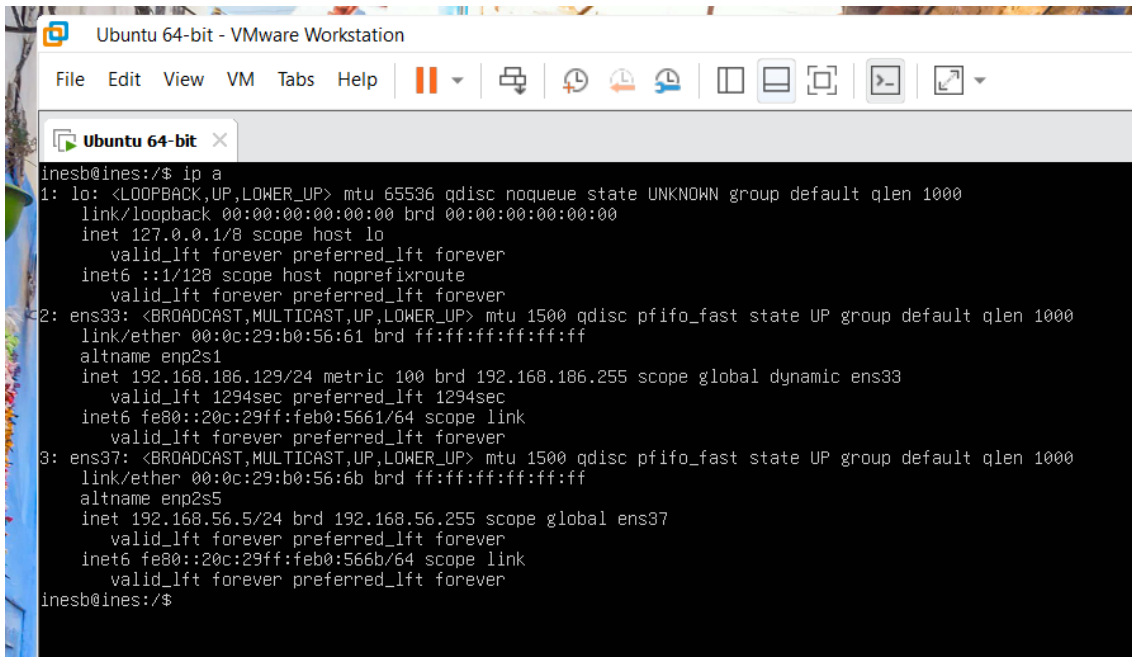


# PL4



```
inesb@ines:/$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:b0:56:61 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.186.129/24 metric 100 brd 192.168.186.255 scope global dynamic ens33
        valid_lft 1294sec preferred_lft 1294sec
    inet6 fe80::20c:29ff:feb0:5661/64 scope link
        valid_lft forever preferred_lft forever
3: ens37: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:b0:56:6b brd ff:ff:ff:ff:ff:ff
    altname enp2s5
    inet 192.168.56.5/24 brd 192.168.56.255 scope global ens37
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:feb0:566b/64 scope link
        valid_lft forever preferred_lft forever
inesb@ines:/$
```

## Ethernet adapter VMware Network Adapter VMnet1:

```
Connection-specific DNS Suffix . : 
Link-local IPv6 Address . . . . . : fe80::1d98:80f2:6741:6e4%23
IPv4 Address. . . . . : 192.168.140.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
```

## Ethernet adapter VMware Network Adapter VMnet8:

```
Connection-specific DNS Suffix . : 
Link-local IPv6 Address . . . . . : fe80::ef60:b0d7:b553:452c%10
IPv4 Address. . . . . : 192.168.186.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
```

## Ethernet adapter VMware Network Adapter VMnet2:

```
Connection-specific DNS Suffix . : 
Link-local IPv6 Address . . . . . : fe80::3f29:89d2:41bf:3db2%12
IPv4 Address. . . . . : 192.168.56.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
```

## Wireless LAN adapter Wi-Fi:

```
Connection-specific DNS Suffix . : home
Link-local IPv6 Address . . . . . : fe80::a593:a473:d665:178c%9
IPv4 Address. . . . . : 192.168.1.6
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
PS C:\Users\inesb> |
```

- 1) Inspect your laptop's current network configuration status to see the value of each of these attributes provided by the DHCP server, either using the graphical user interface tools or the command line. In Windows, you can use `ipconfig /all` in the command line to view detailed network configuration.

Identify:

- Your own IPv4 address: 192.168.1.6
- The IPv4 address of the default-gateway: 192.168.1.1
- The IPv4 addresses of two local DNS servers: 192.168.1.1

- 2) Inside you Linux VM, to quickly identify all available Ethernet interfaces, you can use the `ip` command as shown:

What are the main differences to the older `ifconfig` command?

- ip: Mostra todas as interfaces, mesmo as inativas (`ip addr` ou `ip link show`).
- ip: Mais completo, permite gerir interfaces, rotas, túneis e suporta IPv6 de forma avançada.
- ip: Informação detalhada e estruturada, adequada para configurações avançadas.
- ifconfig: Limitado a configurações básicas de interfaces e com suporte limitado a IPv6.
- ifconfig: Saída simples, mas menos informativa.
- ifconfig: Mostra apenas interfaces ativas (a menos que seja especificado).

- 3) Another application that can help identify all network interfaces available to your system is the `lshw` command. This command provides greater details around the hardware capabilities of specific adapters. Analyze your Linux VM with:

**\$ sudo lshw -class network**

Resposta: O comando `sudo lshw -class network` no Linux é utilizado para listar informações detalhadas sobre os dispositivos de rede do sistema, incluindo interfaces de rede Ethernet, Wi-Fi, e outras. O comando `lshw` é uma ferramenta poderosa para exibir informações sobre o hardware do sistema e, ao utilizar o parâmetro `-class network`, restringe-se a saída para exibir apenas os dispositivos de rede.

- 4) 4. Check IPv4 connectivity with some nodes around you. At the command prompt use

the `ping` command:

- a. Ping your own address (depending on your system, the `ping` command may continue sending ICMP echo requests forever, press `CTRL+C` to stop it).

Resposta: \$ping 192.168.56.5

- b. Ping the loopback address (127.0.0.1).

Resposta: \$ping 127.0.0.1 (para testar a conectividade com a interface de loopback do seu sistema).

- c. Ping the default gateway.

Resposta: \$ping 192.168.1.1 (se não receber respostas, pode indicar um problema de conectividade com o gateway ou configuração de rede incorreta).

**d. Ping the local DNS servers. Notice that some DNS servers might not respond, even though IPv4 nodes should always reply to ICMP echo requests, for security reasons, some servers may have this kind of traffic blocked by a firewall.**

Resposta: \$ping 192.168.1.1

(Para testar a conectividade com os servidores DNS, use o comando ping seguido do endereço IP do servidor DNS. Neste caso, os endereços IP do *Default Gateway* e do *DNS Server* são iguais (192.168.1.1) porque o seu router está a fornecer ambos os serviços — tanto de encaminhamento de tráfego (gateway) como de resolução de nomes (DNS). Esta configuração é bastante comum em redes domésticas, onde o router atua como um servidor DHCP, *gateway* e servidor DNS, fornecendo todos esses serviços aos dispositivos da rede local).

**e. Ping www.google.com. You you can also provide a DNS host name. DNS servers are used to fetch the corresponding IP address. You may also ping some additional DNS names of the internet. This way the ping command also tell us if the local DNS resolution of names is working.**

Resposta: \$ping www.google.com

(Caso o comando falhe, pode ser devido a problemas com o servidor DNS ou com a conectividade à Internet. Para verificar se o problema está na resolução de DNS, pode tentar pingar diretamente um endereço IP, como o do Google DNS (8.8.8.8), com o comando ping 8.8.8.8. Se o ping ao IP funcionar, mas o ping ao nome de domínio falhar, então o problema provavelmente está relacionado ao serviço de resolução de DNS).

**g. From your host machine, ping your Linux VM. Ensure that you have already determined its address.**

Resposta: \$ping 192.168.56.5

(Se estás a ver duas interfaces ativas (ens33 com 192.168.186.129 e ens37 com 192.168.56.5), isso indica que a tua máquina virtual está ligada a duas redes diferentes:

- ens33 (192.168.186.129):

Este IP pertence à sub-rede associada ao VMnet8 (NAT). Esta rede permite que a tua VM acesse a Internet utilizando o IP do host como gateway. É útil para acesso à Internet a partir da VM.

- ens37 (192.168.56.5):

Este IP pertence à sub-rede associada ao VMnet2 (Host-Only). Esta rede permite comunicação direta entre a tua máquina host e a VM, mas sem acesso à Internet.

- lo (127.0.0.1) é a interface de loopback. Esta é uma interface especial usada pelo sistema para se comunicar consigo mesmo.

O IP 127.0.0.1 (e outros IPs no intervalo 127.0.0.0/8) é reservado para testes locais e comunicação interna no sistema (Quando um programa precisa de comunicar com outro programa no mesmo computador (como servidores locais ou aplicações de

teste), utiliza o 127.0.0.1. Se quiser verificar, por exemplo, se a pilha de rede no meu sistema funciona corretamente, executo `$ping 127.0.0.1`.

Resumidamente:

lo: Apenas para comunicações internas no mesmo sistema. Não pode ser usada para comunicação com outras máquinas.

ens33, ens37, etc.:

São interfaces físicas ou virtuais que permitem comunicação com outras máquinas na rede.

#### **h. From your Linux VM, ping your host machine.**

Resposta: no host executo `ipconfig`

IPv4: 192.168.1.6

`$ping 102.168.1.6`

(Quando temos uma máquina virtual a correr, pode ser importante garantir que a VM consegue comunicar com o sistema anfitrião (a máquina host). Fazer o *ping* serve para verificar se a comunicação de rede entre a VM e o PC está a funcionar corretamente).

#### **5. The `tracpath` command is used to conduct a similar test to ping, but instead of displaying the time it takes to connect, it looks at the exact server hops required to connect your computer to the server. Test some of the destination you used with ping, but now with `tracpath`. You can also try the `tracroute` command.**

`$tracpath www.google.com`

`$tracroute www.google.com`

(O comando `tracpath` e o comando `tracroute` são ambos usados para traçar o caminho percorrido pelos pacotes até chegar a um destino. O comando `tracpath` mostra o caminho dos pacotes até um destino, tal como o `tracroute`, mas realiza também a descoberta do MTU (Maximum Transmission Unit) para garantir que o tamanho do pacote é otimizado em cada salto. O comando `tracroute` é uma ferramenta mais conhecida e usada. Funciona de maneira semelhante ao `tracpath`, mas normalmente não realiza a descoberta do MTU).

#### **6. Use `tracpath` to trace the route from your laptop to `www.dei.isep.ipp.pt` and `www.isep.ipp.pt`. Explain the difference in results.**

**If `tracpath` or `tracroute` fail to produce valid output (often due to servers not responding to ICMP packets), you can use the `mtr` command as an alternative. Note: Press `q` to exit the `mtr` interface.**

`www.dei.isep.ipp.pt` e `www.isep.ipp.pt` podem ter rotas diferentes, pois podem estar alojados em servidores diferentes ou conectados através de redes distintas, mesmo que façam parte da mesma instituição (ISEP).

Se houver problemas como configurações de firewall ou routers a bloquear pacotes ICMP, o `tracpath` pode mostrar "no reply" ou não conseguir traçar todo o caminho. Usar `mtr` como alternativa: Se o `tracpath` ou `tracroute` falharem devido ao filtro de pacotes ICMP ou timeouts, podes tentar usar o comando `mtr` (My Traceroute), que combina as funcionalidades de ambos os comandos (`ping` e `tracroute`). O `mtr` fornece uma visualização em tempo real da rota, o que pode contornar os problemas que afetam o `tracpath` ou `tracroute`.

Resumidamente:

tracert: Realiza a descoberta do MTU do caminho e tenta encontrar o maior tamanho de pacote possível que pode ser transmitido sem fragmentação.  
mtr: Mostra em tempo real a rota, com atualizações contínuas, exibindo perdas de pacotes e latência para cada salto, o que pode ser útil para diagnosticar problemas ao longo da rota.

**7. Pick your favorite web site for the following questions. Try nslookup, dig, and host in your Linux VM.**

**a. What is the domain name for this site?**

www.chatgpt.com

**b. What is the IP address of it (just use one if there are multiple)?**

IP address: 172.64.155.209

**c. What is the authoritative name server as a domain name?**

\$dig www.chatgpt.com NS ou \$nslookup -type=ns www.chatgpt.com ou  
\$host -t ns www.chatgpt.com

(Esses servidores de nomes são responsáveis por armazenar as informações DNS do domínio e responder às consultas DNS para esse domínio. Neste caso, o domínio www.chatgpt.com não está registado ou não é um domínio válido atualmente. Quando tento realizar uma consulta de DNS para www.chatgpt.com, recebi um erro a dizer que o domínio não existe).

\$dig www.google.com -> ns1.google.com

**d. What is the IP of the authoritative name server?**

\$ nslookup ns1.google.com ou \$dig ns1.google.com A → Addresses:  
216.239.32.10

Server: UnKnown  
Address: 192.168.1.1

Non-authoritative answer:  
Name: ns1.google.com  
Addresses: 216.239.32.10

Explicação da saída:

Server: Este é o servidor de DNS que está a ser usado para a consulta. No exemplo acima, é o UnKnown porque está a ser feito a partir de uma máquina local (ainda que possa mostrar o IP do servidor de DNS, dependendo da configuração).

Non-authoritative answer: Indica que a resposta não veio diretamente de um servidor de nomes autoritativo. Em vez disso, foi respondida por um servidor de cache ou intermediário.

Name: O nome do servidor de nomes que estás a consultar, que neste caso é ns1.google.com.

Addresses: O endereço IP do servidor de nomes ns1.google.com. No exemplo acima, o endereço IP é 216.239.32.10.

**e. Does this site have any MX records? If so, it has an email server. If not, it does not.**

\$ dig google.com MX ou \$nslookup -type=mx google.com -> google.com mail exchanger= 10 smtp.google.com

(Se a consulta DNS MX retornar resultados, significa que o domínio tem servidores de e-mail configurados. Se o domínio não tiver registros MX, a resposta será algo como "NXDOMAIN" (não existe um domínio) ou simplesmente nenhuma resposta MX).

**8. Use ssh from your host machine to login into your Linux VM. Verify that the login succeeded with the hostname command. Logout with the exit command.**

No linux para saber o ip da VM: ip a

No windows: ssh inesb@192.168.56.5

exit

**9. Use ssh from your host machine to execute the ls -la command on your Linux VM.**

No windows: ssh inesb@192.168.56.5 ls -la

(O comando ls -la vai listar os arquivos e diretórios no diretório atual da VM, mostrando detalhes como permissões, número de links, dono, grupo, tamanho e a data da última modificação).

**10. Use scp to copy a file from your host computer to your home directory in your Linux VM**

scp "C:/SWITCH/tste.txt" inesb@192.168.56.5:/home/inesb/exercise2