REȚEAUA UNEI INSTITUȚII COMERCIALE

TEMA 5

Tarța Antonia-Maria

2025

Îndrumător: Adrian Peculea **Grupa: 30643**

Cuprins

Cerința proiectului

Se considera o institutie comerciala cu 3 cladiri. Se va folosi adresa de retea 172.16.0.0/16 pentru reteaua intranet, adresa de retea 210.1.1.64/27 pentru DMZ si adresa de retea 210.1.1.32/27 pentru accesul in exterior. Se vor proiecta 3 subretele pentru utilizatori (una pentru fiecare cladire). Utilizatorii vor avea posibilitatea de a se conecta la retea atat prin cablu cat si wireless. Prin cablarea si configurarea retelei se va asigura redundanta. Adresele hosturilor vor fi alocate dinamic folosind servere de DHCP configurate la nivelul ruterelor. Numarul minim de utilizatori deserviti de catre fiecare subretea 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. Rutarea se va face cu ajutorul protocolului OSPF pentru care se vor implementa optiunile de securitate. Accesul in exterior se va realiza folosind NAT pe routerul care controleaza DMZ, pe urmatorul interval de adrese publice: 210.1.1.35-210.1.1.62.

Conectarea la ISP se va realiza printr-o interfata de tip Ethernet avand adresa 210.1.1.34/27. Adresa ISP-ului este 210.1.1.33/27. Reteaua Internet se va simula prin intermediul unui server si a unui calculator.

Pentru securizarea echipamentelor de retea se vor realiza urmatoarele configurari: se vor defini utilizatori pe diferite nivele de privilegiu, criptarea parolelor, configurarea remote se va face doar prin ssh, retelele wireless vor fi securizate cu WPA2.

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

Introducere

Proiectul are ca obiectiv realizarea unei rețele informatice pentru o instituție comercială formată din trei clădiri. Scopul principal este de a asigura o comunicare eficientă și sigură între dispozitive, precum și acces controlat la Internet și servicii proprii. Rețeaua este structurată astfel încât să permită conectarea atât prin cablu, cât și prin rețele wireless.

Topologia Rețelei

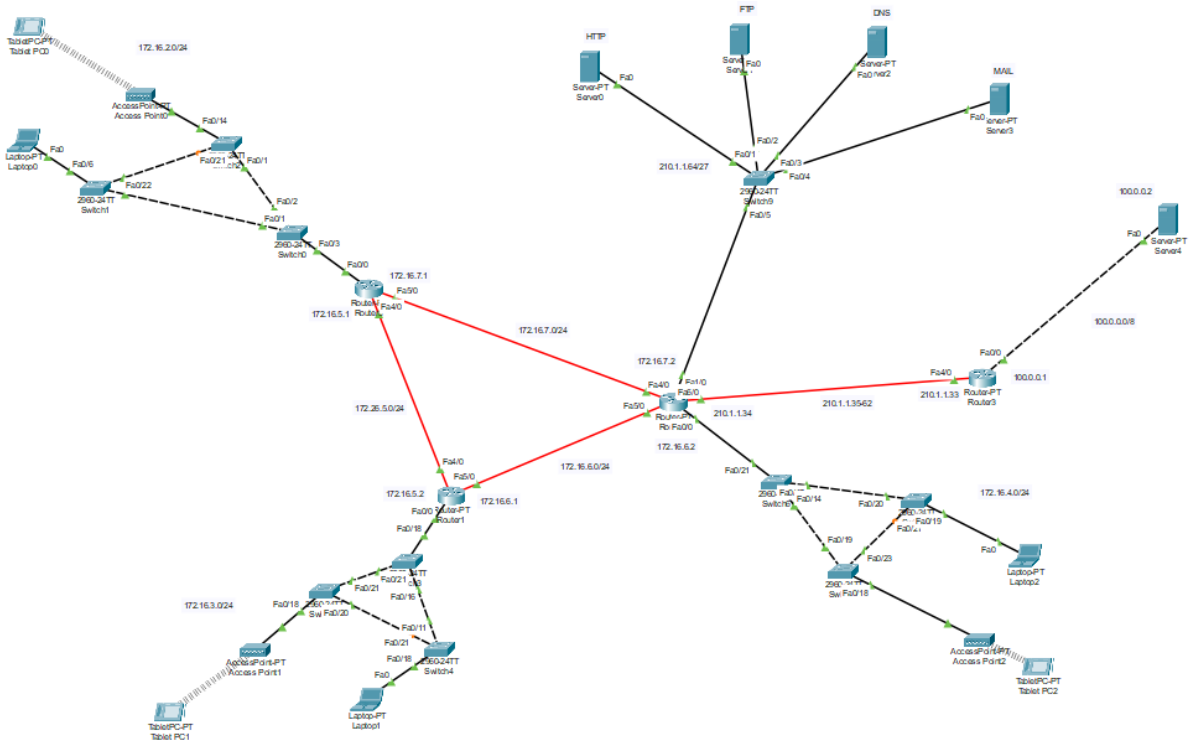
Topologia rețelei este una de tip stea dinamică cu extinderi și căi redundante, ceea ce înseamnă că fiecare dispozitiv este conectat la un switch central, iar în caz de eșec al unei conexiuni, o cale alternativă este disponibilă automat. Această metodă asigură continuitatea traficului de rețea și minimizează impactul unei defecțiuni.

- **Adresă rețea intranet:** 172.16.0.0/16
- **Adresă rețea DMZ:** 210.1.1.64/27
- **Adresă rețea pentru acces în exterior:** 210.1.1.32/27

- **Interval adrese publice:** 210.1.1.35 – 210.1.1.62
- **Adresă conectare la ISP:** 210.1.1.34/27 (adresă ISP: 210.1.1.33)
- **Tipuri de conectivitate:** cablu și wireless
- **Protocol de rutare:** OSPF

Utilizatorii se conectează la rețea fie prin cablu Ethernet, fie prin rețele Wi-Fi securizate.

Pentru a optimiza performanța rețelelor wireless, se utilizează **canalele 1, 6 și 11**, deoarece acestea nu se suprapun, reducând interferențele între punctele de acces.



Figură 1. Tipologia rețelei

Subnetting și Planificarea Adresării

Pentru a acomoda cel puțin 200 de utilizatori per clădire, am utilizat o mască **/24** pentru fiecare subrețea:

- **Clădirea 1**: 172.16.1.0/24
- **Clădirea 2**: 172.16.2.0/24
- **Clădirea 3**: 172.16.3.0/24

Această schemă permite alocarea a până la 254 de adrese IP pentru fiecare clădire.

Configurarea VLAN-urilor și Switch-urilor

Segmentarea rețelei în VLAN-uri permite izolarea traficului dintre clădiri și optimizează performanța. Pentru fiecare clădire a fost creat câte un VLAN dedicat, porturile switch-urilor fiind configurate în mod access:

```
Switch(config)#vlan 2
Switch(config)#interface range fastEthernet 0/1-24
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 2
```

Pentru a asigura redundanță, spanning-tree este activat. Acesta previne buclele de rețea și asigură o cale de rezervă între switch-uri. Astfel dacă principala cale devine inactivă, vom avea siguranța că totuși între 2 puncte avem mereu o legătură.

Dacă am avea un switch now cu un **MAC address mai mic,** acesta ar deveni **root bridge** deoarece rădăcina se alege după prioritate(care e la fel) și MAC. În rețea ar apărea probleme, dar pentru a evita acest lucru, root bridge este configurat manual prin setarea unei **priorități mai mici** pe switch-ul principal.

```
Switch(config)#spanning-tree vlan 1,2 priority 0
```

Configurarea Routerului și DHCP

Pentru a interconecta cele trei clădiri, au fost realizate conexiuni directe între routerele lor. Aceste conexiuni formează un triunghi între clădiri, permițând redundanță la nivel de rețea între routere. Conectivitatea între ele a fost testată folosind comenzi `ping`, iar tabela de rutare a fost verificată cu show ip route. La primul ping, poate apărea un timeout deoarece routerul trebuie să afle adresa MAC a destinației. După această primă încercare, adresa MAC este păstrată temporar în cache, iar ping-urile următoare funcționează imediat.

Pentru ca fiecare router să poată învăța automat rutele către toate celelalte subrețele, a fost implementat protocolul de rutare **OSPF**, cu configurarea rețelelor relevante în **area 0**. De asemenea, interfețele care nu necesită anunțuri de rutare au fost setate ca **interfețe pasive** pentru a reduce traficul de rutare inutil.

```
Router(config)#router ospf 1
Router(config-router)#network 172.16.2.0 0.0.0.255 area 0
Router(config-router)#network 172.16.5.0 0.0.0.255 area 0
Router(config-router)#network 172.16.7.0 0.0.0.255 area 0
Router(config-router)#passive-interface fa0/0
```

Routerul este configurat pentru a aloca dinamic adrese IP utilizatorilor prin DHCP. Această metodă elimină nevoia de a configura manual fiecare dispozitiv și permite o gestionare centralizată a

adreselor IP. Prin excluderea primelor adrese (172.16.2.1 - 172.16.2.9), ne asigurăm că acestea pot fi utilizate pentru echipamente critice (precum gateway-ul sau switch-urile) fără risc de conflict IP.

```
Router(config)#ip dhcp excluded-address 172.16.2.1 172.16.2.9
Router(config)#ip dhcp pool AntoniaNet2
Router(dhcp-config)#network 172.16.2.0 255.255.255.0
Router(dhcp-config)#default-router 172.16.2.1
```

Comportamentul Rețelei și Rutarea

În general, o rută statică este utilizată atunci când există o singură cale de comunicare între două rețele. Aceasta este introdusă manual și nu se adaptează automat în caz de modificări în rețea. În schimb, protocoalele dinamice de rutare, precum OSPF, sunt preferate în medii unde este necesară redundanța și recalcularea traseelor în timp real, de exemplu atunci când una dintre rute cade. Acest comportament face ca rețeaua să fie mai rezistentă la erori și mai ușor de întreținut.

Pentru ca două dispozitive să comunice între ele într-o rețea, este esențial să știm dacă se află în aceeași subrețea IP. Această verificare se face aplicând o operație logică AND între adresa IP și masca de rețea pentru fiecare dispozitiv. Dacă rezultatul este același, dispozitivele se află în aceeași subrețea și pot comunica direct la nivel MAC, fără a trece printr-un router. În schimb, dacă se află în subrețele diferite, pachetele trebuie transmise printr-un router, care determină traseul potrivit consultând tabela sa de rutare.

Configurarea Rețelei DMZ

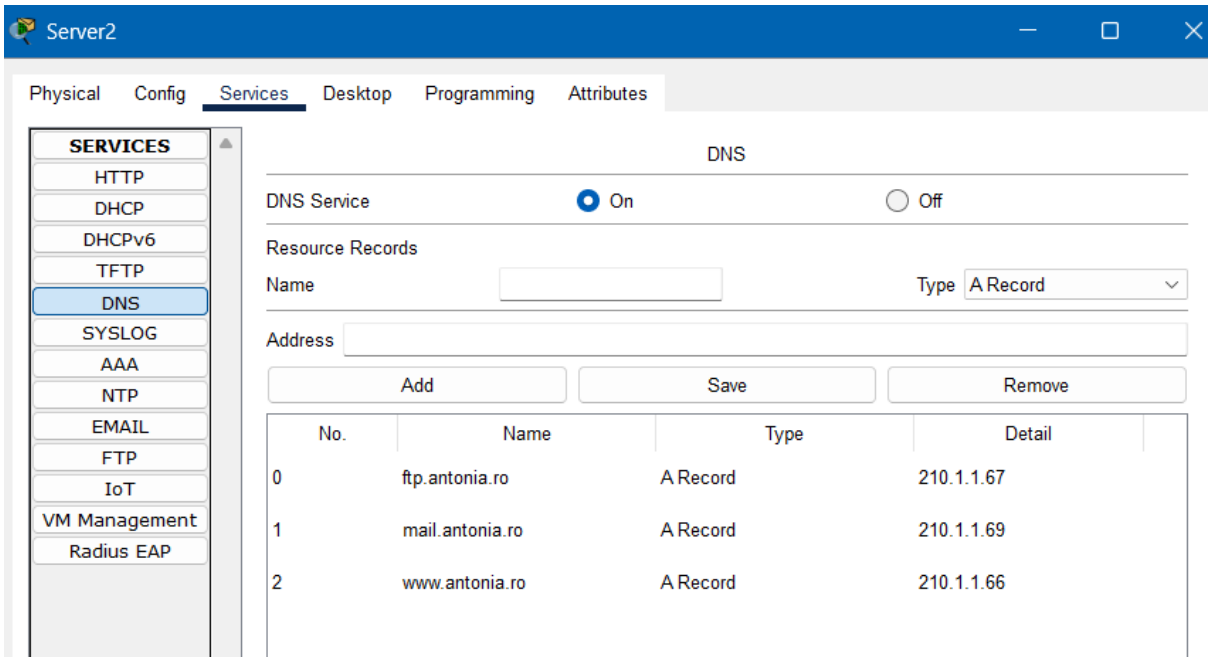
Pentru a izola și proteja serviciile accesibile din exterior, a fost configurată o zonă DMZ. În această zonă au fost plasate serverele principale, cele de tip HTTP, FTP, DNS și Mail. Pentru ca această rețea să fie cunoscută în întregul sistem, a fost adăugată în protocolul OSPF.

Configurarea DNS, FTP, mail, HTTP

Serverul **HTTP** a fost configurat în zona DMZ, folosind o adresă IP publică. Acesta a fost asociat domeniului www.antonia.ro printr-o înregistrare DNS, permițând accesul la conținutul web folosind nume de domeniu.

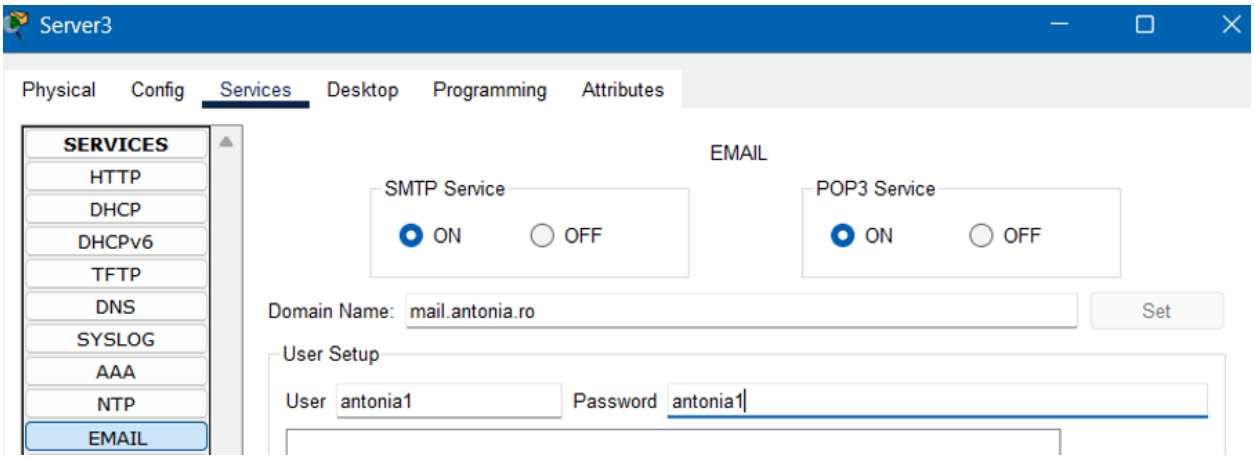
Pe un alt server s-a configurat serviciul **FTP**. Acesta este utilizat pentru transferul de fișiere între un client și server. S-a testat funcționarea trimiterii unui fișier cu comanda `put`, ulterior un alt fișier s-a descărcat cu comanda `get`.

Serviciul **DNS** a fost activat pe un server din DMZ, unde au fost adaugate domenii precum www, mail, ftp. Acest serviciu permite translatarea numelui simbolic în adrese IP, facilitând accesul la servere pe bază de nume.



Figură 2. Configurare DNS

Serviciul de **mail** oferă posibilitatea de a trimite și primi mesaje. S-a utilizat **SMTP** pentru transmiterea mailurilor și **POP3** pentru aducerea acestora la client. Pe serverul de mail s-au adaugat domenii și utilizatori pentru a testa dacă mesajele sunt trimise, livrate și preluate corect.



Figură 3. Configurare mail

Configurarea NAT

Pentru a permite comunicarea rețelei interne cu exteriorul, a fost adăugat un modul suplimentar pe routerul principal, utilizat pentru conectarea prin fibră optică la ISP(furnizorul de servicii de Internet). Accesul stațiilor interne la rețeaua externă este realizat prin NAT, folosind un interval de

adrese publice alocat special pentru translatare. Astfel, fiecare dispozitiv cu adresă IP privată poate comunica cu exteriorul printr-o adresă publică temporară. Serverele aflate în zona DMZ nu necesită translatare, deoarece acestea dețin adrese IP publice și trebuie să fie accesibile direct din afara rețelei.

Exemplu pentru marcarea interfețelor interne și externe:

```
Router(config)#interface fa0/0
Router(config-if)#ip nat inside

Router(config)#interface fa6/0
Router(config-if)#ip nat outside
```

În plus, a fost definită o regulă statică pentru a permite accesul din rețeaua externă către un serviciu specific din rețeaua internă. Pentru direcționarea traficului spre exterior, a fost configurată o rută implicită către furnizor. Această rută a fost propagată și în rețea prin OSPF, asigurând astfel că toate dispozitivele cunosc calea de ieșire. În sens invers, furnizorul a fost configurat cu o rută statică către rețeaua DMZ, astfel încât serviciile oferite intern să poată fi accesate din exterior.

```
Router(config)#ip nat inside source static tcp 172.16.2.2 22 210.1.1.34 22
```

Pentru propagarea unei rute implicite spre furnizor am folosit:

```
Router(config)#ip route 0.0.0.0 0.0.0.0 210.1.1.33
Router(config)#router ospf 1
Router(config-router)#default-information originate
```

Securitate

Accesul la echipamentele de rețea a fost securizat prin definirea de utilizatori cu nivele diferite de privilegii, fiecare având un nivel de acces corespunzător setat prin atributul `privilege`. Parolele definite au fost criptate pentru a nu putea fi vizualizate. Rețelele wireless au fost securizate cu **WPA2-PSK**. Conexiunile remote se pot realiza doar prin **SSH**, care oferă criptare, fiind astfel o metodă sigură de administrare. S-au generat chei RSA și s-a setat accesul doar pentru SSH:

```
(config)#crypto key generate rsa
(config)#line vty 0 4
(config-line)#transport input ssh
(config-line)#login local
```

Pentru gestionarea autentificării utilizatorilor, a fost configurat un server RADIUS. Pe echipamentele de rețea s-a activat funcționalitatea AAA (Authentication, Authorization, Accounting).

```
(config)#aaa authentication login default group radius none
(config)#radius server Antonia
(config-radius-server)#address ipv4 210.1.1.66
(config-radius-server)#key antonia15
(config-radius-server)#line vty 0 4
(config-line)#transport input ssh
(config-line)#login authentication default
```

Măsură extra: Redirecționarea logurilor către un server

Pentru a centraliza și securiza înregistrările generate de echipamentele de rețea am configurat trimiterea logurilor către un server. Am vrut să folosesc un server deja existent, astfel am ales serverul FTP (210.1.1.67). Primul pas a fost să verific dacă serviciul SYSLOG este activ în interfața serverului. Logurile trimise includ informații despre starea echipamentului, evenimente de configurare, erori și mesaje de sistem. Măsura ajută la urmărirea activității din rețea, la identificarea rapidă a problemelor și la înțelegerea situației în cazul în care apare un incident.

Am implementat această măsură de securitate pe un router, mai exact pe Net3R.

```
Net3R>en
Net3R#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Net3R(config)#logging host 210.1.1.67
Net3R(config)#logging trap debugging
Net3R(config)#service timestamps log datetime msec
Net3R(config)#logging on
Net3R(config)#exit
Net3R#
*Mar 01, 00:17:14.1717: SYS-5-CONFIG_I: Configured from console by console
*Mar 01, 00:17:14.1717:  %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 210.1.1.67 port 514 started
- CLI initiated
Net3R#
Net3R#
```

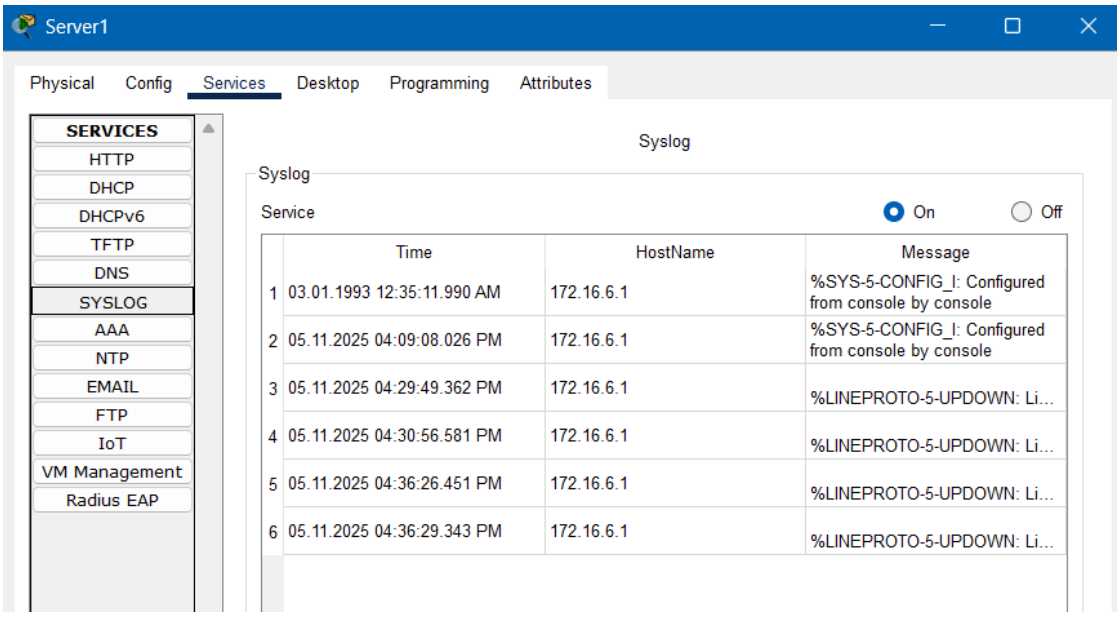
Figură 4. Redirecționarea logurilor către FTP

După ce am configurat trimiterea logurilor către serverul SYSLOG, am observat că toate mesajele aveau data 1 ianuarie 1993. Acest lucru se întâmplă deoarece routerele din Packet Tracer nu au un ceas intern real, iar dacă ora nu este setată manual, ele folosesc o dată prestabilită.

Pentru a corecta problema, am setat manual ora și data pe router cu comanda:

```
clock set 16:05:00 11 May 2025
```

După aplicarea acestei comenzi, mesajele de log au început să apară cu data corectă, ceea ce este important pentru înregistrarea exactă a evenimentelor din rețea.



Figură 5. Afișarea logurilor in Syslog

Măsură extra: Limitarea accesului la porturi

Pentru a preveni conectarea neautorizată la rețea, s-a activat funcționalitatea Port Security pe portul de acces al switch-ului ce conectează echipamentele finale. Aceasta permite conectarea unui singur dispozitiv pe port (în funcție de MAC), iar în caz de încălcare, portul este automat dezactivat.

```
Net4S2>en
```

```
Net4S2#conf t
```

Am selectat portul unde este conectat laptopul:

```
Net4S2(config)#interface fa0/19
```

```
Net4S2(config-if)#switchport mode access
```

```
Net4S2(config-if)#switchport port-security
```

Am permis conectarea unui singur dispozitiv pe acel port. Dacă altul încearcă să se conecteze, este violation:

```
Net4S2(config-if)#switchport port-security maximum 1
```

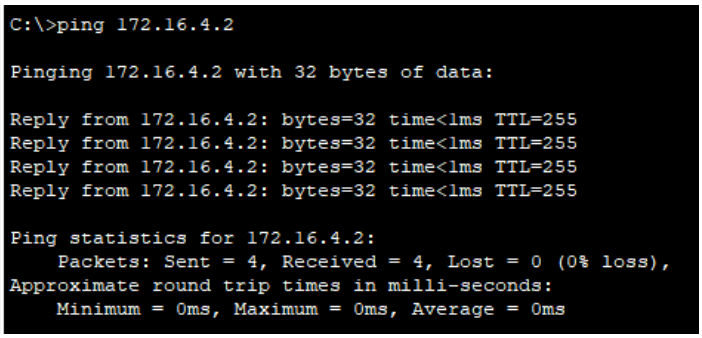
În caz de violation, portul se oprește complet pentru a bloca accesul:

```
Net4S2(config-if)#switchport port-security violation shutdown
```

Am pus switchul să învețe automat adresa MAC a primului dispozitiv conectat și să o salveze ca adresă permisă:

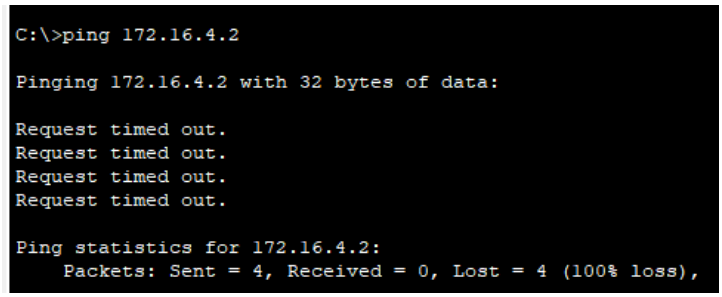
```
Net4S2(config-if)#switchport port-security mac-address sticky
Net4S2(config-if)#exit
```

Pentru verificare, am dat un ping de la laptop la 172.16.4.2, acesta a avut succes, iar in acest fel switchul a invățat adresa MAC a laptopului.



Figură 6. Ping cu adresa MAC validă

Nu am vrut să adaug un laptop nou pentru această verificare, dar am schimbat adresa MAC a laptopului deja existent. La efectuarea unui ping, acesta nu a funcționat. Portul a fost dezactivat, traficul a fost blocat, conexiunea s-a întrerupt, fapt dovedit chiar de marcarea acesteia cu roșu în cadrul topologiei.



Figură 7. Ping cu adresa MAC nouă

```
Net4S2#show port-security interface fa0/19
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 00D0.D31C.9755:4
Security Violation Count   : 1
```

Figură 8. Confirmare încălcare Port Security

Figura 8, demonstreaza, de asemena, că portul a fost blocat (secure-shutdown) în urma unei încălcări: a fost detectat un dispozitiv cu o adresă MAC diferită de cea învățată anterior (Last

Source Address). Valoarea Violation Count: 1 confirmă că portul a fost dezactivat automat, iar măsura de securitate a funcționat conform așteptărilor.

Verificare și Validare

Testarea rețelei s-a realizat în mod practic, folosind metode specifice pentru fiecare componentă configurată:

- **Conectivitate între routere și switch-uri**: a fost verificată folosind comenzi `ping`, inclusiv după prima transmitere care poate duce la timeout până la rezolvarea MAC-ului. După acest pas, conexiunile au funcționat stabil.
- **Testarea DHCP**: alocarea automată a adreselor IP a fost confirmată prin conectarea mai multor stații de lucru și observarea configurării obținute.
- **Testare DNS**: comanda `nslookup` a fost utilizată pentru a verifica translatarea numelui de domeniu în IP, folosind înregistrările definite pentru domeniul antonia.ro.
- **Testare FTP**: clientul FTP s-a conectat la serverul DMZ, s-au încărcat fișiere pe server cu put și s-au descărcat ulterior cu get, confirmând funcționalitatea serviciului.
- **Testare HTTP**: serverul web configurat în DMZ a fost accesat cu succes din rețeaua internă prin introducerea domeniului www.antonia.ro într-un browser, confirmând funcționarea DNS și a serviciului HTTP.
- **Testare Mail**: a fost transmis un mesaj de test prin SMTP și preluat de clientul destinatar prin POP3.
- **Testare wireless**: tabletele au fost conectate cu succes la rețeaua WPA2 configurată în fiecare clădire.
- **Testare SYSLOG:** Routerele au fost configurate să trimită loguri către serverul FTP, unde serviciul SYSLOG a fost activat. După generarea unor evenimente, mesajele s-au afișat corect în interfață.
- **Testare Port Security:** După activarea Port Security pe portul conectat la laptop, s-a schimbat adresa MAC și s-a generat trafic. Portul s-a blocat, conexiunea a devenit roșie în topologie, iar comanda show port-security a confirmat încălcarea.

Concluzii

Proiectul a fost realizat conform cerințelor specificate în Tema 5, toate configurațiile fiind implementate, testate și validate cu succes. Rețeaua este segmentată în mod logic, asigurând atât redundanță cât și securitate.

Am realizat: conectivitatea între clădiri, rutare OSPF, segmentare VLAN, adresare dinamică prin DHCP, conectivitate wireless securizată, DMZ funcțională cu servere accesibile și configurarea completă a NAT. Măsurile de securitate aplicate (privilegii, parole criptate, SSH, AAA și WPA2 și Port Security) oferă protecție adecvată atât la nivel logic, cât și fizic, iar logurile de sistem sunt transmise către un server SYSLOG din DMZ, permițând monitorizarea activității din rețea. Testele efectuate au confirmat funcționarea rețelei și aplicabilitatea practică a soluției implementate.