

Sedinta I

1.Cerinta problemei

Tema 6:

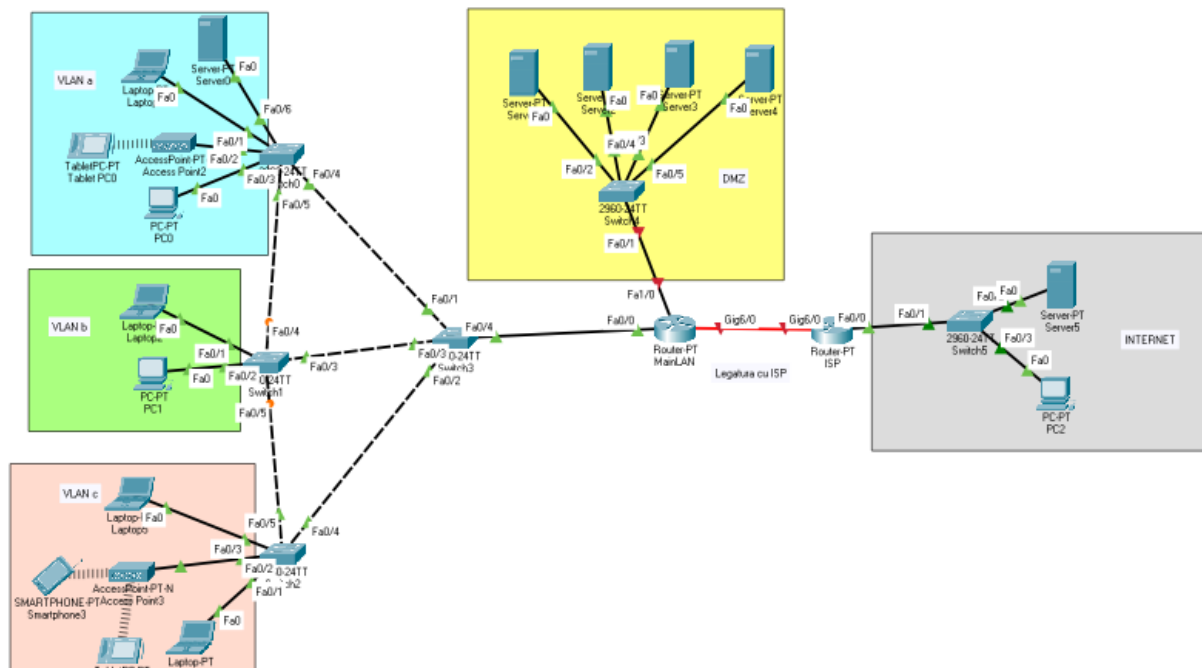
Se considera o cladire comerciala cu 3 niveluri. Se va folosi adresa de retea 10.1.0.0/16 pentru reseaua intranet, adresa de retea 210.2.2.16/29 pentru DMZ si adresa de retea 210.2.2.8/29 pentru accesul in exterior. Se vor proiecta 4 VLAN-uri (unul pentru fiecare etaj si unul pentru traficul de management). 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 cate un server de DHCP. 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 Overload pe routerul care controleaza DMZ, pe urmatorul interval de adrese publice: 210.2.2.11-210.2.2.14.

Conectarea la ISP se va realiza printr-o interfata de tip Ethernet avand adresa 210.2.2.10/29. Adresa ISP-ului este 210.2.2.9/29. 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 privilegiu, criptarea parolelor, configurarea remote se va face doar prin ssh, se va securiza protocolul VTP.

Se vor prezenta si implementa doua masuri suplimentare de securizare a retelei.

2.Crearea topologiei



3.Subnetarea adresei private

Step1: determine the number of bits needed

-how many bits do we need to create 4 subnets? 2 bits

-how many subnets can we compute? $2^2 = 4$ subnets

Step2:determine the new network mask (subnet mask)

-original NM: /16 = 255.255.0.0 or 11111111.11111111.00000000.00000000

-new NM: we need to borrow 2 bits for subnets (step 1) from the host part, so we mark this in the NM: 11111111.11111111.11000000.00000000 = /18 or 255.255.192.0

Step3: determine how many bits are remaining for the hosts

-how many bits are set to 0 in the new NM?

14 bits => 14 bits for hosts => so we can have $2^{14} - 2 = 16384$ hosts/subnet

Step4: compute IP subnets range

SN1:

<div> <div>Network bits</div> <div>Subnet bits</div> <div>Host bits</div> </div>	Conversion to decimal notation
<div> <div>00001010. 00000001.00000000. 000 00000</div> </div>	10.1.0.0 /18- Network Address for SN1
<div> <div>00001010. 00000001.00000000. 000 00001</div> </div>	10.1.0.1 /18
<div> <div>00001010. 00000001.00000000. 000 00010</div> </div>	10.1.0.2 /18
.....
<div> <div>00001010. 00000001.00111111.11111111</div> </div>	10.1.63.255 /18- Broadcast Address for SN1

SN2:

<div> <div>Network bits</div> <div>Subnet bits</div> <div>Host bits</div> </div>	Conversion to decimal notation
<div> <div>00001010. 00000001.01000000. 000 00000</div> </div>	10.1.64.0 /18 - Network Address for SN2
<div> <div>00001010. 00000001.01000000. 000 00001</div> </div>	10.1.64.1 /18
<div> <div>00001010. 00000001.01000000. 000 00010</div> </div>	10.1.64.2 /18
.....
<div> <div>00001010. 00000001.01111111.11111111</div> </div>	10.1.127.255 /18- Broadcast Address for SN2

SN3:

<div> <div>Network bits</div> <div>Subnet bits</div> <div>Host bits</div> </div>	Conversion to decimal notation
<div> <div>00001010. 00000001.10000000. 00000000</div> </div>	10.1.128.0 /18 - Network Address for SN3
<div> <div>00001010. 00000001.10000000. 00000001</div> </div>	10.1.128.1 /18
<div> <div>00001010. 00000001.10000000. 00000010</div> </div>	10.1.128.2 /18
.....
<div> <div>00001010. 00000001.10111111.11111111</div> </div>	10.1.191.255 /18- Broadcast Address for SN3

SN4:

<div> <div>Network bits</div> <div>Subnet bits</div> <div>Host bits</div> </div>	Conversion to decimal notation
<div> <div>00001010. 00000001.11000000. 00000000</div> </div>	10.1.192.0 /18 - Network Address for SN4
<div> <div>00001010. 00000001.11000000. 00000001</div> </div>	10.1.192.1 /18
<div> <div>00001010. 00000001.11000000. 00000010</div> </div>	10.1.192.2 /18
.....
<div> <div>00001010. 00000001.11111111.11111111</div> </div>	10.1.255.255 /18- Broadcast Address for SN4

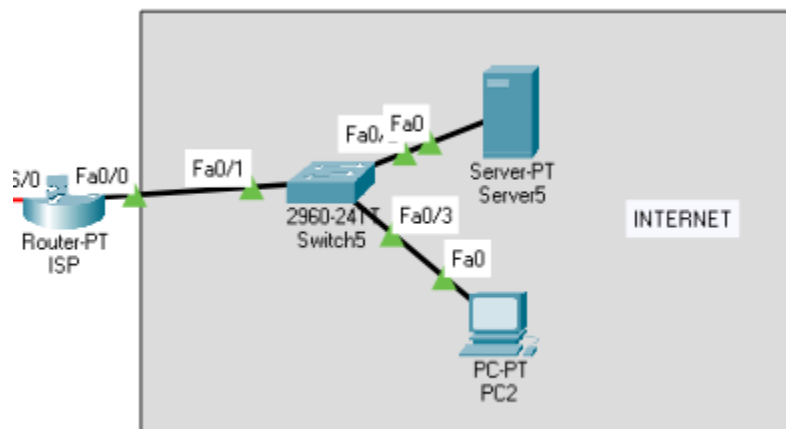
4.Subnetarea adresei publice

210.2.2.10-210.2.2.22 /29 (255.255.255.248)

Subnet	Adresa IP	Sn Host		
SN1	210.2.2.8	00001 000	Adresa SN1	
	210.2.2.9	00001 001	Adresa Host SN1	ISP
	210.2.2.10	00001 010	Adresa Host SN1	
	210.2.2.11	00001 011	Adresa Host SN1	
			NAT
	210.2.2.14	00001 110	Adresa Host SN1	
	210.2.2.15	00001 111	Adresa Broadcast SN1	
SN2	210.2.2.16	00010 000	Adresa SN2	
	210.2.2.17	00010 001	Adresa Host SN2	
	...			DMZ
	210.2.2.22	00010 110	Adresa Host SN2	

5.Configurare

5.1 Blocul de Internet



Pentru a configure interfata Fa0/0 a rutarului am executat comenzile : click pe ruter -> CLI->enable->configure terminal -> interface Fa0/0 -> ip address 1.1.1.1 255.0.0.0 -> no shutdown .

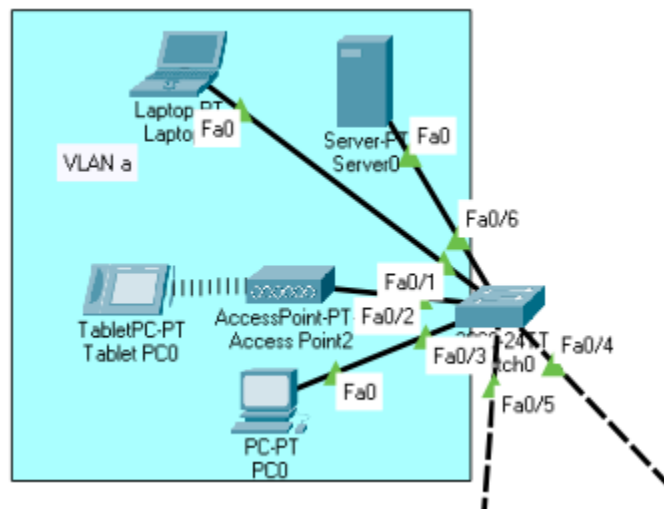
Pentru a configure serverul 5 am executat comenzile : click pe server -> Desktop-> ip configuration si am pus adresa si masca si adresa de gateway(care este adresa de pe interfata router-ului).

IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	<input type="text" value="1.1.1.3"/>
Subnet Mask	<input type="text" value="255.0.0.0"/>
Default Gateway	<input type="text" value="1.1.1.1"/>
DNS Server	<input type="text" value="0.0.0.0"/>

Pentru a configura Pc2 am executat comenzile : click pe server -> Desktop-> ip configuration si am pus adresa si masca si adresa de gateway.

IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	1.1.1.2
Subnet Mask	255.0.0.0
Default Gateway	1.1.1.1
DNS Server	0.0.0.0

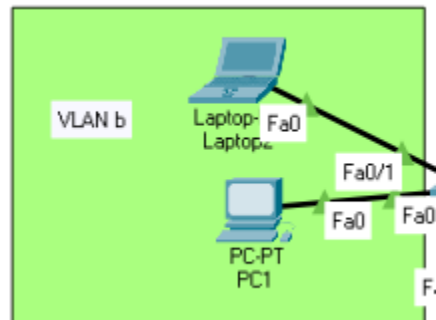
5.2 Blocul VLAN a



Pentru acest bloc am folosit prima subnetare si am folosit aceeasi pasi ca si la dispozitivele de mai sus astfel:

Dispozitiv	Ip din SN1
Laptop 0	10.1.0.2 /18
Server 0	10.1.0.3 /18
Tablet PC 0	10.1.0.4 /18
PC 0	10.1.0.5 /18

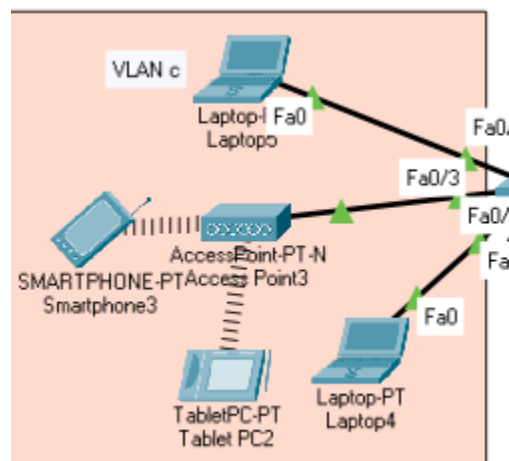
5.3 Blocul VLAN b



Pentru acest bloc am folosit cea de-a doua subnetare:

Dispozitiv	Ip din SN2
Laptop 2	10.1.64.2 /18
PC 1	10.1.64.3 /18

5.4 Blocul VLAN c

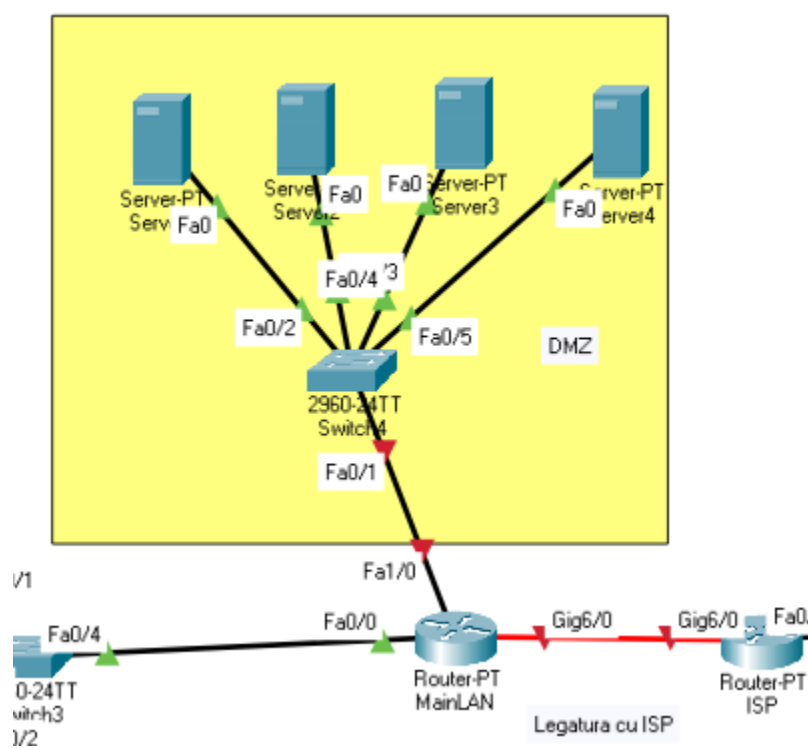


Pentru acest bloc am folosit adrese din subnetare 3:

Dispozitiv	Ip din SN3
Laptop 5	10.1.128.2 /18
Smartphone 3	10.1.128.3 /18
Tablet PC 2	10.1.128.4 /18
Laptop 4	10.1.128.5 /18

Block vlan	Gateway
10	10.1.0.1
20	10.1.64.1
30	10.1.128.1
40	10.1.192.1

5.5 Blocul DMZ si legatura cu ISP



Pentru servere am folosit adresele publice:

Device	Adresa IP	Adresa Gateway(Fa1/0)
Server 1	210.2.2.18 /29	210.2.2.17
Server 2	210.2.2.19 /29	210.2.2.17
Server 3	210.2.2.20 /29	210.2.2.17
Server 4	210.2.2.21 /29	210.2.2.17

Configurearea interfatei Fa1/0:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface fa1/0
Router(config-if)#ip address 210.2.2.17 255.255.255.248
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet1/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
```

Legatura cu ISP:

Interfata-Router	Adresa IP
Gig 6/0-MainLAN	210.2.2.9
Gig6/0-ISP	210.2.2.10

Router MainLAN

```
Router(config-if)#
Router(config-if)#exit
Router(config)#interface gig6/0
Router(config-if)#ip address 210.2.2.9 255.255.255.248
Router(config-if)#no shutdown
```

Router ISP

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface gig6/0
Router(config-if)#ip address 210.2.2.10 255.255.255.248
Router(config-if)#no shutdown
```


Sedinta 2

1.Crearea Vlan-urilor

Cu aceste comenzi am creat vlan-urile pe switch-ul principal. Dupa care am verificat crearea lor.

```
Switch#config terminal
Enter configuration commands, one per line.
Switch(config)#vlan 10
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#exit
Switch(config)#vlan 40
Switch(config-vlan)#exit
```

```
Switch#show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, 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 Gig0/1, Gig0/2
10 VLAN0010	active	
20 VLAN0020	active	
30 VLAN0030	active	
40 VLAN0040	active	
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

2.Configurarea switch-ului principal ca VTP server si a celorlate switchuri ca si client.

Pentru a configure switch-ul principal ca server am folosit comenzile.

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vtp version 2
Switch(config)#vtp domain 9tut
Changing VTP domain name from NULL to 9tut
Switch(config)#vtp mode server
Device mode already VTP SERVER.
Switch(config)#vtp password 123456789
Setting device VLAN database password to 123456789
Switch(config)#
Switch(config)#exit
```

Pentru celelate 3 switchuri am folosit comenzile urmatoare:

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vtp version 2
Switch(config)#vtp domain 9tut
Changing VTP domain name from NULL to 9tut
Switch(config)#vtp password 123456789
Setting device VLAN database password to 123456789
Switch(config)#vtp mode client
Setting device to VTP CLIENT mode.
```

3.Linii trunk

Pentru a face legaturile dintre switch-urile de nivel 2 in mod trunk am folosit comenzile:

```
Switch(config)#interface fa0/1          Switch(config)#interface fa 0/2
Switch(config-if)#switchport mode trunk Switch(config-if)#switchport mode trunk
Switch(config)#interface fa0/3
Switch(config-if)#switchport mode trunk
```

4.Setarea interfetelor catre end-device in vlan-ul corespunzator

Pentru a face acest lucru am dat click pe switchurile client dupa care Config->click pe interfata corespunzatoare si am setat valanul si modul ca access.Am facut acest lucru pentru fiecare interfata.

INTERFACE		VLAN
FastEthernet0/1	Access	30

5.Subinterfata pentru vlanuri

Pentru a configura ruterul am folosit comenzile de mai jos pentru fiecare subinterfata pentru a permite traficul pentru fiecare Vlan.

```
Router(config)#interface FastEthernet0/0.40
Router(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.40, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.40, changed state to up

Router(config-subif)#encapsulation dot1q 40
Router(config-subif)#ip address 10.1.192.1 255.255.192.0
Router(config-subif)#no shutdown
```

Dupa configurare am folosit comanda show ip route pentru a verifica daca totul este in regula.

```
10.0.0.0/18 is subnetted, 4 subnets
  10.1.0.0 is directly connected, FastEthernet0/0.10
  10.1.64.0 is directly connected, FastEthernet0/0.20
  10.1.128.0 is directly connected, FastEthernet0/0.30
  10.1.192.0 is directly connected, FastEthernet0/0.40
```

Sedinta 3

1.Configurarea translatarei adreselor prin tehnica NAT

Pentru a configura translatarea adreselor prin tehnica NAT am folosit comenzile urmatoare:

```
Router#access-list 1 permit 10.1.0.0 0.0.255.255
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 1 permit 10.1.0.0 0.0.255.255
Router(config)#ip nat pool NAT-Trif-Andrei 210.2.2.11 210.2.2.14 netmask 255.255.
Router(config)#ip nat inside source list 1 pool NAT-Trif-Andrei overload
^
% Invalid input detected at '^' marker.

Router(config)#ip nat inside source list 1 pool NAT-Trif-Andrei overload
Router(config)#interface fa0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface Gig6/0
Router(config-if)#ip nat outside
Router(config-if)#exit
```

Dupa aceasta configurate am facut fiecare subinterfata de tip inside folosind comenzile :

```
Router(config)#interface fa 0/0.10
Router(config-subif)#ip nat inside
Router(config-subif)#interface fa0/0.20
Router(config-subif)#ip nat inside
Router(config-subif)#interface fa0/0.30
Router(config-subif)#ip nat inside
Router(config-subif)#interface fa0/0.40
Router(config-subif)#ip nat inside
Router(config-subif)#
```

2.Adaugarea rutelor statice

Am adaugat 2 rute statice :

1. Prima ruta am configurat-o pe router-ul MainLan folosind comanda:

```
Router(config)#ip route 0.0.0.0 0.0.0.0 210.2.2.10
```

Aceasta ruta identifica adresa de Gateway catre care rutarul trimite pachetele si nu are o ruta statica.

2. A doua ruta este pentru router-ul ISP.Pentru aceasta am folosit aceasi comanda si am configurat adresa de next hop.Acum exista ruta statica 210.2.2.16 via 210.2.2.9.

```
C    1.0.0.0/8 is directly connected, FastEthernet
    210.2.2.0/29 is subnetted, 2 subnets
C        210.2.2.8 is directly connected, Gigabit
S        210.2.2.16 [1/0] via 210.2.2.9
```

3. Configurare DHCP

Am creat instante dhcp la nivel de router pentru toate cele 4 subretele folosind comenzile urmatoare:

```
Router(config)#ip dhcp pool v30
Router(dhcp-config)#netwo
Router(dhcp-config)#network 10.1.128.0 255.255.192.0
Router(dhcp-config)#
Router#
%SYS-5-CONFIG_I: Configured from console by console
configure terminal
Enter configuration commands, one per line. End with CN
Router(config)#ip dhcp pool v30
Router(dhcp-config)#network 10.1.128.0 255.255.192.0
Router(dhcp-config)#de
Router(dhcp-config)#default-router 10.1.128.1
Router(dhcp-config)#dns-server 210.2.2.19
Router(dhcp-config)#exit
Router(config)#ip dhcp excluded-address 10.1.128.1
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
Router#conf
Router#configure t
Router#configure terminal
Enter configuration commands, one per line. End with CN
Router(config)#
Router(config)#ip dhcp pool v40
Router(dhcp-config)#network 10.1.192.0 255.255.192.0
Router(dhcp-config)#default-router 10.1.192.1
Router(dhcp-config)#dns-server 210.2.2.19
Router(dhcp-config)#exit
Router(config)#ip dhcp excluded-address 10.1.192.1
Router(config)#exit
```

4. Testarea configurari

Pentru a testa configurarea si faptul ca totul functioneaza am trimis pachete de la un Pc din vlan 10 la un Pc din internet.

```

C:\>ping 1.1.1.2

Pinging 1.1.1.2 with 32 bytes of data:

Reply from 1.1.1.2: bytes=32 time<1ms TTL=126
Reply from 1.1.1.2: bytes=32 time=10ms TTL=126
Reply from 1.1.1.2: bytes=32 time=10ms TTL=126
Reply from 1.1.1.2: bytes=32 time=12ms TTL=126

Ping statistics for 1.1.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 12ms, Average = 8ms

```

Dupa care am rulat comanda show ip nat translations pe router-ul Main pentru a vedea asocierile facute de router.

```

Router#show ip nat translations

```

Pro	Inside global	Inside local	Outside local	Outside global
icmp	210.2.2.11:1	10.1.0.2:1	1.1.1.3:1	1.1.1.3:1
icmp	210.2.2.11:2	10.1.0.2:2	1.1.1.3:2	1.1.1.3:2

In urmatorul test am dat un ping de pe un server din dmz spre un pc din internet.

```

C:\>ping 1.1.1.2

Pinging 1.1.1.2 with 32 bytes of data:

Reply from 1.1.1.2: bytes=32 time<1ms TTL=126
Reply from 1.1.1.2: bytes=32 time<1ms TTL=126
Reply from 1.1.1.2: bytes=32 time<1ms TTL=126
Reply from 1.1.1.2: bytes=32 time=10ms TTL=126

Ping statistics for 1.1.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms

```

Sedinta 4

1.Configurare server de DNS

Pentru a configure server-ul de DNS am executat urmatoorii pasi:click pe un server->Services->DNS->DNS Service on->dupa am adaugat entitatea www.trif-andrei.ro cu ip 210.2.2.18 care este adresa server-ului de HTTP.

Physical Config **Services** Desktop Programming Attributes

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

DNS

DNS Service ☒ On ☐ Off

Resource Records

Name Type

Address

No.	Name	Type	Detail
0	ftp.andrei.ro	A Record	210.2.2.20
1	www.trif_andrei.ro	A Record	210.2.2.18
2	andreimail.ro	A Record	210.2.2.21

Dupa aceasta configurare am setat la toate dispozitivele serverul de DNS ca avand adresa 210.2.2.19.

☐ DHCP
 ☒ Static

IPv4 Address

Subnet Mask

Default Gateway

DNS Server

2. Configurare server de FTP

Pentru a configure serverul de Ftp in Services->DNS->FTP am creat un cont cu anumite permisiuni si am facut serviciul on. Dupa aceea am adaugat o noua entitate la serverul de DNS numita [ftp.andrei.ro](#) cu adresa 210.2.2.20 care este adresa serverului de ftp.

Service
☒ On
☐ Off

User Setup

Username
Password

☐ Write
☐ Read
☐ Delete
☐ Rename
☐ List

	Username	Password	Permission	
1	andrei	test	RWDNL	<div>Add</div> <div>Save</div>
2	cisco	cisco	RWDNL	

3.Configurare server de MAIL

Pentru a configura server-ul de MAIL am setat un domeniu si am creat un user.Domeniul a fost creat pe server-ul de DNS cu adresa 210.2.2.21.

SERVICES

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

EMAIL

SMTP Service
☒ ON
☐ OFF

POP3 Service
☒ ON
☐ OFF

Domain Name:

Set

User Setup

User
Password

andrei

4. Configurarea server HTTP

Pentru a configura serverul de HTTP am trecut in mod on HTTP SI HTTPS si am creat pagina trif_andrei.html.



The screenshot shows the Mikrotik WinBox interface. On the left, the 'SERVICES' menu is open, with 'HTTP' selected. The main panel shows the 'HTTP' configuration page. Both 'HTTP' and 'HTTPS' services are set to 'On' (indicated by a filled radio button). Below the service settings is a 'File Manager' table listing files for the web server.

	File Name	Edit	Delete
1	copyrights.html	(edit)	(delete)
2	cscoptlogo177x111.jpg		(delete)
3	helloworld.html	(edit)	(delete)
4	image.html	(edit)	(delete)
5	index.html	(edit)	(delete)
6	trif_andrei.html	(edit)	(delete)

5. Testare

Testarea configurari server-ului de DNS.

```
C:\>ping www.trif_andrei.ro

Pinging 210.2.2.18 with 32 bytes of data:

Reply from 210.2.2.18: bytes=32 time=1ms TTL=127
Reply from 210.2.2.18: bytes=32 time=1ms TTL=127
Reply from 210.2.2.18: bytes=32 time=1ms TTL=127
Reply from 210.2.2.18: bytes=32 time<1ms TTL=127

Ping statistics for 210.2.2.18:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```


Testarea configurarii server-ului de FTP.

```
C:\>ftp ftp.andrei.ro
Trying to connect...ftp.andrei.ro
Connected to ftp.andrei.ro
220- Welcome to PT Ftp server
Username:andrei
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>get
remote filename not specified
ftp>get asa842-k8.bin

Reading file asa842-k8.bin from ftp.andrei.ro:
File transfer in progress...

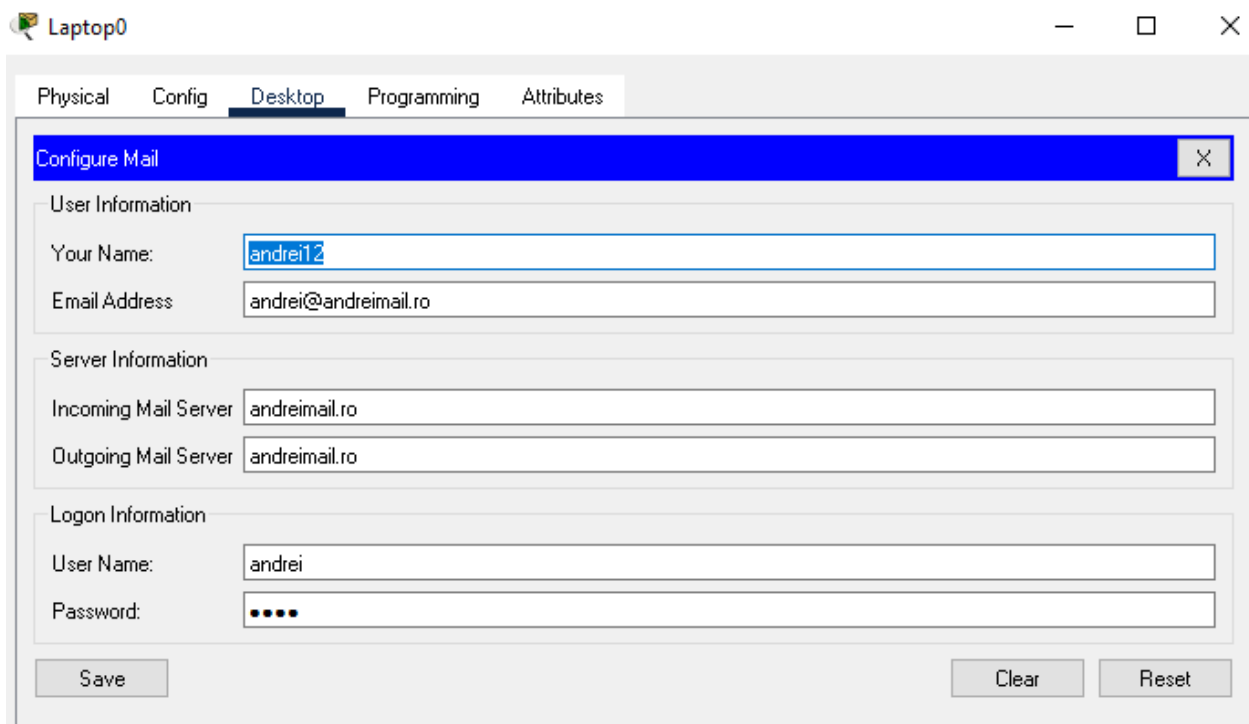
[Transfer complete - 5571584 bytes]

5571584 bytes copied in 14.497 secs (88060 bytes/sec)
```

Testarea configurarii serverului de HTTP.Pe unul dintre pc am acesat browserul si am mers la adresa urmatoare.



Testarea configurarii serverului de Mail



Aici am trimis si receptionat un e-mail.

Mails			
<div>Compose</div> <div>Reply</div> <div>Receive</div> <div>Delete</div> <div>Configure Mail</div>			
	From	Subject	Received
1	andrei@andreimail.ro	test	Sun Mar 15 202018:12:50

Sedinta 5

1.Criptarea parolelor si crearea utilizatorilor

Aici am definit diferiti utilizatori cu niveluri diferite de privilegiu.

```
Router>enable
Password:
Password:
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#user andrei1 password andrei1 privilege 15
Router(config)#user andrei2 password andrei2 privilege 8
Router(config)#user andrei3 password andrei3 privilege 1
Router(config)#user andrei4 password andrei4 privilege 1
Router(config)#exit
Router#
```

2.Configurarea SSH

Pentru a configure conectarea securizata am folosit urmatoarele comenzi:

```
R1-Trif-Andrei(config)#ip domain-name www.trif_andrei.ro
R1-Trif-Andrei(config)#crypto key generate rsa
The name for the keys will be: R1-Trif-Andrei.www.trif_andrei.ro
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 360
% Generating 360 bit RSA keys, keys will be non-exportable...[OK]

R1-Trif-Andrei(config)#username andreiAdmin secret adminpass
*Mar 1 1:14:37.905: RSA key size needs to be at least 768 bits for ssh version 2
*Mar 1 1:14:37.905: %SSH-5-ENABLED: SSH 1.5 has been enabled
R1-Trif-Andrei(config)#line vty 0 4
R1-Trif-Andrei(config-line)#transport input ssh
R1-Trif-Andrei(config-line)#login local
R1-Trif-Andrei(config-line)#
```

3.Testare SSH

Pentru a testa conecatarea am ales un PC si in command prompt am executat comanda **ssh -l andreiAdmin 10.1.0.1** dupa care am introdus parola **adminpass** , iar testul a fost un success.

```
C:\>
C:\>ssh -l andreiAdmin 10.1.0.1

Password:

R1-Trif-Andrei>
```

4.AAA Security

Pentru a configura AAA Security am folosit comenzile :

- **Aaa new model**- activeaza aaa pe router
- **aaa authentication enable default group radius**- Folosește parola de activare pentru autentificare;
- **aaa authentication login default group radius**- Toți utilizatorii sunt autentificați utilizând serverul Radius .Dacă serverul Radius nu răspunde, atunci se utilizează baza de date locală a routerului.
- **aaa authorization exec default group radius**- Determină nivelul de privilegiu al utilizatorului atunci când utilizatorii sunt autentificați.
- **radius-server host 10.1.192.1 key andrei** –specifica adresa server-ului radius.

5.Testare AAA

Dupa cum se poate vedea securitatea sa inbunatatit, iar acum este necesara introducerea de doua ori a username-ului si a parolei.Username-ul este **username1** si parola **password1**.

```
C:\>ssh -l username1 10.1.192.1

Password:
andrei>enable
Username:
Password:
andrei#exit

[Connection to 10.1.192.1 closed by foreign host]
C:\>ssh -l andrei1 10.1.192.1

Password:
andrei>enable
Username:
Password:
andrei#exit
```

6.Switch port-security

Pentru a configura Switch port-security am folosit comenzile urmatoare :

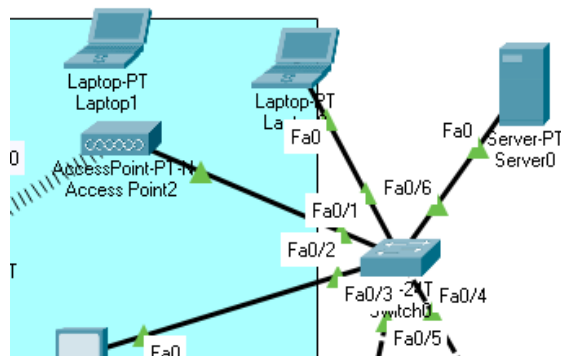
- **switchport port-security**-activeaza caracteristica de securitate a portului pe acest port;
- **switchport port-security maximum 1**- seteaza limita pentru gazdele care pot fi asociate cu interfața;
- **switchport port-security mac-address sticky**- activeaza funcția lipicioasă.
- **switchport port-security violation restrict** - setează modul de încălcare, acțiunea care trebuie luată atunci când este detectată o încălcare a securității, este o restricționare. O încălcare a securității portului restricționează datele și face ca contorul SecurityViolation să crească și să trimită o notificare SNMP trap.

```
Switch(config-if)#switchport port-security
Switch(config-if)#s
Switch(config-if)#s
Switch(config-if)#sw
Switch(config-if)#switchport m
Switch(config-if)#switchport max
Switch(config-if)#switchport maximum 1
Switch(config-if)#switchport maximum 1
^
% Invalid input detected at '^' marker.

Switch(config-if)#switchport por maximum 1
Switch(config-if)#switchport port-
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#sw
Switch(config-if)#switchport port
Switch(config-if)#switchport port-security mac
Switch(config-if)#switchport port-security mac-address sti
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security vi
Switch(config-if)#switchport port-security violation restrict
Switch(config-if)#switchport port-security violation restrict
```

7. Testare

Interfata fa0/1 era conectata la Leptop1 prin aceasta interfata leptopul prima adresele in mod dynamic.Dupa configurarea Switchport Security am mutat interfata Fa0/6 la un alt leptop.



Dupa cum se poate vedea acest nou laptop care a fost legat la interfata fa0/1 nu mai primeste adresele prin DHCP.

<input checked="" type="radio"/> DHCP	<input type="radio"/> Static	DHCP failed. APIPA is being used.
IPv4 Address	<input type="text" value="169.254.144.60"/>	
Subnet Mask	<input type="text" value="255.255.0.0"/>	
Default Gateway	<input type="text" value="0.0.0.0"/>	
DNS Server	<input type="text" value="0.0.0.0"/>	

Am rulat comanda show port-security pentru a vedea violarile de securitate si informatiile pentru interfata Fa0/1.

```
Switch#show port
Switch#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
          (Count)          (Count)          (Count)
-----
Fa0/1      1              1              8          Restrict
-----
```

Concluzia

Am rezolvat toate cerintele !!