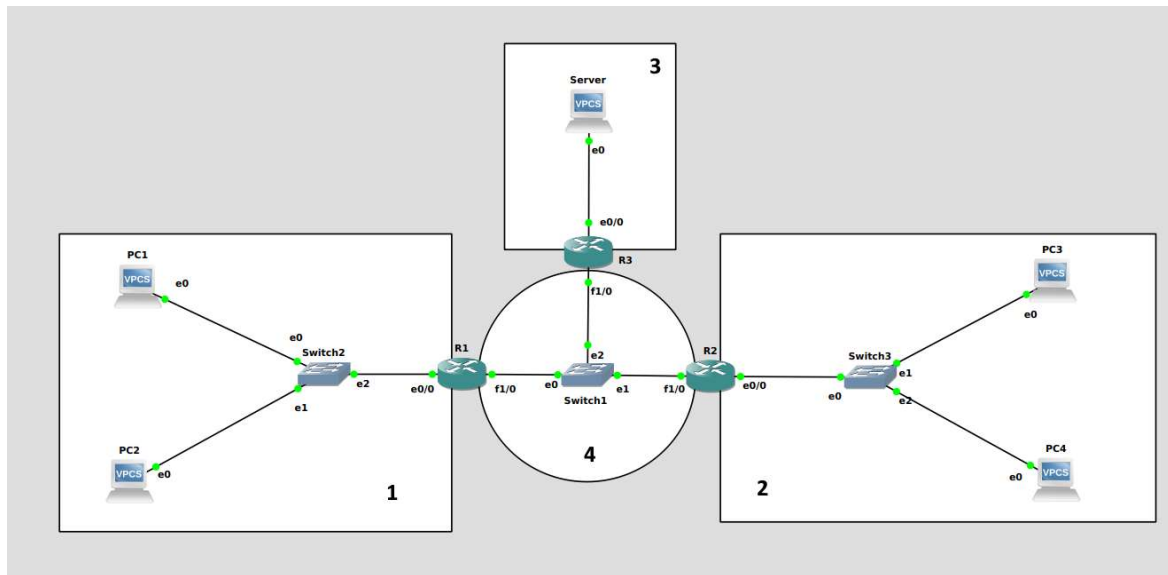


Redes de Comunicação 2020/2021

Relatório da meta intermédia

Alexandre Andrade – 2019220216

Tomás Mendes – 2019232272



1

Network – 193.136.212.128/26

- **R1** – 193.136.212.190/26
- **PC1** – 193.136.212.129/26
- **PC2** – 193.136.212.130

3

Network – 10.90.0.0/24

- **R3** – 10.90.0.245/24
- **Server** – 10.90.0.1/24

2

Network – 193.136.212.192/27

- **R2** – 193.136.212.222/27
- **PC3** – 193.136.212.193/27
- **PC4** – 193.136.212.194/27

4

Network – 193.136.212.224/29

- **R1** – 193.136.212.225/29
- **R2** – 193.136.212.226/29
- **R3** – 193.136.212.227/29

Comandos de configuração:

R1:

```
conf t
interface e0/0
ip address 193.136.212.190 255.255.255.192
no shut
exit
interface f1/0
ip address 193.136.212.225 255.255.255.248
no shut
exit
ip route 193.136.212.192 255.255.255.224 193.136.212.226
exit
```

R2:

```
conf t
interface e0/0
ip address 193.136.212.222 255.255.255.224
no shut
exit
interface f1/0
ip address 193.136.212.226 255.255.255.248
no shut
exit
ip route 193.136.212.128 255.255.255.192 193.136.212.225
exit
```

R3:

```
conf t
interface e0/0
ip address 10.90.0.254 255.255.255.0
ip nat inside
no shut
exit
interface f1/0
ip address 193.136.212.227 255.255.255.248
ip nat outside
no shut
exit
ip route 193.136.212.128 255.255.255.192 193.136.212.225
ip route 193.136.212.192 255.255.255.224 193.136.212.226
access-list 1 permit 10.90.0.0 0.0.0.255
ip nat inside source list 1 interface f1/0 overload
ip nat inside source static tcp 10.90.0.1 9002 193.136.212.227 9002
ip nat inside source static udp 10.90.0.1 9003 193.136.212.227 9003
exit
```

PC1: ip 193.136.212.129/26 193.136.212.190

PC2: ip 193.136.212.130/26 193.136.212.190

PC3: ip 193.136.212.193/27 193.136.212.222

PC4: ip 193.136.212.194/27 193.136.212.222

Server: ip 10.90.0.1/24 10.90.0.254

Ping 1 -> 2 e 1 -> 4

```
PC1> ping 193.136.212.227 -3 -p 80

Connect 808193.136.212.227 seq=1 ttl=62 time=21.689 ms
SendData 808193.136.212.227 seq=1 ttl=62 time=27.655 ms
Close 808193.136.212.227 seq=1 ttl=62 time=27.655 ms
Connect 808193.136.212.227 seq=2 ttl=62 time=27.613 ms
SendData 808193.136.212.227 seq=2 ttl=62 time=24.410 ms
Close 808193.136.212.227 seq=2 ttl=62 time=24.429 ms
Connect 808193.136.212.227 seq=3 ttl=62 time=26.673 ms
SendData 808193.136.212.227 seq=3 ttl=62 time=24.457 ms
Close 808193.136.212.227 seq=3 ttl=62 time=25.643 ms
Connect 808193.136.212.227 seq=4 ttl=62 time=26.295 ms
SendData 808193.136.212.227 seq=4 ttl=62 time=24.608 ms
Close 808193.136.212.227 seq=4 ttl=62 time=26.670 ms
Connect 808193.136.212.227 seq=5 ttl=62 time=26.609 ms
SendData 808193.136.212.227 seq=5 ttl=62 time=25.574 ms
Close 808193.136.212.227 seq=5 ttl=62 time=25.709 ms

PC1> ping 193.136.212.193

84 bytes from 193.136.212.193 icmp_seq=1 ttl=62 time=21.836 ms
84 bytes from 193.136.212.193 icmp_seq=2 ttl=62 time=27.263 ms
84 bytes from 193.136.212.193 icmp_seq=3 ttl=62 time=26.799 ms
84 bytes from 193.136.212.193 icmp_seq=4 ttl=62 time=28.344 ms
84 bytes from 193.136.212.193 icmp_seq=5 ttl=62 time=28.848 ms
```

Ping 2 -> 1 e 2 -> 4

```
PC3> ping 193.136.212.227 -3 -p 80

Connect 808193.136.212.227 seq=1 ttl=62 time=49.924 ms
SendData 808193.136.212.227 seq=1 ttl=62 time=31.844 ms
Close 808193.136.212.227 seq=1 ttl=62 time=42.385 ms
Connect 808193.136.212.227 seq=2 ttl=62 time=26.574 ms
SendData 808193.136.212.227 seq=2 ttl=62 time=25.558 ms
Close 808193.136.212.227 seq=2 ttl=62 time=25.878 ms
Connect 808193.136.212.227 seq=3 ttl=62 time=27.612 ms
SendData 808193.136.212.227 seq=3 ttl=62 time=24.374 ms
Close 808193.136.212.227 seq=3 ttl=62 time=25.465 ms
Connect 808193.136.212.227 seq=4 ttl=62 time=36.948 ms
SendData 808193.136.212.227 seq=4 ttl=62 time=39.248 ms
Close 808193.136.212.227 seq=4 ttl=62 time=40.443 ms
Connect 808193.136.212.227 seq=5 ttl=62 time=37.745 ms
SendData 808193.136.212.227 seq=5 ttl=62 time=37.614 ms
Close 808193.136.212.227 seq=5 ttl=62 time=39.398 ms

PC3> ping 193.136.212.129

84 bytes from 193.136.212.129 icmp_seq=1 ttl=62 time=38.473 ms
84 bytes from 193.136.212.129 icmp_seq=2 ttl=62 time=27.150 ms
84 bytes from 193.136.212.129 icmp_seq=3 ttl=62 time=27.489 ms
84 bytes from 193.136.212.129 icmp_seq=4 ttl=62 time=28.317 ms
```

Ping 3 -> 1 e 3 -> 2

```
Server> ping 193.136.212.129

84 bytes from 193.136.212.129 icmp_seq=1 ttl=62 time=40.106 ms
84 bytes from 193.136.212.129 icmp_seq=2 ttl=62 time=26.677 ms
84 bytes from 193.136.212.129 icmp_seq=3 ttl=62 time=26.867 ms
84 bytes from 193.136.212.129 icmp_seq=4 ttl=62 time=26.227 ms
84 bytes from 193.136.212.129 icmp_seq=5 ttl=62 time=27.110 ms

Server> ping 193.136.212.193

193.136.212.193 icmp_seq=1 timeout
84 bytes from 193.136.212.193 icmp_seq=2 ttl=62 time=38.033 ms
84 bytes from 193.136.212.193 icmp_seq=3 ttl=62 time=27.542 ms
84 bytes from 193.136.212.193 icmp_seq=4 ttl=62 time=27.477 ms
84 bytes from 193.136.212.193 icmp_seq=5 ttl=62 time=27.906 ms
```

Teste DNAT

Wireshark capture showing DNAT test results. The packet list shows a sequence of packets from 193.136.212.129 to 193.136.212.227. The packet details show the destination IP being changed from 193.136.212.129 to 193.136.212.227. The packet bytes show the raw data of the packets.

Teste SNAT

Wireshark capture showing SNAT test results. The packet list shows a sequence of packets from 193.136.212.129 to 193.136.212.227. The packet details show the source IP being changed from 193.136.212.129 to 193.136.212.227. The packet bytes show the raw data of the packets.

Escolhas feitas

Para facilitar a gestão dos IP's e portos dos utilizadores, foram criadas várias estruturas, do lado dos clientes e do lado do servidor. Do lado do cliente, a estrutura *node* guarda o *username*, IP e porto dos utilizadores para o qual já fez uma comunicação P2P, apenas sendo necessário pedir estes dados ao servidor uma vez, diminuindo assim os acessos ao servidor. A outra estrutura do lado do cliente, *nodeGrp*, guarda o nome do grupo e o IP de *multicast* em que esse utilizador pode participar.

Do lado do servidor, existe uma estrutura que guarda os mesmos dados que estão no ficheiro dos *users*, diminuindo os acessos ao ficheiro. A outra estrutura guarda o nome, IP *multicast* e os nomes dos vários participantes dos vários grupos criados pelos utilizadores que tenham permissões.

Quando os clientes fazem *login*, é criada uma entrada na estrutura gerida pelo servidor, onde estão todos os utilizadores autenticados. Quando um cliente sai, seja pelo comando QUIT ou por um *ctrl + c*, a sua entrada é removida, deixando de estar autenticado. Apenas um cliente que esteja autenticado poderá enviar/receber as mensagens, se tiver as devidas permissões. Os clientes, com as devidas permissões, podem enviar mensagens para outro utilizador pelo servidor ou diretamente (*peer to peer*) e criar grupos. Um utilizador sem permissões de grupo, não pode criar, entrar ou receber mensagens.

Para a comunicação em grupo, um utilizador define o nome do grupo, pede ao servidor um IP *multicast* disponível e associa os utilizadores que poderão aceder ao grupo. O número máximo de grupos que podem existir de uma vez está definido por MAX_GROUPS.

O servidor cria um processo para cada *admin* que se conecta pelo porto de configuração, podendo haver vários *admins* em simultâneo, apesar de não haver nenhum mecanismo de sincronização para o acesso ao ficheiro com os dados dos utilizadores nem às estruturas com os dados dos grupos e utilizadores.