universidade de aveiro
theoria poiesis praxis

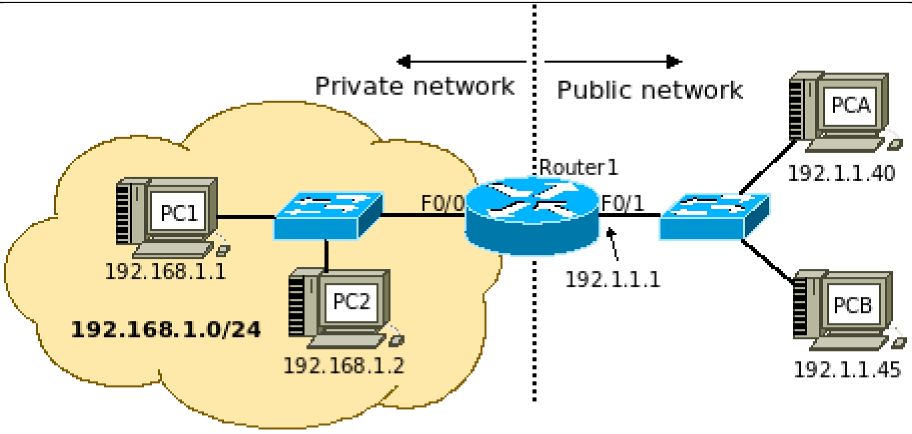
Redes e Serviços

Objectives

- Study of the NAT/PAT mechanisms.

Dynamic NAT

1. Assemble and configure (using the GNS3 and VPCS hosts) the network depicted in the following figure which represents a small company network. The company decided to configure IP private addressing using the network 192.168.1.0/24 and NAT mechanism (without PAT) to manage all Internet accesses. IP addresses and the respective gateway addresses must be manually configured. The company only have 2 public addresses (192.1.1.1/24 and 192.1.1.21/24).



Dynamic NAT Configuration

In order to define a pool of global addresses to be allocated by the dynamic NAT process, issue the following command on Router 1:

```
      Router (config)# ip nat pool MYNATPOOL 192.1.1.21 192.1.1.21 netmask 255.255.255.0
```

that defines a pool with a single public address.

The name MYNATPOOL is the name of the address pool. The first 192.1.1.21 in the command is the first IP address in the pool and the second 192.1.1.21 is the last IP address in the pool (this command creates a pool that contains only a single address).

Next, configure a standard access list to define which internal source addresses can be translated. Since any users on the private network are being translated, use the following command:

```
      Router 1(config)# access-list 2 permit 192.168.1.0 0.0.0.255
```

To establish the dynamic source translation, link the access list to the name of the NAT pool, as shown in the following:

```
      Router (config)# ip nat inside source list 2 pool MYNATPOOL
```

Finally, specify an interface on Router to be used by inside network hosts requiring address translation:

```
      Router (config)# interface f0/0
                  #change the interface name to the one used in your router
      Router (config-if)# ip nat inside
```

Also specify an interface to be used as the outside NAT interface as follows:

```
      Router (config)#interface f0/1
                  #change the interface name to the one used in your router
      Router (config-if)#ip nat outside
```

2. Start a packet capture on the public network and another on the private network. At PC1 execute a ping to 192.1.1.45 and on PC2 execute a ping to 192.1.1.45. Verify (on the router) the active NAT translations and NAT activity statistics, use the commands

```
      Router# show ip nat translations
      Router# show ip nat statistics
```

Which packets add the source IP addresses translated? Explain the obtained results.

3. Execute on the router the command to clear the NAT translation table:

```
  Router# clear ip nat translation *
```

and execute again at PC2 a ping to 192.1.1.40. Explain the observed results.

4. To block all traffic with a private source IP address use a Cisco extended ACL

```
  Router(config)# ip access-list extended notPrivate
  Router(config-ext-nacl)# deny   ip 192.168.0.0 0.0.255.255 any
  Router(config-ext-nacl)# permit ip any any
  Router(config)# interface f0/1
  Router(config-if)# ip access-group notPrivate out
```

Repeat experience 2 and explain the obtained results.

5. Change NAT timeout to 60 seconds and clear the NAT translations table:

```
 Router(config)# ip nat translation timeout 60
 Router# clear ip nat translation *
```

At PC1 execute a ping to 192.1.1.40 and immediately after at PC2 execute repeatedly a ping to 192.1.1.40. How much time does it take to obtain connectivity between PC2 and host 192.1.1.40. Explain the observed results.

Restore NAT timeout value to 86400 seconds (24 hours):

```
 Router(config)# ip nat translation timeout 86400
```

Dynamic NAT/PAT

6. Reconfigure the router in order to activate NAT and PAT mechanisms.

The most powerful feature of NAT is address overloading, or port address translation. Overloading allows multiple inside addresses to map to a single global address. With PAT, the NAT router keeps track of the different conversations by mapping TCP and UDP port numbers.
After defining the pool of global addresses to be allocated by the dynamic NAT process and configuring the standard access list that defines which internal source addresses can be translated, configure address overloading on Router with the following command:

```
      Router (config)#ip nat inside source list 2 pool MYNATPOOL overload
```

Repeat experience 2. Which are the advantages of using NAT and PAT mechanisms?

7. From PC1 (and PC2) try to establish UDP and TCP connections (ports 80 and 22) to host 192.1.1.40:

```
  PC> ping 192.1.1.40 -2 -p 80                    ! UDP port 80
  PC> ping 192.1.1.40 -2 -p 22                    ! UDP port 22
  PC> ping 192.1.1.40 -3 -p 80                    ! TCP port 80
  PC> ping 192.1.1.40 -3 -p 22                    ! TCP port 22
```

Verify (on the router) the active NAT translations and NAT activity statistics. Explain the obtained results.

Static NAT/PAT Translations

8. Suppose that know you have another public IP address available (192.1.1.201), configure the router in order to allow the PCA to access PC1.

A static translation between the inside local address of an host and one of the inside global addresses can be created using the following commands:

```
  Router (config)#ip nat inside source static 192.168.1.1 192.1.1.201
```

From PCA ping PC1's static public address (192.1.1.201)

```
 PCA> ping 192.1.1.201
```

Analise the captured packets on the private network and explain the obtained results.