Lucrarea de laborator №6

Configurarea serverelor NAT, DHCP, DNS şi Email

Scopul lucrării constă în formarea abilităţilor practice de configurare în Cisco Packet Tracer a serverelor NAT, DHCP, DNS şi Email

Obiective:

- A explica conceptul de NAT şi a ilustra în Cisco Packet Tracer modul de funcţionare al acestuia
- A arăta cum se configurează NAT pe routerele de frontieră din reţelele locale
- A arăta cum se configurează pe server şi pe router protocolul DHCP pentru distribuirea automatizată a datelor IP host-urilor din reţeaua locală
- A arăta cum se configurează serverul DNS pentru a transla numele de domeniu în adresa IP corespunzătoare
- A arăta cum se configurează serverul de email prin intermediul căruia utilizatorii reţelei îşi pot transmite mesaje de e-mail

Indicaţii metodice privind realizarea lucrării

Configurarea routerului NAT

NAT (Network Address Translation) – translarea adreselor de reţea

NAT -> are ca obiectiv să ascundă adresele din interiorul reţelei locale de dispozitivele din exterior. Tehnologia este bazată pe înlocuirea adresei private a host-ului sursă, la ieşirea din reţeaua locală, cu o adresă publică. Soft-ul NAT este configurat pe routerul de frontieră, care separă reţeaua locală de reţeaua din exteriorul acesteia.

Vom explica modul de funcţionare al tehnologiei NAT pe exemplul următoarei configuraţii de reţea (a se vedea Figura 1):

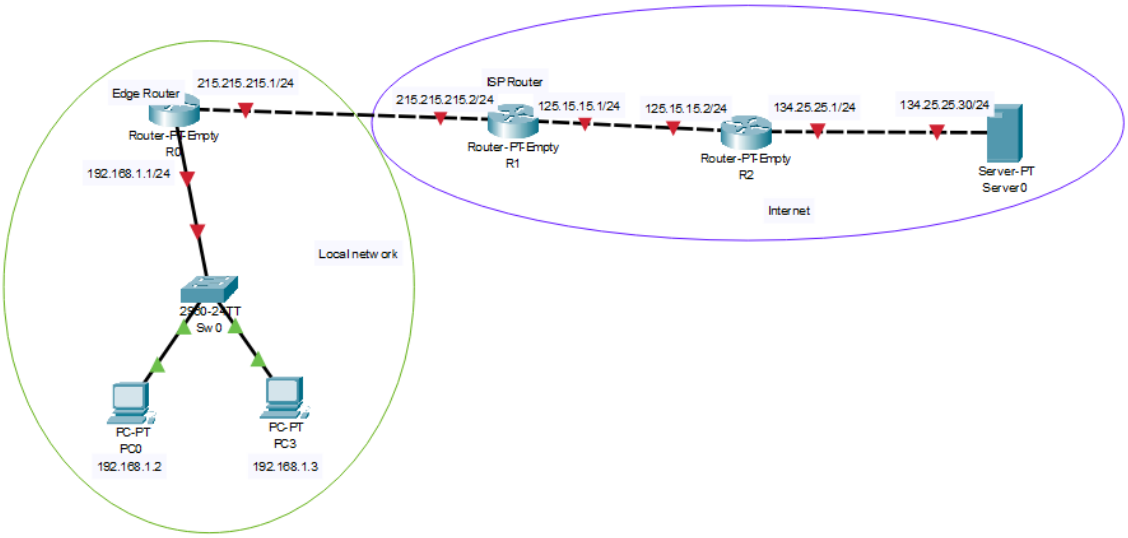


Figura 1

1) Setăm adrese IP pe interfeţele routerelor şi pe host-uri:

`Router>en`
`Router#conf ter`
`Router(config)#host R0`
`R0(config)#int fa 9/0`
`R0(config-if)#ip add 192.168.1.1 255.255.255.0`
`R0(config-if)#no sh`
`R0(config)#int fa 8/0`
`R0(config-if)#ip add 215.215.215.1 255.255.255.0`
`R0(config-if)#no sh`
`R0(config-if)#exit`
	`Router>en`
	`Router#conf ter`
	`Router(config)#host R1`
	`R1(config)#int fa 8/0`
	`R1(config-if)#ip add 215.215.215.2 255.255.255.0`
	`R1(config-if)#no sh`
	`R1(config-if)#exit`
	`R1(config)#int fa 9/0`
	`R1(config-if)#ip add 125.15.15.1 255.255.255.0`
	`R1(config-if)#no sh`
	`R1(config-if)#exit`
	`R1(config)#do wr`

`Router>en`
`Router#conf ter`
`Router(config)#host R2`
	`Server0:`
	`IP Address: 134.25.25.30`
	`Subnet Mask: 255.255.255.0`

```
R2(config)#int fa 8/0
R2(config-if)#ip add 125.15.15.2 255.255.255.0
R2(config-if)#no sh
R2(config-if)#exit
R2(config)#int fa 9/0
R2(config-if)#ip add 134.25.25.1 255.255.255.0
R2(config-if)#no sh
R2(config-if)#exit
R2(config)#do wr
```

```
Default Gateway: 134.25.25.1

PC0:
IP Address: 192.168.1.2
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.1

PC3:
IP Address: 192.168.1.3
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.1
```

2) Configurăm rutarea:

```
R0(config)#ip route 0.0.0.0 0.0.0.0 215.215.215.2   // rută statică implicită
R0(config)#do wr

R1(config)#ip route 134.25.25.0 255.255.255.0 125.15.15.2  // rută statică
R1(config)#do wr

R2(config)#ip route 215.215.215.0 255.255.255.0 125.15.15.1 // rută statică
R2(config)#do wr
```

3) Despre adresele IP private şi publice:

Adresele IP private – nu sunt rutate în Internet

Trei intervale de adrese IP private:

10.0.0.0/8 (adică adresele cu primul octet 10)

172.16.0.0/12 (adică adresele de la 172.16.0.0 până la 172.31.255.255 inclusiv)

192.168.0.0/16 (adică adresele de la 192.168.0.0 până la 192.168.255.255 inclusiv)

Exemple de adrese IP publice – care pot fi rutate în Internet

178.217.16.246	217.69.139.200	78.110.50.125	81.192.76.172

În reţelele locale (organizaţii) host-urilor li se atribuie adrese IP private. Dar atunci când este necesar ca un host cu o adresă privată să acceseze Internet – adresa sa privată este înlocuită cu o adresă publică prin mecanismul numit NAT.

În diferite organizaţii, de regulă sunt reţele cu aceleaşi adrese private, de exemplu, 192.168.x.x. Iar dacă este necesar de ieşit în exterior – adresa privată este translată într-o adresă publică, care va putea fi rutată.

În loc să se repartizeze adrese publice către host-uri – PC0, PC1, ..., se repartizează o singură adresă publică, care este setată pe interfaţa de ieşire a routerului de frontieră (de exemplu, 215.215.215.1). Serverul cu adresa 134.25.25.30 îi va răspunde pe această adresă publică routerului de frontieră, iar NAT-ul ce funcţionează pe router va decide cărui host anume din interiorul reţelei îi este destinat pachetul recepţionat.

Nu am setat pe routerele R1 şi R2 cum se poate ajunge până la reţeaua 192.168.1.0, deoarece aceasta este o reţea locală, iar în tabelul de rutare al routerelor R1 şi R2 nu sunt adrese IP private (amintim că reţeaua 192.168.1.0 există în reţelele locale ale unui număr enorm de organizaţii => nu are sens să se stocheze adrese private în tabelul de rutare)

În modul Simulation de pe host-ul PC0 dăm un ping (vom lăsa să fie văzute doar pachetele ICMP): ping 134.25.25.30 => pachetul ajunge până la Server0, dar nu poate ajunge înapoi, deoarece în tabelul de rutare al lui R2 nu există IP adresa 192.168.1.2

În acest moment se dovedeşte a fi util conceptul de NAT:

NAT-ul static (Static NAT) – translarea unei adrese IP private într-o adresă adresă IP publică. Fiecărui host cu adresa privată îi corespunde o adresă publică pentru ieşire în exterior

NAT-ul dinamic (Dynamic NAT) – translarea mai multor adrese IP private în mai multe adrese IP publice. Fiecărui dispozitiv din reţeaua locală i se atribuie o adresă publică (din setul disponibil) la ieşire în exterior

NAT cu supraîncărcare (numit şi PAT, NAPT, NAT Overload) – translarea mai multor adrese IP private în aceeaşi adresă IP publică, dar cu implicarea numerelor de port (sau a numerelor de secvenţă)

Static NAT:

R0(config)#	int fa 9/0	Este accesată interfaţa fast ethernet 9/0
R0(config-if)#	ip nat inside	Se stabileşte interfaţa fa9/0 ca de interior (reţeaua locală) din punct

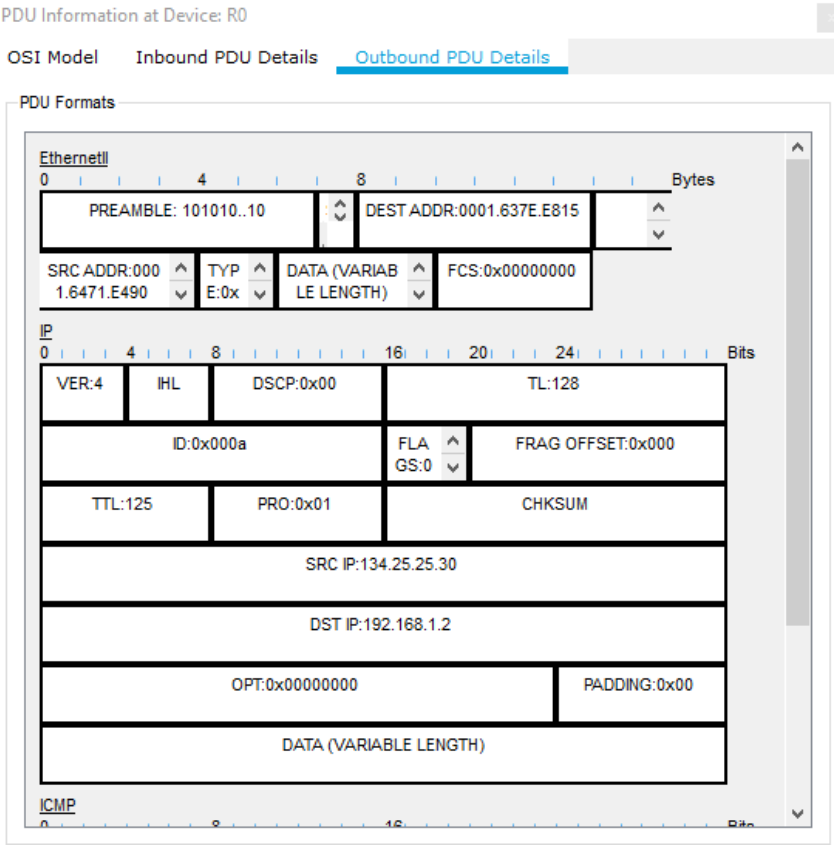
		de vedere NAT
R0(config)#	int fa 8/0	Este accesată interfața fast ethernet 8/0
R0(config-if)#	ip nat outside	Se stabilește interfața fa8/0 ca de exterior (Internet)
R0(config)#	ip nat inside source static 192.168.1.2 215.215.215.20 (se consideră că provider-ul a repartizat acest IP, dar se poate de folosit adresa IP 215.215.215.1 a interfeței)	Se activează NAT-ul static. IP adresa 192.168.1.2 se va translata în 215.215.215.20

De pe host-ul PC0: ping 134.25.25.30 – este conexiune
De ce este conexiune? Trecem în modul Simulation şi lăsăm să treacă doar pachetele ICMP. Dăm în execuţie:

ping 134.25.25.30

Examinăm conţinutul pachetului care a ajuns la switch-ul Sw0. Vedem acolo că:
SRC IP (sursa): 192.168.1.2
DST IP (destinaţia): 134.25.25.30

La ieşirea din routerul R0, pe care este activat NAT avem SRC IP: 215.215.215.20 (adresa 192.168.1.2 este înlocuită cu una publică)
Când pachetul trece în sens invers:
Mai întâi DST IP: 215.215.215.20
Însă pe routerul R0 (NAT): DST IP: 192.168.1.2



Pe router se poate vedea procesul de translatare prin comanda: *show ip nat translations*

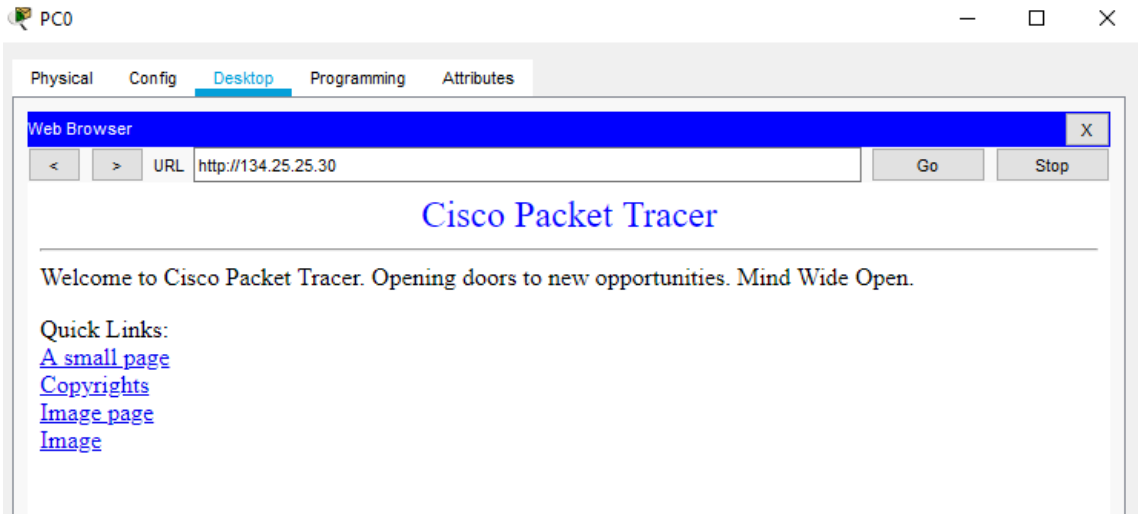
```
R0(config)#do show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 215.215.215.20:13 192.168.1.2:13     134.25.25.30:13    134.25.25.30:13
icmp 215.215.215.20:14 192.168.1.2:14     134.25.25.30:14    134.25.25.30:14
icmp 215.215.215.20:15 192.168.1.2:15     134.25.25.30:15    134.25.25.30:15
icmp 215.215.215.20:16 192.168.1.2:16     134.25.25.30:16    134.25.25.30:16
---  215.215.215.20    192.168.1.2        ---                ---
```

Inside local => IP adresa din reţeaua locală, adresă ce este înlocuită
Inside global => IP adresă prin care se înlocuieşte
Outside local & Outside global => coincid => IP adresa destinaţiei

Înregistrarea cu procesul de translare este stocată o perioadă limitată de timp. Dacă peste ceva timp vom da din nou comanda *show ip nat translations*, atunci nu vom mai vedea întregul tabel ca mai sus (ci doar ceea ce am definit prin intermediul comenzilor)

```
R0#show ip nat tran
Pro  Inside global     Inside local       Outside local      Outside global
---  215.215.215.20    192.168.1.2        ---                ---
```

Dacă din nou dăm un ping, vor apărea date noi despre procesul de translatare
Atunci când dăm în execuţie comanda *ping*, tabelul de translatare arată pachetele ICMP corespunzătoare
Atunci când pe host-ul PC0 accesăm Web Server (pe PC0 în Desktop alegem Web Browser şi scriem adresa 134.25.25.30) => arată pachete *tcp*:




```
R0#show ip nat tran
Pro  Inside global     Inside local       Outside local      Outside global
---  215.215.215.20    192.168.1.2        ---                ---
tcp 215.215.215.20:1025192.168.1.2:1025   134.25.25.30:80    134.25.25.30:80
```

Pentru a elibera (a şterge toate datele) tabelul de translatare dăm comanda: *clear ip nat translation **
Dacă dăm de pe host-ul PC3 comanda ping 134.25.25.30 => vom vedea că nu trece
Asta deoarece anterior am definit doar regula de translatare: 192.168.1.2 este înlocuit prin 215.215.215.20
În cazul dat avem 192.168.1.3! => este necesar de definit o nouă regulă de translatare, dar pentru aceasta se va utiliza o altă adresă publică (dacă se aplică NAT-ul static!). De exemplu, dacă provider-ul a oferit o a doua adresă publică 215.215.215.21 pentru ieşire în Internet
Pe routerul R0 dăm comanda: *ip nat inside source static 192.168.1.3 215.215.215.21*
De pe PC3 dăm comanda: *ping 134.25.25.30* => deja trece!
Adresa IP privată se va înlocui prin adresa publică 215.215.215.21
În modul Simulation cum se deplasează pachetele (de la PC0 şi PC3)
În sens invers, dacă serverul va transmite un mesaj de răspuns către PC0, atunci acesta (serverul) va utiliza adresa 215.215.215.20
Dacă serverul va transmite un răspuns către PC3, atunci va utiliza adresa publică 215.215.215.21
Fiecare adresă privată este translatată într-o adresă IP publică
Mecanismul NAT în forma examinată nu este aplicat, deoarece acesta nu face economie de adrese publice utilizate. Se ştie că numărul de adrese IPv4 publice este aproape epuizat.
Dynamic NAT:
Translarea mai multor adrese IP private în mai multe adrese IP publice
Mai întâi, pe routerul R0 se va dezactiva Static NAT pe care l-am activat anterior (vom folosi aceeaşi configuraţie):

```
R0(config)# no ip nat inside source static 192.168.1.2 215.215.215.20
R0(config)# no ip nat inside source static 192.168.1.3 215.215.215.21
```

Vom considera că provider-ul a distribuit reţelei un set (un stoc) de adrese IP publice 215.215.215.20 – 215.215.215.30. În continuare, vom configura NAT-ul dinamic:

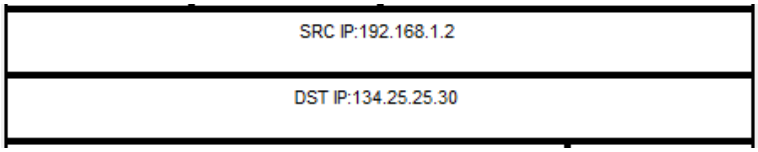
`R0(config)#`	`int fa9/0`	Accesăm interfaţa fast ethernet 9/0

R0(config-if)#	ip nat inside	Stabilim interfaţa fa9/0 ca de interior (reţeaua locală)
R0(config)#	int fa8/0	Accesăm interfaţa fast ethernet 8/0
R0(config-if)#	ip nat outside	Stabilim interfaţa fa8/0 ca de exterior (Internet)
R0(config)#	access-list 1 permit 192.168.1.0 0.0.0.255	Generăm o listă de acces standard ACL, care va arăta intervalul de adrese private cărora li se va permite să fie translatate în adrese publice pentru ieşire în exterior. (Atenţie! Adresele private care nu au nimerit în listă – nu vor fi translatate!)
R0(config)#	ip nat pool TRANS 215.215.215.20 215.215.215.30 netmask 255.255.255.0	Creăm set-ul de adrese IP cu numele TRANS. Aceste adrese IP vor înlocui pe cele private din lista de acces 1. În acest caz, adresele IP private vor fi translatate în adrese publice, începând cu 215.215.215.20 până la 215.215.215.30
R0(config)#	ip nat inside source list 1 pool TRANS	Activăm NAT-ul dinamic, unde list 1 – intervalul de adrese private, pool TRANS – intervalul de adrese IP publice

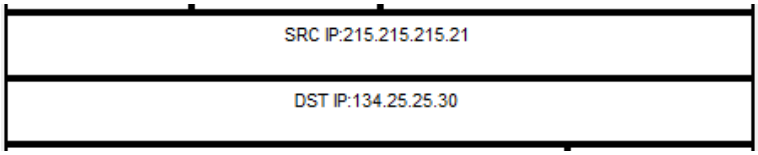
Dacă este necesar să se definească mai multe reţele cărora li se va permite ieşirea în exteriorul reţelei locale, atunci la definirea listei de acces vom aplica o construcţie de genul:

```
Router(config)#ip access-list standard For-Nat
Router(config-std-nacl)#permit 192.168.2.0 0.0.0.255
Router(config-std-nacl)#permit 192.168.3.0 0.0.0.255
Router(config-std-nacl)#permit 192.168.4.0 0.0.0.255
Router(config-std-nacl)#exit
```

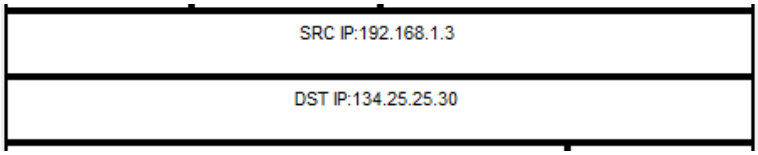
De pe PC0: ping 134.25.25.30 – este conexiune
De pe PC3: ping 134.25.25.30 – este conexiune
Trecem în modul Simulation:
De pe PC0: ping 134.25.25.30 => pe routerul R0 vedem:
La intrare:



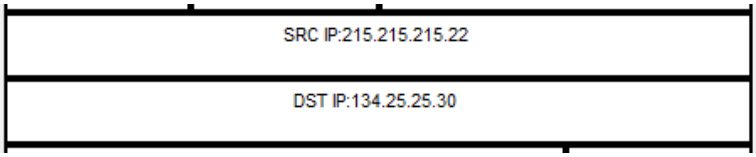
La ieşire:



De pe PC3: ping 134.25.25.30 => pe routerul R0 vedem:
La intrare:



La ieşire:



Dacă PC0 nu se va adresa ceva timp în Internet, atunci IP-ul 215.215.215.21 se va elibera.

Comanda
show ip nat translations – permite să vedem tabelul de translatare

```
R0(config)#do show ip nat tr
Pro  Inside global     Inside local       Outside local      Outside global
icmp 215.215.215.21:10 192.168.1.2:10     134.25.25.30:10    134.25.25.30:10
icmp 215.215.215.21:11 192.168.1.2:11     134.25.25.30:11    134.25.25.30:11
icmp 215.215.215.21:12 192.168.1.2:12     134.25.25.30:12    134.25.25.30:12
icmp 215.215.215.21:9  192.168.1.2:9      134.25.25.30:9     134.25.25.30:9
icmp 215.215.215.22:5  192.168.1.3:5      134.25.25.30:5     134.25.25.30:5
```

show ip nat statistics – permite să vedem o statistică a procesului de translatare

```
R0(config)#do show ip nat stat
Total translations: 5 (0 static, 5 dynamic, 5 extended)
Outside Interfaces: FastEthernet8/0
Inside Interfaces: FastEthernet9/0
Hits: 11  Misses: 17
Expired translations: 12
Dynamic mappings:
-- Inside Source
access-list 1 pool TRANS refCount 5
 pool TRANS: netmask 255.255.255.0
       start 215.215.215.20 end 215.215.215.30
       type generic, total addresses 11 , allocated 2 (18%), misses 0
```

Static NAT – am indicat manual pentru fiecare adresă IP privată o adresă IP publică concretă
Dynamic NAT – la fel, dar în mod dinamic – se indică un set de adrese IP private şi un set de adrese Ip publice, iar routerul NAT în mod automatizat decide care va fi corespondenţa între adrese
Host-ul ce nu mai are nevoie de Internet – eliberează acea IP adresă, care este atribuită ulterior unui alt host
Oricum, în acest mod nu se contribuie nicidecum la minimizarea numărului de IP adrese publice utilizate pentru ieşire în Internet
În forma descrisă Static NAT şi Dynamic NAT nu sunt aplicate

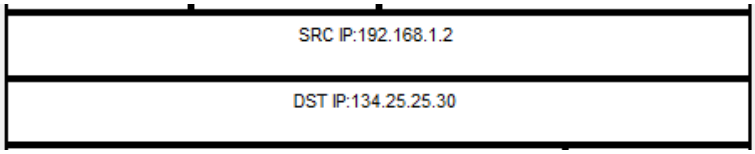
NAT-ul cu supraîncărcare (PAT, NAPT, NAT Overload)
NAT-ul overload – translatarea mai multor adrese IP private într-o adresă IP publică => procedeul este aplicat actualmente pe routere în reţele
Pentru a ieşi în Internet, toate host-urile din cadrul organizaţiei folosesc aceeaşi adresă IP publică, dar pentru a determina sursa căreia i se răspunde din exterior, se aplică mecanismul numerelor de port (sau a numerelor de secvenţă – sequence number)
Fie că provider-ul a distribuit pentru translatarea adreselor private din reţeaua locală a organizaţiei adresa publică 215.215.215.20
Trecem la configurarea PAT (Port Address Translation):
Mai întâi anulăm configurările precedente ale NAT-ului dinamic:

```
R0(config)# no ip nat inside source list 1 pool TRANS
R0(config)# no ip nat pool TRANS 215.215.215.20 215.215.215.30 netmask 255.255.255.0
R0(config)# no access-list 1 permit 192.168.1.0 0.0.0.255
```

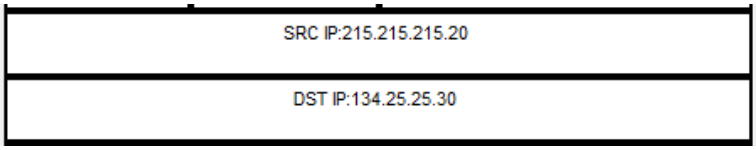
R0(config)#	int fa9/0	Accesăm interfaţa fast ethernet 9/0
R0(config-if)#	ip nat inside	Stabilim interfaţa fa9/0 ca de interior (reţeaua locală)
R0(config)#	int fa8/0	Accesăm interfaţa fast ethernet 8/0
R0(config-if)#	ip nat outside	Stabilim interfaţa fa8/0 ca de exterior (Internet)
R0(config)#	access-list 1 permit 192.168.1.0 0.0.0.255	Se indică set-ul de adrese private, care vor fi translatate (Atenţie! Adresele private ce nu vor fi incluse în listă – nu vor fi translatate!)
R0(config)#	ip nat pool TRANS 215.215.215.20 215.215.215.20 netmask 255.255.255.0	Se indică adresa IP publică în care vor fi translatate adresele private din reţeaua locală

R0(config)#	ip nat inside source list 1 pool TRANS overload	Se activează PAT, unde list 1 – intervalul de adrese IP private, pool TRANS – intervalul de adrese IP publice

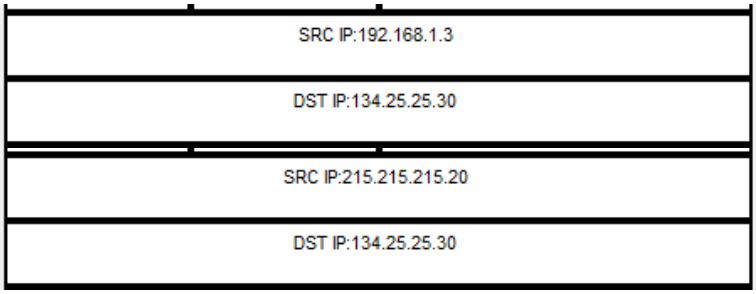
De pe PC0: ping 134.25.25.30 => este conexiune
De pe PC3: ping 134.25.25.30 => este conexiune
În modul Simulation lăsăm să treacă doar pachetele ICMP (apăsăm *Show All/None*, după care pe *Edit Filters* şi punem bifa la *ICMP*). Dăm un ping de pe PC0 şi de pe PC3 (simultan) către serverul cu adresa IP 134.25.25.30:
Atunci când pachetele pe rând vor ajunge până la routerul R0, vom vedea că R0 a translatat adresele IP ale lui PC0 şi PC3 în aceeaşi adresă IP publică 215.215.215.20:
La intrarea în R0 avem



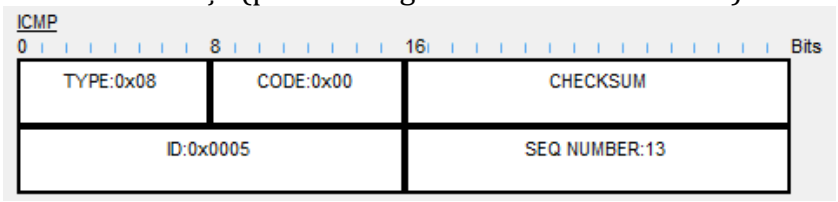
iar la ieşire



La fel



Întrebare: atunci când serverul transmite mesajul de răspuns către sursă, cum determină routerul NAT cu ce adresă privată trebuie să înlocuiască adresa publică indicată?
Server0 transmite toate pachetele la o singură adresă - 215.215.215.20. Nu e clar care pachet este destinat către 192.168.1.2 şi care către 192.168.1.3? În acest caz, routerul NAT stabileşte destinaţia pachetului după numărul de secvenţă (pe care l-a generat host-ul din start):

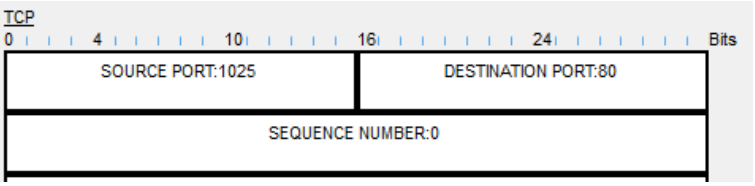


Host-ul PC0 a generat numărul 13. Dacă pachetele ce au fost transmise anterior nu au utilizat acest număr, atunci pachetul este transmis mai departe fără modificări şi ajunge la server. Serverul transmite un mesaj de răspuns, incluzând acest număr în acel mesaj. Pachetul de răspuns de la server ajunge la routerul NAT R0, care în baza acestui număr determină în tabelul său de translatare linia corespunzătoare (a se vedea Figura 2), unde găseşte adresa IP a host-ului din reţeaua locală, căruia îi şi transmite pachetul.

```
R0(config)#do show ip nat tr
Pro  Inside global     Inside local       Outside local      Outside global
icmp 215.215.215.20:10 192.168.1.2:10     134.25.25.30:10    134.25.25.30:10
icmp 215.215.215.20:11 192.168.1.2:11     134.25.25.30:11    134.25.25.30:11
icmp 215.215.215.20:12 192.168.1.2:12     134.25.25.30:12    134.25.25.30:12
icmp 215.215.215.20:13 192.168.1.2:13     134.25.25.30:13    134.25.25.30:13
icmp 215.215.215.20:5  192.168.1.2:5      134.25.25.30:5     134.25.25.30:5
icmp 215.215.215.20:6  192.168.1.2:6      134.25.25.30:6     134.25.25.30:6
icmp 215.215.215.20:7  192.168.1.2:7      134.25.25.30:7     134.25.25.30:7
icmp 215.215.215.20:8  192.168.1.2:8      134.25.25.30:8     134.25.25.30:8
icmp 215.215.215.20:9  192.168.1.2:9      134.25.25.30:9     134.25.25.30:9
```

Figura 2

Dacă ne adresăm la server de pe host-ul PC0 ca la web browser:
Apăsăm pe PC0, apoi pe Web Browser şi culegem adresa 134.25.25.30, apoi trecem în modul Simulation, lăsând să treacă doar pachetele TCP. În Web Browser apăsăm butonul *Go* şi analizăm cum trece pachetul. Se poate vedea că translatarea adresei are loc în baza numărului de port (Source Port), pe care host-ul îl generează în mod aleator.



Atunci când pachetele de la PC0 şi PC3 trec prin R0 către server, atunci routerul R0 înregistrează care adresă IP privată şi de sub care port se adresează la serverul web.
Serverul răspunde cu un pachet ce conţine acel număr de port ca destinaţie (a se vedea Figura 3)

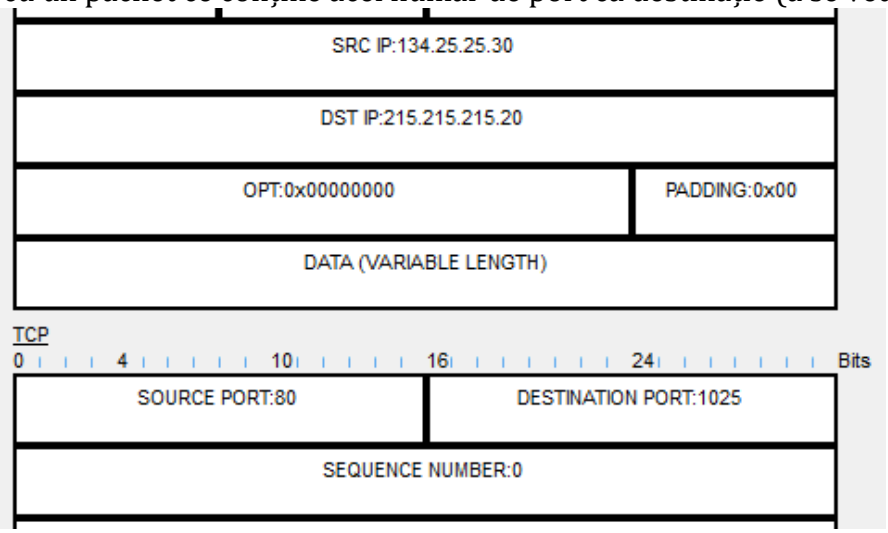


Figura 3

Routerul R0 în baza numărului de port destinaţie recepţionat găseşte în tabelul său de translatare IP-ul host-ului corespunzător (PC0 sau PC3).
Ştergem conţinutul tabelului de translatare dinamică prin comanda: *clear ip nat tr ** (configurările nu sunt şterse)
Ce se întâmplă dacă PC0 şi PC3 se vor adresa la server cu acelaşi număr de port? De exemplu, PC0 şi PC3 au generat acelaşi număr de port 1025. Putem modela o astfel de situaţie cu ajutorul instrumentului Traffic Generator (Generatorul de trafic).
Trecem în modul Simulation. Lăsăm să treacă doar pachetele TCP şi UDP
Pe PC0 apăsăm pe butonul Traffic Generator şi completăm cu următoarele date:
Select Applications: alegem OTHER
Destination IP Address: 134.25.25.30
Source IP Address: 192.168.1.2
Starting Source Port: 1025
Destination Port: 80
Jos apăsăm pe butonul Send
Pe PC3 apăsăm pe Traffic Generator şi completăm cu următoarele date:
Select Applications: alegem OTHER
Destination IP Address: 134.25.25.30
Source IP Address: 192.168.1.3
Starting Source Port: 1025
Destination Port: 80
Jos apăsăm pe butonul Send
Urmărim cum trec pachetele. Când pe routerul R0 a ajuns primul pachet (de la PC0), în linia de comandă a lui R0 scriem *do show ip nat tr*:

```
R0(config)#do show ip nat tr
Pro  Inside global     Inside local       Outside local      Outside global
udp 215.215.215.20:1025192.168.1.2:1025   134.25.25.30:80    134.25.25.30:80
```

Atunci când la routerul R0 ajunge al doilea pachet (de la PC3), în linia de comandă a lui R0 scriem *do show ip nat tr*:

```
R0(config)#do show ip nat tr
Pro  Inside global     Inside local       Outside local      Outside global
udp 215.215.215.20:1024192.168.1.3:1025   134.25.25.30:80    134.25.25.30:80
udp 215.215.215.20:1025192.168.1.2:1025   134.25.25.30:80    134.25.25.30:80
```

Vedem că routerul a înlocuit nu doar adresa IP a sursei, dar şi numărul de port corespunzător (deoarece acesta coincide cu precedentul). În Internet pachetele pleacă cu numere de port diferite. Atunci când pachetul se întoarce de la server înapoi la routerul R0, atunci R0 va şti că dacă numărul de port este 1024, atunci adresa IP se va înlocui cu 192.168.1.3 şi portul 1025.
Dacă două host-uri se adresează la aceeaşi adresă de IP, în acelaşi timp, cu numere de port identice, atunci se înlocuieşte nu doar IP-ul iniţial, dar şi portul iniţial.

Protocolul DHCP (Dynamic Host Configuration Protocol) – protocolul de configurare dinamică a host-ului => permite host-urilor din reţea să obţină şi să seteze în mod automatizat o IP adresă
Dacă se vor atribui în mod manual IP adrese host-urilor, atunci administratorul reţelei va trebui să formeze manual şi să întreţină o bază de date cu aceste adrese, ceea ce poate fi un lucru migălos
De ce DHCP nu este numit protocol de stabilire automatizată a IP adresei? Deoarece DHCP distribuie (şi atribuie) nu doar IP adresa, ci şi masca de subreţea, adresa routerului implicit, adresa serverului DNS şi alte date.
Protocolul DHCP poate fi configurat atât pe un server dedicat, cât şi pe un router din reţea
În continuare, examinăm cum se efectuează configurarea serverului DHCP pe dispozitive Cisco (server dedicat sau router), folosind Cisco Packet Tracer

1. Cazul în care clientul DHCP se află în acelaşi domeniu broadcast ca şi serverul DHCP

Să considerăm o configuraţie de reţea formată din 2 host-uri, 1 switch şi 1 server, care va îndeplini rolul de DHCP server (a se vedea Figura 4)

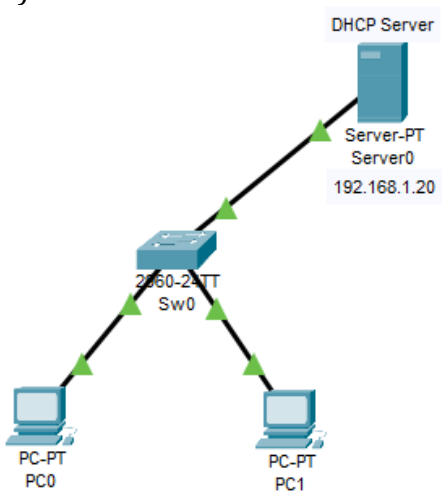


Figura 4

Deoarece un server DHCP nu poate să-şi atribuie IP adresă, o vom atribui manual acestuia şi anume IP adresa 192.168.1.20 şi masca de subreţea 255.255.255.0.
Dăm un click pe serverul DHCP, apoi pe tab-ul Services şi pe butonul DHCP (amplasat pe stânga), după care bifăm pe *On* pe lângă *Service* (a se vedea Figura 5).

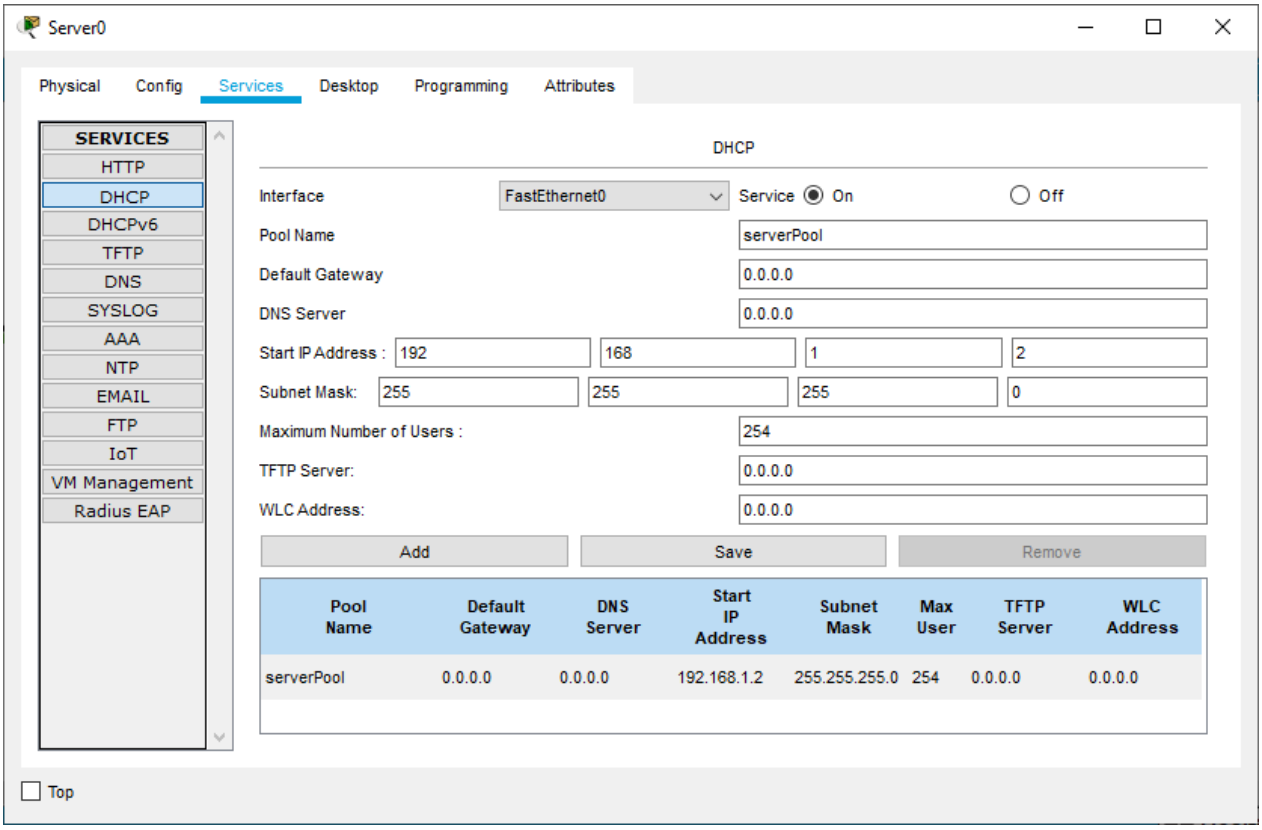


Figura 5

Indicăm intervalul din care se vor distribui IP adrese:

Start IP Address: 192.168.1.2

Subnet Mask: 255.255.255.0

La moment, nu vom indica valori pentru *Default Gateway* şi *DNS Server*

Apăsăm butonul *Save*

Mai jos în Figura 5 se vede că host-uri cu masca indicată pot fi maxim 254

În lucrările precedente pe host-uri completam manual IP Address, Subnet Mask şi Default Gateway. Acum pe *PC0 -> Desktop -> IP Configuration* punem bifa la DHCP. Peste un interval relative mic de timp host-ul PC0 va obţine IP adresa 192.168.1.2 şi masca de subreţea 255.255.255.0. Nu au fost atribuite valori pentru Default Gateway şi DNS deoarece acestea nu au fost configurate pe serverul DHCP. Să setăm pe serverul DHCP (Server0) valoarea Default Gateway la 192.168.1.1 (DNS îl vom atribui mai târziu) => Save. După aceasta, încă o dată bifăm la DHCP pe hostul PC0 => în mod automatizat vom obţine şi Default Gateway 192.168.1.1.

În mod analog se obţin valori pentru IP Address, Subnet Mask şi Default Gateway pe host-ul PC1.

Vom explica cum are loc stabilirea datelor IP prin protocolul DHCP:

Host-ul care solicită o IP adresă, încearcă să afle locaţia serverului DHCP. Pentru aceasta, host-ul formează un mesaj DHCP Discover (Identificare DHCP), care este transmis către toate dispozitivele din limitele domeniului broadcast. După ce serverul DHCP a recepţionat acest mesaj, serverul caută în baza sa cu adrese IP dacă sunt disponibile adrese IP. Dacă da, serverul DHCP selectează o adresă IP şi formează mesajul DHCP Offer (Oferta DHCP), pe care îl transmite clientului. Clientul examinează oferta şi dacă aceasta îl satisface, atunci formează mesajul DHCP Request (Cerere de IP către DHCP). Prin acest mesaj clientul confirmă că este de acord să utilizeze adresa IP propusă şi transmite acest mesaj sub formă broadcast, pentru ca celelalte servere DHCP (dacă există) din reţea să vadă că această IP adresă este atribuită acestui client. Serverul după recepţionarea mesajului DHCP Request, dacă încă nu a atribuit IP adresa curentă unui alt client, atunci formează şi transmite clientului mesajul DHCP Ack (confirmare DHCP), prin care îl anunţă pe client că contractul de închiriere a IP adresei este încheiat.

Dacă în domeniul broadcast există mai multe servere DHCP, atunci mesajul DHCP Discover este recepţionat de către toate aceste servere şi, în acest caz, acestea formează mesajul DHCP Offer pe care îl transmit clientului. Clientul alege o IP adresă şi transmite mesajul broadcast DHCP Request, deşi interacţiunea are loc doar cu serverul selectat.

Să ilustrăm acest proces în modul Simulation. Scoatem adresa IP de la PC0 şi bifăm din nou pe DHCP. Pe host-ul PC0 se formează mesajul broadcast DHCP Discover. Acest mesaj ajunge până la server, iar serverul găseşte un IP în baza sa de IP-uri, dar înainte ca să îl propună clientului, verifică dacă acest IP nu este utilizat de către vreun host în reţea (poate a fost atribuit de către un alt server!), printr-o solicitare ARP (pachet broadcast) prin care întreabă dacă în reţea este utilizată adresa IP curentă. Dacă la solicitarea ARP nu va fi un răspuns => rezultă că IP adresa este liberă şi poate fi atribuită clientului. Dar dacă va veni un răspuns la solicitarea ARP, atunci serverul va selecta o altă adresă IP pe care la fel o va verifica.
Peste ceva timp serverul va forma mesajul DHCP Offer pe care îl va transmite clientului. Dacă clientul este de acord cu oferta, atunci formează mesajul DHCP Request pe care îl transmite serverului, iar serverul transmite clientului mesajul de confirmare.
În partea finală a procesului, în mod analog, printr-o solicitare ARP clientul verifică IP adresa primită de la server.
Dacă în modul Simulation vom examina conţinutul pachetului DHCP, atunci ne vom convinge că DHCP este un protocol de nivel aplicaţie (ale modelelor OSI şi TCP/IP). Mesajul DHCP este încapsulat în câmpul de date al user datagramei UDP (la nivelul transport), care, la rândul său, este încapsulată într-o datagramă IP la nivelul reţea.
Prin definiţie, adresa IP este atribuită clientului pentru perioada de 24 ore (lease time = timpul de arendare a IP adresei). La expirarea a jumătate din acest interval de timp alocat, clientul PC0 iniţiază procedura de prelungire a arendei, prin transmiterea unui mesaj DHCP Request către server. Dacă de la serverul DHCP se va recepţiona un mesaj de confirmare DHCP Ack, aceasta va însemna că perioada *Lease time* a fost prelungită cu încă o zi. Dacă după o jumătate din timp serverul nu a trimis vreun răspuns, clientul în continuare transmite mesaje DHCP Request. Dar dacă şi în a doua jumătate de zi clientul nu reuşeşte să prelungească termenul de arendare a IP adresei, atunci clientul nu va mai putea să utilizeze IP adresa curentă şi va fi nevoit să solicite o altă adresă IP.
Pentru ce este necesar mecanismul de arendare a adresei IP? Dacă un careva host nu va funcţiona o perioadă de timp (24 de ore, de exemplu), atunci DHCP serverul trebuie să elimine înregistrarea conform căreia IP adresa este atribuită acestui client (pentru a avea posibilitate să o atribuie unui alt client, care solicită o IP adresă). Este necesar ca baza de date de pe server să fie permanent (dinamic) actualizată.
Timpul de arendare a adresei IP poate fi modificat. De exemplu, la o cafenea clientul a stat vreo 20 de minute în Internet, după care a plecat. În acest caz, nu are sens ca timpul de arendare să fie o zi, deoarece aceasta poate să conducă la epuizarea adreselor IP disponibile. Clientul demult a plecat, dar adresa IP este atribuită dispozitivului acestuia şi nu se repartizează unui alt client.
Serverul DHCP setat pe router
Nu numaidecât ca serverul DHCP să fie un dispozitiv dedicat. Acesta poate fi configurat pe un router din reţea. Să considerăm schema din Figura 6.

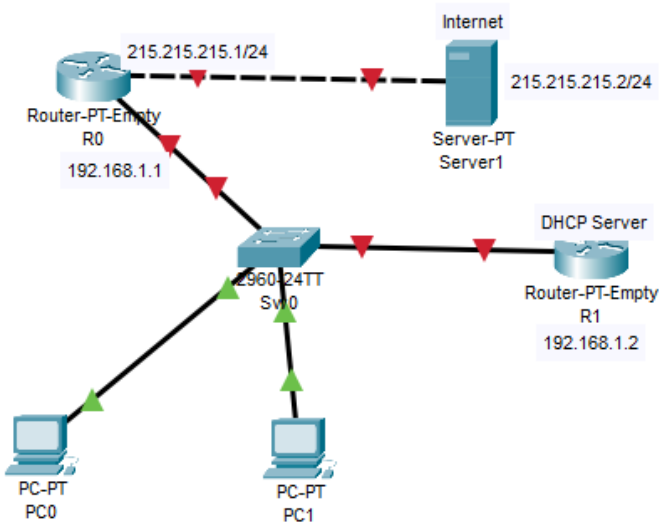


Figura 6

Inițial configurăm adresele IP pe routerele R0 și R1, dar și pe serverul Internet.
După aceea, pe routerul R1 definim mulțimea de adrese IP pe care le va putea atribui serverul DHCP:

```
Router(config)#ip dhcp pool NOVLANPOOL  // numele setului
Router(dhcp-config)#network 192.168.1.0 255.255.255.0 // se destribuie adrese de la 192.168.1.1 până la 192.168.1.254
Router(dhcp-config)#default-router 192.168.1.1    // adresa routerului implicit, care nu va fi atribuită host-urilor
Router(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.2 // se exclude posibilitatea atribuirii acestor adrese
```

Accesăm host-ul PC0 => activăm DHCP => a fost atribuită host-ului adresa IP 192.168.1.3
De pe PC0 dăm un ping 215.215.215.2 (pentru ieșire în Internet) => este conexiune
Accesăm host-ul PC1 => activăm DHCP => a fost atribuită adresa IP 192.168.1.4
De pe PC1 dăm un ping 215.215.215.2 (pentru ieșire în Internet) => este conexiune
Comanda *show ip dhcp binding* arată adresele IP (la fel și adresele MAC) care au fost atribuite clienților

```
Router(config)#do show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
192.168.1.3      00E0.F774.743A          --                      Automatic
192.168.1.4      000C.8554.0260          --                      Automatic
```

Dacă accesăm PC0 și schimbăm bifa de la DHCP la Static, atunci PC0 va trimite către serverul DHCP un mesaj prin care îl anunță că nu mai are nevoie de acel IP
Trecem în modul Simulation. Pe host-ul PC0 schimbăm bifa pe Static => vedem că de la PC0 se transmite pachetul DHCP Release (eliberare). Dăm încă o dată comanda *show ip dhcp binding* => vedem că adresa IP 192.168.1.3 a fost eliberată și poate fi repartizată unui alt client
Acum pe PC0 schimbăm bifa de la Static la DHCP => dăm comanda *show ip dhcp binding* => vedem că adresa IP 192.168.1.3 din nou a fost repartizată lui PC0.
Totuși, dacă vom întrerupe conexiunea dintre PC0 și Sw0 => vom vedea că adresa IP 192.168.1.3 nu a fost eliberată. Iată aici și își găsește aplicație perioada Lease time – dacă peste o zi PC0 nu va transmite mesajul cu cererea de actualizare => adresa IP 192.168.1.3 va fi eliberată (înregistrarea din tabel va fi eliminată)
Perioada de arendare a adresei IP poate fi modificată, folosind comanda

```
lease {days [hours] [minutes]| infinite}
```

Valoarea *infinite* specifică posibilitatea de arendare nelimitată a adresei IP. Un exemplu de comandă este

```
Router(dhcp-config)# lease 30
```

Schimbăm pe host-urile PC0 și PC1 bifele de pe DHCP pe Static => tabelul cu adresele IP atribuite nu mai conține date
Pe PC1 definim adresa statică:
IP Address: 192.168.1.3
Subnet Mask: 255.255.255.0
Atunci când punem bifa la DHCP pe host-ul PC0, serverul DHCP va încerca să atribuie adresa IP 192.168.1.3
Să trecem în modul Simulation pentru a vedea ce se întâmplă:
Serverul încearcă să afle dacă este deja atrbuită adresa IP 192.168.1.3 și, într-adevăr, vede că aceasta este deja utilizată de altcineva
Apoi verifică adresa 192.168.1.4 și vede că este liberă
Comanda *show ip dhcp conflict* arată adresele IP pe care serverul DHCP a încercat să le repartizeze și a stabilit că acestea sunt deja ocupate:

```
Router(config)#do show ip dhcp conflict
IP address       Detection method   Detection time          VRF
192.168.1.3      Ping               mar. 1 1993 01:10 a.m.
```

Comanda *clear ip dhcp conflict ** elimină tot conținutul tabelului cu IP-urile ce nu au putut fi distribuite

Configurarea serverului DHCP care ține cont că în rețea sunt VLAN-uri

Cum se configurează un server DHCP în cazul în care în rețea avem mai multe VLAN-uri? Cum se poate indica serverului DHCP că dacă host-urile sunt din același VLAN – atunci urmează ca serverul să distribuie adrese IP din aceeași subrețea, iar dacă host-urile sunt din VLAN-uri diferite – atunci lor li se vor atribui adrese IP din diferite subrețele? Să considerăm configurația din Figura 7.

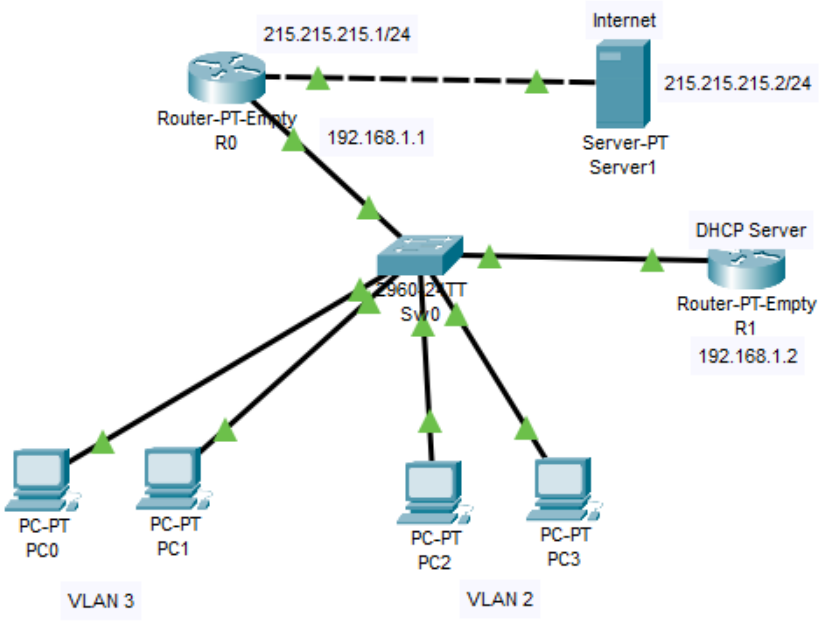


Figura 7

Mai întâi se configurează switch-ul Sw0 astfel încât să funcţioneze cu VLAN-uri:

```
Switch(config)#int fa 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access VLAN 3
Switch(config-if)#exit
Switch(config)#int fa 0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access VLAN 3
Switch(config-if)#exit
Switch(config)#int fa 0/5
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access VLAN 2
Switch(config-if)#exit
Switch(config)#int fa 0/6
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access VLAN 2
Switch(config-if)#exit
Switch(config)#do wr
```

Mai întâi pe toate host-urile se pune bifa la Static. Pe routerul cu rol de server DHCP se vor crea două subinterfeţe logice (deoarece avem două VLAN-uri în reţea):

```
R1(config)#int fa 9/0
R1(config-if)#no ip add
R1(config-if)#exit
R1(config)#no ip dhcp pool NOVLANPOOL
R1(config)#no ip dhcp excluded-address 192.168.1.1 192.168.1.2
R1(config)#int fa 9/0.2
R1(config-subif)#
R1(config-subif)#encapsulation dot1Q 2
R1(config-subif)#ip add 192.168.2.2 255.255.255.0
R1(config-subif)#no shut
R1(config-subif)#exit
R1(config)#int fa 9/0.3
R1(config-subif)#encapsulation dot1Q 3
R1(config-subif)#ip add 192.168.3.2 255.255.255.0
R1(config-subif)#no shut
R1(config-subif)#exit
```

Mai departe, pe routerul R1 se va crea set-ul de IP-uri pentru VLAN-ul 2 şi set-ul de IP-uri pentru VLAN-ul 3:

```
R1(config)#ip dhcp pool VLAN2POOL
R1(dhcp-config)#network 192.168.2.0 255.255.255.0
```

```
R1(dhcp-config)#default-router 192.168.2.1 // va trebui să completăm şi pe R0
R1(dhcp-config)#exit
R1(config)#ip dhcp pool VLAN3POOL
R1(dhcp-config)#network 192.168.3.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.3.1
R1(dhcp-config)#exit
```

În fine, conexiunea dintre Sw0 şi R1 trebuie făcută de tip trunk. Serverul DHCP va lucra cu frame-uri Ethernet etichetate (cu tag-uri VLAN). Pe Sw0 scriem:

```
Switch(config)#int fa 0/4
Switch(config-if)#sw mode trunk
Switch(config-if)#exit
```

Acum intrăm pe host-uri şi punem bifa la DHCP. Vedem că acestora li se atribuie IP adrese şi se ţine cont de VLAN-ul din care face parte host-ul.
Adresele IP 192.168.2.1, 192.168.2.2, 192.168.3.1 şi 192.168.3.2 trebuie să fie rezervate:

```
R1(config)#ip dhcp excluded-address 192.168.2.1 192.168.2.2
R1(config)#ip dhcp excluded-address 192.168.3.1 192.168.3.2
```

În ce mod serverul DHCP înţelege cărui host urmează să îi repartizeze un IP din subreţeaua doi şi cărui host – un IP din subreţeaua trei? Răspuns - în baza interfeţei de la care a recepţionat această interogare. Pentru a asigura ieşirea în Internet pe interfaţa Fa9/0 a routerului R0 este necesar de creat subinterfeţele Fa 9/0.2 şi Fa 9/0.3, cu adresa IP 192.168.2.1 şi, corespunzător, 192.168.3.1:

```
Router(config)#int fa 9/0.2
Router(config-subif)#encapsulation dot1Q 2
Router(config-subif)#ip add 192.168.2.1 255.255.255.0
Router(config-subif)#int fa 9/0.3
Router(config-subif)#encapsulation dot1Q 3
Router(config-subif)#ip add 192.168.3.1 255.255.255.0
Router(config-subif)#int fa 9/0
Router(config-if)#no ip add
Router(config-if)#exit
```

Pe legătura dintre R0 şi Sw0 se va crea un port trunk:

```
Switch>en
Switch#conf ter
Switch(config)#int fa 0/3
Switch(config-if)#switchport mode trunk
```

Pe fiecare host punem bifa la DHCP
De pe host-urile PC2 şi PC3: ping 215.215.215.2 => este conexiune
De pe host-urile PC0 şi PC1: ping 215.215.215.2 => este conexiune

2. Cazul în care clientul se află într-un alt domeniu broadcast în raport cu serverul DHCP

Ce e de făcut dacă serverul DHCP nu se află în acelaşi domeniu broadcast ca şi host-ul ce solicită date IP? Pentru soluţionarea acestei probleme este aplicată schema DHCP Relay (retranslaţie), care utilizează în calitate de retranslator un switch de nivelul 3 (L3 Switch). Retranslatorul va „prinde" frame-urile broadcast ce conţin mesaje DHCP şi le va muta într-un alt domeniu broadcast. Pentru aceasta pe switch-ul de nivel 3 se activează funcţia de retranslare corespunzătoare.
Să examinăm următoarea configuraţie de reţea (a se vedea Figura 8):

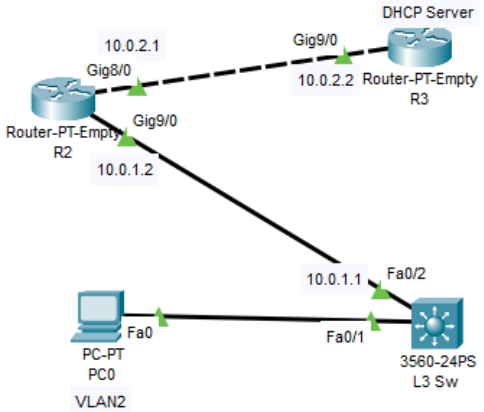


Figura 8

Host-ul PC0 se află la distanţă de 3 domenii broadcast de la serverul DHCP R3

```
Pe R2:
Router(config)#int gig 8/0
Router(config-if)#ip add 10.0.2.1 255.255.255.0
Router(config-if)#no sh
Router(config-if)#exit
Router(config)#int gig 9/0
Router(config-if)#ip add 10.0.1.2 255.255.255.0
Router(config-if)#no sh
Router(config-if)#exit

Pe R3:
Router(config)#int gig 9/0
Router(config-if)#ip add 10.0.2.2 255.255.255.0
Router(config-if)#no sh
Router(config-if)#exit
```

La fel, pe routerul R3 creăm set-ul de IP adrese pe care va putea să le repartizeze serverul DHCP:

```
Router(config)#ip dhcp pool VLAN2POOL
Router(dhcp-config)#network 192.168.2.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.2.1
```

Configurările de pe switch-ul de nivel 3, L3 Sw:

```
Switch(config)#int fa 0/2
Switch(config-if)#no switchport
Switch(config-if)#ip add 10.0.1.1 255.255.255.0
Switch(config-if)#exit
Switch(config)#ip routing
Switch(config)#int fa 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#spanning-tree mode rapid-pvst
```

Dacă la acest moment vom încerca să obţinem o adresă IP prin DHCP (punem bifa la DHCP!), vom vedea că serverul DHCP nu funcţionează corect. Este necesar de făcut ca L3 Sw să transforme pachetul broadcast în unul unicast şi să îl retransleze anume către serverul DHCP. Pentru aceasta pe L3 Sw dăm comenzile:

```
Switch(config)#int vlan 2
Switch(config-if)#ip add 192.168.2.1 255.255.255.0
Switch(config-if)#ip helper-address 10.0.2.2   // IP-ul serverului DHCP
```

Adică L3 Sw pe interfaţa virtuală vlan 2 va „prinde” frame-urile broadcast şi dacă va vedea că sunt destinate pentru DHCP server, le va transmite ca unicast către server pe adresa IP 10.0.2.2. Dar până când L3 Sw nu ştie cum să ajungă până la reţeaua 10.0.2.0 (unde se află serverul DHCP). Deci este necesar pe L3 Sw de scris ruta:

```
Switch(config)#ip route 0.0.0.0 0.0.0.0 10.0.1.2
```

Iar pe serverul DHCP:

```
R3(config)#ip route 192.168.2.0 255.255.255.0 10.0.2.1
```

Iar pe routerul R2:

```
R2(config)#ip route 192.168.2.0 255.255.255.0 10.0.1.1
```

Acum dacă schimbăm pe host-ul PC0 bifa de la Static la DHCP => se atribuie corect adresa IP

Varianta când avem mai multe VLAN-uri

Să examinăm configuraţia de reţea din Figura 9:

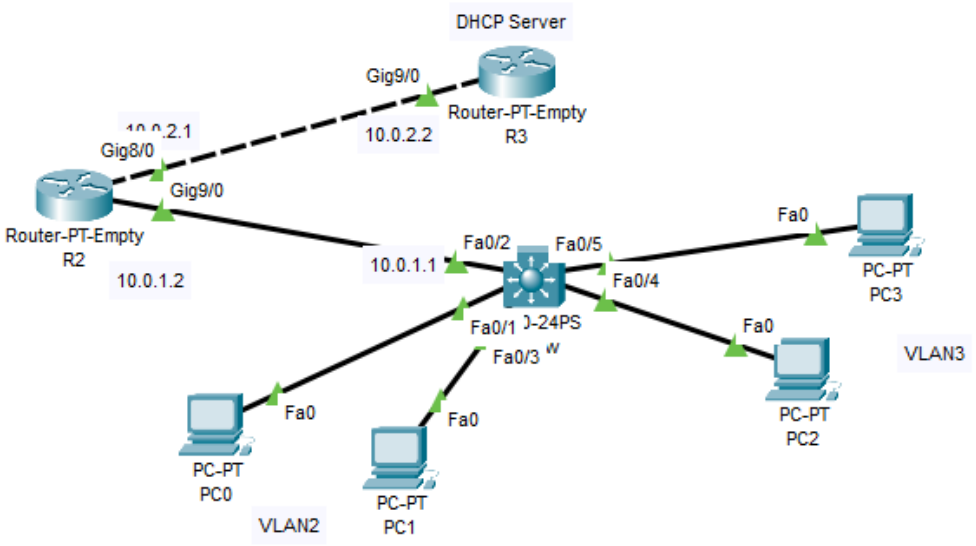


Figura 9

Salvăm configurările efectuate mai sus.
Dar adăugăm următoarele:
pe L3 Sw:

```
Switch(config)#int fa 0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#int fa 0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 3
Switch(config-if)#exit
Switch(config)#int fa 0/5
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 3
Switch(config-if)#exit
```

```
Pe R3:
R3(config)#ip route 192.168.3.0 255.255.255.0 10.0.2.1
Pe R2:
R2(config)#ip route 192.168.3.0 255.255.255.0 10.0.1.1
```

Pe serverul DHCP este necesar de creat set-ul de adrese IP pentru VLAN 3:

```
R3(config)#ip dhcp pool VLAN3POOL
R3(dhcp-config)#network 192.168.3.0 255.255.255.0
R3(dhcp-config)#default-router 192.168.3.1
```

Pe routerul R3 interzicem atribuirea adreselor IP 192.168.2.1, 192.168.2.2, 192.168.3.1 şi 192.168.3.2:

```
R3(config)#ip dhcp excluded-address 192.168.2.1 192.168.2.2
R3(config)#ip dhcp excluded-address 192.168.3.1 192.168.3.2
```

Pe L3 Sw se va crea interfaţa virtuală:

```
Switch(config)#int vlan 3
Switch(config-if)#ip add 192.168.3.1 255.255.255.0
Switch(config-if)#ip helper-address 10.0.2.2
Switch(config-if)#exit
```

Acum intrăm pe host-urile PC0, PC1, PC2, PC3 şi bifăm pe DHCP => se atribuie corect IP adrese în fiecare VLAN.

Etichetarea VLAN funcţionează doar în limitele unui domeniu broadcast, adică la ieşirea din L3 Sw din frame se va şterge eticheta. Când mesajul DHCP va ajunge la L3 Sw, pe care este activată funcţia de retranslator, L3 Sw va plasa în câmpul Agent IP Address adresa IP de pe interfaţa lui virtuală: dacă este VLAN 2, atunci va lucra a doua interfaţă virtuală, iar în mesajul DHCP în câmpul Relay Agent Address se va scrie această adresă IP.
Să vedem în modul Simulation – pachetul DHCP de la PC0 (bifăm la DHCP) ajunge la L3 Sw => deschidem

Outbound PDU pe L3 Sw – în pachetul DHCP avem câmpul RELAY AGENT ADDRESS inițializat cu valoarea 192.168.2.1 => această adresă IP este stocată. Când pachetul ajunge la serverul DHCP, acela vede acest IP şi astfel află care set de IP-uri să utilizeze pentru a repartiza un IP către client (dacă IP-ul este din subrețeaua 2 => se va repartiza un IP din subrețeaua 2).

Configurarea serverului DNS

DNS = Domain Name System = Sistemul numelor de domeniu

Pentru a accesa un site web se poate scrie în câmpul de adrese IP adresa serverului web al site-ului

Dar în Internet pentru a accesa un site se scrie, de regulă, numele de domeniu asociat (acesta poate fi uşor memorat de către utilizator), iar serviciul DNS translează acest nume în IP-ul corespunzător. Dacă în configurările host-ului nu este indicată adresa IP a serverului DNS, atunci host-ul nu ştie unde să se adreseze atunci când în linia de comandă se introduce numele de domeniu al căruiva site.

DNS – un grup de servere care colaborează pentru a identifica adresa IP în baza numelui de domeniu corespunzător

Să examinăm schema din Figura 7 pe care o completăm cu un server DNS (a se vedea Figura 10):

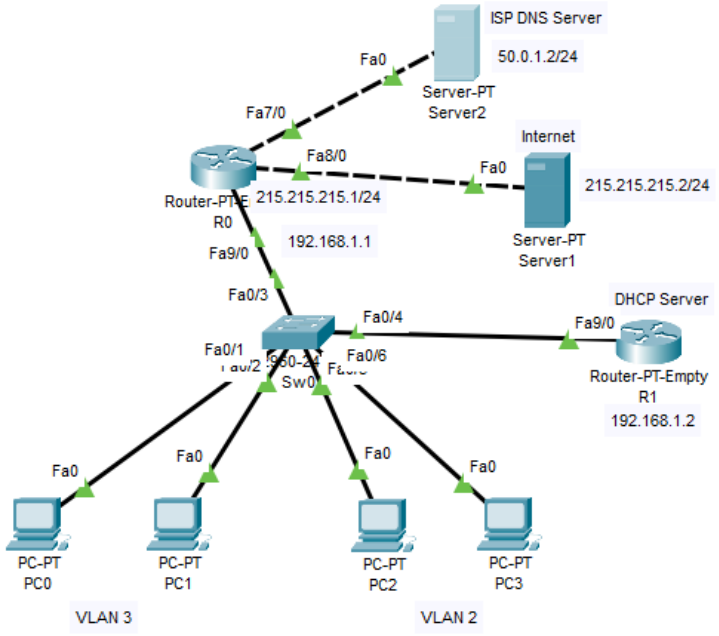
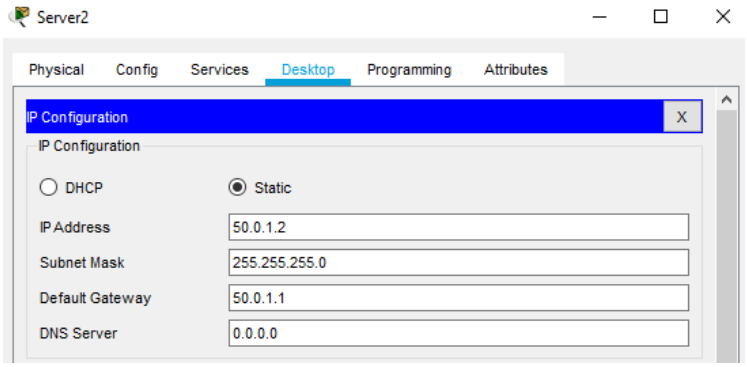


Figura 10

Atribuim o IP adresă pe interfața Fast Ethernet 7/0 a routerului R0:

```
Router(config)#int fa 7/0
Router(config-if)#ip add 50.0.1.1 255.255.255.0
Router(config-if)#no sh
Router(config-if)#exit
```

Atribuim o IP adresă pe serverul DNS:



Pe serverul DHCP se definește pentru fiecare VLAN adresa serverului DNS:

```
R1(config)#ip dhcp pool VLAN2POOL
R1(dhcp-config)#dns-server 50.0.1.2
R1(dhcp-config)#ip dhcp pool VLAN3POOL
R1(dhcp-config)#dns-server 50.0.1.2
R1(dhcp-config)#exit
```

Pe host-urile PC0, PC1, PC2 şi PC3 punem bifa pe DHCP => pe lângă IP Address, Subnet Mask şi Default Gateway a apărut şi adresa serverului DNS.
Acum vom configura însăşi serverul DNS:
Dăm click pe Server 2 şi în partea de sus selectăm tab-ul Services, iar în stânga apăsăm butonul DNS => completăm în câmpul Name numele site-ului, iar în câmpul Address – adresa IP a acestuia. După aceasta apăsăm butonul Add => astfel am realizat o înregistrare DNS. Pentru a activa serverul DNS punem bifa pe On (a se vedea Figura 11).

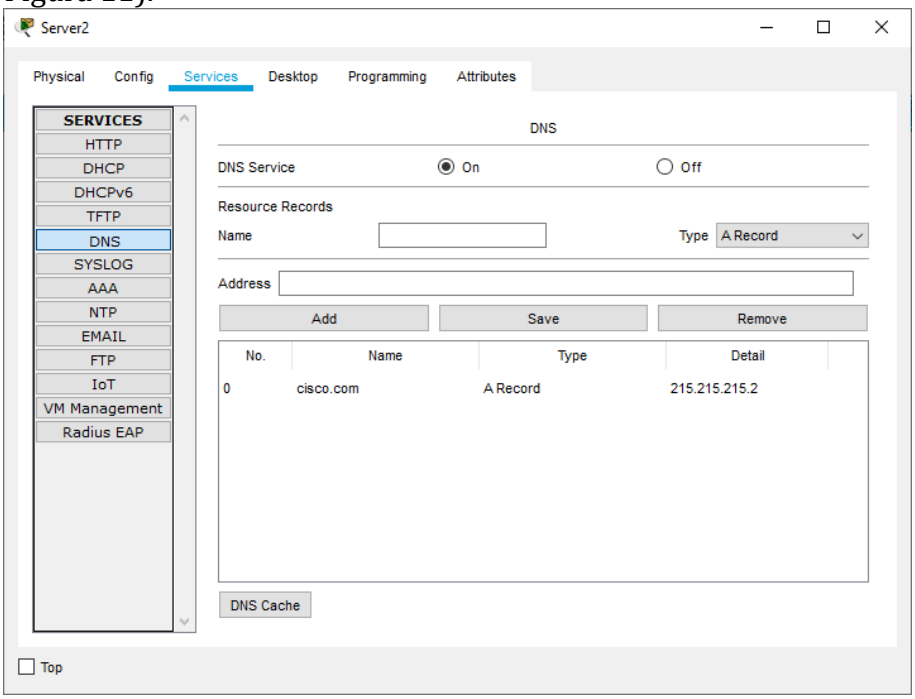


Figura 11

Accesăm host-urile şi selectăm Web Browser (de exemplu, pe PC0-> Desktop->Web Browser), iar în câmpul URL scriem numele de domeniu *cisco.com* => apăsăm butonul *Go* => lucrează corect (am accesat pagina site-ului) => astfel este accesibil Web Server-ul în baza numelui lui de domeniu.
În modul Simulation: accesăm PC0 şi punem bifa la DHCP (vedem că a apărut şi adresa DNS). În Web Browser introducem numele cisco.com => s-a format pachetul DNS => dacă examinăm conţinutul acestuia, ne putem convinge că DNS este un protocol de nivel aplicaţie al modelului TCP/IP, iar la nivelul transport mesajul este încapsulat într-o user datagramă UDP (a se vedea Figura 12).

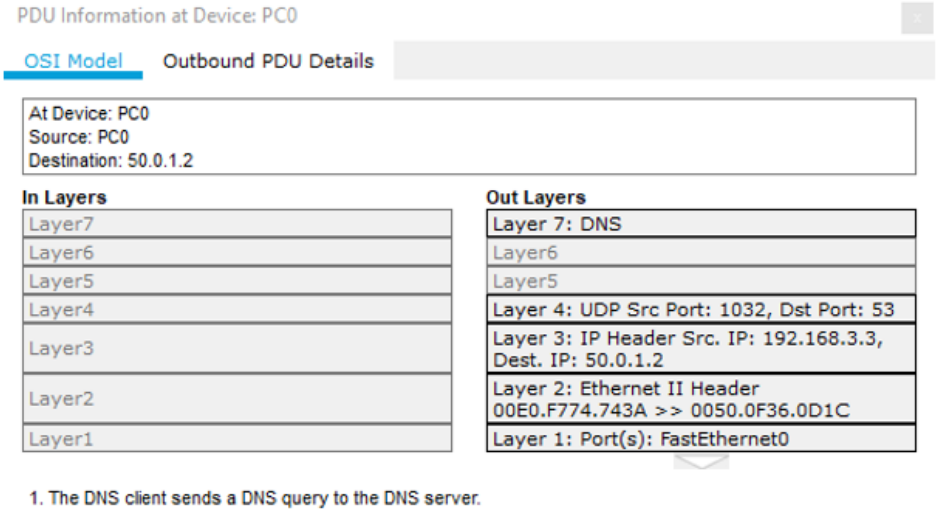


Figura 12

La fel se poate vedea că mai întâi se formează o solicitare ARP a adresei IP a serverului DNS, iar după ce host-ul PC0 află IP adresa serverului DNS, transmite pachetul DNS către acest server, solicitând adresa IP a site-ului cisco.com, pe care o obţine ca răspuns de la serverul DNS. Ştiind adresa IP a site-ului cisco.com, host-ul PC0 se adresează în Internet pe acest site (se transmite un pachet TCP pentru a stabili

o sesiune cu Server1, iar apoi cu HTTP).
Am examinat o schemă simplificată, deoarece serverul DNS este conectat direct la routerul R0 al organizației. Mai real ar fi fost dacă se considera că serverul DNS este conectat la routerul provider-ului ISP.
Serverul DNS poate fi atât în Internet, cât şi în reţeaua locală

Configurarea serverului de Email

Pentru a configura serverul de poştă electronică vom adăuga la schema din Figura 10 încă un server (a se vedea Figura 13):

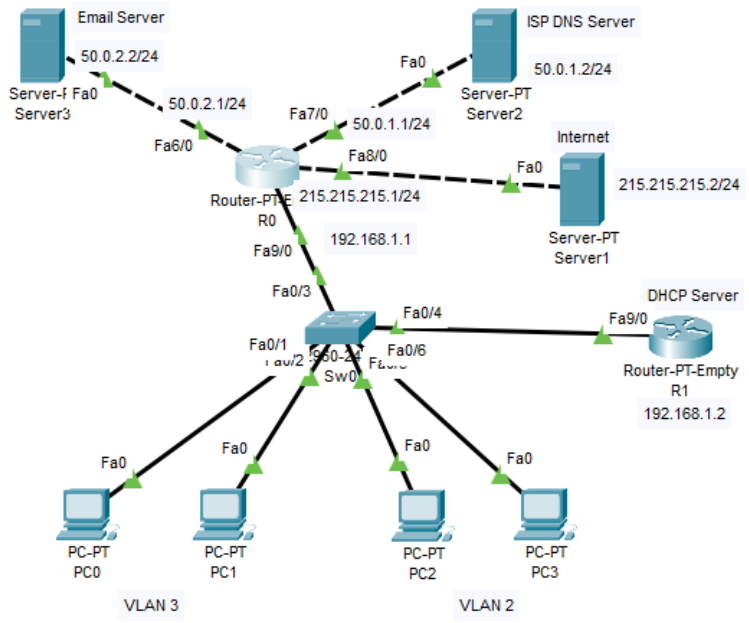
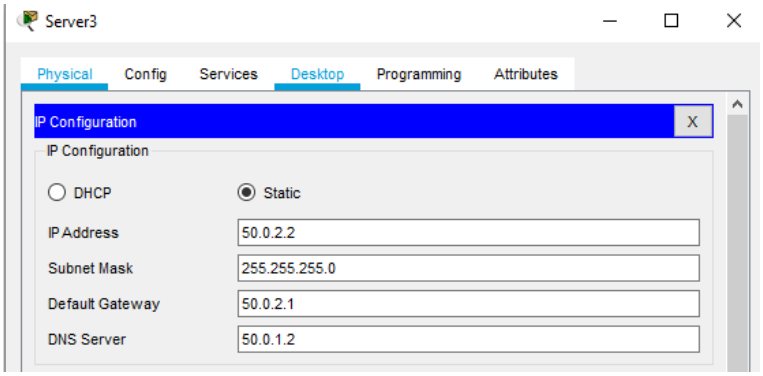


Figura 13

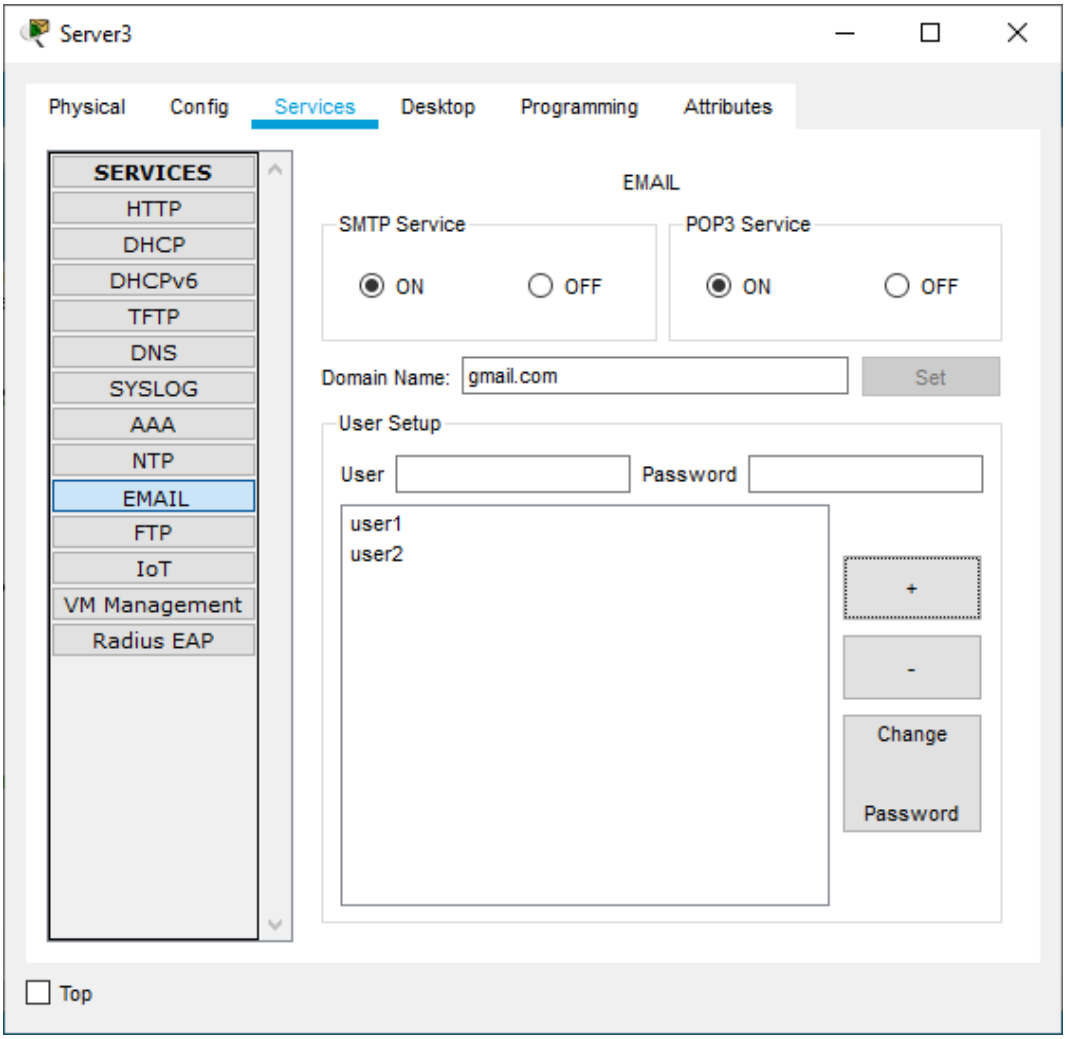
Stabilim pe interfaţa Fast Ethernet 6/0 a routerului R0 adresa IP 50.0.2.1:

```
Router(config)#int fa 6/0
Router(config-if)#ip address 50.0.2.1 255.255.255.0
Router(config-if)#no sh
Router(config-if)#exit
```

Pe serverul de poştă electronică stabilim adresa IP 50.0.2.2:



În continaure, configurăm nemijlocit serverul de poştă electronică:
Server 3 -> Services -> Email şi completăm următoarele câmpuri:
Domain Name – de exemplu, gmail.com şi apăsăm butonul *Set*
User – de exemplu, user1
Password - de exemplu, 123
Apăsăm butonul **+** => am adăugat un utilizator
Pentru a avea posibilitatea de a transmite reciproc e-mail-uri, vom crea încă un utilizator:
User – de exemplu, user2
Password - de exemplu, 321
Apăsăm butonul **+** => am adăugat un utilizator
Astfel am obţinut următoarele date:



De exemplu, utilizatorul user1 lucrează pe host-ul PC0, iar utilizatorul user2 - pe PC2
Accesăm PC0 -> Desktop -> Email şi completăm următoarele:

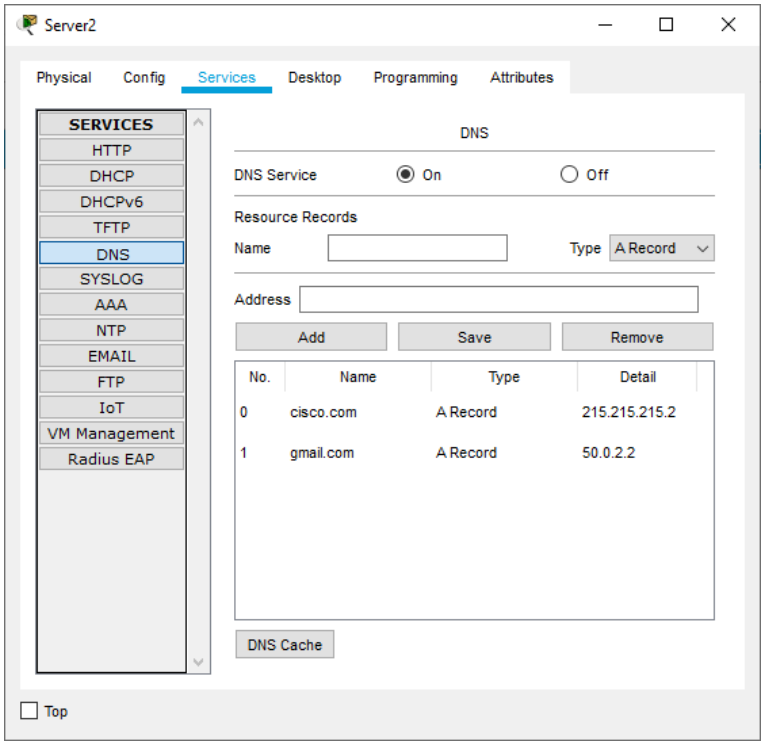
Your Name – John
Email Address – user1@gmail.com
Incoming Mail Server – gmail.com
Outgoing Mail Server – gmail.com
User Name – user1
Password – 123
Apăsăm butonul *Save*

Analog, pe host-ul PC2 se completează datele pentru user2:

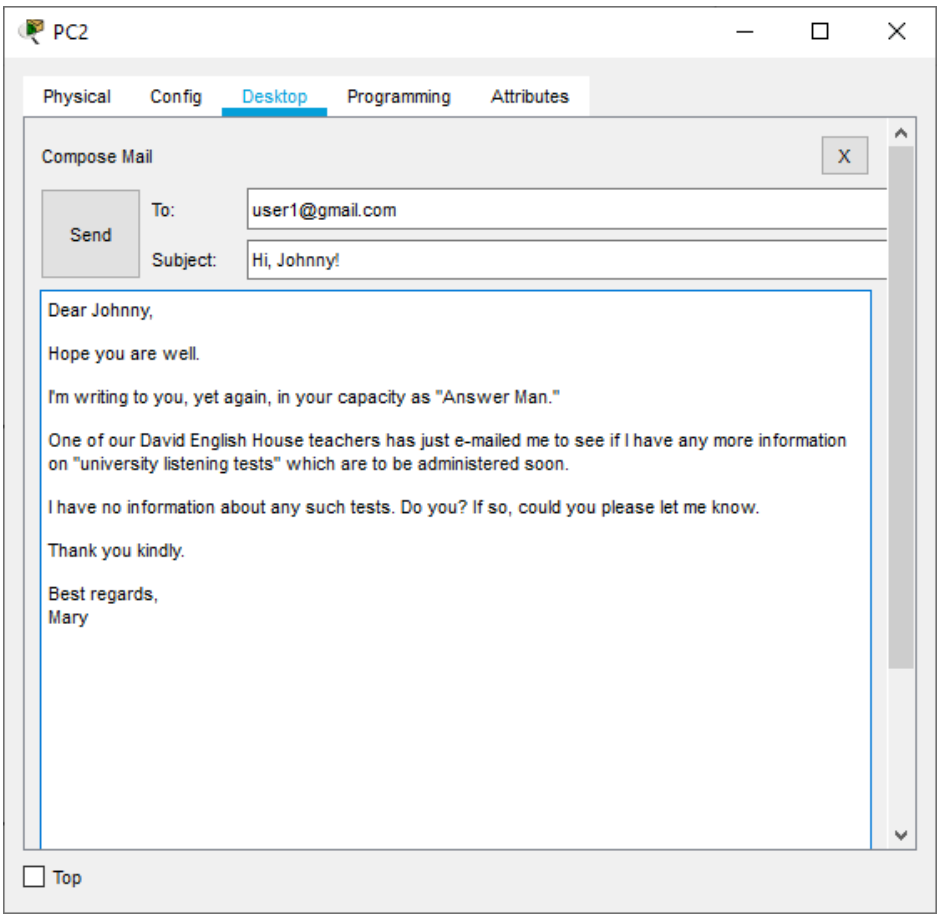
Your Name – Mary
Email Address – user2@gmail.com
Incoming Mail Server – gmail.com
Outgoing Mail Server – gmail.com
User Name – user2
Password – 321
Se apasă pe *Save*

Pe serverul DNS (Server2) se adaugă înregistrarea

Name – gmail.com
Address – 50.0.2.2
Se apasă *Add*



De exemplu, Mary vrea să îi transmită un mesaj lui John. Mary deschide pe host-ul PC2 serviciul de poştă (Desktop -> Email) şi apasă pe Compose, după care culege conţinutul mesajului



iar, la final, apasă butonul *Send*.

John deschide serviciul de poştă electronică pe host-ul PC0 (Desktop -> Email) şi apasă pe *Receive*, vede mesajele recepţionate, selectează mesajul de la Mary, apasă pe denumirea mesajului şi îi vede conţinutul.

A se vedea în modul Simulation cum decurge procesul de transmitere şi de recepţionare a mesajului de e-mail!

Cerinţe pentru realizarea lucrării de laborator №6

Se consideră configuraţia de reţea din Figura 14.

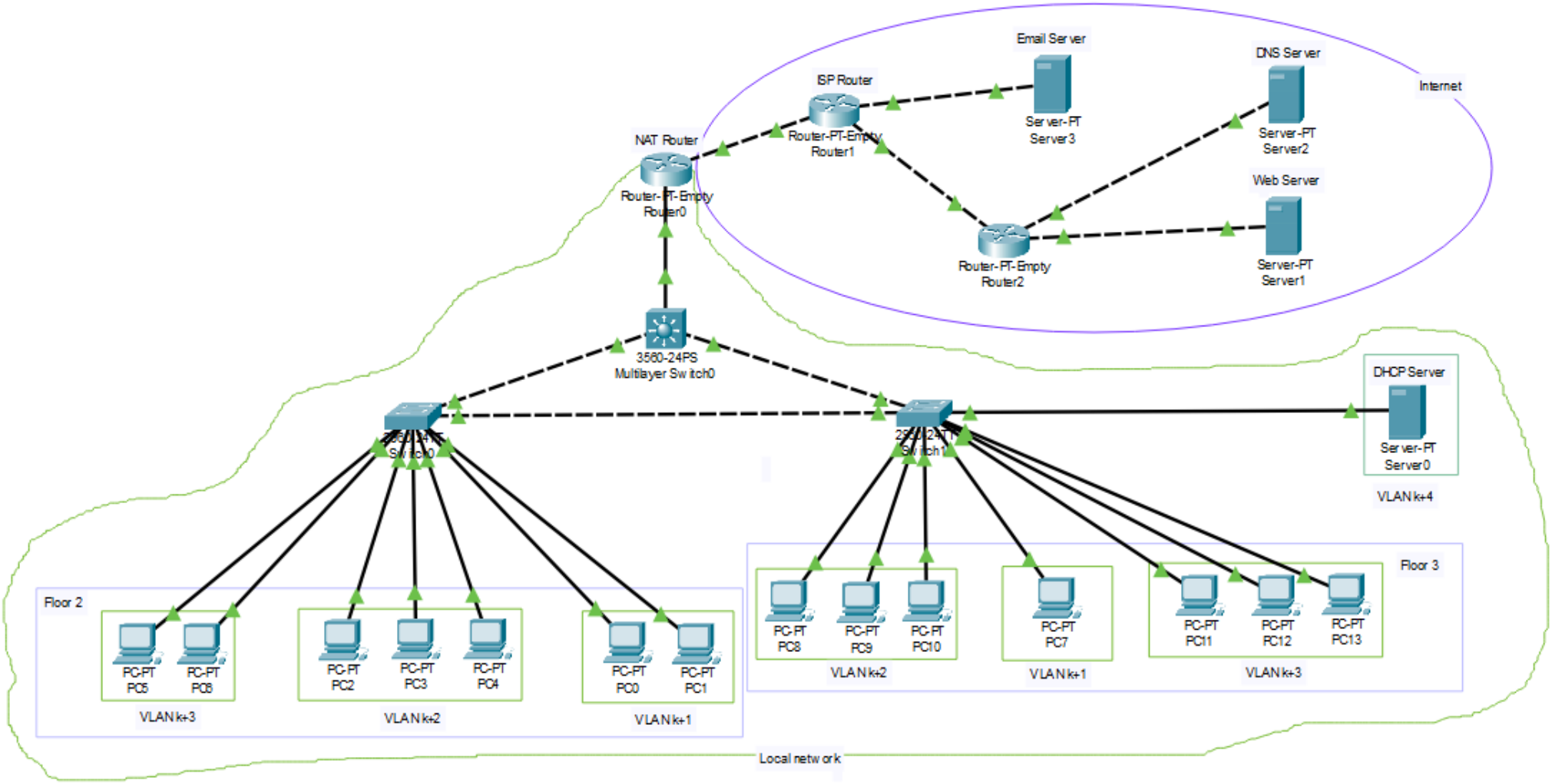


Figura 14

În Cisco Packet Tracer, efectuaţi următoarele:

1. Construiţi configuraţia de reţea prezentată în Figura 14. De menţionat că dispozitivele din interiorul reţelei locale formează patru VLAN-uri numerotate prin k+1, k+2, k+3 şi k+4, unde k este numărul de ordine al studentului în registrul grupei. Serverul DHCP stă în VLAN-ul k+4. Salvaţi configuraţia de reţea realizată în fişierul **Nume_Prenume_Grupa_Retea6a.pkt**
2. Atribuiţi IP adrese dispozitivelor din reţea (inclusiv pe subinterfeţele necesare), astfel încât
   a) în interiorul reţelei locale să fie atribuite IP adrese private din intervalul 192.168.i.j, unde i este numărul VLAN-ului corespunzător, iar j – valoarea ultimului octet al adresei (de exemplu, din intervalul [1,20]),
   b) în exteriorul reţelei locale să fie atribuite IP adrese publice.

   Schema de adrese IP elaborată stocaţi-o într-un tabel pe care îl includeţi în darea de seamă. Adresele IP atribuite dispozitivelor le reflectaţi în configuraţia de reţea, folosind instrumentul Place Note (N). Configuraţi manual IP adresele elaborate pe dispozitivele din exteriorul reţelei.
3. Configuraţi VLAN-urile şi legătura dintre VLAN-uri pe switch-ul de nivel 3 (Multilayer Switch0). Includeţi comenzile corespunzătoare în darea de seamă.
4. Configuraţi serverul DHCP (la fel, adăugaţi comanda *ip helper-address* pe switch-ul de nivel 3) astfel încât acesta să atribuie în mod automatizat IP adrese, măşti de subreţea corespunzătoare şi adresa IP a routerului implicit tuturor host-urilor din reţeaua locală – PC0, PC1, ..., PC13. Arătaţi că există legătură (prin comanda *ping*, atât în modul Realtime, cât şi în modul Simulation) între dispozitivele din acelaşi VLAN, dar şi între dispozitivele din diferite VLAN-uri. Print screen-urile ce demonstrează existenţa legăturii le includeţi în darea de seamă.
5. Pe switch-ul de nivel 3 (Multilayer Switch0) şi pe routerul NAT (Router0) configuraţi protocolul de rutare dinamică OSPF pentru a asigura conexiunea între oricare dispozitiv din interiorul reţelei locale cu routerul NAT. La fel, pe ISP Router şi pe Router2 configuraţi protocolul de rutare dinamică OSPF pentru a asigura conexiunea între oricare dispozitiv din exteriorul reţelei locale cu routerul NAT. Comenzile aplicate şi listele cu rutele definite pe fiecare router le includeţi în darea de seamă.
6. Pe switch-ul de nivel 3 definiţi o rută implicită către routerul NAT, iar pe routerul NAT o rută implicită către routerul ISP. Explicaţi pentru ce este necesar acest procedeu şi de ce nu se aplică procedeul de redistribuire a rutelor între cele două procese OSPF definite anterior.
7. Configuraţi schema NAT cu overload (PAT) pe routerul NAT, folosind în calitate de adresă publică pentru translare adresa interfeţei de ieşire spre exterior 215.215.215.1. Comenzile aplicate le includeţi în darea de seamă. Ilustraţi în modul Simulation procesul de translare a adresei private în adresă publică (şi reciproc), iar print screen-urile corespunzătoare le includeţi în darea de seamă.
8. Configuraţi serverul DNS (Server2). Se va testa pe exemplul http://cisco.com. Serverul DHCP trebuie să atribuie automatizat host-urilor din interiorul reţelei locale adresa IP a serverului DNS. Acţiunile efectuate le descrieţi în darea de seamă.
9. Configuraţi şi testaţi serverul de e-mail (Server3). Acţiunile efectuate şi rezultatele testării le includeţi în darea de seamă.
10. Salvaţi configuraţia de reţea realizată în fişierul **Nume_Prenume_Grupa_Retea6b.pkt**

Realizaţi o dare de seamă asupra lucrului efectuat, care să conţină răspunsuri explicite la fiecare punct formulat în cerinţe.

Încărcaţi fişierul cu darea de seamă şi fişierele .pkt în mapa *Lucrarea de laborator N6* din pagina dedicată cursului de Reţele de Calculatoare a platformei educaţionale moodle.usm.md.