

Documentatie proiect PPRC

Author: Andercou Alexandru Stefan

Profesor: Iancu Bogdan

## Cuprins

1. Prezentare generala .....	3
2. Setarea manuala a ip-urilor publice .....	3
3. Setarea ip-urilor private: .....	4
4. Crearea vlanurilor: .....	5
4.1. Protocolul VTP .....	5
4.1.1 VTP Server .....	5
4.1.2 VTP Clients: .....	5
4.1.3 Legaturile dintre switch-urile .....	5
4.1.4 Configurarea Legaturilor intre deviceuri si switchurile lor. ....	5
4.2 Testarea vlanurilor .....	6
5. Subinterfete .....	6
6. Servere de DHCP .....	7
7. Configurare default static routing .....	7
8. NAT(Network adress transfer) .....	8
9. Setarea serverelor: .....	9
9.1. Server DNS: .....	9
9.2. Server http/https: .....	10
9.2.1 Testare server web .....	11
9.3 Server ftp: .....	12
9.4 Server email: .....	13
10. Internetul/exteriorul .....	13
11. Securitatea de baza .....	14
11.1. Setarea de parole pe router .....	14
11.1.2 Testarea autentificare .....	15
11.2. Setarea SSH .....	15
11.1.2 Testare ssh .....	16
11.3. Configurare W--FI .....	16
12. Securitate complexa .....	17

## 1. Prezentare generala

Proiectul rezolva Tema 2.5-a rezolvat pana la securitate simpla: parole pe routerul Main si ssh, ramane de rezolvat alte 2 metode de securitate.

Cerinte:

Se considera o cladire comerciala cu 3 niveluri. Se va folosi adresa de retea 172.27.0.0/16 pentru retea intranet, adresa de retea 210.2.2.64/27 pentru DMZ si adresa de retea 210.2.2.32/27 pentru accesul in exterior. Se vor proiecta 4 VLAN-uri (unul pentru fiecare etaj si unul pentru traficul de management). Pentru configurarea VLAN-urilor se va folosi protocolul VTP. Prin cablarea si configurarea retelei se va asigura redundanta. Adresele hosturilor vor fi alocate dinamic folosind un singur server de DHCP aflat in VLAN-ul corespunzator primului etaj. Numarul minim de utilizatori deserviti de catre fiecare VLAN este 200. Serverele de HTTP, FTP, DNS si MAIL vor fi plasate in DMZ si vor avea adrese publice. Numele domeniului web va include numele studentului. Pentru asigurarea conectivitatii se vor configura rute statice. Accesul in exterior se va realiza folosind NAT pe routerul care controleaza DMZ, pe urmatorul interval de adrese publice: 210.2.2.35-210.2.2.62. Conectarea la ISP se va realiza printr-o interfata de tip Ethernet avand adresa 210.2.2.34/27. Adresa ISP-ului este 210.2.2.33/27. Reteaua Internet se va simula prin intermediul unui server si a unui calculator. Pentru securizarea echipamentelor de retea se vor realiza urmatoarele configurari: se vor defini utilizatori pe diferite niveluri de privilegiu, criptarea parolilor, 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.

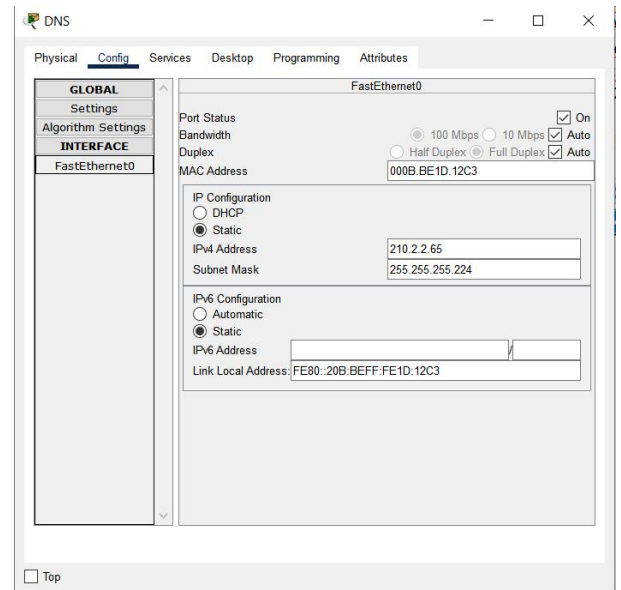
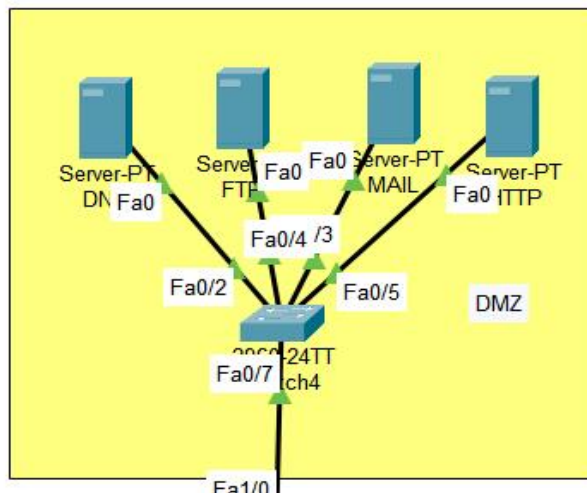
Topologia creata prezinta o zona privata cu 4 VLANURI distribuite pe 3 etaje si vlan de management, o zona publica DMZ cu servere de DNS, HTTP, FTP, MAIL, un router intern: MAIN, 3 switchuri si un router de conexiune cu internetul de la ISP, internetul fiind reprezentat de un calculator si un server.

Zona cu calculatoare/servele cu adrese ip publice sunt accesibile din afara retelei (internet)  
Prin routerul isp (internet source provider).

## 2. Setarea manuala a ip-urilor publice

Adresele publice din interiorul retelei incep de la adresa : 210.2.2.33 si se termina cu 210.2.2.68, adresele sunt divizate intre adresele din DMZ, adresele publice pentru NAT si pentru conexiunea intre routere. Zona DMZ, se foloseste adresa de retea: 210.2.2.64, contine servere de DNS (210.2.2.65) care ofera posibilitatea folosirii denumirilor cu semnificatie logica pentru utilizatori pentru a masca adresele de IP, un server de ftp (210.2.2.66), mail (210.2.2.67) si http (210.2.2.68).

Zona DMZ este conectata de routerul MAIN pe interfata Fa0/7 a switchului DMZ si Fa1/0 a routerului MAIN. Adresa ip a interfetei fa1/0 este 210.2.2.69 si este default router gateway pentru zona DMZ. DNS-ul este 210.2.2.65.



Routerul ISP se conecteaza cu routerul Main prin interfetele GigabitEthernet6/0 ale celor 2 routere. Adresele folosite sunt : 210.2.2.33/27 pentru ISP si 210.2.2.34/27 pentru interfata Routerului MAIN. Masca pentru retea este: 255.255.255.224

Pasii pentru setarea manuala a adreselor de ip pe interfețe/calculatoare/routere in modulul cli sunt: enable->configure terminal->interface numele\_interfeței->ip address adresa\_ip masca\_retea->no shutdown

Pentru a se asigura ca exista conexiune intre routere trebuie si din interfata grafica a routerelor sa se verifice ca ambele sunt on si sa se bifeze in caz contrar.

### 3. Setarea ip-urilor private:

Adresele private incep cu adresa: 172.27.0.0/16 si sunt subnetate pe 4 vlanuri rezultand din acest fapt masca mai castiga 2 biti : \18 cu masca: 255.255.192.

Subnetare si partitionarea ip-urilor private: IP-urile private sunt impartite pe cele 4 vlanuri astfel: Cu masca de retea: 255.255.192.000/18, subnet1: 172.27.0.0-172.27.63.255, subnet2: 172.27.64.0-172.27.127.255, subnet 3: 172.27.128.0-172.27.191.255, subnet 4: 172.27.192.0-172.27.255.255.

## 4. Crearea vlanurilor:

Un VLAN este un lan virtual. Un LAN este un local address network, o retea fizica de calculatoare, un VLAN este o retea virtuala sau logica , calculatoarele nu trebuie sa fie in aceeasi incapere.

Cele 4 Vlanuri vor avea denumirea:10,11,12,13 si vor fi setate prin protocolul VTP.

### 4.1. Protocolul VTP

VTP= Vlan trunking protocol.

Asigura propagarea accesului la VLAN-ului de la un switch server la mai multe switchuri cliente in modulelul server-client.

#### 4.1.1 VTP Server

Este pe switch-ul principal

Configurare cli pe switch-ul principal

Enable->configure terminal->vtp version 2 ->vtp domain alex21 ->vtp mode server ->vtp password leu\_21

#### 4.1.2 VTP Clients:

Clinetii sunt cele 3 switch-uri conectate direct la deviceuri

Configurare:

Enable->configure terminal->vtp version 2 ->vtp domain alex21 ->vtp mode client ->vtp password leu\_21

#### 4.1.3 Legaturile dintre switch-urile

Legaturile dintre switch-urile de layer 2 si intre layer 1 si 2 sunt linii de trunk.

O line de trunk permite ca pe acea linie sa treaca trafic din mai multe vlanuri.

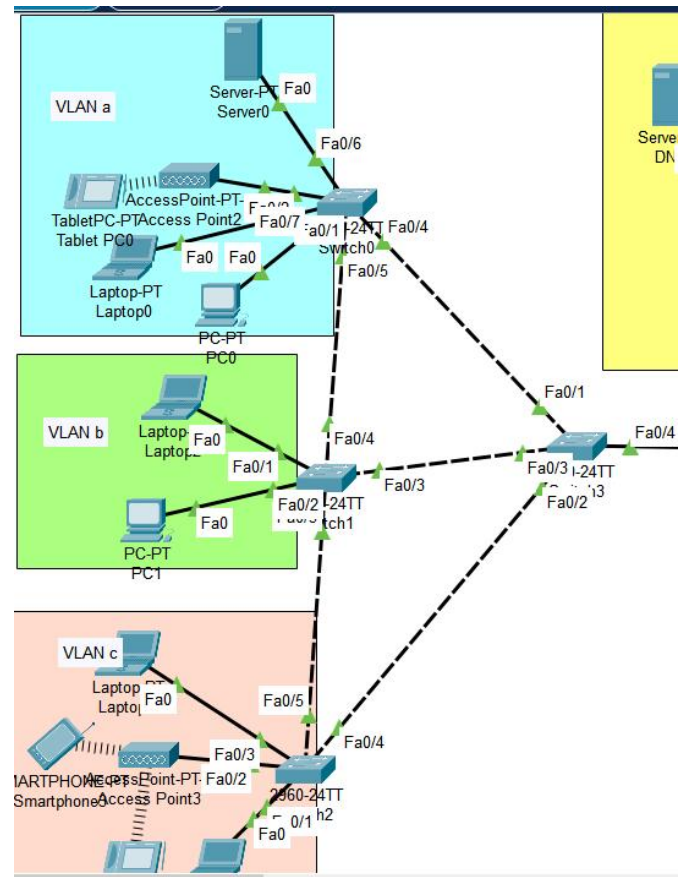
Configurare:

Client(config)#interface nume\_interfata

Client(config-if)#switchport mode trunk

#### 4.1.4 Configurarea Legaturilor intre deviceuri si switchurile lor.

Legaturile sunt de tip trunk a unui singur VLAN, pe fiecare interfata se specifica vlan-ul.



Exemplu: Setarea unei interfete pentru a apartine VLAN-ului 10:

```
Client(config)#interface fa0/1
Client(config-if)#switchport mode access
Client(config-if)#switchport access VLAN 10
```

## 4.2 Testarea vlanurilor

Pentru a verifica vlanurile , pe switchuri se poate folosi comanda: show vla brief

```
Switch>enable
Switch#show vlan brief

VLAN Name                Status
-----
1      default              active
Fa0/5, Fa0/6, Fa0/7, Fa0/8
Fa0/9, Fa0/10, Fa0/11, Fa0/12
Fa0/13, Fa0/14, Fa0/15, Fa0/16
Fa0/17, Fa0/18, Fa0/19, Fa0/20
Fa0/21, Fa0/22, Fa0/23, Fa0/24
Gig0/1, Gig0/2
10     VLAN10               active
11     VLAN11               active
12     VLAN12               active
13     VLAN13               active
1002   fddi-default         active
1003   token-ring-default   active
1004   fddinet-default      active
1005   trnet-default        active
Switch#
```

## 5. Subinterfete

Routerul MAIN este legat de VANURI prin interfata fa0/0. Fiecare din cele 4 VLANURI va primi p subinterfata:fa0/0.10,fa0/0.11,fa0/0.12,fa0/0.13  
Fa 0/0 este de tip trunk iar subinterfetele pe mode access.

Fiecare din subinterfete vor fi configurate cu adresele din subnetarea lor si cu incapsularea dot1q cu vlanul lor.fa0/0.10,fa0/0.11,fa0.0/12,fa0/0.13 cu adresele ip: 172.27.0.1, 172.27.64.1,172.27.128.1,172.27.192.1

Ex configurare

```
Router(config)# interface Fa0/0.10
Router(config-if)# encapsulation dot1q 10
Router(config-if)# ip address 172.27.0.1 255.255.192.0
Router(config-if)# no shutdown
```

Verificarea statusului ,starii vtp se face prin : show vtp status

## 6. Servere de DHCP

Hosted de pe routerul MAIN.Cate unul pentru fiecare din cele 4 VLANURI.

Atribuire adresele private conform vlanului si configurariilor.

Default routerul ar trebui sa fie pe adresa subinterfetei asiguate vlanului prin encapsulation dot1q.

La network trebuie specificata adresa de network(base adress)

Ex de configurare:

```
Router(config)#ip dhcp pool VLAN10
Router(config)#network 172.27.0.0 255.255.192.0
Router(config)#default-router 172.27.0.1
Router(config)#dns-server 210.2.2.65
Router(config)#exit
Router(config)#ip dhcp excluded-address 172.27.0.1 //address_range exclude router ip
Router(config)#ip dhcp excluded-address 172.64.0.1
Router(config)#ip dhcp excluded-address 172.128.0.1
Router(config)#ip dhcp excluded-address 172.192.0.1
```

Pe toate deviceurile la Config->IP Configuration, trebuie bifata casuta DHCP

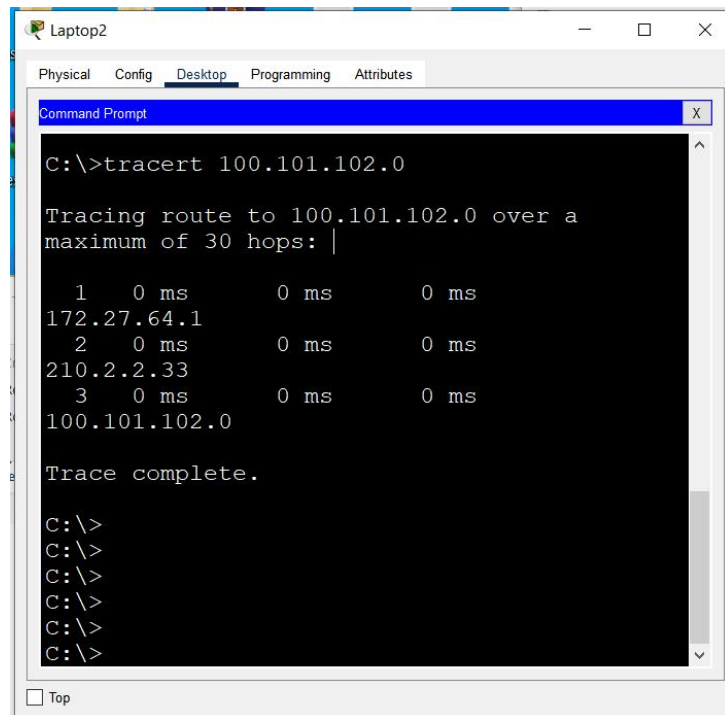
## 7.Configurare default static routing

A default route identifies the gateway IP address to which the router sends all IP packets for which it does not have a learned or static route. A default static route is simply a static route with 0.0.0.0/0 as the destination IP address. Routes that identify a specific destination take precedence over the default route.

```
Router2(config)#ip route 0.0.0.0 0.0.0.0 210.2.2.33
```

Instructiune ca sa vezi configurarea routerului/switchului:  
show running-config

## 8. NAT(Network adress transfer)



```
C:\>tracert 100.101.102.0

Tracing route to 100.101.102.0 over a
maximum of 30 hops: |

  1    0 ms      0 ms      0 ms
172.27.64.1
  2    0 ms      0 ms      0 ms
210.2.2.33
  3    0 ms      0 ms      0 ms
100.101.102.0

Trace complete.

C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
```

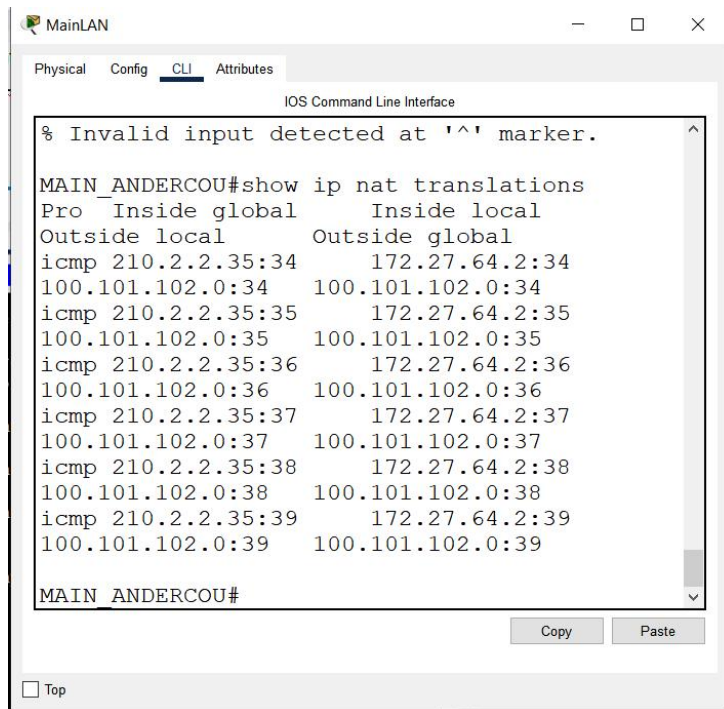
Configurarea se realizeaza pe routerul main.

NAT realizeaza translatarea intre adrese private (172.27.0.0-172.27.255.255) cu adresele publice (210.2.2.35-210.2.2.62) la iesirea din retea.

Pentru a se realiza configurarile trebuie trimis un mesaj pana in internet de pe un calculator local ex Laptop2 pana pe un calculator din internet ex PC2 cu ip-ul 100.101.102.101.

Apoi cu comanda pe routerul main "show ip nat translations" se pot vedea translatariile.





Comenzi de configurare:

Se creaza listele de adrese private cu masca inversata(complementara) pentru cele 4 vlanuri

```
Router(config)#access-list 1 permit 172.27.0.0 0.0.63.255
```

```
Router(config)#access-list 1 permit 172.27.27.0 0.0.63.255
```

```
Router(config)#access-list 1 permit 172.27.128.0 0.0.63.255
```

```
Router(config)#access-list 1 permit 172.27.192.0 0.0.63.255
```

Se declara nat poolul cu nume si rangeul de adrese publice:

```
Router(config)#ip nat inside source list 1 pool alex21 210.2.2.35 210.2.2.62
```

Apoi pentru cele 4 subinterfete: fa0/0.10,fa0/0.11,fa0/0.12,fa0/0.13 se specifica ca sunt inauntru:

```
interface l_name->ip nat inside
```

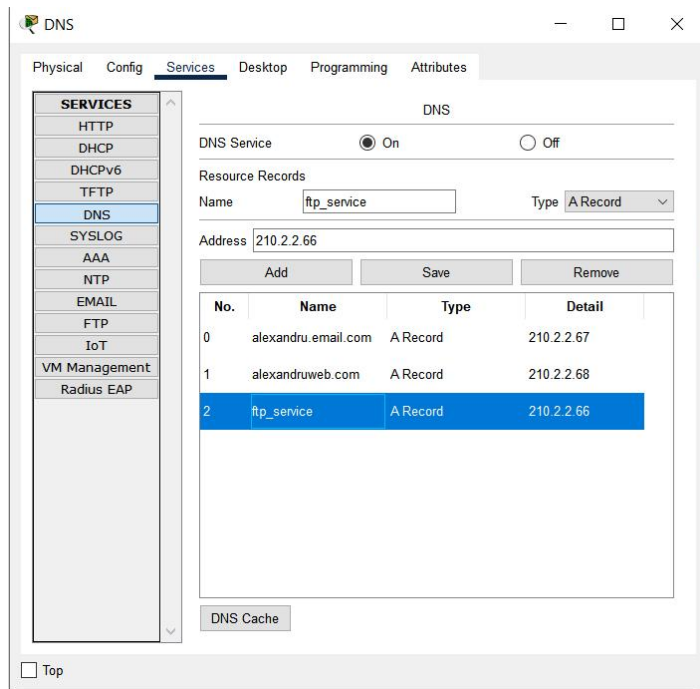
Pentru interfețele fa1/0 si gig6/0 se specifica ca sunt inafara:

```
interface l_name->ip nat outside
```

## 9. Setarea serverelor:

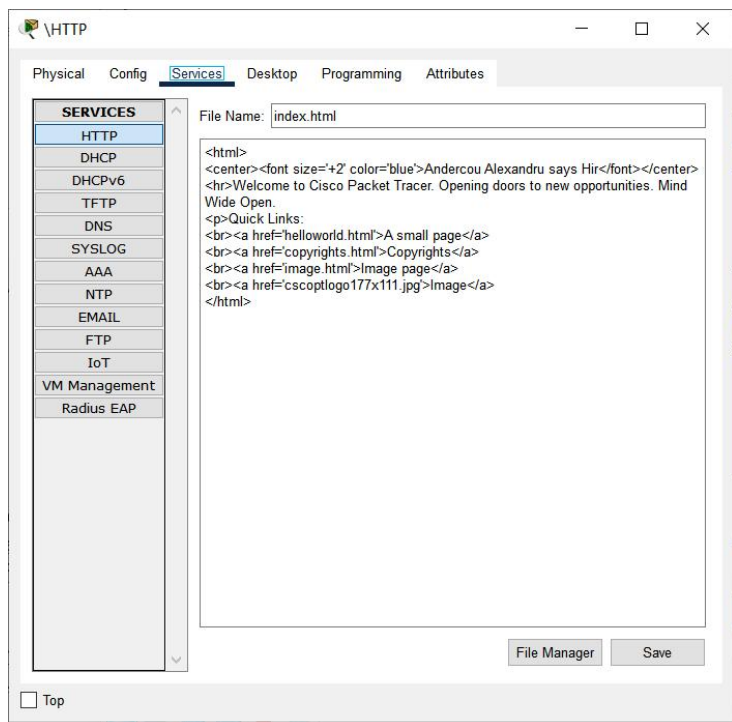
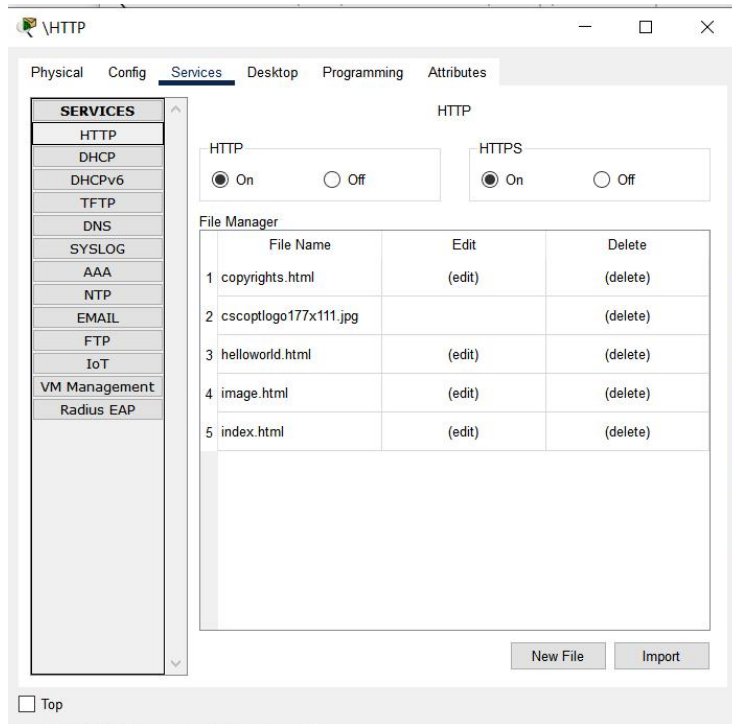
### 9.1. Server DNS:

Serverul de DNS ofera diferite tipuri de mapari .Acestea pot fi de tipul A Record care realizeaza o mapare intre o adresa ip si un URL/ nume sugestiv. Mai exista mapari de tipul alias de tipul: CNAME care redenumesc o adresa de URL si indica spre un alt URL care la randul sau indica spre o adresa ip. Mai exista mapari de tipul:AAAA Record, NS Record si SOA. In DNS avem 3 recorduri de tip A Record: "alexandruweb.com" care este url-ul pentru serverul web cu ip-ul 210.2.2.68 , "alexandru.email.com" care este denumirea serverului de EMAIL cu adresa ip:210.2.2.67 si "ftp\_service" care indica spre serverul de ftp cu ip-ul:210.2.2.66



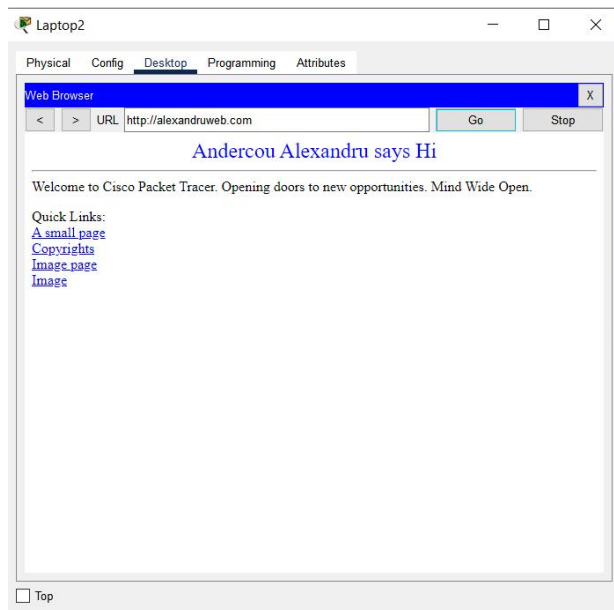
## 9.2. Server http/https:

Pentru a putea folosi un server de http din tabul Services se alege http se bifeaza on pentru http si https. Serverul HTTP pune la dispozitie accesul la fisierul html dintre care cel mai important e index.html. URL-ul site-ului reprezentat de aceste pagini html este setat la DNS ca un A RECORD. Site-ul se numeste "alexandruweb.com" cu adresa ip:210.2.2.68 ,



### 9.2.1 Testare server web

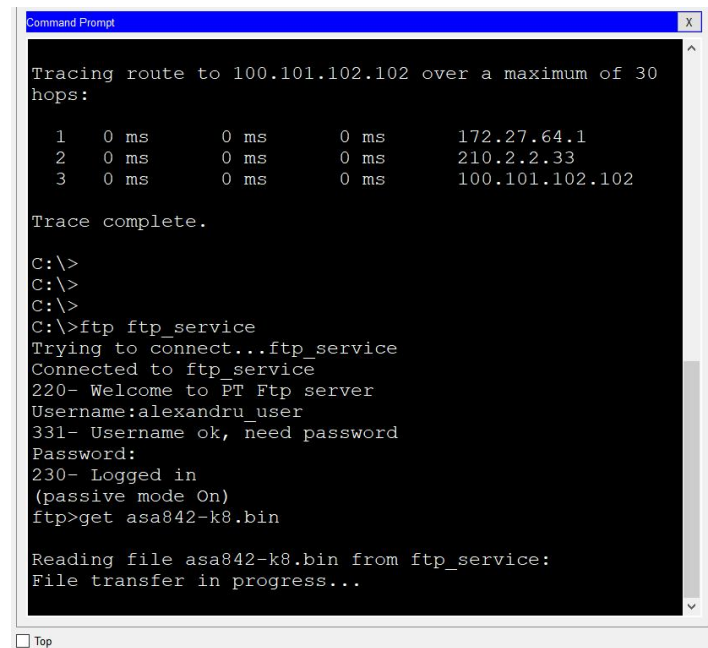
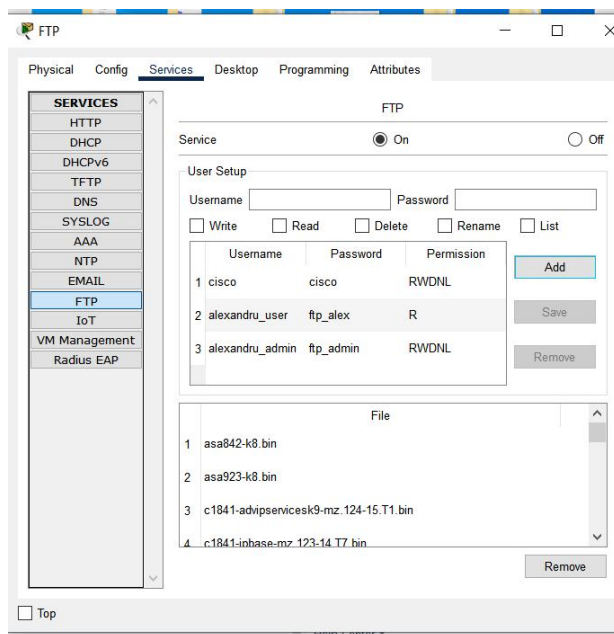
De pe un device in browser. Ex. Laptop2 Se scrie in bara de URL, adresa: alexandruweb.com



### 9.3 Server ftp:

Pentru a putea folosi un server de ftp trebuie bifat din interfata din tabul Services on for ftp  
 Folosirea serverului de ftp presupune crearea unor conturi de utilizatori cu parole si cu anumite permisiuni de actiuni peste fisiere. Fisiere se pot citi/salva si se pot incarca pe serverul de ftp folosind metodele de get/put.

Folosirea ftp-ului este protejata de un login. Permisunile sunt de scriere,citire,stergere,redenumire si listare si sunt alese la crearea contului de utilizator.  
 Accesul se face din linia de comanda, prin comanda "ftp" urmata de adresa :url sau ip a serverului de ftp,urmata de un login,



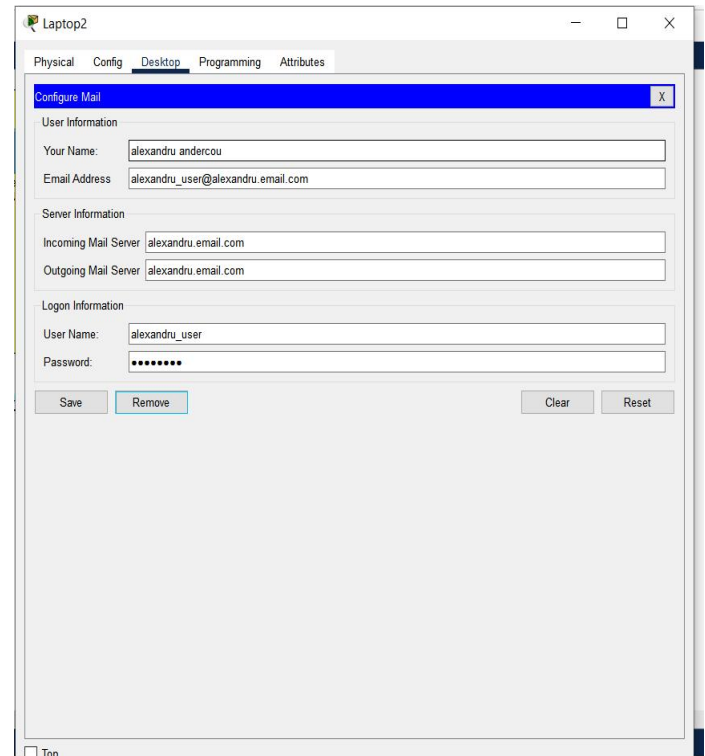
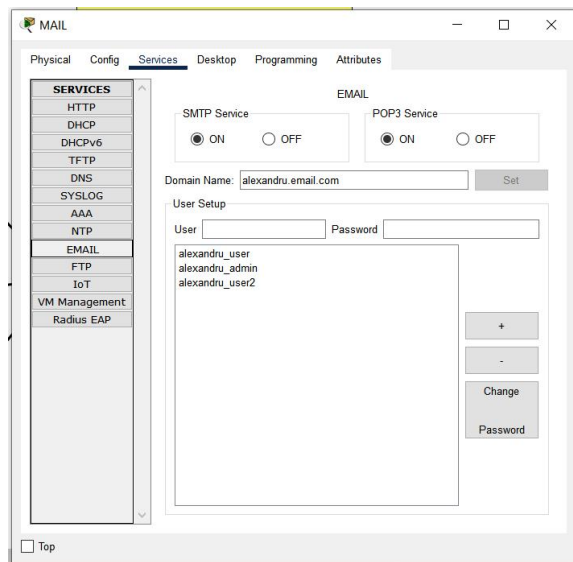
## 9.4 Server email:

Serverul de email este reprezentat de 2 tipuri de servicii : SMTP si POP3.

Pentru configurarea serverului este nevoie de un nume de domeniu. In cadrul serviciului se definesc conturi de utilizatori cu parole care vor putea comunica prin email. Serverul are numele de domeniu "alexandru.email.com", acest domeniu trebuie specificat si in DNS.

Configurare cont de mail. De pe un device se alege iconul de Email, apoi butonul de Configure Mail. Apoi in fereastra deschisa se completeaza datele. Campul de Email Address trebuie sa corespunda in felul urmatoar: adresa de email trebuie sa aiba formatul: User Name @domain\_email.

De exemplu pentru utilizatorul: "alexandru\_user" si domeniul "alexandru.email.com", emailul va fi: "alexandru\_user@alexandru.email.com", Incoming si Outgoing Mail Server va fi acelasi in configurarea facuta va fi: "alexandru.email.com"



## 10. Internetul/exteriorul

Reteaua de calculatoare construita se leaga la internet din routerul Main cu interfata Gig6/0 adresa ip :210.2.2.34 cu routerul ISP pe interfata Gig6/0 cu ip-ul 210.2.2.33

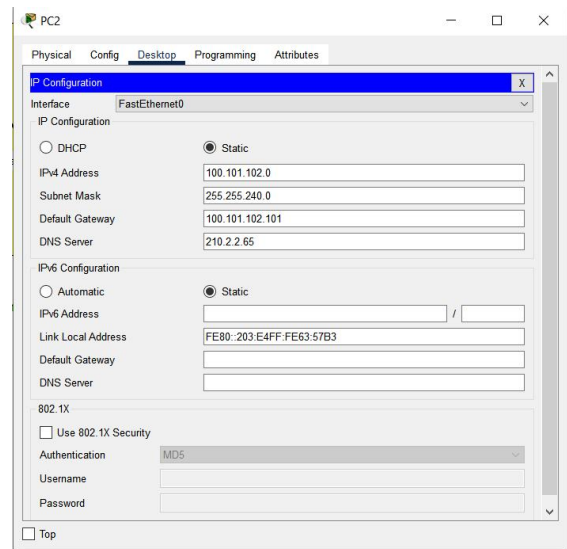
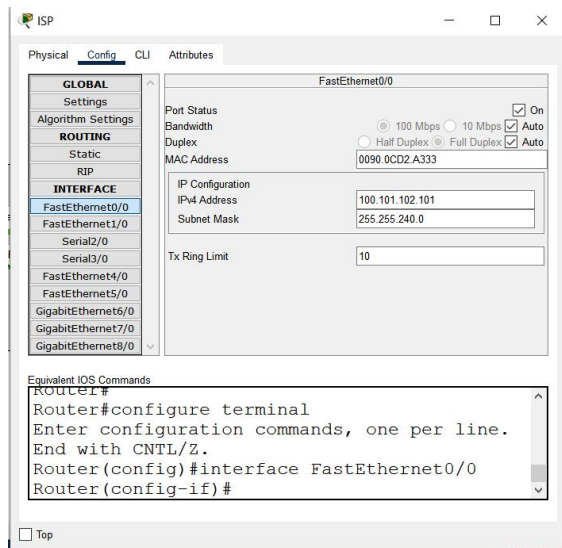
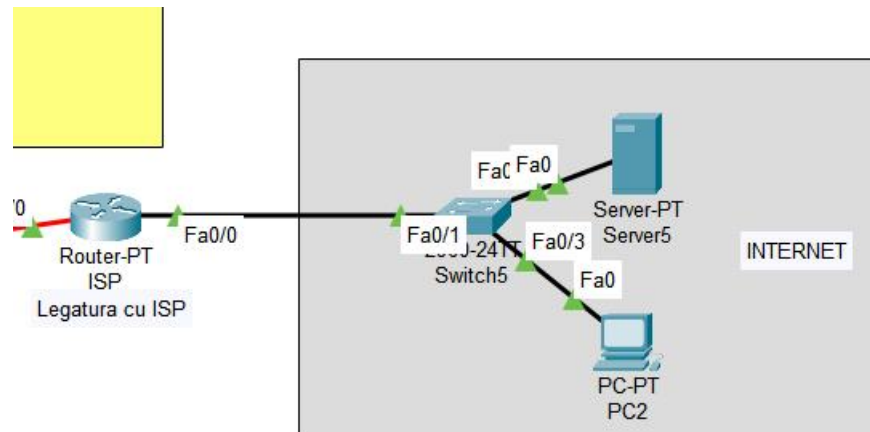
Internetul/exteriorul este reprezentat de routerul ISP conectat la un calculator PC2 cu adresa ip: 100.101.102.0 /27 conectat la interfata fa0/0 a routerului de isp, interfata fa0/0 a routerului are adresa de ip :100.101.102.101/27

Un alt device este un server cu adresa ip 100.101.102.102

Pentru conectarea din internet la DMZ se seteaza o cale statica pe routerul ISP cu comanda:

Structura comanda: ip route destinatie masca next\_hop\_ip

Router(config)# ip route 210.2.2.64 255.255.255.224 210.2.2.34



## 11. Securitatea de baza

### 11.1. Setarea de parole pe router

```
MAIN_ANDERCOU(config-if)#exit
MAIN_ANDERCOU(config)#enable password
andercou1234
MAIN_ANDERCOU(config)#username alex password
andercoualex
MAIN_ANDERCOU(config)#service password-
encryption
MAIN ANDERCOU(config)#enable secret alex1234
```

### 11.1.2 Testarea autentificare

Verificare configurare cu show running-config arata parolele codificate

```
MAIN_ANDERCOU#show running-config
Building configuration...

Current configuration : 2703 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname MAIN_ANDERCOU
!
!
!
enable secret 5 $1$mERr$RY0R2iXyBVu9pBLBzgeSW/
enable password 7 0820424A0C0B0618075A5E577E
```

## 11.2. Setarea SSH

Secure Shell (SSH) este un protocol de rețea criptografic ce permite ca datele să fie transferate folosind un canal securizat între dispozitive de rețea. Cele două mari versiuni ale protocolului sunt SSH1 sau SSH-1 și SSH2 sau SSH-2

To enable SSH on the router, the following parameters must be configured:

- Hostname

```
R1(config)#hostname MAIN_ANDERCOU
```

- Domain name

```
MAIN_ANDERCOU(config)#ip domain-name alexandru_pprc.ro
```

- Asymmetrical keys (Cisco recommends using a minimum modulus length of 1024)

```
MAIN_ANDERCOU(config)#crypto key generate rsa
```

How many bits in the modulus[512]: 1024

- Local authentication

```
MAIN_ANDERCOU(config)#username alex_admin secret alexandru_Admin1234
```

```
MAIN_ANDERCOU(config)#line vty 0 4
```

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

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

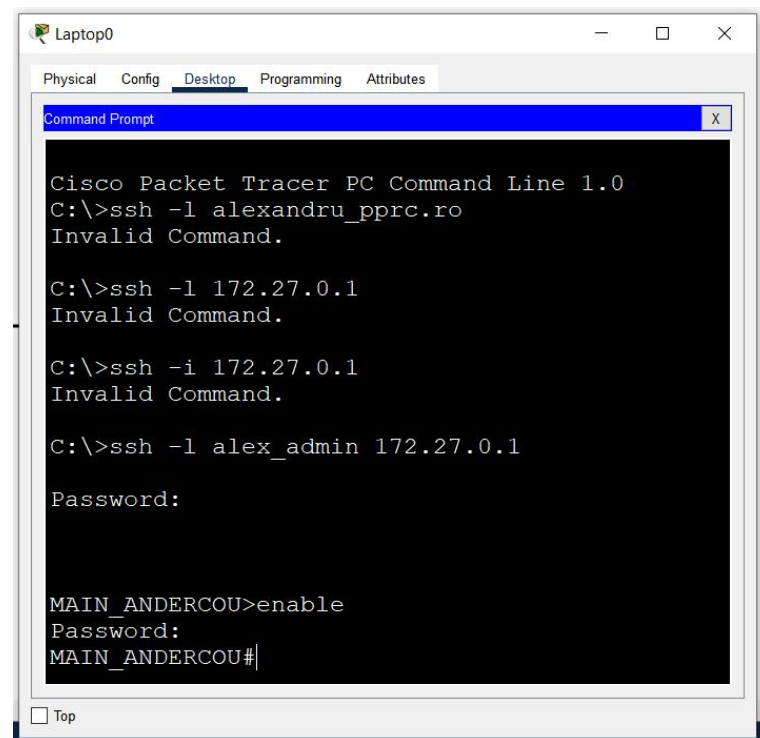
Testare SSH: Open command prompt on a device.

Forma ssh -l <username> <traget\_device\_IP or name>

### 11.1.2 Testare ssh

De pe laptopul:Laptop 0 din vlan 10 cu adresa ip la subinterfata fa0/0.10 de: 172.27.0.1

Enter command: ssh -l alex\_admin 172.27.0.1

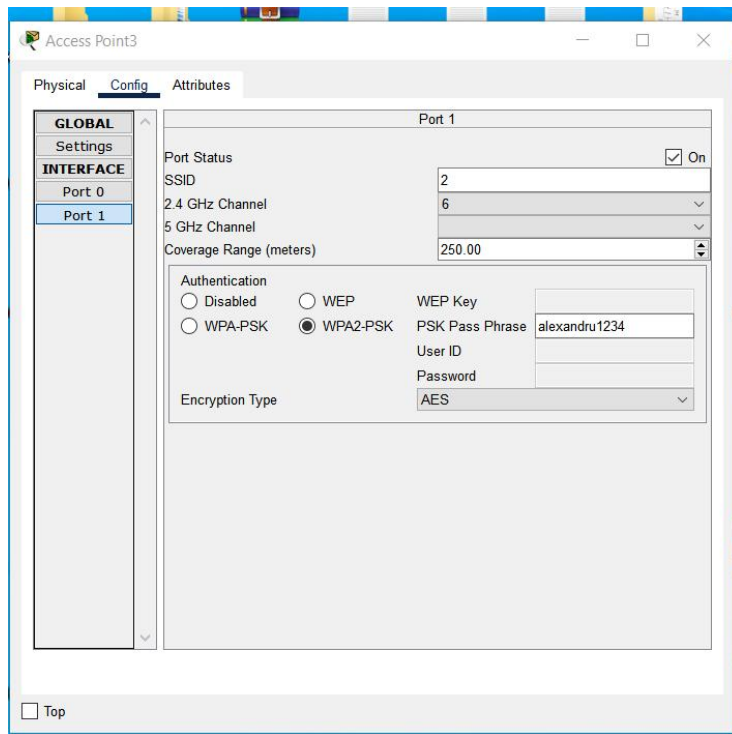


### 11.3. Configurare W--FI

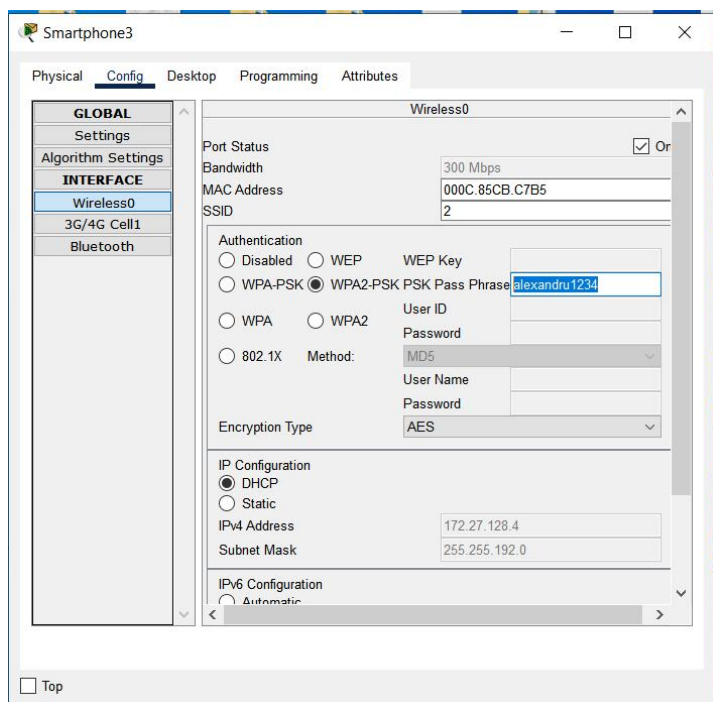
Configurare:

Acces 3 cu SSID 2 si parola de tipul WPA2-PSK:alexandru1234





Pe partea de device se va specifica SSID 2 si parola de la router.



## 12.Securitate complexa