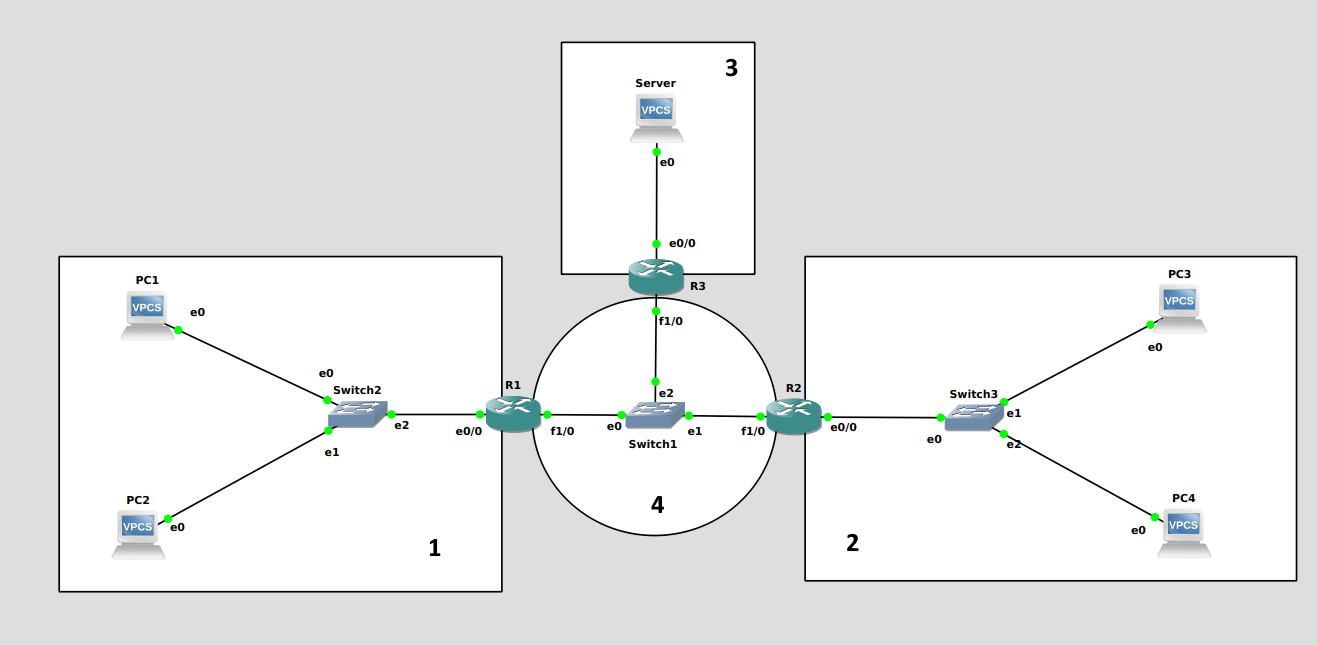
**Redes de Comunicação 2020/2021**

**Relatório da meta intermédia**

**Alexandre Andrade – 2019220216**

**Tomás Mendes – 2019232272**

**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

**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

**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

**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

**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

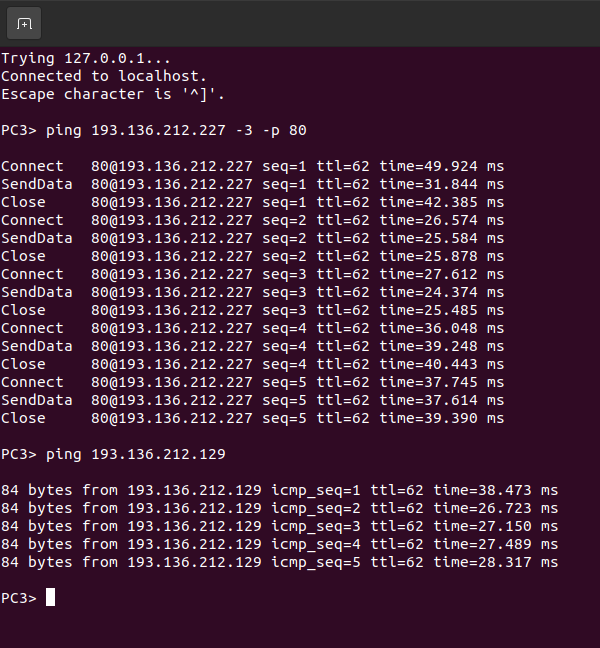
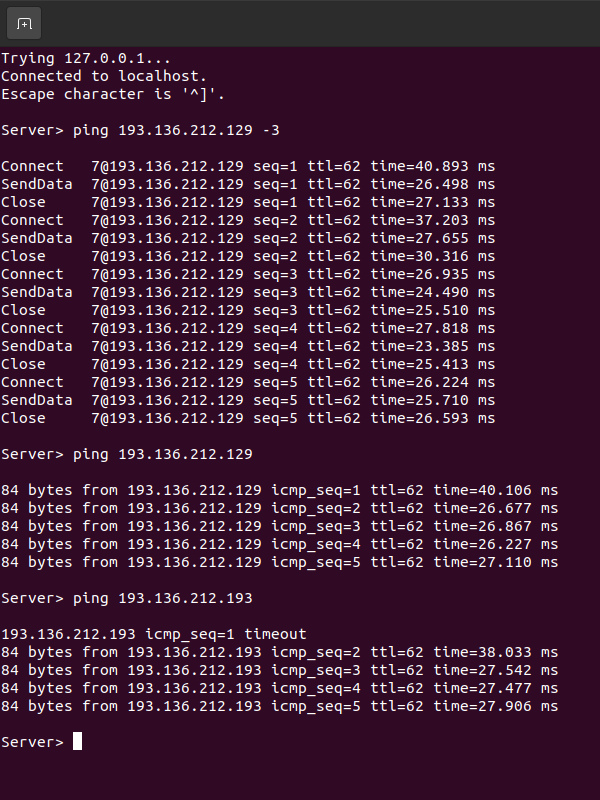
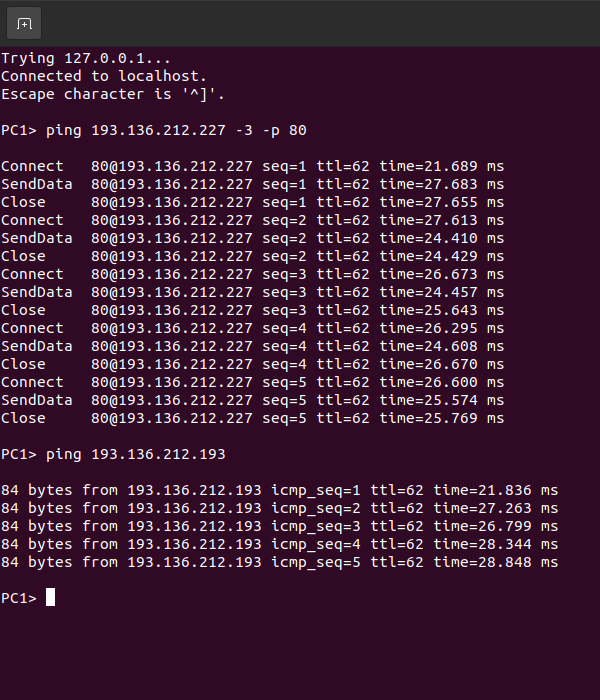
ip address 193.136.212.226 255.255.255.248

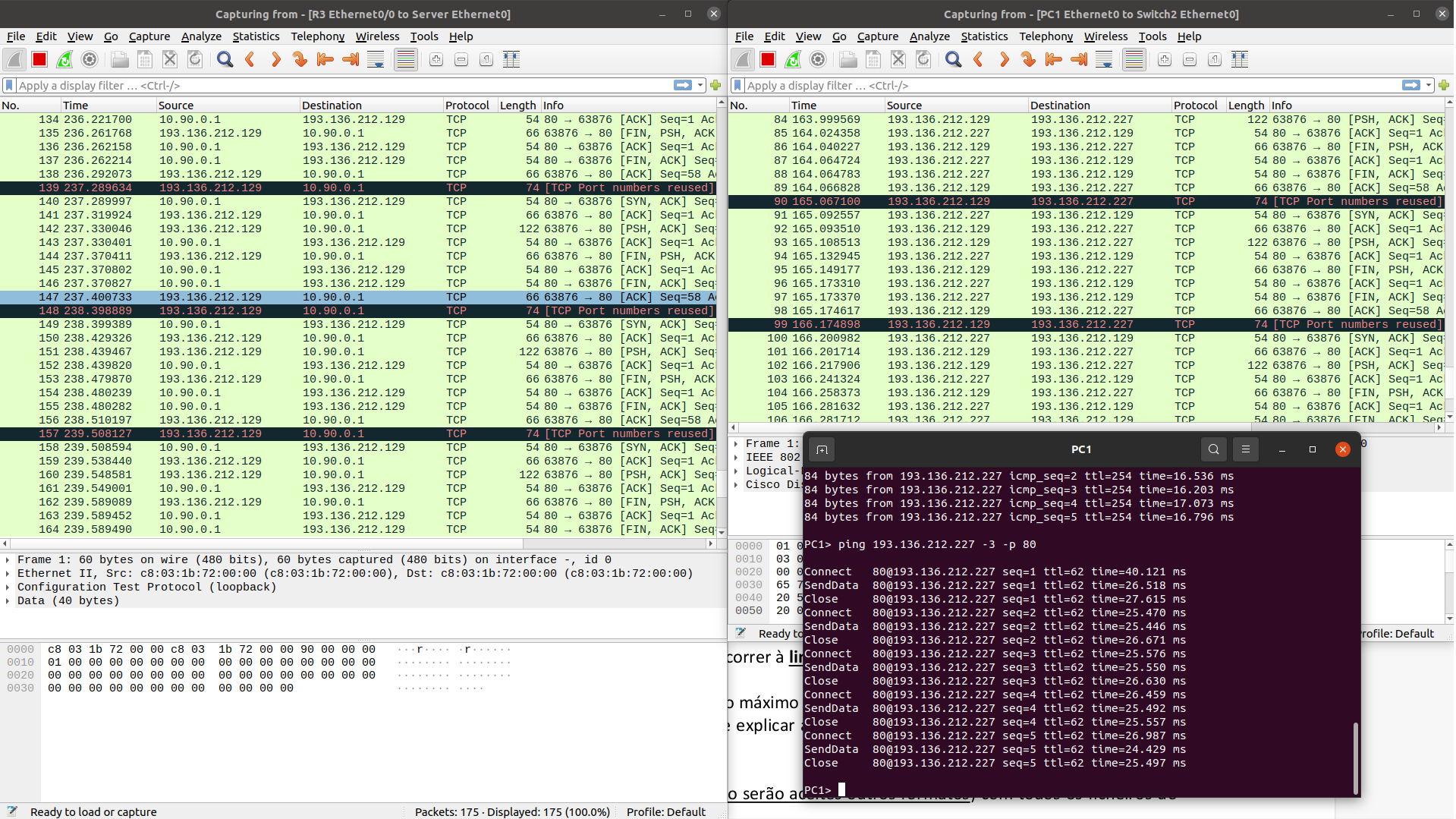
no shut

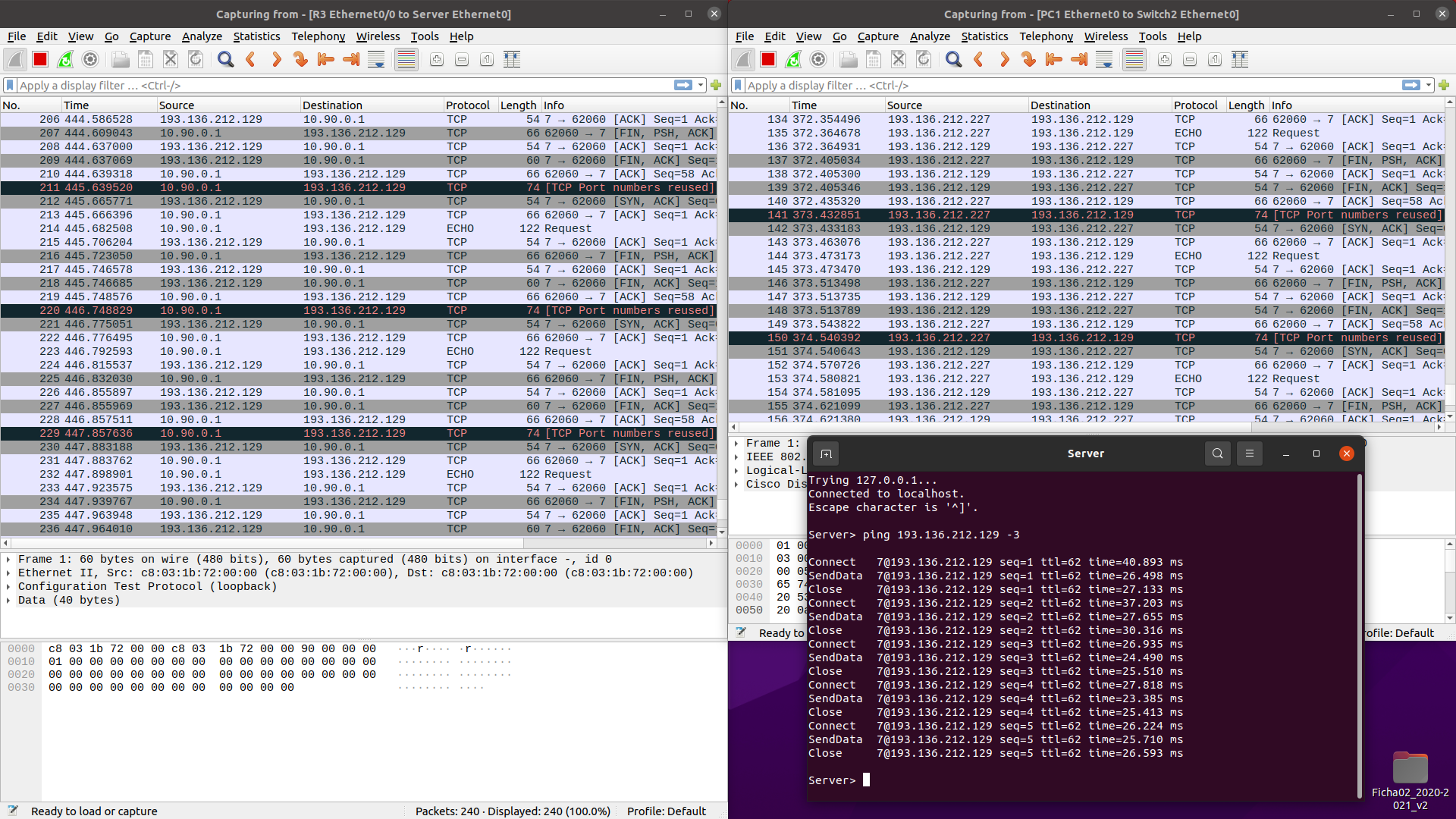
exit

ip route 193.136.212.128 255.255.255.192 193.136.212.225

exit

**Ping 1 –> 2 e 1 –> 4 Ping 2 –> 1 e 2 –> 4 Ping 3 –> 1 e 3 –> 2**

**Teste DNAT**

**Teste SNAT**

**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 devias 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 conecte 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.