

Proiect Protocole și Rețele de Comunicații

Proiectarea unei infrastructuri rețelistice
pentru o clădire comercială cu trei nivele

- Tema 2 -

Vlad-Alexandru Bartolomei

Grupa 30643

Profesor îndrumător: Adrian Lucian Peculea



MEMBRĂ A



Facultatea de Automatică și Calculatoare
Universitatea Tehnică din Cluj-Napoca
România
Martie 2025

Cuprins

0 Specificația problemei	2
1 Etapa 1 - stabilirea topologiei tip mapătă problemei expuse	2
1.1 Layout	2
1.2 Comenzi	4
1.3 Memoriu tehnic	5
1.3.1 Minimum Spanning Tree	5
1.3.2 Virtual Local Area Network - VLAN	5
1.3.3 Virtual (LAN) Trunking Protocol - VTP	6
1.3.4 VLAN pentru traficul de management	8
1.3.5 Bridge-ul rădăcină	9
1.3.6 Adresarea de IP-uri	10
1.3.7 Serverul de DHCP	10
2 Etapa 2 - Adăugarea zonei demilitarizate (DMZ)	13
2.1 Layout	13
2.2 Comenzi	13
2.3 Memoriu tehnic	14
2.3.1 Hop-by-hop routing	14
2.3.2 Zona demilitarizată - DMZ	15

Rezumat

Prezenta documentație își propune să documenteze printr-un procedeu etapizat parcursul implementării acestui proiect pe durata fiecărei ședințe de lucru și să marcheze, acolo unde este cazul, noțiunile folosite în subcapitole - memorii tehnice.

0 Specificația problemei

0.1: Specificație

Se consideră o clădire comercială cu 3 nivele. Se va folosi adresa de rețea 172.16.0.0/16 pentru rețeaua intranet, adresa de rețea 210.1.1.64/27 pentru DMZ și adresa de rețea 210.1.1.32/27 pentru accesul în exterior. Se vor proiecta 4 VLAN-uri (unul pentru fiecare etaj și unul pentru traficul de management). Pentru configurarea VLAN-urilor se va folosi protocolul VTP. Prin cablarea și configurarea rețelei se va asigura redundanță. Adresele hosturilor vor fi alocate dinamic folosind un singur server de DHCP aflat în VLAN-ul corespunzător primului etaj. Numărul minim de utilizatori deserviți de către fiecare VLAN este 200. Serverele de HTTP, FTP, DNS și MAIL vor fi plasate în DMZ și vor avea adrese publice. Numele domeniului web va include numele studentului. Pentru asigurarea conectivității se vor configura rute statice. Accesul în exterior se va realiza folosind NAT pe routerul care controlează DMZ, pe următorul interval de adrese publice: 210.1.1.35-210.1.1.62.

Conecțarea la ISP se va realiza printr-o interfață de tip Ethernet având adresa 210.1.1.34/27. Adresa ISP-ului este 210.1.1.33/27. Reteaua Internet se va simula prin intermediul unui server și a unui calculator.

Pentru securizarea echipamentelor de rețea se vor realiza următoarele configurații:

- se vor defini utilizatori pe diferite nivele de privilegiu;
- criptarea parolelor;
- configurarea remote se va face doar prin ssh;
- se va securiza protocolul VTP.

Se vor prezenta și implementa două măsuri suplimentare de securizare a rețelei.

1 Etapa 1 - stabilirea topologiei tip mapată problemei expuse

1.1 Layout

De regulă, într-un astfel de proiect din lumea reală se alege o topologie de tip **stea extinsă**. Această topologie oferă scalabilitate; spre exemplu, dacă aş mai dori să mai cablez o cameră, este posibil să fie tras încă un *app link* și adăugat un *fulg nou*¹. Pentru problema noastră am ales aceeași variantă, rezultând următoarea figură:

¹stea extinsă

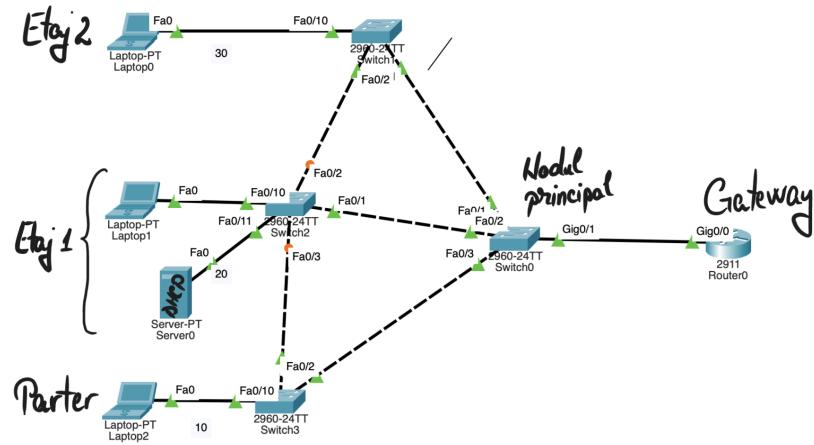


Figura 1: Reprezentarea celor trei etaje, a nodului principal și a celorlalte noduri

Figura 1 respectă specificația de redundanță în felul următor: fiecare etaj are propriul său switch; între toate switch-urile există legături, dar datorită faptului că acestea vor fi configurate pentru a funcționa pe baza algoritmului MINIMUM SPANNING TREE, legăturile redundante vor fi *down*. Algoritmul cunoaște nodul principal, iar când acesta este *down*, celelalte legături se vor activa și vor fi *up*.

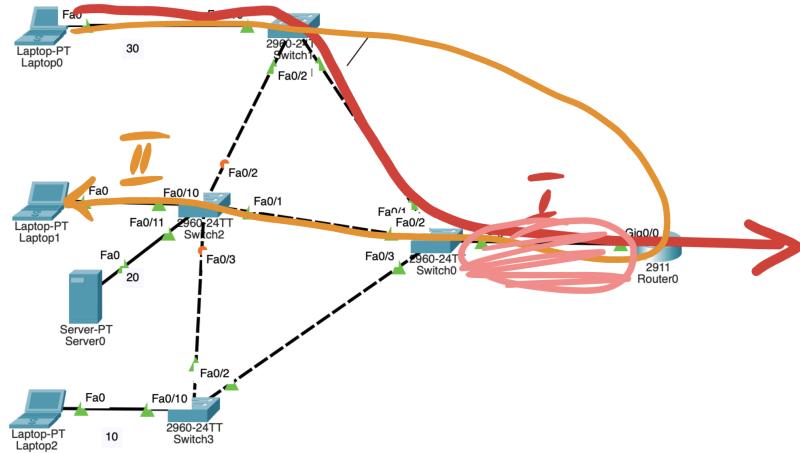


Figura 2: I: accesul stației de pe etajul 2 pe Internet; II: accesul stației de pe etajul 2 la o stație pe etajul 1, într-un alt VLAN

```

Physical Config CLI Attributes
IOS Command Line Interface
1005 trnet-default active
VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
-----
1 enet 100001 1500 - - - - 0 0
1002 fddi 101002 1500 - - - - 0 0
1003 tr 101003 1500 - - - - 0 0
1004 fdnet 101004 1500 - - - ieee - 0 0
1005 trnet 101005 1500 - - - ibm - 0 0
VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
-----
Remote SPAN VLANs
-----
Primary Secondary Type Ports
-----
MainSwitch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MainSwitch(config)#vlan 10
MainSwitch(config-vlan)#name Net10
MainSwitch(config-vlan)#exit
MainSwitch(config)#vlan 20
MainSwitch(config-vlan)#name Net20
MainSwitch(config-vlan)#exit
MainSwitch(config)#vlan 30

```

Figura 5: Crearea VLAN-urilor pe switch-ul principal

1.2 Comenzi

```

Switch>ena
Switch#
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#host
Switch(config)#hostname MainSwitch
MainSwitch(config)#int
MainSwitch(config)#interface ra
MainSwitch(config)#interface range fa
MainSwitch(config)#interface range fastEthernet 0/1-2
MainSwitch(config-if-range)#exit
MainSwitch(config)#interface range fastEthernet 0/1-3
MainSwitch(config-if-range)#sw
MainSwitch(config-if-range)#switchport mo
MainSwitch(config-if-range)#switchport mode acc
MainSwitch(config-if-range)#switchport mode access
MainSwitch(config-if-range)#exit

```

Figura 3: Exemplu pentru configurarea Switch-ului principal și configurarea porturilor aferente, legate la celealte Switch-uri ale fiecărui VLAN, pentru a comunica pe linii de trunk

```

MainSwitch>ena
MainSwitch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MainSwitch(config)#vtp do
MainSwitch(config)#vtp domain Adrian
Changing VTP domain name from NULL to Adrian
MainSwitch(config)#vtp pass
MainSwitch(config)#vtp password Adrian
Setting device VLAN database password to Adrian
MainSwitch(config)#vtp mode ser
MainSwitch(config)#vtp mode server
Device mode already VTP SERVER.
MainSwitch(config)#

```

Figura 4: Activarea protocolului VTP pe switch-ul principal. Captură de ecran de la laboratorul online ținut de domnul profesor Adrian Peculea, de pe stația sa

```

MainSwitch>
MainSwitch>ena
MainSwitch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MainSwitch(config)#spa
MainSwitch(config)#spanning-tree vlan 1,10,20,30,99 prior
MainSwitch(config)#spanning-tree vlan 1,10,20,30,99 priority 0
MainSwitch(config)#sh
MainSwitch(config)#do

```

Figura 6: Setarea VLAN-urilor în Spanning Tree

```

MainRouter(config-if)#exit
MainRouter(config)#int
MainRouter(config)#interface gi
MainRouter(config)#interface gigabitEthernet 0/0.20
MainRouter(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.20, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.20,
changed state to up

MainRouter(config-subif)#enc
MainRouter(config-subif)#encapsulation d
MainRouter(config-subif)#encapsulation dot1Q 20
MainRouter(config-subif)#ip add
MainRouter(config-subif)#ip address 172.16.20.1 255.255.255.0
MainRouter(config-subif)#

```

Figura 7: Configurarea serverului de DHCP. Protocolul folosit este 802.1Q, încrucișând acesta menține și informații despre VLAN-uri, iar protocolul Ethernet este insuficient.

```

MainRouter(config-subif)#enc
MainRouter(config-subif)#encapsulation dot1Q 30
MainRouter(config-subif)#ip add
MainRouter(config-subif)#ip address 172.16.30.1 255.255.255.0
MainRouter(config-subif)#ip h
MainRouter(config-subif)#ip he
MainRouter(config-subif)#ip hel
MainRouter(config-subif)#ip helpe
MainRouter(config-subif)#ip helper-address 172.16.20.2
MainRouter(config-subif)#

```

Figura 8: Exemplu de rerutare a unui DHCPDiscover request dintr-un VLAN diferit de VLAN-ul în care se află serverul de DHCP

1.3 Memoriu tehnic

1.3.1 Minimum Spanning Tree

1.3.2 Virtual Local Area Network - VLAN

Un VLAN este util pentru a virtualiza resurse. Se economisesc bani, hardware și echipamente. Ca aplicabilitate în viața reală, VLAN-urile se folosesc în cadrul același companii pentru a lega între ele stații din aceeași departamente. Spre exemplu, departamentul de Marketing are un VLAN, cel de Resurse Umane alt VLAN. Această *clusterizare* a stațiilor aduc un mare avantaj: reduc din traficul generat pe router-ul principal, ținând chestiunile interne strict pentru acel VLAN.

În locul unui VLAN, fiecare departament ar fi putut avea propriul său router, numai că aceasta ar fi implicat costuri suplimentare și overhead tehnic. Protocolul folosit este 802.1Q.

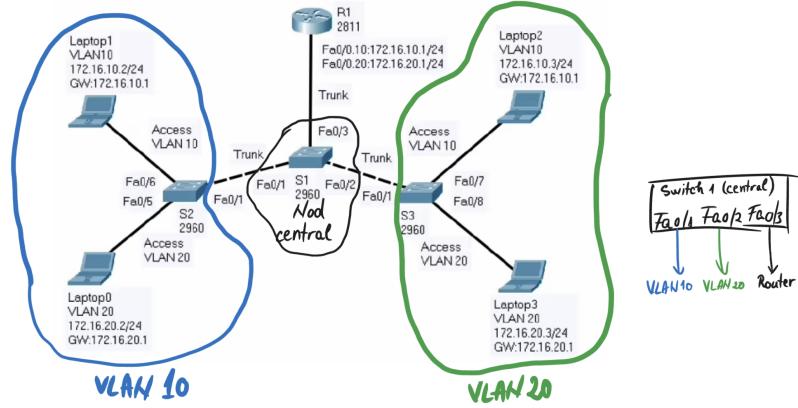


Figura 9: Exemplu cu două VLAN-uri diferite legate de un switch central și un router

Figura 9 ilustrează perfect o situație în care un VLAN poate fi aplicat. Două departamente vorbesc separat în VLAN-uri diferite (10 și 20). Pentru ca o stație din VLAN 10 să vorbească cu o alta din VLAN 20, trebuie să treacă prin Switch-ul principal, apoi prin Router (prezența acestuia este absolut necesară) și apoi să fie redirectată către VLAN-ul potrivit. Între cele trei switch-uri din poză, comunicarea se face în mod **trunk**, spre deosebire de celelalte linii, care comunică pe mode **access**.

În scenarii reale, VLAN-urile nu vor fi identificate după numere (VLAN 10, VLAN 20), ci după nume (VLAN Engineering, VLAN Accounting). Din motive de securitate, VLAN-ul 1 este un VLAN preconfigurat și el nu se schimbă.

1.3.3 Virtual (LAN) Trunking Protocol - VTP

Definirea de VLAN-uri în mod manual poate fi laborioasă. Adăugarea unui nou VLAN mai adaugă un număr de comenzi și nu este scalabil.

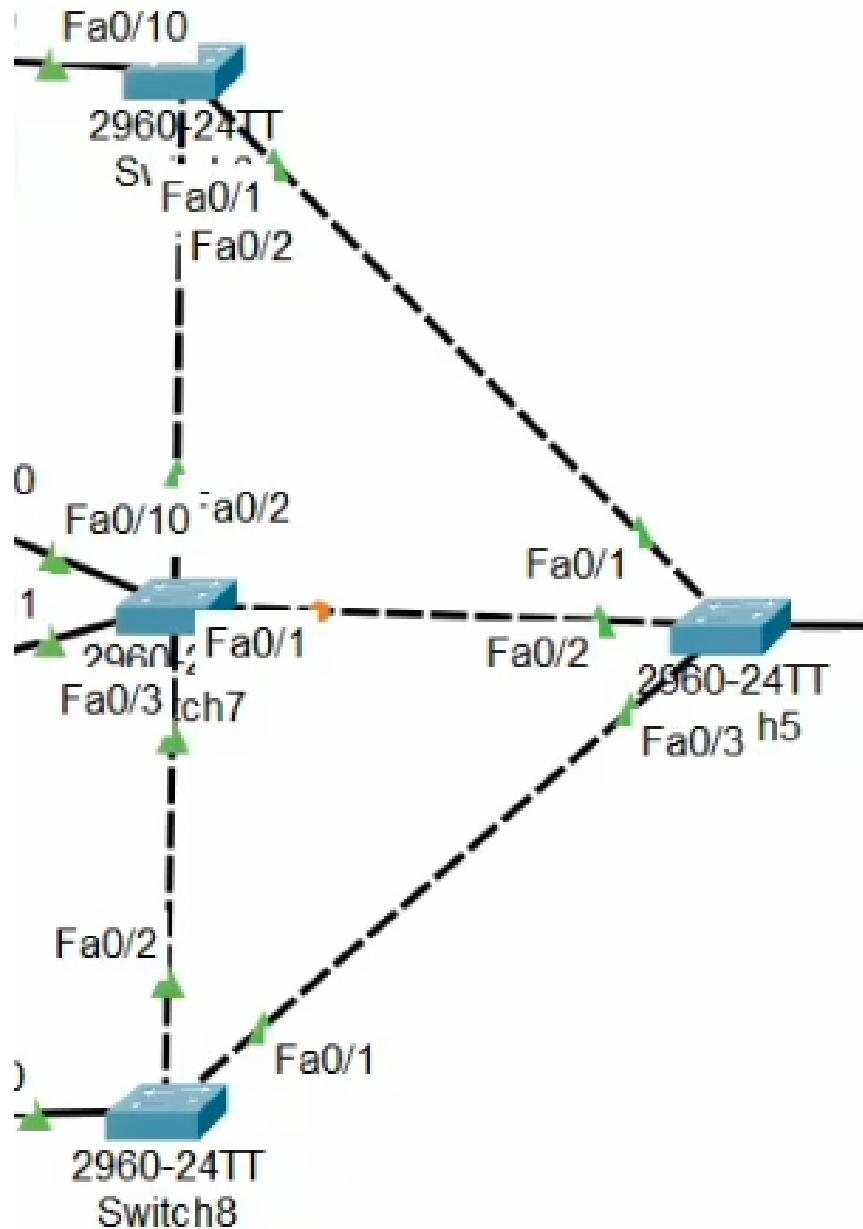


Figura 10: Numai pentru 4 VLAN-uri (10, 20, 30 și 99) avem $12 \times 4 = 48$ de comenzi

Ca răspuns la această problemă a apărut protocolul VTP, un protocol enterprise scalabil. Acest protocol spune că eu pot așeza toate switch-urile **într-un singur domeniu**, iar ele să se autentifice unul cu celălalt prin intermediul unei **parole**². Adițional, switch-urile trebuie să activeze într-unul dintre cele două moduri³: *server* și *client*.

²Domeniul și parola trebuie să fie **aceleași** pentru toată infrastructura de switch-uri dorită. În caz contrar, switch-urile nu se pot autentifica între ele

³sunt mai multe, însă numai despre acestea două merită discutat

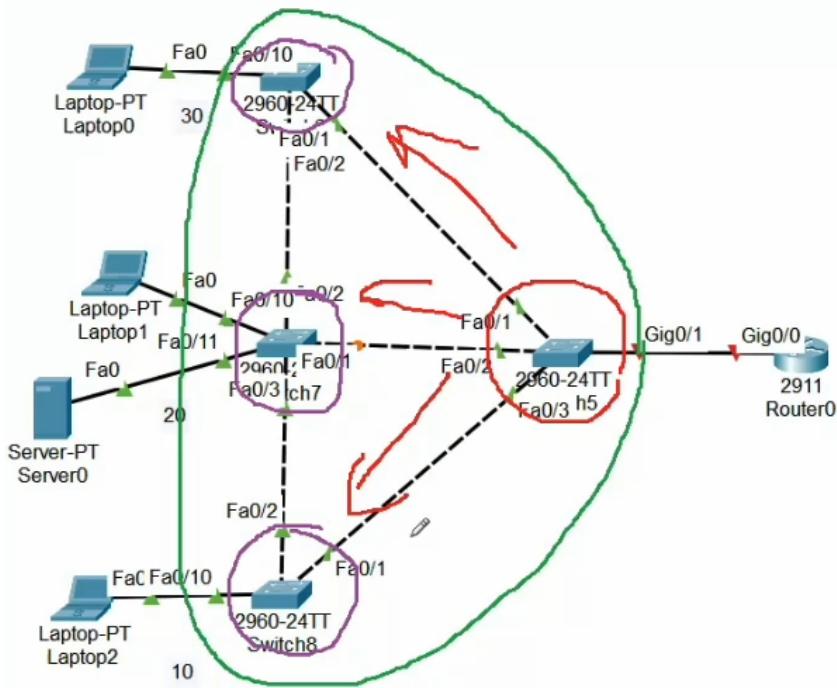


Figura 11: Switch-ul principal este considerat a fi cel în mod server; celelalte sunt în mod client

Switch-ul server (unul singur!) ține o bază de date de VLAN-uri. Procedeul de adăugare al unui nou VLAN implică:

- adăugarea VLAN-ului nou la switch-ul server
- advertise din partea switch-ului server către toate switch-urile client deja existente

Ca efect, toate switch-urile client vor învăța existența noului VLAN. În mod similar are loc ștergerea unui VLAN.

1.3.4 VLAN pentru traficul de management

Prin acest VLAN trece tot traficul ce ține de administrare și gestionare al echipamentelor, trafic izolat de cel al clientului. Acest VLAN este destinat folosirii de către inginerul de sistem, care de oriunde se poate conecta la VLAN și poate monitoriza traficul și echipamente; drept urmare aceste date au caracter confidențial.

1.3.5 Bridge-ul rădăcină

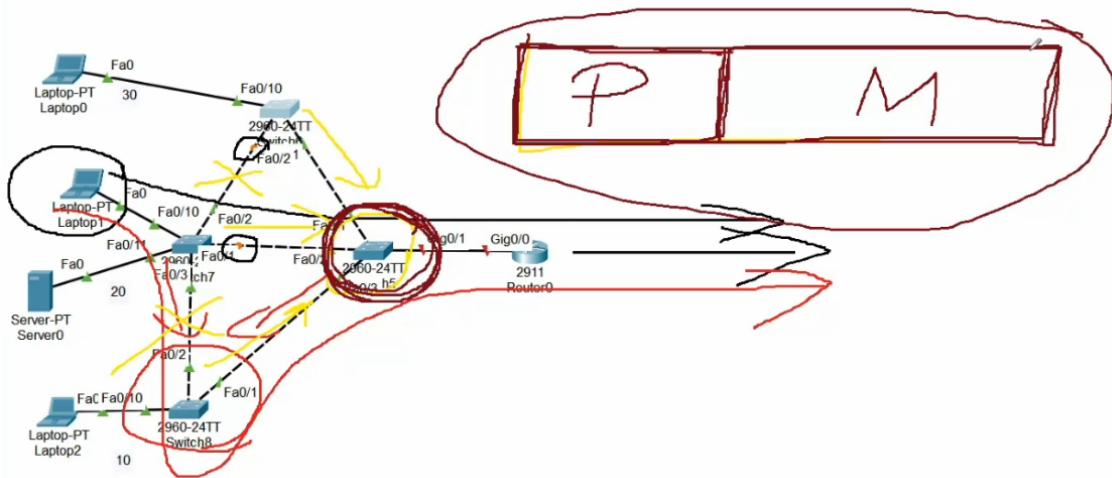


Figura 12: Laptop-ul de pe etajul 1 încearcă să comunice cu internetul (negru), însă se vede nevoie să o ia pe la parter (roșu) (a se vedea LED-urile portocalii)

Ideea de a merge pe la parter sau pe orice alt etaj în afară de cel de origine nu este bună pentru controlul traficului. În varianta ideală ar trebui ca bridge-ul rădăcină să coincidă, în acest caz, cu switch-ul principal, astfel încât fiecare switch să-și calculeze cea mai scurtă cale către nodul principal și implicit backup-ul (redundanță) să fie stabilit între etaje (semnalizat de x-urile galbene).

Cum se alege bridge-ul rădăcină? În funcție de identificatorul switch-ului. Structura sa constă în:

- câmpul P - Prioritate
 - cea mai semnificativă parte
 - cu cât e mai mic numărul, cu atât e mai prioritar
- câmpul M - MAC
 - cea mai puțin semnificativă parte

În mod normal, în cazul în care n switch-uri au priorități egale, bridge rădăcină devine cel cu MAC mai mic. Dar ce mă fac dacă mai adaug un switch care întămplător are MAC mai mic (și încurcă calculele)? Soluția vine din următoarea idee: oricât ar fi MAC-ul, dacă pe acest nou switch va fi setată o prioritate mai mică ca toate celelalte, el va deveni noul bridge rădăcină⁴.

⁴indiferent cât vor fi celelalte MAC-uri

1.3.6 Adresarea de IP-uri

**172.16.0.0/16
255.255.0.0**

**172.16.20.0/24
255.255.255.0
172.16.20.1 gw
172.16.20.2 dhcp**

Figura 13:

Din cerință cunoaștem adresa de rețea pentru rețeaua intranet și masca sa (primele două linii). În continuare știm că serverul de DHCP va funcționa în VLAN-ul 20, drept urmare va fi definit în *subrețeaua 172.16.20.0*.

1.3.7 Serverul de DHCP

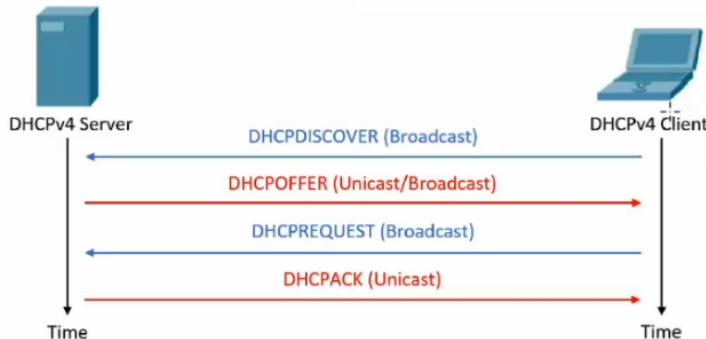


Figure 6.12 DHCP process

The previous sequence of operations can also be observed in Wireshark (Figure 6.13) when using the `ipconfig /release` and `ipconfig /renew` (on Windows OS) and `dhclient` (on Linux OS) commands:

No	Time	Source	Destination	Protocol	Length	Info
1		171.10.92.55.62	192.168.0.100	DHCP	342	DHCP Release - Transaction ID 0x9a7c44e2
2		41.17.86.198.2	0.0.0.0	DHCP	342	DHCP Discover - Transaction ID 0x31d82096
3		41.17.86.67.07	192.168.0.1	DHCP	590	DHCP Offer - Transaction ID 0x31d82096
4		41.17.86.91.87	0.0.0.0	DHCP	366	DHCP Request - Transaction ID 0x31d82096
5		42.718.38.134.2	192.168.0.1	DHCP	590	DHCP ACK - Transaction ID 0x31d82096

Figure 6.13 Wireshark capture of DHCP process

Figura 14: Prinzipiul de funcționare al unui server de DHCP

Clientul nu știe inițial nimic, nici măcar unde e serverul de DHCP. Așa că el aruncă în broadcast un mesaj standard definit de **DHCP discover**. Înapoi, serverul de DHCP îi face o **ofertă** clientului: „băi, adresa ta e asta, masca ta e asta, gateway-ul tău e asta, DNS-ul asta etc.”. Mai rămâne să se întâmpăre un handshake.

Pentru a configura un server de DHCP, trebuie să se configureze pe acesta adresa serverului în sine și adresa gateway-ului.

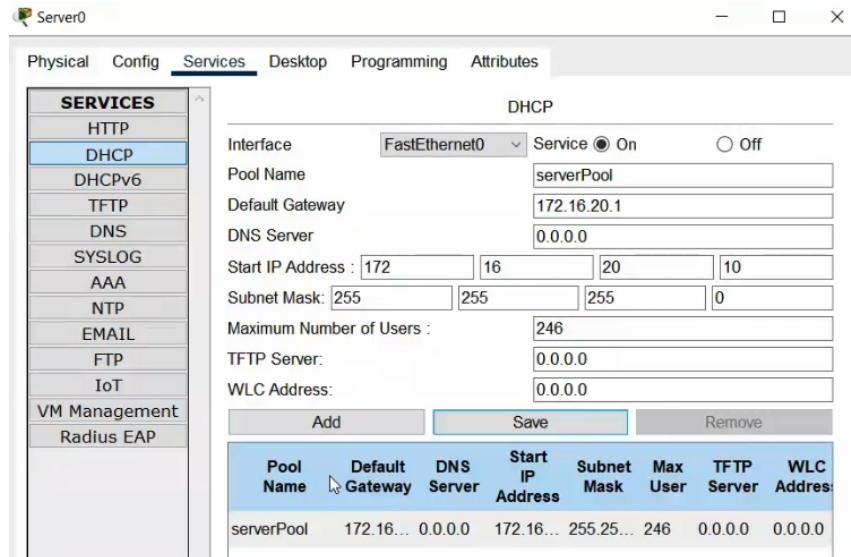


Figura 15: Configurarea serviciului de DHCP

Default gateway se setează la adresa router-ului⁵. DNS serverul este, în această etapă, încă necunoscut. Adresele de IP nu vor începe de la 1 (blocat de gateway), nici de la 2 (fiind adresa serverului DHCP), ci de la 10. Ca best practice, adresele 3-7 (sau alt număr de adrese) este lăsat liber ca, în cazul în care eu îmi doresc să setez ceva (de exemplu o imprimantă), să o pot face static.

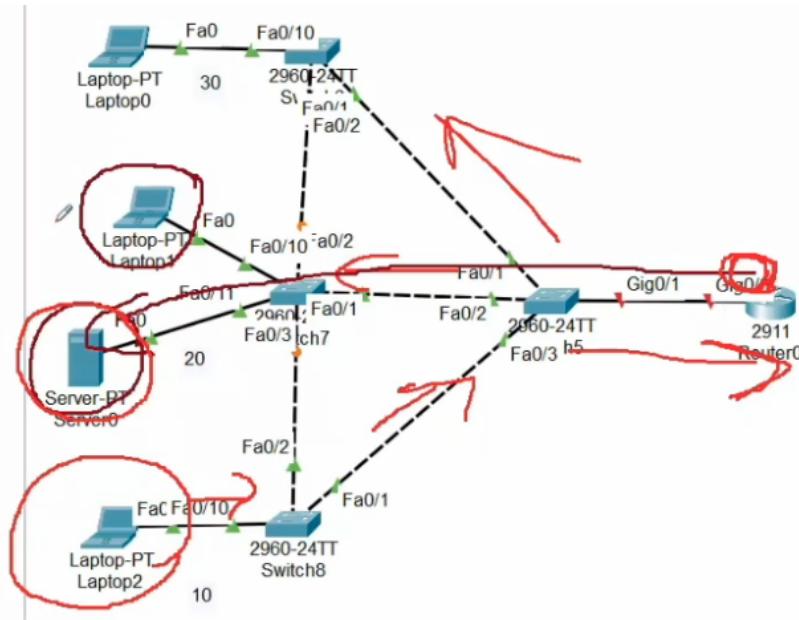


Figura 16: Cazul în care o stație din afara VLAN-ului serverului de DHCP cere o adresă IP

VLAN-ul 20 (implicit serverul de DHCP) este marcat cu maro. Oricărei stații din VLAN 20 îi este ușor să obțină o adresă IP, fiind tot acolo. Dar, în momentul în care stația din VLAN 10 (deci diferit) (marcată cu roșu) lansează un DHCP discover request⁶ care se împărtășie în toată rețea, dar doar în VLAN 10.

Pentru a adresa această problemă, fie pui câte un DHCP server în fiecare VLAN⁷, fie se folosește următoarea tehnică: în momentul în care DHCP discover loveste gateway-ul, el este redirectat către serverul respectiv. Redirectarea se face cu adresa de gateway din VLAN-ul meu, în care vreau să

⁵în cazul unui DHCP discover, stația care a lansat requestul va vedea această adresă din partea serverului de DHCP

⁶marcat de săgețile roșii

⁷e posibil să definești 4000 de VLAN-uri, ceea ce ar însemna costuri ridicate

obțin adresele (VLAN 10), așa încât serverul de DHCP să înțeleagă că trebuie să dea adrese din *pool*-ul de adrese aferente VLAN-ului 10.

```
172.16.10.0/24
172.16.10.1 gw
redirectare spre 172.16.20.2 spre DHCP
```

Figura 17: Rezumat

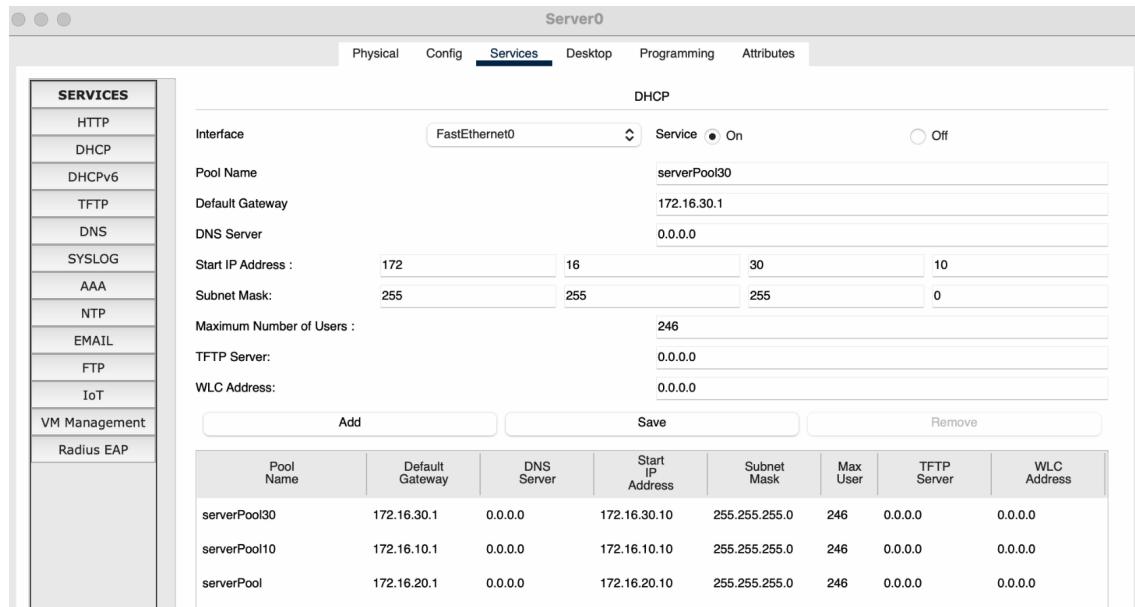


Figura 18: Cele trei pool-uri de adrese ale DHCP server, pentru VLAN 10, VLAN 20 și VLAN 30

Această configurare se face pe routerul principal. Se definește adițional un `ip address-helper` 172.16.20.2, adică adresa serverului de DHCP, pentru fiecare interfață, așa încât la orice DHCP Discover request să știe routerul unde să reruteze cererea (8).

2 Etapa 2 - Adăugarea zonei demilitarizate (DMZ)

2.1 Layout

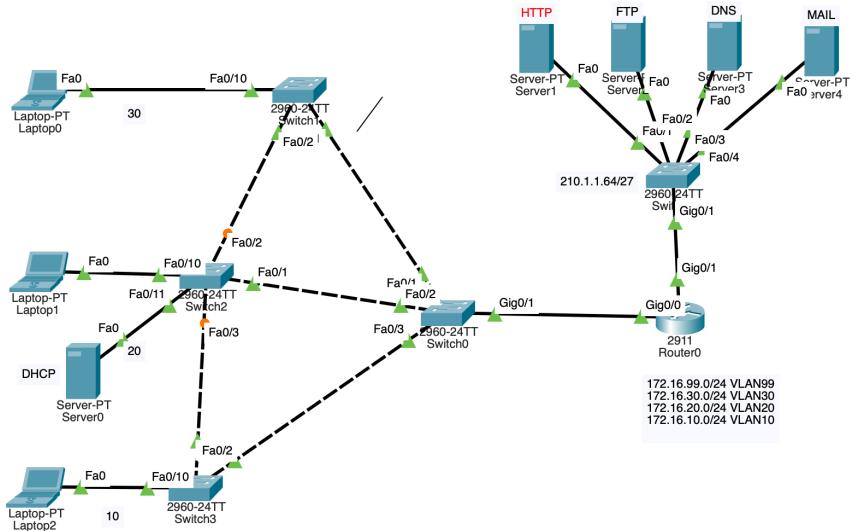


Figura 19: La finalul configurărilor, fiecare stație poate vorbi cu orice altă stație, fie că e din rețeaua locală, fie că e din DMZ

2.2 Comenzi

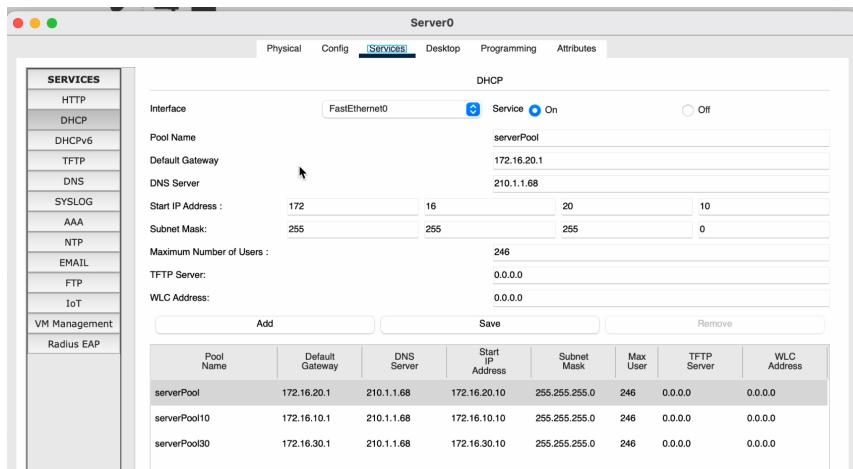


Figura 20: Configurarea switch-ului din DMZ

```

DMZ(config)#int ra gi 0/1-2
DMZ(config-if-range)#sw mo acc
DMZ(config-if-range)#sw acc vlan 2
DMZ(config-if-range)#do show vlan

VLAN Name          Status    Ports
----- 
1     default      active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
2     DMZ          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
1002 fddi-default   active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default   active

```

Figura 21: Efectul 20: toate interfețele selectate se mută în VLAN-ul DMZ

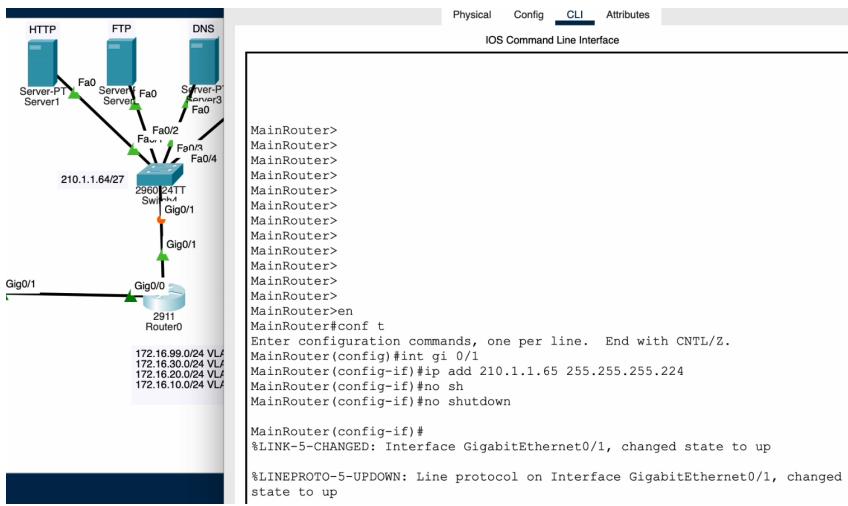


Figura 22: Enter Caption

2.3 Memoriu tehnic

2.3.1 Hop-by-hop routing

Spre deosebire de rutarea de la sursă⁸, hop-by-hop routing este un procedeu de rutare ad-hoc. Fiecare router are propria sa tabelă de rutare și decide către ce router să dea mai departe pachetul transmis, până când IP-ul destinație match-uește cu stația la care a ajuns.

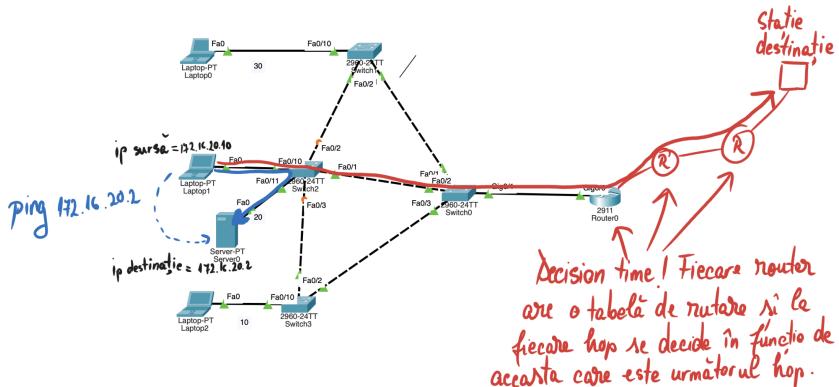


Figura 23: Rutare hop-by-hop

```

MainRouter#sh ip route
Codes: L - local, C - connected, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

172.16.0.0/16 is variably subnetted, 8 subnets, 2 masks
C   172.16.10.0/24 is directly connected, GigabitEthernet0/0.10
L   172.16.10.1/32 is directly connected, GigabitEthernet0/0.10
C   172.16.20.0/24 is directly connected, GigabitEthernet0/0.20
L   172.16.20.1/32 is directly connected, GigabitEthernet0/0.20
C   172.16.30.0/24 is directly connected, GigabitEthernet0/0.30
L   172.16.30.1/32 is directly connected, GigabitEthernet0/0.30
C   172.16.99.0/24 is directly connected, GigabitEthernet0/0.99
L   172.16.99.1/32 is directly connected, GigabitEthernet0/0.99

```

Figura 24: Tabela de rutare pentru MainSwitch, cu `sh ip route`

⁸Exemplul clasic este cel al GPS-urilor care de la sursă configuraază un traseu complet către destinație

2.3.2 Zona demilitarizată - DMZ

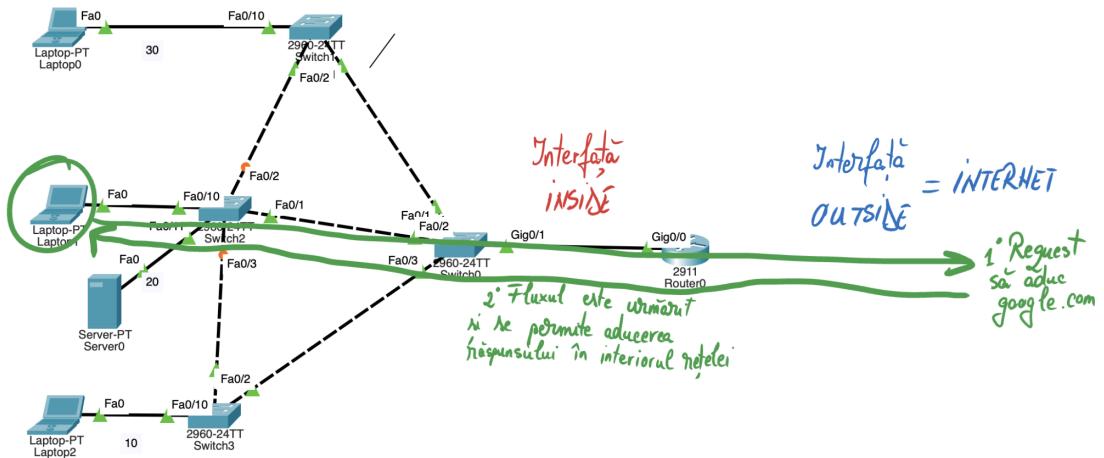


Figura 25: O stație încearcă să acceseze din interior internetul

Situația se schimbă în cazul unui request inițiat din exterior. Pe principala poartă de acces în rețea, adică pe gateway, se configurează un **firewall**. Acest gen de protecție este foarte bun pentru securitate, însă foarte prost pentru business⁹. Astfel apare necesitatea existenței unei zone demilitarizate - DMZ.

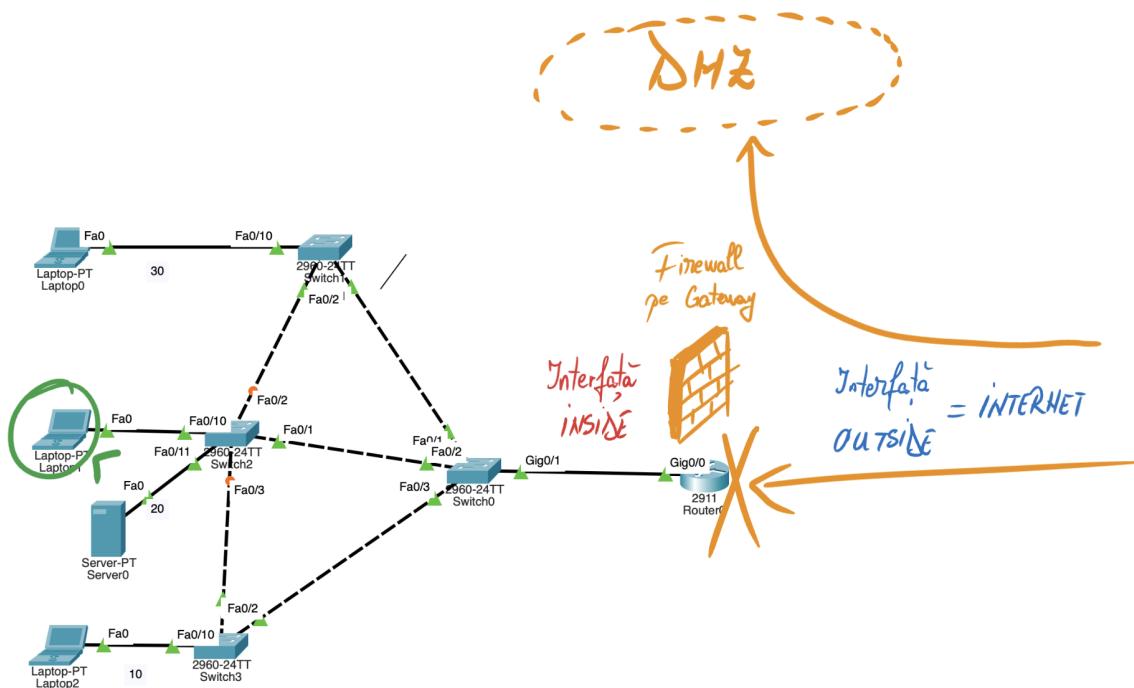


Figura 26: Requestul inițiat din exterior este blocat de către firewall-ul rețelei

⁹De exemplu un server de mail poate exista aici, aşa încât atunci când angajatul este acasă (home office), să poată să citească

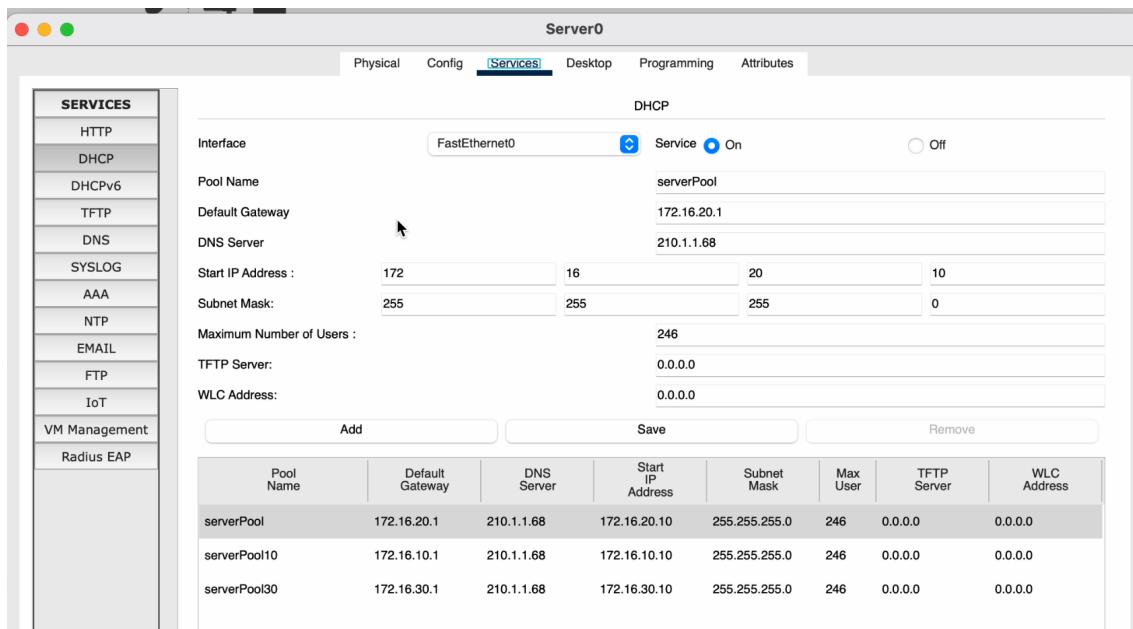


Figura 27: Pe serverul de DHCP se actualizează adresa DNS server pentru fiecare pool, acum fiind cunoscută