REDES E SERVIÇOS

**Objectives**

- Access Control (Cisco's Access Lists)

Introduction to Cisco ACLs

1. Start your PC in Linux and configure your network according to the following figure. Use the specified IP addresses with network masks 255.255.255.0. Configure Router1 as the PC's default gateway in order to obtain full connectivity:

```
PC$ ifconfig eth0 192.10.#group.100/24
PC$ ifconfig eth0:0 192.10.#group.200/24
PC$ route add default gw 192.10.#group.1
```

Test the connectivity from the PC to both servers using both IP addresses:

```
PC$ ping 192.1.1.40 -I 192.10.#group.100
PC$ ping 192.1.1.45 -I 192.10.#group.100
PC$ ping 192.1.1.40 -I 192.10.#group.200
PC$ ping 192.1.1.45 -I 192.10.#group.200
```
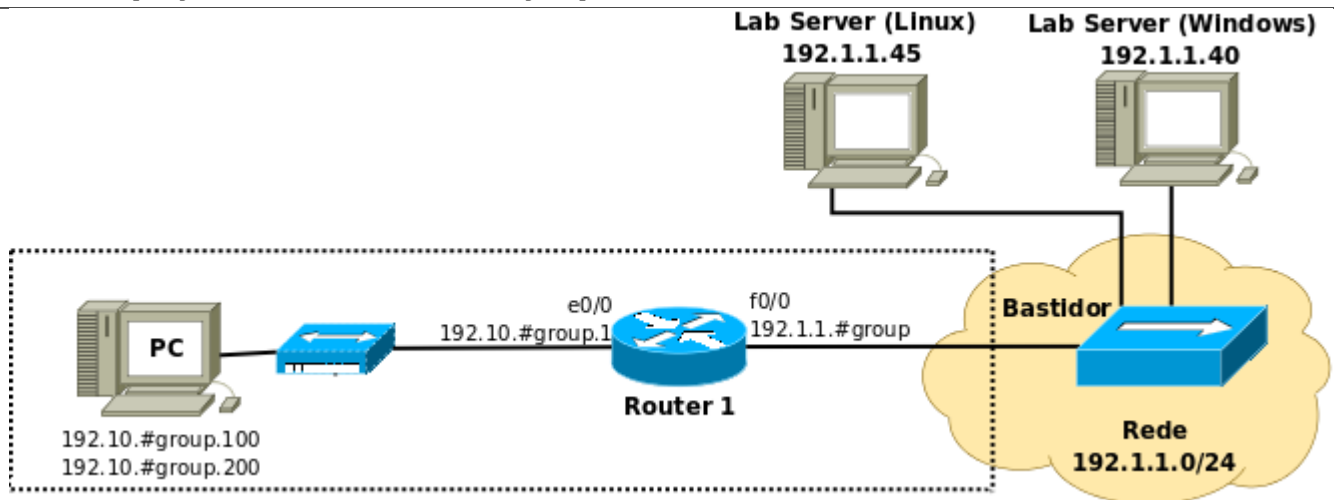

2. Configure in Router 1 the following standard ACL:

```
Router1(config)#access-list 1 permit 192.10.#group.100 0.0.0.0
```
! NOTE: creates a standard ACL that permits only traffic from PC1
```
Router1(config)#interface f0/0
Router1(config-if)#ip access-group 1 out
```
! NOTE: applies the ACL to outgoing traffic at interface f0/0

Start a packet capture on the PC and execute connectivity tests (ping) from PC to the servers in network 192.1.1.0. Analyze the captured (ICMP) packets. Explain how this ACL works.

3. Modify the ACL previously created in order to all devices, except the PC, be able to access the servers.

```
Router1(config)#no access-list 1 permit 192.10.#group.100 0.0.0.0
```
#NOTE: deletes the previous ACL
```
Router1(config)#access-list 1 deny 192.10.#group.100 0.0.0.0
Router1(config)#access-list 1 permit any
```
Execute connectivity tests (ping) from PC to the servers in network 192.1.1.0. Analyze the captured (ICMP) packets. Explain how this ACL works.

4. Remove the standard ACL in Router 1,

```
Router1(config)#no access-list 1 deny 192.10.#group.100 0.0.0.0
Router1(config)#no access-list 1 permit any
Router1(config)#interface f0/0
Router1(config-if)#no ip access-group 1 out
```
And configure the following extended ACL:
```
Router1(config)#access-list 101 permit tcp host 192.10.#group.100 host 192.1.1.45 eq 80
Router1(config)#access-list 101 permit tcp host 192.10.#group.200 host 192.1.1.45 eq 80
Router1(config)#interface e0/0
Router1(config-if)#ip access-group 101 in
Router1(config-if)#end
```
Execute connectivity tests (ping) from PC to the servers in network 192.1.1.0. Analyze the captured (ICMP) packets. Using a browser access the server 192.1.1.45's web page. Explain how this ACL works.