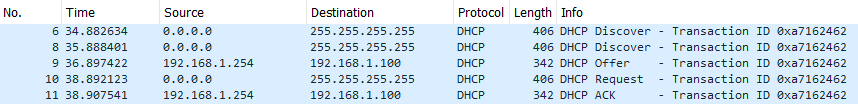
**DHCP**

**10)**

**Parte 1:**

Ao executar o comando “ip dhcp” no terminal do PC1, este vai receber um ip novo automaticamente a partir do protocolo “dhcp”.



Pela captura da interface F0/0 do router, podemos verificar o método usado para atribuir um ip ao PC1.

Discover:

O processo começa por descobrir um servidor DHCP livre. Podemos verificar que o processo de “discover” acontece duas vezes até encontrar um servidor DHCP livre neste caso, no entanto este processo pode acontecer ainda mais vezes. Além disso, podemos também verificar que o Broadcast do “discover” vai desde o ip “0.0.0.0” até “255.255.255.255”, devido ao facto de o PC1 não ter conhecimento nenhum sobre onde poderá estar o o servidor DHCP.

Offer:

Após o PC1 descobrir o servidor DHCP, este oferece ao PC1 um ip que tenha e que esteja livre. Neste caso ele oferece o ip 192.168.1.100, devido a dois motivos:

* Nós limitamos anteriormente o DHCP a apenas oferecer endereços na faixa dos 192.168.1.100 até o 192.168.1.200;
* Quando este oferece ao PC1 um ip, este oferece o primeiro que esteja livre, logo, uma vez que todos estão livres, é atribuído o primeiro que é o 192.168.1.100;

Request:

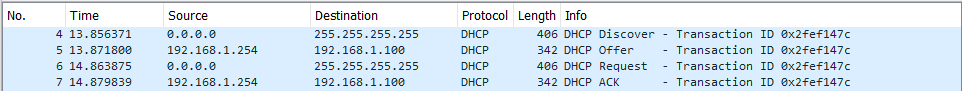
Assim que o PC1 recebe a oferta de endereço do servidor DHCP, este envia uma “request” a indicar que pretende ficar com o endereço ip que lhe foi oferecido. Devido ao facto de só termos 1 servidor DHCP nesta simulação, este passo pode não parecer tão importante, no entanto, nos casos em que existem vários servidores DHCP e, por consequência, varias ofertas de endereço de ip, este passo já se torna mais importante pois é onde o cliente (neste caso o PC1) vai escolher entre as varias ofertas, o endereço de ip com que se pretende associar.

ACK:

Por ultimo, após a escolha de ip pela parte do PC1, o servidor DHCP que forneceu o endereço de ip reponde dando “luz verde”, dando finalmente o novo ip ao PC1.

**Parte 2:**

Ao executar o comando “ip dhcp -r” no terminal do PC1, este vai renovar, dinamicamente, o seu endereço de ip. No entando, como o endereço 192.168.1.100 ainda está livre, e por causa da forma que o protocolo DHCP dá ips (que já foi explicada em cima, junto com o “Request”), este volta a receber o mesmo ip (192.168.1.100).



Podemos ver que mais uma vez é usado o método dddora( Discover, Offer, Request, ACK) que já foi explicado em cima para renovar o endereço de ip do PC1.

**Parte 3:**

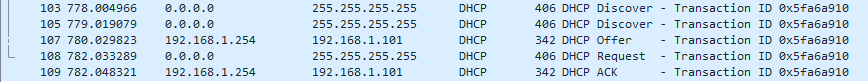
Ao executar o comando “ip dhcp -x” no terminal do PC1, este vai se livrar do endereço de ip que lhe foi atribuído anteriormente, ficando com o ip básico 0.0.0.0.



Como podemos observar a partir do wireshark, ao executar o comando aparece o pacote “DHCP Release”, que indica que o endereço 192.168.1.100 já não pertence ao PC1.

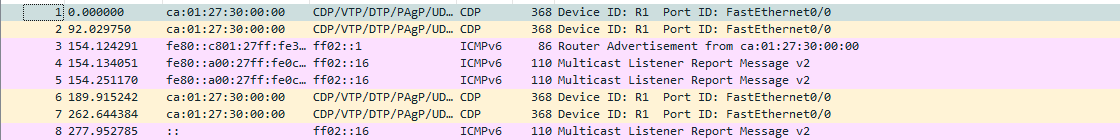
**Parte 4:**

Ao executar o comando “ip dhcp” no terminal do PC1, este vai novamente receber um ip novo automaticamente a partir do protocolo “dhcp”, no entanto desta vez vai receber o ip 192.168.1.101 invés do 192.168.1.100. Isto deve-se ao facto de o comando anterior , apesar de ter “disconectado” o ip 192.168.1.100 do PC1, não libertou de forma correta o ip 192.168.1.100, logo este é visto como não estando livre, apesar de não estar associado a nenhum dispositivo. Para o endereço de ip ficar livre novamente agora existem duas soluções, ou esperar que o seu tempo de uso expire, ou manualmente usar um comando para o libertar corretamente.

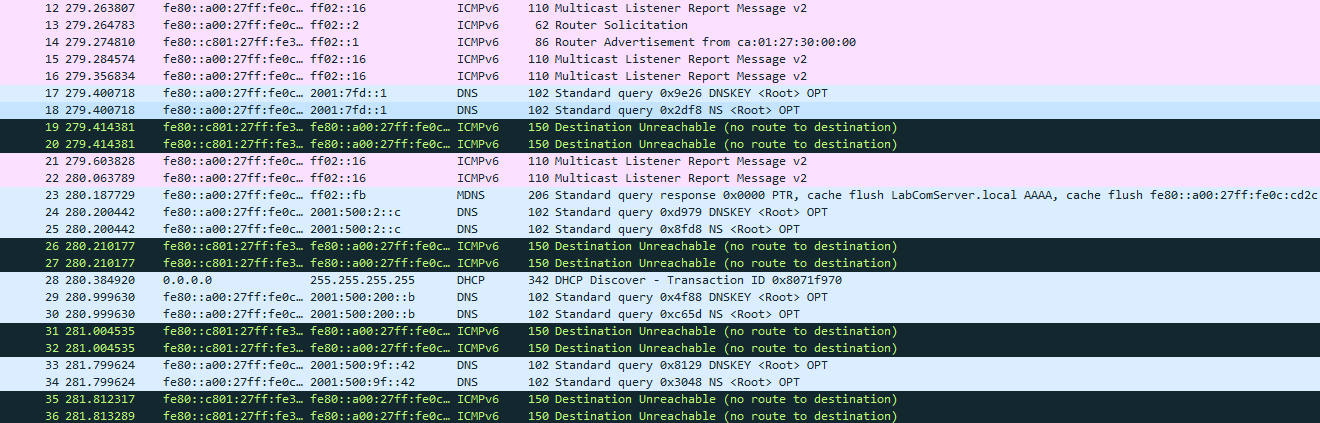


Nos pacotes que apanhamos podemos verificar aquilo discutido acima, onde no processo Offer, o servidor DHCP oferece o ip 192.168.1.101, devido ao facto de não ver o ip 192.168.1.100 como estando livre.

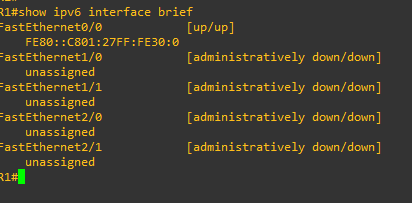
**IPV6**

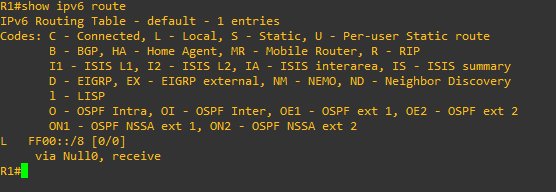
**2)**

Pacotes capturados após o comando "sudo ifconfig enp0s3 down ". Com o IPV6 habilitado alguns pacotes IPV6 multicast listener são capturados mas ainda não existem tentativas de ligação.



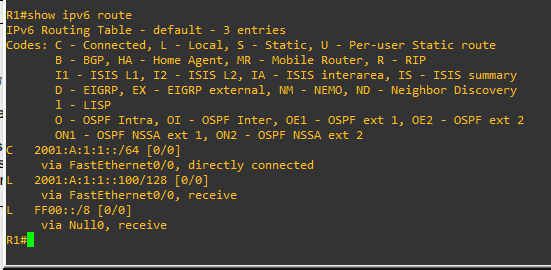
Pacotes capturados após o comando "sudo ifconfig enp0s3 up", já podemos observar tentativas de ligação, mas como o IPV6 ainda não possui endereços para utilizar, recebemos constantemente "Destination Unrecheable".

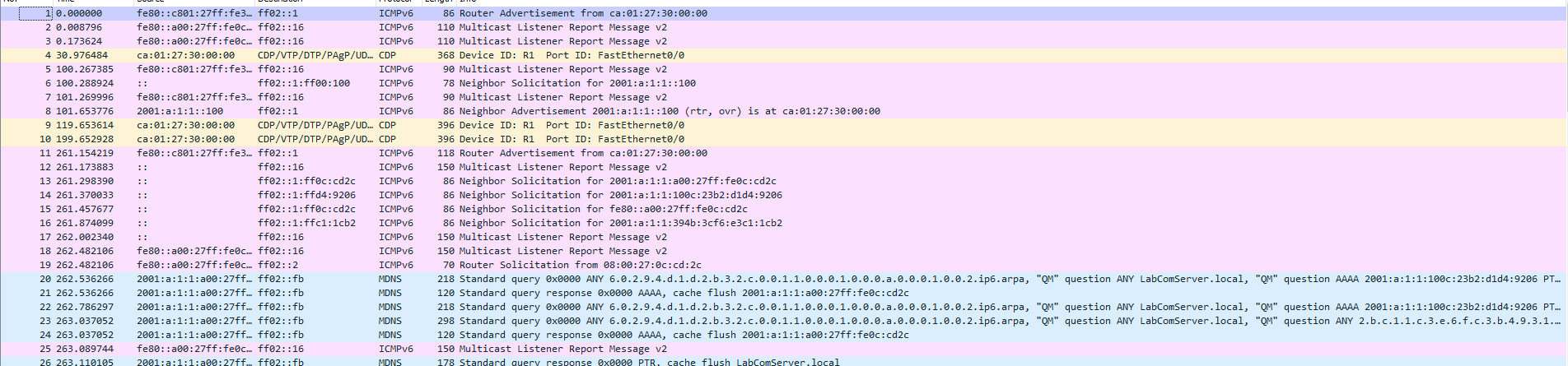
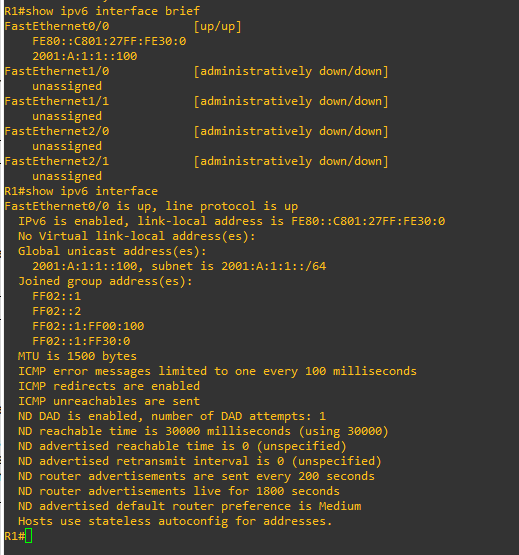




Observamos que como ainda não fizemos a atribuição de endereços do IPV6, temos apenas uma rota local.

**3)**

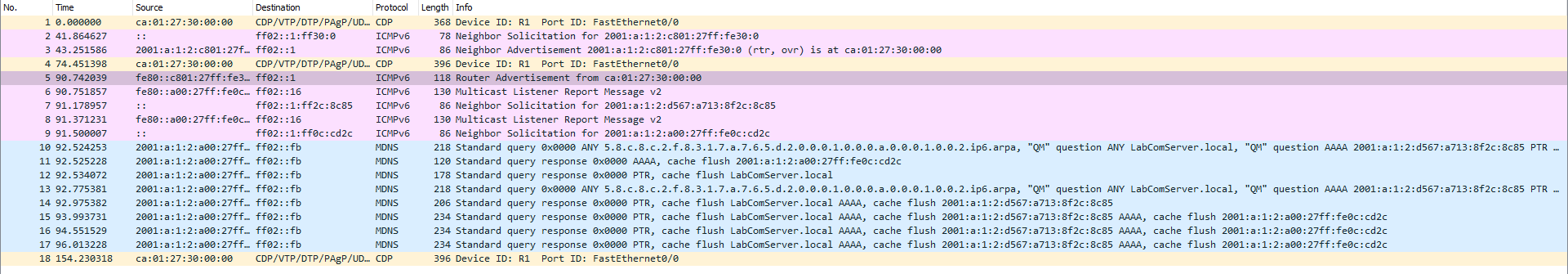




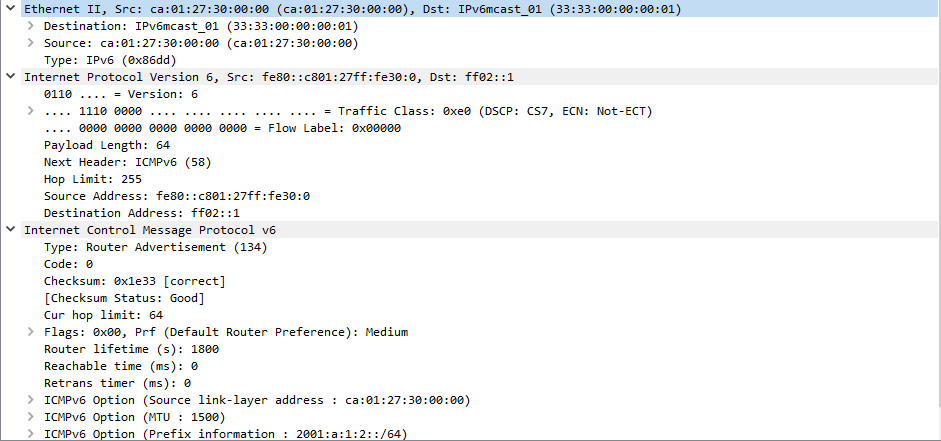
Após configurar a interface do router com um endereço de IPV6 podemos observar que a mensagem de "Destination Unrecheable" não é mais enviada, isto porque agora o nosso VPC pode ligar-se corretamente a um endereço IPV6.

Também podemos verificar o funcionamento da conexão do IPV6 com o PC, começando com um pacote de advertisement do router, seguido de vários pacotes de Listener Report e um Neighbour advertisement para o endereço IPV6 fornecido (indicando também o endereço físico onde está alocado). Isto é seguido por pacotes de Neighbour Solicitation pelo VPC e confirmação do router.

**4)**



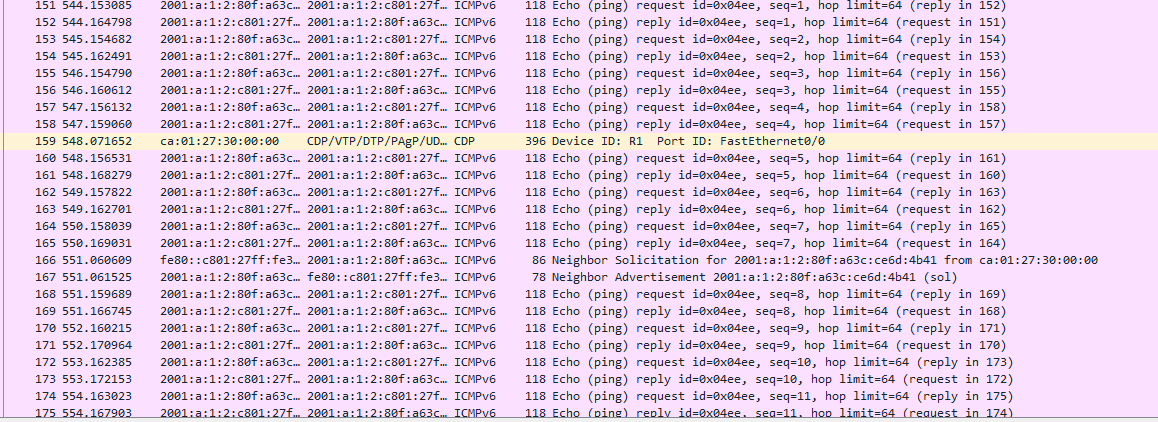
Observamos que o processo de ligação manteve-se praticamente idêntico em termos de que passos foram seguidos, mas também é de notar que o processo é considerávelmente mais curto do que o anterior.



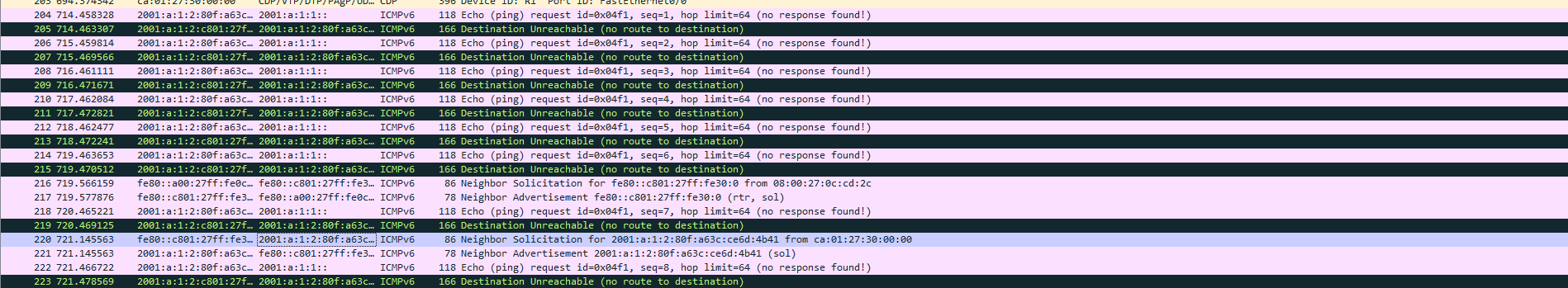


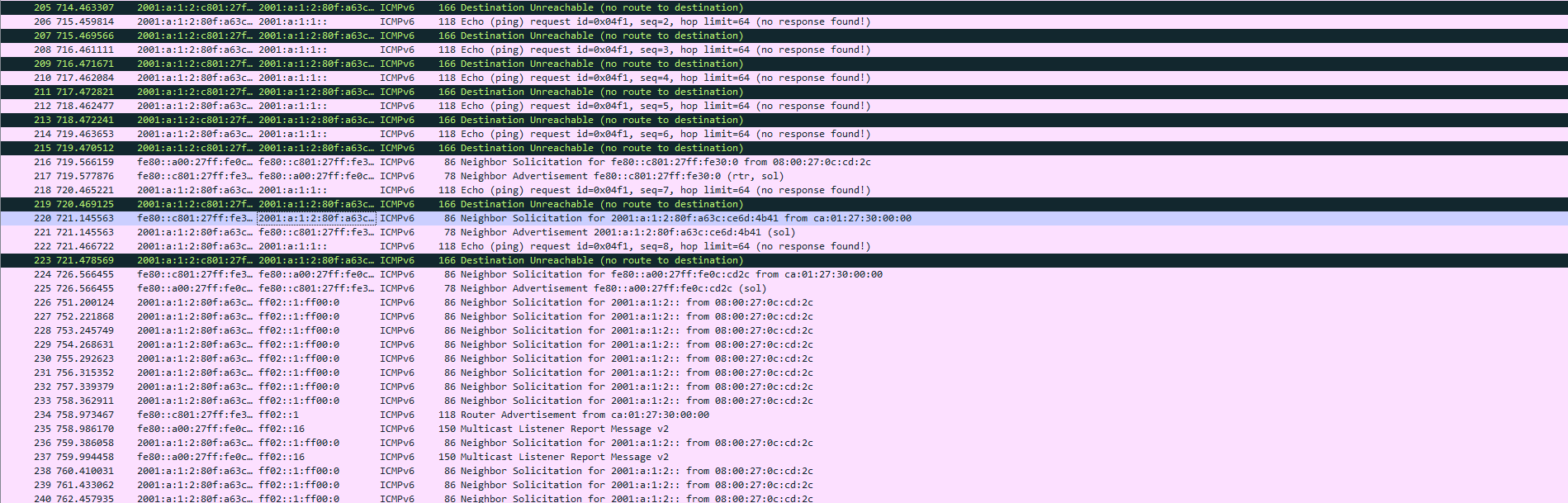
Processo de extensão de bits do IPV6, utilizando zeros.

**5)**



ping6 feito ao Router Link-local addess.





Pings efetuados aos 2001:A:1:1:: e 2001:A:1:2:: respetivamente. Observamos que no os pings feitos ao primeiro global address resultaram numa mensagem de "destination unrecheable", ao contrário dos enviados ao segundo global address.