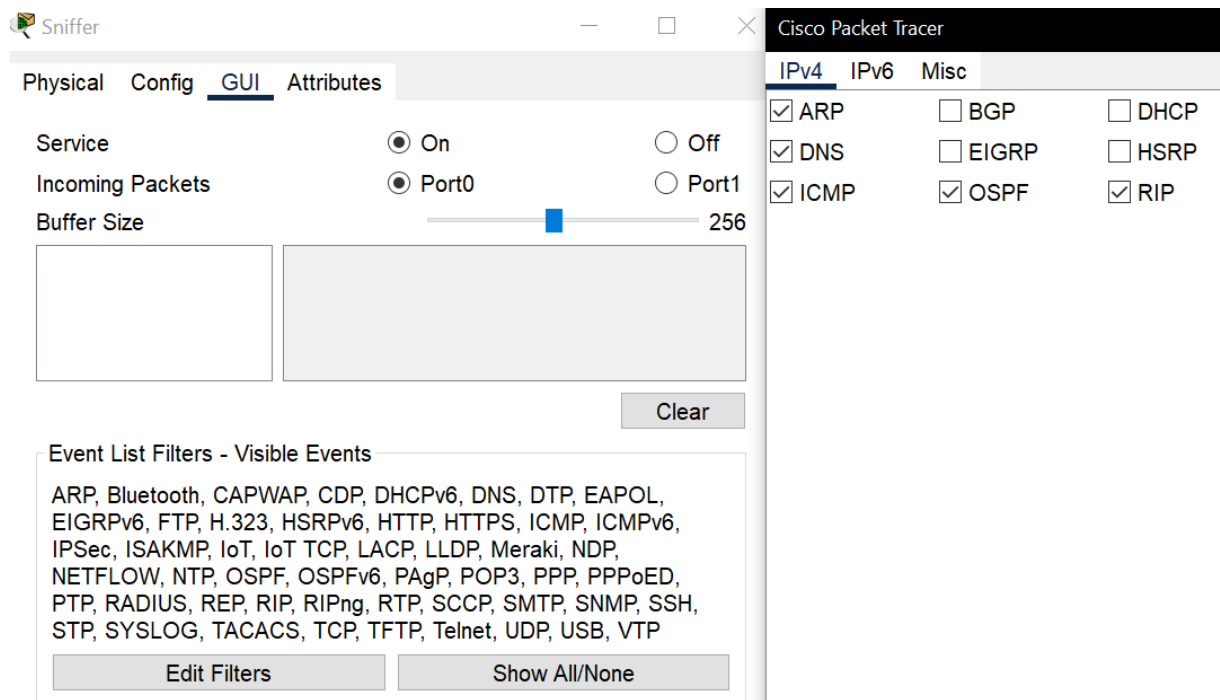
Rezultat:



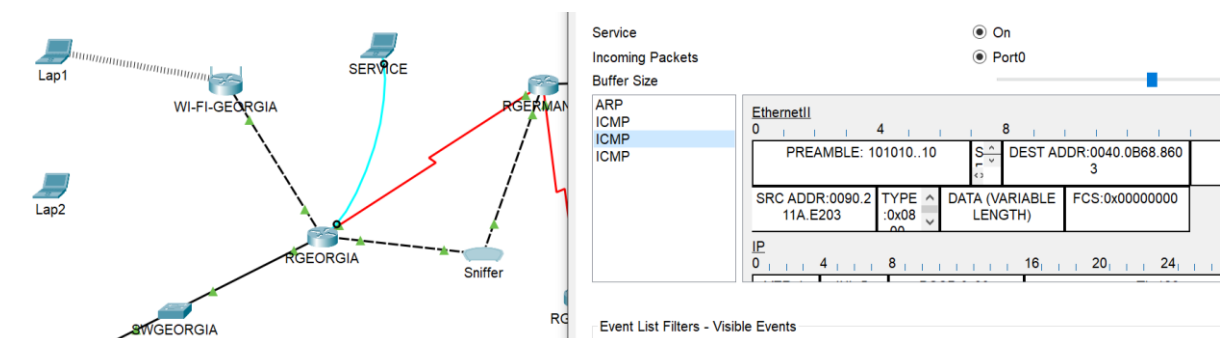
- **Pași Configurare Sniffer:**

Pas1: Luăm Sniffer-ul din End Devices. Este ultimul.

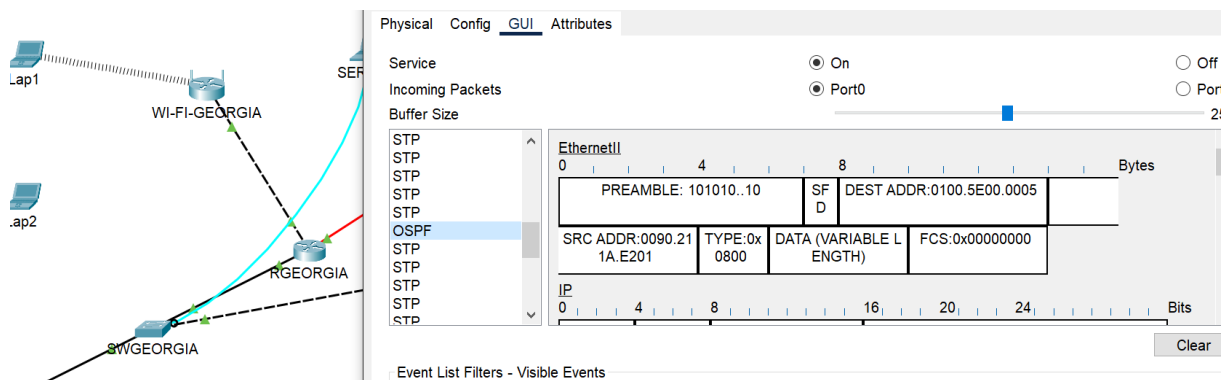
Pas2: **GUI → Edit Filters** (și selectăm doar **ARP, DNS, ICMP, OSPF, RIP**. Mai sar filtrele. Dacă se întâmplă asta, dați clear și editați din nou filtrele.)



Pas3: Cu cablul **Copper Cross-Over** (negru, întretăiat) ne conectăm la **GigabitEthernet0/2** la **RGEORGIA/RGERMANIA**. Și setăm IP-uri în **GigabitEthernet0/2** în ambele rutere (**10.10.10.8/30**). Dăm un ping din **HGEORGIA** în **10.10.10.10**. Apoi, în GUI, trebuie să primim trafic.



Putem să conectăm Sniffer la **SWGEORGIA** (**FastEthernet0/1**; trebuie să pornim interfața înainte → din laptop accesăm **interface fa0/1** și **no sh**) și acum primim trafic în continuu.



Laboratorul 7 (14 Noiembrie)

În acest laborator, avem suplimentar DHCP-ul la server și sintaxă nouă pentru securizare switch-uri.

- **Configurare DHCP Server:**

Pas1: Services → DHCP

(Interface: **GigabitEthernet0** //de aia este important să avem Giga0/0 între Router și Switch

Service: **ON**

Pool Name: **GEORGIA/GHANA**

Default Gateway: **192.168.100.1/192.168.110.1**

DNS Server: **209.165.205.190**

Start IP Address: **192.168.100.13/192.168.110.13** // **.12 de la PC + 1**

Subnet Mask: **255.255.255.0**

Maximum Number of Users: **242** // **32-24=8; 2⁸=256; 256-2=254; 254-12=242**

Add)

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
GHANA	192.168.110.1	209.165.205.190	192.168.110.13	255.255.255.0	242	0.0.0.0	0.0.0.0
GEORGIA	192.168.100.1	209.165.205.190	192.168.100.13	255.255.255.0	242	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	209.165.205.160	255.255.255.224	31	0.0.0.0	0.0.0.0

Pentru a funcționa, în **RGEORGIA** și **RGHANA**, pe interfața **Gigabit0/0**, trebuie să adăugăm următoarea comandă:

R (config)# interface Gigabitethernet 0/0

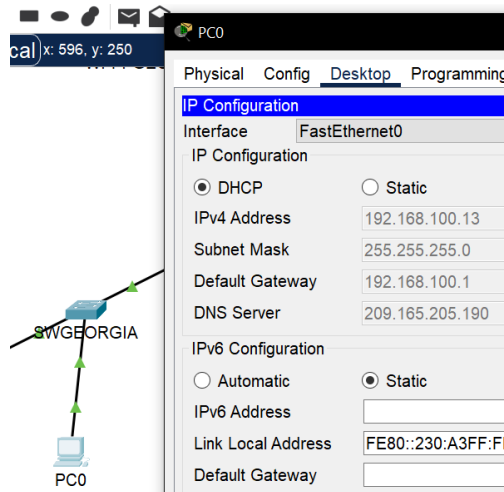
R (config-if)# ip helper-address 209.165.205.190

Ca să ne verificăm, în **SWGEORGIA** și **SWGIANA** activăm interfața **Fa0/24**:

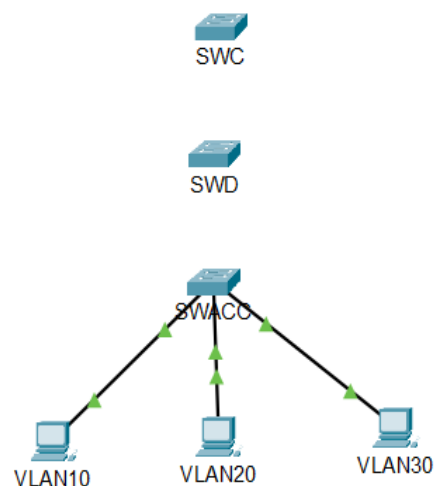
SW (config)# interface fa0/24

SW (config-if)# no shutdown

...legăm un PC (acesta nu trebuie configurat) de switch și **Desktop → IP Configuration**, dăm click pe **DHCP** și ar trebui să ia automat IP address **.13**.



În continuare, adăugăm un layer suplimentar de securitate pe switch-uri. Luăm 3 switch-uri **SWACC**, **SWD** și **SWC** și 3 PC-uri numite **VLAN10**, **VLAN20** și **VLAN30**.



PC-uri (configurate cu *placă rețea*, *IP Config* și *Mail* – ca orice host normal; Le adăugăm și în **SERVER**, la *mail* și *ftp*):

- **VLAN10**: 192.168.10.0/24 (.12 pt PC; **fa0/1** legat SWACC)
- **VLAN20**: 192.168.20.0/24 (.12 pt PC; **fa0/8** legat SWACC)
- **VLAN30**: 192.168.30.0/24 (.12 pt PC; **fa0/15** legat SWACC)

Switch-uri:

- **VLAN 10 → SLA**: fa0/1-5
- **VLAN 20 → MASTER**: fa0/8-13
- **VLAN 30 → FMI**: fa0/15-19
- **VLAN 45 → NULL**: fa0/6-7, fa0/14
- **VLAN 99 → MAN**

Cele **3 switch-uri** le configurăm normal, dar nu punem nicio comandă care conține IP-uri. Și, suplimentar, adăugăm:

```
SW (config)# vlan 10
```

```
SW (config-if)# name SLA
```

```
SW (config-if)# exit
```

```
SW (config)# vlan 20
```

```
SW (config-if)# name MASTER
```

```
SW (config-if)# exit
```

```
SW (config)# vlan 30
```

```
SW (config-if)# name FMI
```

```
SW (config-if)# exit
```

```
SW (config)# vlan 45
```

```
SW (config-if)# name NULL
```

```
SW (config-if)# exit
```

```
SW (config)# vlan 99
```

```
SW (config-if)# name MAN
```

```
SW (config-if)# exit
```

Apoi, pentru **VLAN 10, 20, 30, 45** repetăm comenzile următoare (schimbăm doar numerele și interfețele) – **!!!Doar pentru SWACC:**

```
SW (config)# interface range fa0/1-5
SW (config-if-range)# switchport mode access
SW (config-if-range)# switchport access vlan 10
SW (config-if-range)# switchport port-security
SW (config-if-range)# switchport port-security maximum 2
SW (config-if-range)# switchport port-security mac-address sticky
SW (config-if-range)# switchport port-security violation shutdown
SW (config-if-range)# switchport port-security aging time 1
SW (config-if-range)# spanning-tree bpduguard enable
SW (config-if-range)# spanning-tree portfast
SW (config-if-range)# exit
```

Apoi, mai adăugăm următoarele linii de comandă – **!!!pentru SWACC, SWD, SWC:**

```
SW (config)# interface range fa0/20-24, g0/1-2
SW (config-if-range)# switchport mode trunk
SW (config-if-range)# switchport trunk native vlan 99
SW (config-if-range)# switchport trunk allowed vlan 10,20,30,99
SW (config-if-range)# exit
```

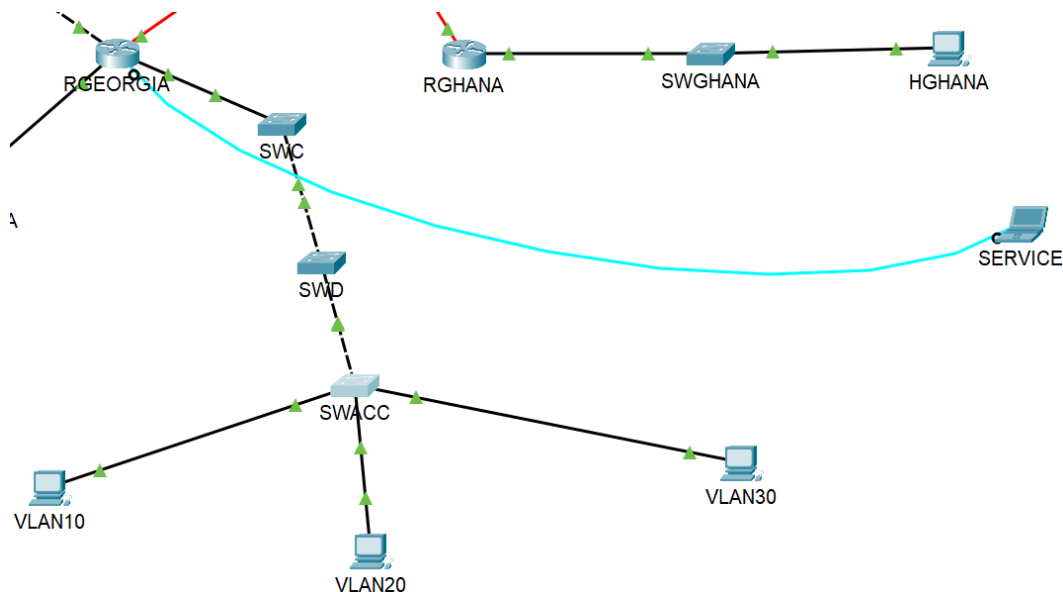
Pentru a ne verifica, putem să scriem (așa apare la **SWACC**):

```
SWC>show vlan
```

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

Laboratorul 8 (21 Noiembrie)

Continuăm configurarea VLAN-urilor de laboratorul trecut. Trebuie să obținem:



- **Porturi și Legături (!!! Le vrea mereu așa):**
 - RGEORGIA (*GigabitEthernet0/2*) – SWC (*GigabitEthernet0/2*)
 - SWC (*GigabitEthernet0/1*) – SWD (*GigabitEthernet0/1*)
 - SWD (*GigabitEthernet0/2*) – SWACC (*GigabitEthernet0/2*)
 - SWACC (*Fa0/1*) – VLAN10 (*GigabitEthernet0/0*)
 - SWACC (*Fa0/8*) – VLAN20 (*GigabitEthernet0/0*)
 - SWACC (*Fa0/15*) – VLAN30 (*GigabitEthernet0/0*)

Explicație este logică: VLAN-urile se conectează în rang-urile definite de noi, mai sus. Adică VLAN10 ar putea să fie conectat oriunde între fa0/1 – 5, dar Drăgan le vrea pe primele, ca să avem ordine. Și conexiunea cu Gigabit este așa pentru că **RGEORGIA** mai are doar giga0/2 liber și încercăm să avem acea simetrie.

Ca să avem conectivitate, trebuie să adăugăm următoarele comenzi în **RGEORGIA**:

```
R (config)# interface GigabitEthernet 0/2.10
R (config-if)# description Legatura cu VLAN10
R (config-if)# encapsulation dot1Q 10
R (config-if)# ip address 192.168.10.1 255.255.255.0
R (config-if)# exit
R (config)# interface GigabitEthernet 0/2.20
R (config-if)# description Legatura cu VLAN20
R (config-if)# encapsulation dot1Q 20
R (config-if)# ip address 192.168.20.1 255.255.255.0
```

```
R (config-if)# exit
R (config)# interface GigabitEthernet 0/2.30
R (config-if)# description Legatura cu VLAN30
R (config-if)# encapsulation dot1Q 30
R (config-if)# ip address 192.168.30.1 255.255.255.0
R (config-if)# exit
R (config)# interface GigabitEthernet 0/2
R (config-if)# no shutdown
```

Și, suplimentar, adăugăm în protocolul **OSPF** din router-ul **RGEORGIA** aceste 3 IP-uri de VLAN-uri. Acum putem face ping, trimite mail-uri și folosi ftp din cele 3 VLAN-uri.

Ca să vedem ce comenzi au fost introduse pe echipamente, putem folosi comanda: **show run**.

```
RGEORGIA>en
Password:
RGEORGIA#show run
Building configuration...

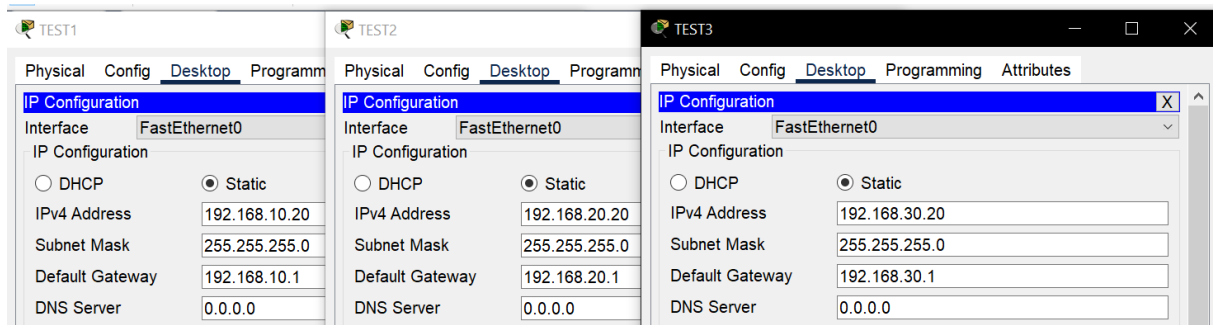
Current configuration : 2721 bytes
!
version 15.1
service timestamps log datetime msec
service timestamps debug datetime msec
service password-encryption
security passwords min-length 10
!
hostname RGEORGIA
!
login block-for 60 attempts 3 within 15
!
!
enable secret 5 $1$mERr$/RLeWf7h7xqihhg.u8p0V/
enable password 7 0822455D0A160019131B0D517F
!
!
```

În continuare, vom securiza interfețele **serial** din routere. Vom folosi următoarele comenzi:

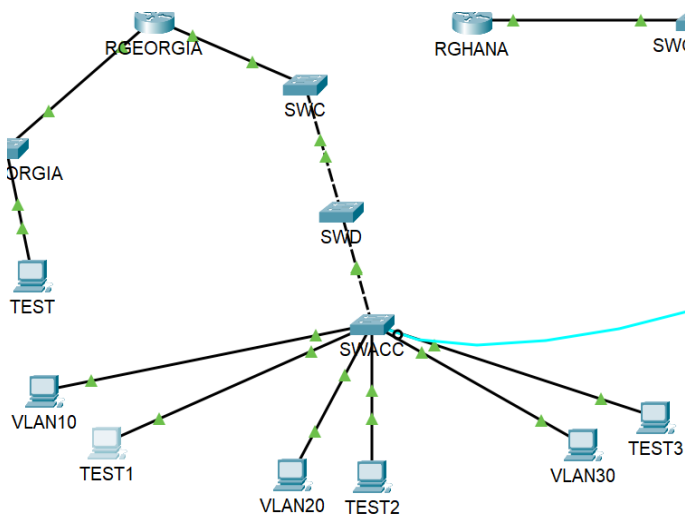
```
R (config)# interface serial 0/0/0    //sau serial0/0/1, în funcție de ce router avem
R (config-if)# ip ospf authentication message-digest
R (config-if)# ip ospf message-digest-key 1 md5 MD5pa55
```

Dacă facem ping-uri, ar trebui să ne putem conecta de oriunde din rețea (dacă am lucrat corect).

Conectăm 3 PC-uri de test (nu schimbăm placa de rețea) la **SWACC** pe interfețele **fa0/2**, **fa0/9**, **fa0/16** (ne asigurăm că sunt **UP**) și le setăm, în **IP Configuration**, doar **Ipv4**, **SM** și **D.Gw.**:



Din nou, dacă facem ping-uri și din aceste PC-uri de test, ar trebui să ne putem conecta oriunde din rețea (dacă am lucrat corect). Obținem:



Dacă am încerca să mai conectăm încă un PC de test la VLAN10, spre exemplu, nu am putea pentru că am pus opțiunea, mai sus, de `SW (config-if-range)# switchport port-security maximum 2`.

Ultimul obiectiv este să creăm un **ACL**, denumit **88**, pe intrare, în **RGEORGIA**, care să nu permită PC-urile de teste, definite mai sus, să facă ssh. Introducem următoarele comenzi:

```
R (config)# access-list 88 deny host 192.168.10.20
```

```
R (config)# access-list 88 deny host 192.168.20.20
```

```
R (config)# access-list 88 deny host 192.168.30.20
```

```
R (config)# access-list 88 permit any
```

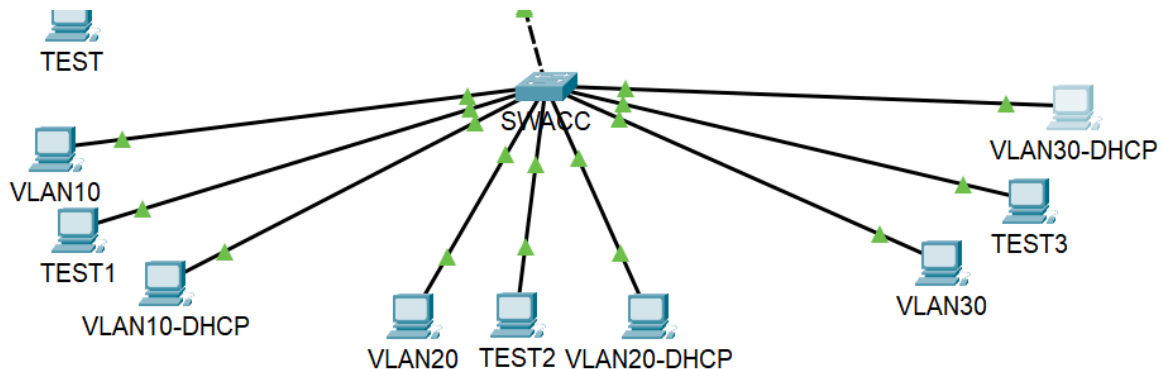
```
R (config-if)# line vty 0 15
```

```
R (config-line)# access-class 88 in
```

Dacă testăm, o să remarcăm că cele 3 PC-uri de test nu mai pot face ssh în 192.168.10.1, 192.168.20.1, 192.168.30.1, 192.168.100.1, 20.20.20.21 și 20.20.20.25, dar VLAN10/20/30 pot.

Laboratorul 9 (28 Noiembrie)

Luăm 3 PC-uri noi (**VLAN10-DHCP**, **VLAN20-DHCP**, **VLAN30-DHCP**) și încercăm să le conectăm la DHCP (PC-urile vor fi configurate similar cu **HGEORGIA/HGHANA**, aka placă de rețea, email, ftp, teste, etc...).



Pași:

- Luăm 3 PC-uri noi, le redenumim, le schimbăm placa de rețea (**CGE**) și le punem doar mail-ul;
- Legăm **VLAN10-DHCP** la **SWACC** prin **Fa0/3**, **VLAN20-DHCP** prin **Fa0/10** și **VLAN30-DHCP** prin **Fa0/17**;
- În terminal **SWACC**, introducem comenzile: **interface range fa0/3, fa0/10, fa0/17; no shutdown** (pentru a activa interfețele);
- În **SERVERGERMANIA**, la **Services**, adăugăm la **EMAIL** și **FTP** cele 3 PC-uri și la **DHCP** cele 3 zone:

SERVICES

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

DHCP

Interface: GigabitEthernet0 Service: ☒ On ☐ Off

Pool Name: VLAN10

Default Gateway: 192.168.10.1

DNS Server: 209.165.205.190

Start IP Address: 192.168.10.13

Subnet Mask: 255.255.255.0

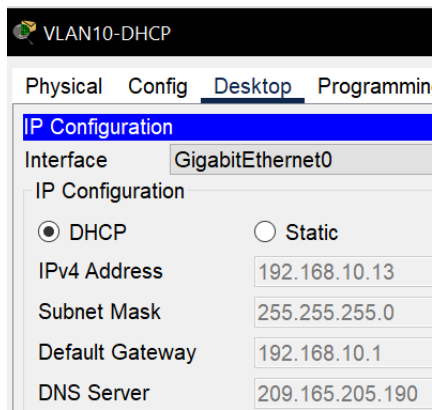
Maximum Number of Users: 242

TFTP Server: 0.0.0.0

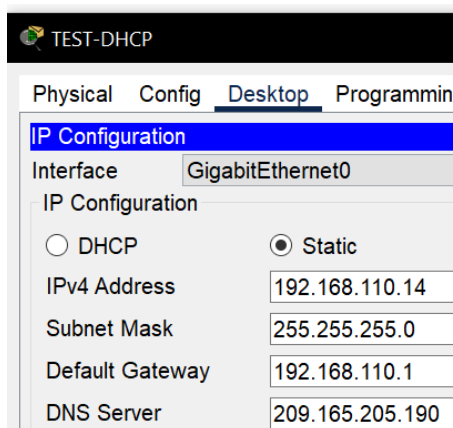
WLC Address: 0.0.0.0

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WL Addr
VLAN30	192.168.30.1	209.165.205.190	192.168.30.13	255.255.255.0	242	0.0.0.0	0.0.0.0
VLAN20	192.168.20.1	209.165.205.190	192.168.20.13	255.255.255.0	242	0.0.0.0	0.0.0.0
VLAN10	192.168.10.1	209.165.205.190	192.168.10.13	255.255.255.0	242	0.0.0.0	0.0.0.0

- În **RGEORGIA**, introducem următoarea sintaxă pentru fiecare interfață Giga0/2.10, Giga0/2.20, Giga0/2.30: **interface giga0/2.10; ip helper-address 209.165.205.190**;
- În cele 3 PC-uri, la **IP Config**, mutăm din **Static** în **DHCP** și ar trebui să primim noi IP-uri pentru dispozitivele noastre;
- Facem testele pentru PC-uri.



Încercăm să introducem un **ACL** pentru **VLAN10-DHCP**, care să nu permită ssh. Luăm un PC nou (**TEST-DHCP**) în **Ghana** și încercăm același lucru (acest PC nu trebuie configurat, schimbăm doar placa de rețea și punem IP-ul). Începem cu **TEST-DHCP**, pentru că este mai simplu:



În **RGHANA**, introducem următoarele comenzi:

```
R (config)# access-list 88 deny host 192.168.110.14
```

```
R (config)# access-list 88 permit any
```

```
R (config-if)# line vty 0 15
```

```
R (config-line)# access-class 88 in
```

Și dacă încercăm să facem **ssh -l Admin01 192.168.110.1** din acest PC, avem eroare.

Mai departe, pentru **VLAN10-DHCP** nu putem defini ACL-ul în mod similar, pentru că IP-ul se poate schimba rapid (avem DHCP). De aceea, trebuie să interzicem toată rețeaua și să lăsăm doar IP-urile care ne interesează. În **RGEORGIA**, introducem următoarele comenzi:

```
R (config)# no access-list 88 //ștergem ACL-ul inițial
```

```
R (config-if)# line vty 0 15
```

```
R (config-line)# no access-class 88 in
```

```
R (config-line)# exit
```

```
R (config)# access-list 88 permit host 192.168.10.12
```

```
R (config)# access-list 88 deny 192.168.10.0 0.0.0.255
```

```
R (config-if)# line vty 0 15
```

```
R (config-line)# access-class 88 in
```

Acum, **VLAN10** este singurul care poate folosi ssh.

În interfețele **serial**, introducem encapsularea ppp. Pentru **RGEORGIA**, introducem:

```
R (config)# interface s0/0/0
```

```
R (config-if)# encapsulation ppp
```

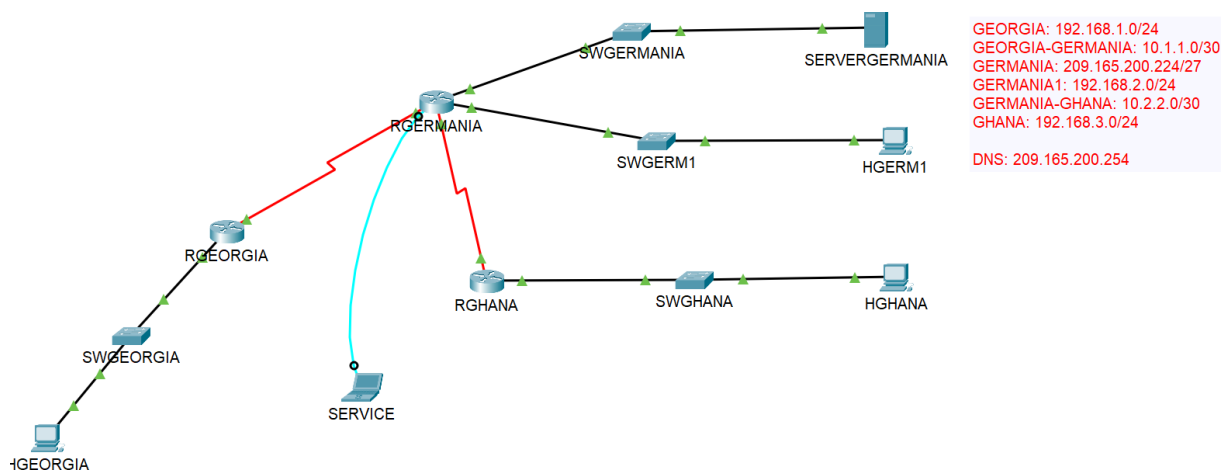
```
R (config-if)# ppp authentication chap
```

```
R (config-if)# username RGERMANIA secret 0123456789
```

În mod similar pentru **RGERMANIA** (doar că username-ul va fi **RGEORGIA**). Și același lucru pentru interfața **s0/0/1** (**RGERMANIA** și **RGHANA**).

Laboratorul 10 (5 Decembrie)

Realizăm o topologie nouă (ATENȚIE LA PAȘII DE CONFIGURARE – nu o să mai avem toți pașii de securitate):



PC-urile, serverul și switch-urile sunt configurate normal. Routerule le configurăm fără rutare OSPF și fără encapsulare ppp. Aici recomand să salvăm fișierul și să lucrăm pe o copie de acum încolo. (Verificări ca să meargă serviciile: ping, ssh, email, ftp, etc...; avem nevoie mai jos)

Realizăm **rutarea dinamică**, cu următoarele instrucțiuni:

```
RGEORGIA (config)# ip route 209.165.200.224 255.255.255.224 s0/0/0 //N.A. S.M. serialul de intrare
```

```
RGEORGIA (config)# ip route 192.168.2.0 255.255.255.0 s0/0/0
```



```
RGEORGIA (config)# ip route 10.2.2.0 255.255.255.252 s0/0/0
```

```
RGEORGIA (config)# ip route 192.168.3.0 255.255.255.0 s0/0/0
```

!!!Nu luăm rețelele adiacente.

Pentru **RGHANA** este similar (tot 4 comenzi), dar pe **s0/0/1**. Iar pentru **RGERMANIA**:

```
RGERMANIA (config)# ip route 192.168.1.0 255.255.255.0 s0/0/0
```

```
RGERMANIA (config)# ip route 192.168.3.0 255.255.255.0 s0/0/1
```

Creăm ACL-uri:

Pe toate cele 3 routere introducem această sintaxă:

```
R (config)# access-list 10 permit host 192.168.3.12
```

```
R (config)# line vty 0 15
```

```
R (config-line)# access-class 10 in
```

Vom remarca că doar **HGHANA** poate să realizeze ssh pe cele 3 routere, iar celelalte 2 PC-uri nu au permisiunea.

Pe **RGEORGIA** creăm următorul ACL:

```
RGEORGIA (config)# access-list 120 permit udp any host 192.168.1.12 eq domain //orice cu excepția lui  
HGEORGIA pot accesa DNS-ul; pentru test, din HGEORGIA ping sla.ro și nu o să meargă
```

```
RGEORGIA (config)# access-list 120 permit tcp any host 192.168.1.12 eq smtp //MAIL
```

```
RGEORGIA (config)# access-list 120 permit tcp any host 192.168.1.12 eq ftp //FTP
```

```
RGEORGIA (config)# access-list 120 deny tcp any host 192.168.1.12 eq 443 //HTTPS
```

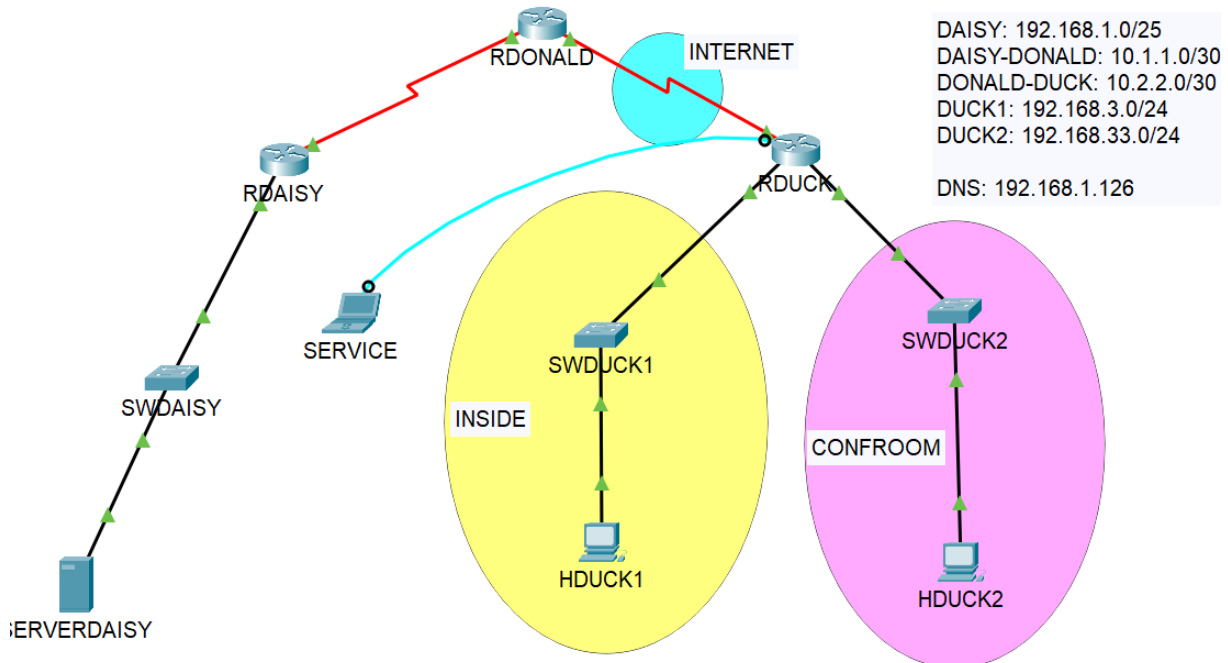
```
RGEORGIA (config)# access-list 120 permit tcp host 192.168.1.12 host 192.168.3.12 eq 22 //SSH
```

```
RGEORGIA (config)# interface s0/0/0
```

```
RGEORGIA (config-line)# ip access-group 120 in
```

Laboratorul 11 (12 Decembrie)

Realizăm o topologie nouă (ATENȚIE LA PAȘII DE CONFIGURARE – nu o să mai avem toți pașii de securitate):



PC-urile, serverul și switch-urile sunt configurate normal. Routerule le configurăm fără rutare OSPF și fără encapsulare ppp. Realizăm **rutarea statică**, cu următoarele instrucțiuni:

```
RDAISY (config)# ip route 0.0.0.0 0.0.0.0 10.1.1.2 //IP-ul router-ului vecin
```

```
RDUCK (config)# ip route 0.0.0.0 0.0.0.0 10.2.2.1
```

```
RDONALD (config)# ip route 192.168.1.0 255.255.255.128 10.1.1.1
```

```
RDONALD (config)# ip route 192.168.3.0 255.255.255.0 10.2.2.2
```

```
RDONALD (config)# ip route 192.168.33.0 255.255.255.0 10.2.2.2
```

Facem testele (ping, ssh, mail, ftp, etc...) și trebuie să avem conectivitate în toată topologia.

Construim zonele de securitate:

```
RDUCK (config)# license boot module c2900 technology-package securityk9 → YES (dăm de 2 ori comanda ca să apară acel meniu mare și să putem scrie YES) → exit → reload → YES → ENTER
```

```
RDUCK (config)# zone security INSIDE
```

```
RDUCK (config)# zone security CONFROOM
```

```
RDUCK (config)# zone security INTERNET
```

```
RDUCK (config)# class-map type inspect match-any INSIDE_PROTOCOLS
```

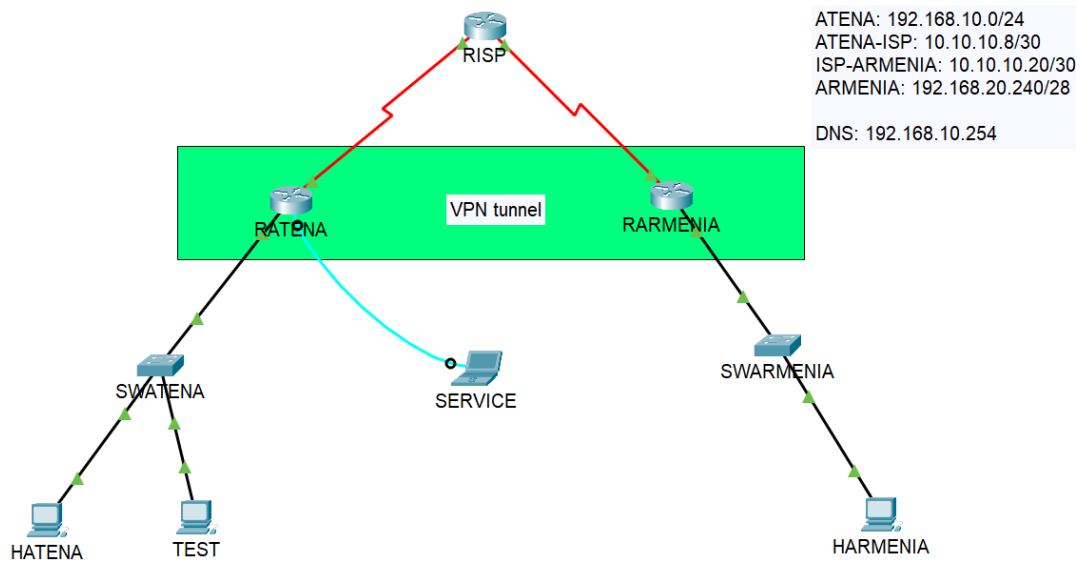
```
RDUCK (config)# match protocol tcp
```

```
RDUCK (config)# match protocol udp
RDUCK (config)# match protocol icmp
RDUCK (config)# exit
RDUCK (config)# class-map type inspect match-any CONFROOM_PROTOCOLS
RDUCK (config)# match protocol http
RDUCK (config)# match protocol https
RDUCK (config)# match protocol dns
RDUCK (config)# exit
RDUCK (config)# policy-map type inspect INSIDE_TO_INTERNET
RDUCK (config)# class type inspect INSIDE_PROTOCOLS
RDUCK (config)# inspect → exit → exit
RDUCK (config)# policy-map type inspect CONFROOM_TO_INTERNET
RDUCK (config)# class type inspect CONFROOM_PROTOCOLS
RDUCK (config)# inspect → exit → exit
RDUCK (config)# zone-pair security INSIDE_TO_INTERNET source INSIDE destination INTERNET
RDUCK (config)# service-policy type inspect INSIDE_TO_INTERNET
RDUCK (config)# zone-pair security CONFROOM_TO_INTERNET source CONFROOM destination INTERNET
RDUCK (config)# service-policy type inspect CONFROOM_TO_INTERNET
(RDUCK# show zone-pair security || show policy-map type inspect zone-pair sessions)
RDUCK (config)# interface giga0/0
RDUCK (config-if)# zone-member security INSIDE
RDUCK (config)# interface giga0/1
RDUCK (config-if)# zone-member security CONFROOM
RDUCK (config)# interface serial0/0/1
RDUCK (config-if)# zone-member security INTERNET
```

Facem testele (ping, ssh, mail, ftp, etc...) și o să avem că nu mai avem conectivitate (datorită regulilor definite de noi anterior):

- HDUCK1 → DA ping și ssh în DAISY și RDONALD / ftp DA / dns DA (ping sla.ro) / https NU / NU ping și ssh în DUCK2 (switch și PC) / mail în DAISY DA / mail în DUCK2 NU;
- HDUCK2 → NU ping și ssh în DAISY și RDONALD / ftp NU / dns NU / https DA / NU ping și ssh în DUCK1 (switch și PC) / mail NU;
- SERVERDAISY → NU ping și ssh la DUCK1 și DUCK2 (switch-uri și PC-uri) / dns DA / mail în HDUCK1 DA / mail în HDUCK2 NU;

Laboratorul 12 (19 Decembrie)



Realizăm o topologie nouă. PC-urile și switch-urile sunt configurate normal. **RISP** nu are absolut nicio configurare, punem doar IP-urile pe interfețe și atât (acesta nu e router management de noi; e din afara rețelei noastre). Pentru **RATENA** și **RARMENIA** scriem toate comenzile în afară de cele de rutare și cele de criptare.

Dacă încercăm să facem ping din **ATENA** în **ARMENIA**, nu putem. Pentru asta, vom crea **tunel VPN** și, astfel, putem face ping, fără să trecem prin **RISP** (în acest router ping-ul nu va funcționa):

```
RATENA (config)# interface tunnel 0

RATENA (config-if)# ip address 172.16.31.13 255.255.255.252 // una dată de noi

RATENA (config-if)# tunnel source s0/0/0

RATENA (config-if)# tunnel destination 10.10.10.22

RATENA (config-if)# exit

RATENA (config)# router ospf 1

RATENA (config-router)# network 192.168.10.0 0.0.0.255 area 0

RATENA (config-router)# network 172.16.31.12 0.0.0.3 area 0

RATENA (config-router)# exit

RATENA (config)# ip route 0.0.0.0 0.0.0.0 10.10.10.10
```

```
RARMENIA (config)# interface tunnel 0

RARMENIA (config-if)# ip address 172.16.31.14 255.255.255.252 // una dată de noi

RARMENIA (config-if)# tunnel source s0/0/1

RARMENIA (config-if)# tunnel destination 10.10.10.9

RARMENIA (config-if)# exit
```

```

RARMENIA (config)# router ospf 1
RARMENIA (config-router)# network 192.168.20.240 0.0.0.15 area 0
RARMENIA (config-router)# network 172.16.31.12 0.0.0.3 area 0
RARMENIA (config-router)# exit
RATENA (config)# ip route 0.0.0.0 0.0.0.0 10.10.10.21

```

Dacă testăm, acum avem ping între Atena și Armenia (nu în **RISP**).

Pentru **TEST**, creăm un **ACL** care să nu îi permită să realizeze ssh în **RATENA**:

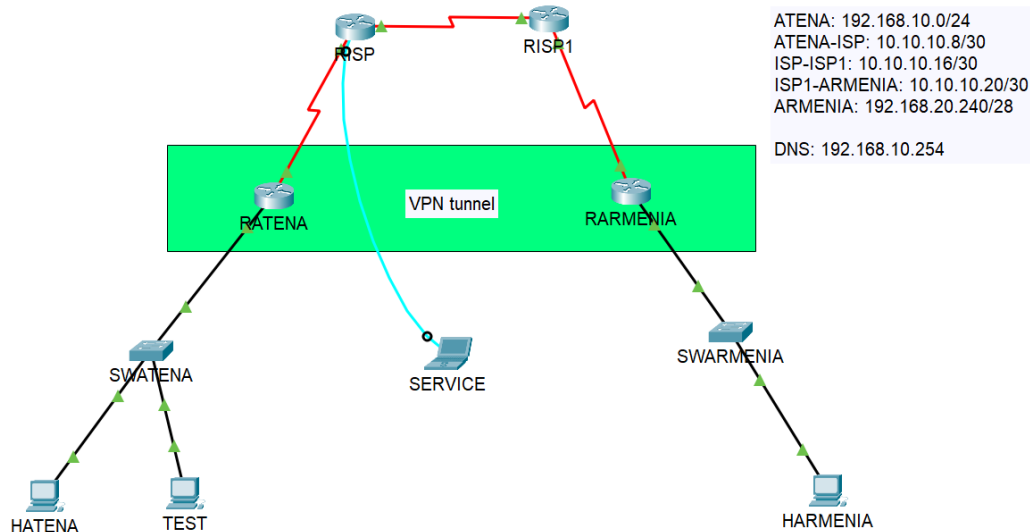
```

RATENA (config)# access-list 77 deny host 192.168.10.13 // IP-ul PC-ului „TEST”
RATENA (config)# access-list 77 permit any // fără linia aceasta, toate PC-urile nu vor putea face ssh în RATENA
RATENA (config)# line vty 0 15
RATENA (config-line)# access-class 77 in

```

Testăm și remarcăm faptul că nu putem face ssh din **TEST** în **RATENA**, dar putem din **HATENA**.

Următorul pas este să adăugăm încă un router **RISP2** (punem doar IP-urile pe interfețe și atât, similar cu **RISP**) între **RISP** și **RARMENIA** și să recreăm tunelul VPN:



Tot ce trebuie să facem este să adăugăm rutare ospf în **RISP** și **RISP1**:

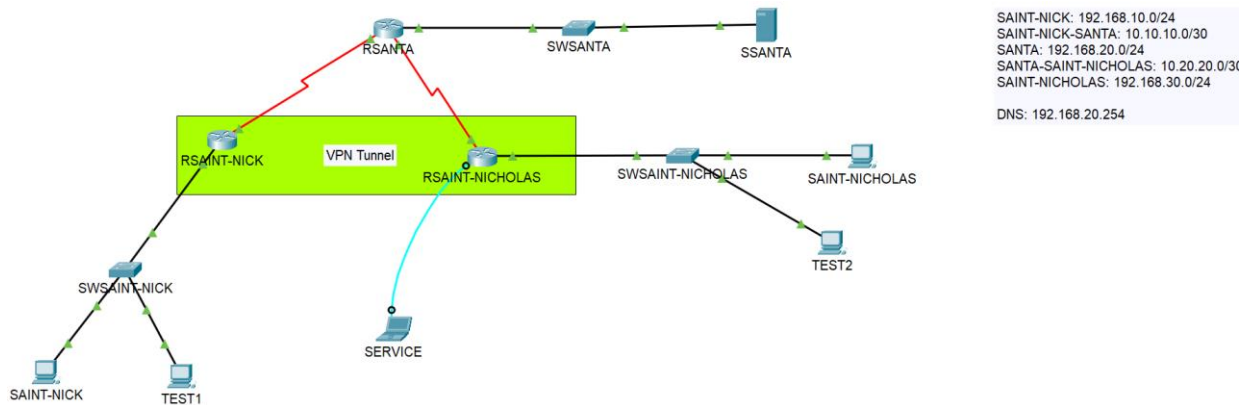
```

RISP (config)# router ospf 1
RISP (config)# network 10.10.10.8 0.0.0.3 area 0
RISP (config)# network 10.10.10.16 0.0.0.3 area 0
RISP1 (config)# router ospf 1
RISP1 (config)# network 10.10.10.16 0.0.0.3 area 0
RISP1 (config)# network 10.10.10.20 0.0.0.3 area 0

```

Laboratorul 13 (9 Ianuarie)

Realizăm următoarea topologie (serverul să aibă toate serviciile, inclusiv DHCP – PC-urile de „TEST” nu trebuie configurate și sunt folosite doar pentru a demonstra că își iau IP-urile în mod dinamic, de la DHCP; routerele să aibă OSPF).



Testăm serviciile. De reținut că avem conectivitate între **SAINT-NICK** și **SAINT-NICHOLAS** (funcționează ping-ul între ele).

Configurăm routerele **RSAINT-NICK** și **RSAINT-NICHOLAS**:

RSAINT-NICK (config)# `license boot module c2900 technology-package securityk9` → YES (dăm de 2 ori comanda ca să apară acel meniu mare și să putem scrie YES) → exit → `reload` → YES → ENTER

RSAINT-NICK (config)# `access-list 110 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255`

RSAINT-NICK (config)# `crypto isakmp policy 10`

RSAINT-NICK (config)# `encryption aes 256`

RSAINT-NICK (config)# `authentication pre-share`

RSAINT-NICK (config)# `group 5`

RSAINT-NICK (config)# `exit`

RSAINT-NICK (config)# `crypto isakmp key VPNpa55 address 10.20.20.2`

RSAINT-NICK (config)# `crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac`

RSAINT-NICK (config)# `crypto map VPN-MAP 10 ipsec-isakmp`

RSAINT-NICK (config)# `description VPN connection`

RSAINT-NICK (config)# `set peer 10.20.20.2`

RSAINT-NICK (config)# `set transform-set VPN-SET`

RSAINT-NICK (config)# `match address 110`

RSAINT-NICK (config)# `exit`

RSAINT-NICK (config)# `interface s0/0/0`

RSAINT-NICK (config)# `crypto map VPN-MAP`

RSAIN-NICHOLAS (config)# license boot module c2900 technology-package securityk9 → YES (dăm de 2 ori comanda ca să apară acel meniu mare și să putem scrie YES) → exit → reload → YES → ENTER

RSAIN-NICHOLAS (config)# access-list 110 permit ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255

RSAIN-NICHOLAS (config)# crypto isakmp policy 10

RSAIN-NICHOLAS (config)# encryption aes 256

RSAIN-NICHOLAS (config)# authentication pre-share

RSAIN-NICHOLAS (config)# group 5

RSAIN-NICHOLAS (config)# exit

RSAIN-NICHOLAS (config)# crypto isakmp key VPNpa55 address 10.10.10.1

RSAIN-NICHOLAS (config)# crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac

RSAIN-NICHOLAS (config)# crypto map VPN-MAP 10 ipsec-isakmp

RSAIN-NICHOLAS (config)# description VPN connection

RSAIN-NICHOLAS (config)# set peer 10.10.10.1

RSAIN-NICHOLAS (config)# set transform-set VPN-SET

RSAIN-NICHOLAS (config)# match address 110

RSAIN-NICHOLAS (config)# exit

RSAIN-NICHOLAS (config)# interface s0/0/0

RSAIN-NICHOLAS (config)# crypto map VPN-MAP

Ca să ne testăm că modificările au fost luate:

```

Password:
RSAIN-NICK#show crypto ipsec sa

interface: Serial0/0/0
  Crypto map tag: VPN-MAP, local addr 10.10.10.1

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (192.168.30.0/255.255.255.0/0/0)
  current_peer 10.20.20.2 port 500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

    local crypto endpt.: 10.10.10.1, remote crypto endpt.:10.20.20.2
    path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
    current outbound spi: 0x0(0)

  inbound esp sas:

--More--

```

Acum, dacă încercăm să facem ping între SAINT-NICK și SAINT-NICHOLAS, vom avea eroare.