ВЕЖБА 8

ПРЕВОЂЕЊЕ IP АДРЕСА И ЛИСТЕ ЗА КОНТРОЛУ ПРИСТУПА

Опис вежбе:

Циљ вежбе је да се студенти упознају са принципима примене приватних IP адресних опсега и превођења истих у јавне. Поред тога биће речи и о појму и примени листа за контролу приступа.

ПРЕВОЂЕЊЕ ПРИВАТНИХ IP АДРЕСА У ЈАВНЕ

IP протокол верзије 4 специфицира 32 бита која се могу користити за извођење IP адресе. Постулат самог протокола је да сваки ентитет мора имати уникатну IP адресу како би могао да учествује у комуникацији на мрежи. Рапидни развој Интернета доводи до тога да се број клијената којима требају уникатне IP адресе драстично повећава, те се расположиви адресни простор који обезбеђује IPv4 протокол рапидно троши. Како би се рационализовало коришћење постојећег IPv4 опсега адреса, организација IETF је усвојила документ RFC1918 1996. године који дефинише приватне адресне опсеге који се могу користити унутар локалних рачунарских мрежа при чему администратори тих мрежа не морају да воде рачуна да ли је неко други користи изабрани приватни опсег. Приватни адресни опсези дефинисани у наведеном документу су:

- 10.0.0.0 / 8
- 172.16.0.0 / 12
- 192.168.0.0 / 16

Приликом пројектовања локалне рачунарске мреже, администратор може изабрати било који од наведених опсега по личном нахођењу како би обезбедио адресе уређајима у мрежи. Такође, изабрани опсег се даље може подмрежавати како би се изашло у сусрет потребама.

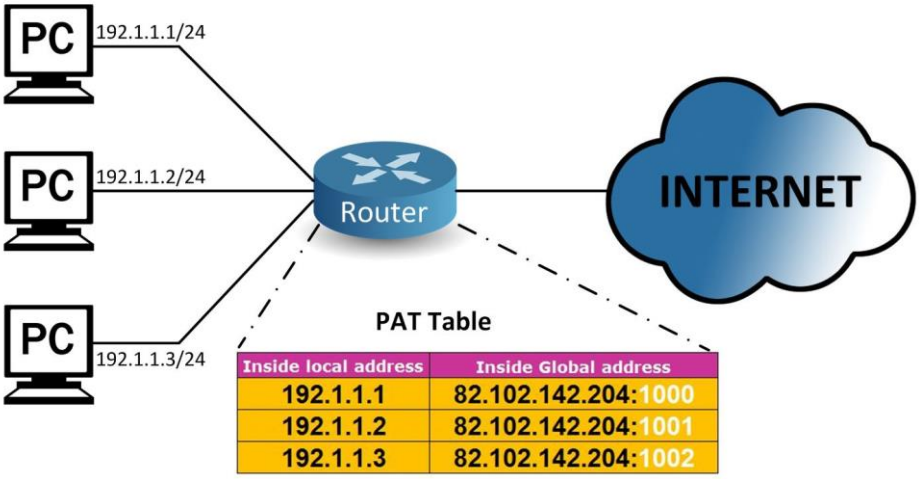
Али, у случају да локална мрежа, односно уређај у локалној мрежи има потребу да приступа сервисима ван тог LAN-а, тачније сервисима на Интернету, не може користити додељену му приватну адресу. Због тога је неопходно конфигурисати превођење приватних у јавне IP адресе, односно сав саобраћај који генерише уређај са приватном IP адресом, мора бити представљен јавном. Улога преводиоца адреса се најчешће додељује рутеру кроз који пролази сав саобраћај из LAN-а ка Интернету и обрнуто. Процес је следећи: рачунар са приватном адресом хоће да приступи неком сервису на Интернету и он саобраћај шаље свом подразумеваном пролазу, при чему је као изворишна адреса постављена приватна IP адреса тог рачунара (*Default Gateway*). Рутер прихвата тај саобраћај и пошто је конфигурисан као преводилац адреса, све пакете који долазе из LAN-а обрађује тако што уместо приватне изворшне адресе рачунара, поставља своју јавну адресу интерфејса којим је повезан са Интернетом. На овај начин рутер добија улогу посредника у комуникацији између уређаја са приватним адресама и Интернета. Свако превођење које изврши рутер је дужан да евидентира. Када добије одговоре са Интернета на захтеве које је генерисао рачунар са приватном адресом, рутер је дужан да на основу табеле превођења изврши обрнут процес: у примљеном одговору као одредишна адреса наведена је адреса интерфејса рутера према Интернету, што значи да рутер мора да уклони ову адресу, постави приватну адресу из табеле превођења и такав пакет проследи у локалну рачунарску мрежу где се налази рачунар који је иницирао саобраћај.

Постоје две врсте превођења приватних у јавне IP адресе и то:

- NAT (енг. *Network Address Translation)*
- PAT (енг. *Port Address Translation)*

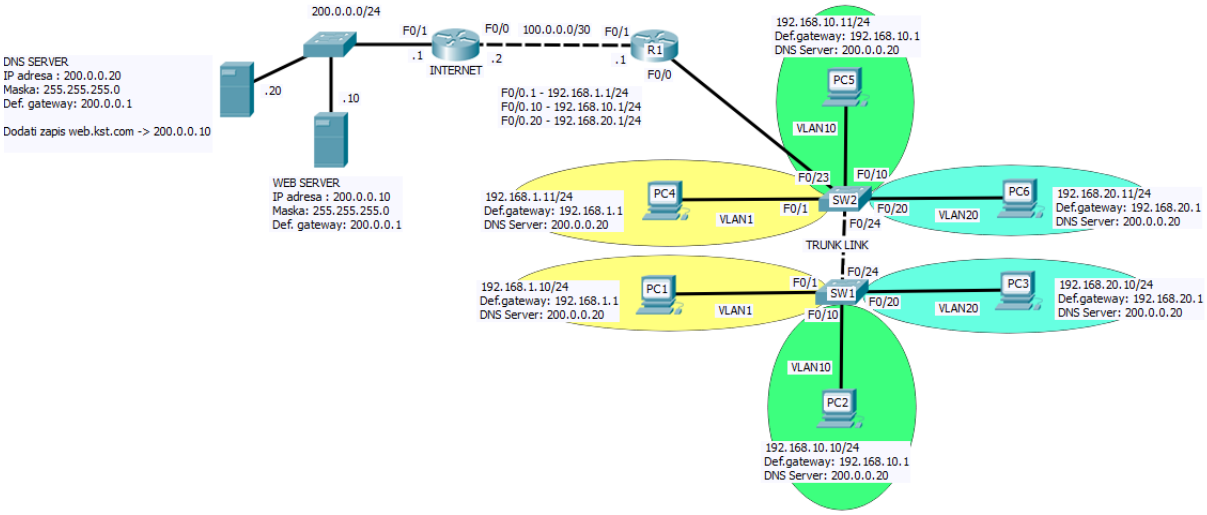
NAT превођење подразумева да се тачно једна приватна адреса преводи у тачно једну јавну IP адресу, што само по себи и не доноси уштеду када су у питању потребне јавне адресе, те је овакав принцип превођења превазиђен. Како би више приватних адреса било преведено у једну јавну адресу осмишљен је PAT принцип превођења при чему се као додатна информација приликом превођења користи и број порта који припада TCP или UDP протоколу. На слици 1 је

приказан пример како изгледа PAT процес у пракси. Неопходно је напоменути да се данас у литератури наводи NAT, при чему се мисли на PAT.

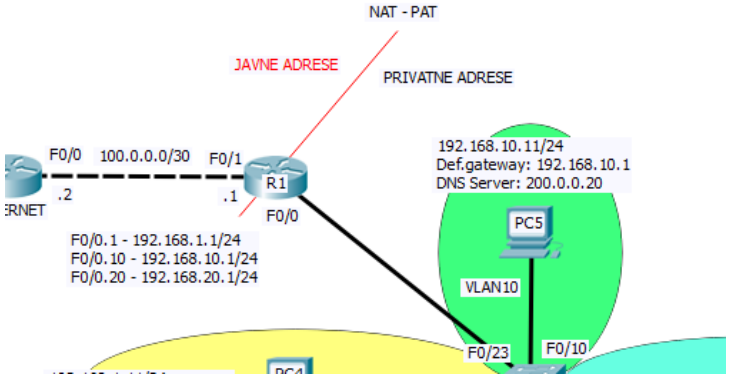


Слика 1 – PAT превођење

У оквиру лабораторијске вежбе неопходно је дорадити топологију из вежбе 7, тако што ћемо додати рутер који обезбеђује везу са Интернетом, а на кога су прикључени сервери који за функцију имају симулацију Интернет сервиса (слика 2). Идеја је да се линк између рутера R1 и Internet адресира са јавним IP адресама, као и сегмент где се налазе DNS и WEB сервер. Да би омогућили рачунарима из VLAN1, VLAN10 и VLAN20 приступ сервисима на наведеним серверима, неопходно је подесити PAT процес на рутеру R1 који ће приватне адресе рачунара преводити у своју јавну адресу која је додељена интерфејсу F0/1 (слика 3).



Слика 2 - Топологија



Слика 3 – PAT превођење на рутеру R1

Листе за контролу приступа

Листе за контролу приступа (енг. *Access Control List - ACL*) представљају механизам који се може конфигурисати на рутеру у сврху контроле долазног и одлазног саобраћаја. ACL се састоје из низа правила где свако правило дефинише који тип саобраћаја се дозвољава при чему се као параметри могу користити изворишна и одредишна адреса, тип протокола, изворишни и одредишни порт ... Скуп правила се групише у ACL која се затим везује за интерфејс при чему се специфицира који смер саобраћаја ACL треба да надгледа. Сваки примљени пакет се пропушта кроз ACL, правило по правило, и ако је неки од наведених параметара у пакету исти као и у правилу, онда се пакет пропушта или одбацује у зависности како је специфицирано.

На Cisco рутерима постоје две врсте ACL и то:

- стандардне листе за контролу приступа које се обележавају редним бројевима од 1 до 99
- проширене листе за контролу приступа са редним бројевима од 100 до 199

Конфигурација превођења мрежних адреса (PAT)

Циљ вежбе је да се рутер R1 конфигурише тако да саобраћај који долази из свих VLAN-ова слике 2, чија је дестинација Интернет, буде преведен у јавну адресу рутера R1 и то интерфејса F0/1. Да би ово постигли неопходно је:

- креирати стандардну листу за контролу приступа за сваки VLAN која ће дозволити превођење саобраћаја који је потекао из тог VLAN-а (слика 4);
- дефинисати у ком смеру се ради превођење inside/outside (очекујемо саобраћај на подинтерфејсима као улазни, при чему ће излаз бити интерфјес F0/1) (слика 5);
- конфигурисати само превођење при чему се наводи која листа дозвољава превођење саобраћаја и кључна реч ***overload*** која укључује PAT тип превођења (слика 6).

```
R1(config)#access-list 1 permit 192.168.1.0 0.0.0.255
R1(config)#access-list 10 permit 192.168.10.0 0.0.0.255
R1(config)#access-list 20 permit 192.168.20.0 0.0.0.255
```

Слика 4 – Конфигурација стандардних листи за контролу приступа

```
R1(config)#interface fastethernet 0/0.1
R1(config-subif)#ip nat inside
R1(config-subif)#exit
R1(config)#interface fastethernet 0/0.10
R1(config-subif)#ip nat inside
R1(config-subif)#exit
R1(config)#interface fastethernet 0/0.20
R1(config-subif)#ip nat inside
R1(config-subif)#exit
R1(config)#
R1(config)#interface fastethernet 0/1
R1(config-if)#ip nat outside
R1(config-if)#exit
```

Слика 5 – Дефинисање смерова превођења

```
R1(config)#ip nat inside source list 1 interface fastEthernet 0/1 overload
R1(config)#ip nat inside source list 10 interface fastEthernet 0/1 overload
R1(config)#ip nat inside source list 20 interface fastEthernet 0/1 overload
```

Слика 6 – Активирање PAT превођења

```
PC>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.....: FE80::2D0:BCFF:FEB0:D144
   IP Address.....: 192.168.10.10
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: 192.168.10.1

PC>ping 200.0.0.20

Pinging 200.0.0.20 with 32 bytes of data:

Reply from 200.0.0.20: bytes=32 time=0ms TTL=126
Reply from 200.0.0.20: bytes=32 time=0ms TTL=126
Reply from 200.0.0.20: bytes=32 time=0ms TTL=126
Reply from 200.0.0.20: bytes=32 time=1ms TTL=126

Ping statistics for 200.0.0.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Слика 7 – Тестирање доступности сервера на адреси 200.0.0.20

```
R1#show ip nat translation
Pro  Inside global     Inside local       Outside local      Outside global
icmp 100.0.0.1:23      192.168.10.10:23   200.0.0.20:23      200.0.0.20:23
icmp 100.0.0.1:24      192.168.10.10:24   200.0.0.20:24      200.0.0.20:24
```

Слика 8 – Увид у табелу превођења на рутеру R1 после извршеног тестирања