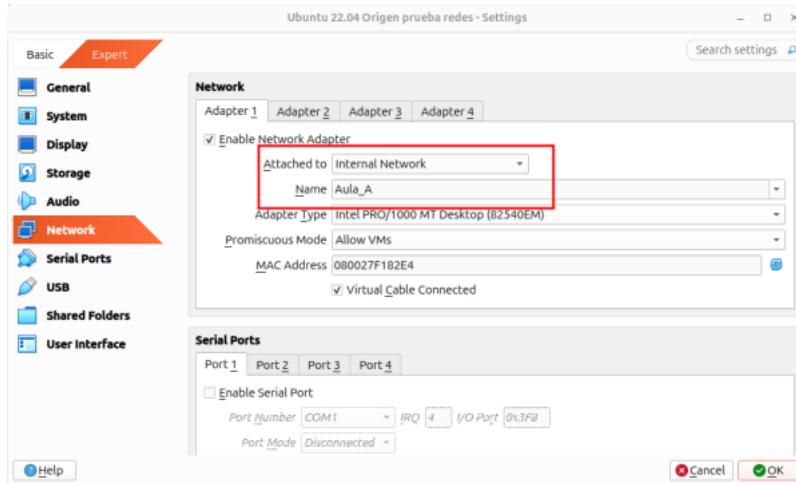


CONFIGURAR SUBREDES

1. Configurar Network de las máquinas que pertenezcan a la subred:

Internal Network + nombre



2. Arrancar máquinas, configurar IPs* y guardar:

sudo nano /etc/netplan/01-network-manager-all.yaml + sudo netplan try

```
usuario@equipo: ~
GNU nano 6.2          /etc/netplan/01-network-manager-all.yaml
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    enp0s3:
      dhcp4: false
      addresses:
        - 192.168.200.25/24
```

Comprobar con ping si se comunican entre ellos y anotar IPs

CONFIGURAR ROUTER

1. Configurar Network de la máquina:

Adapter 1 (NAT), Adapter 2 (subred1), Adapter 3 (subred2)

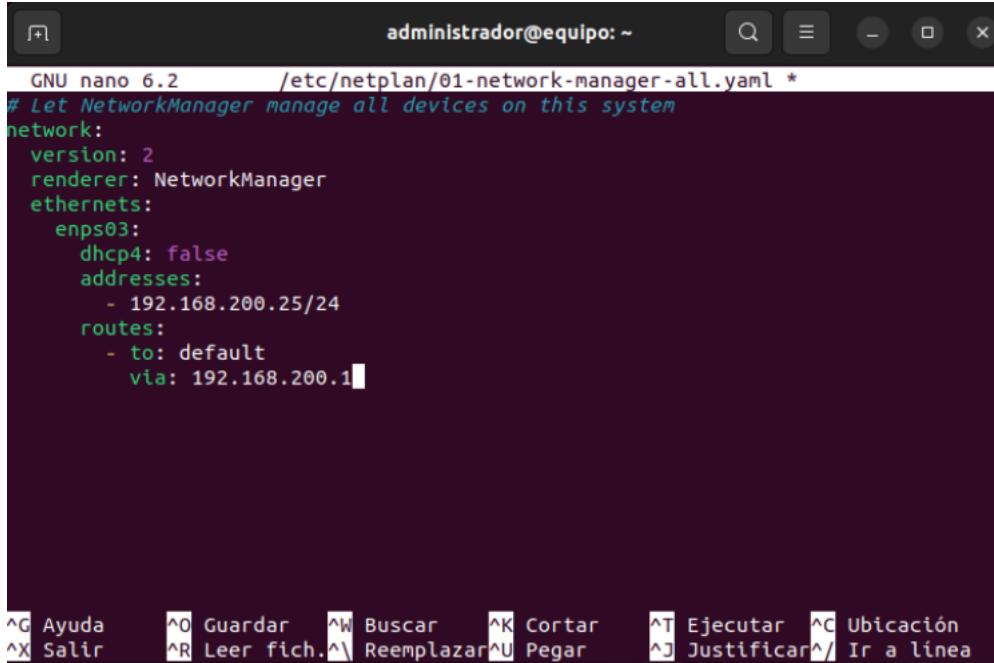
2. Averiguar nombres de las interfaces y configurarles la primera IP de su subred:

ip a + sudo nano /etc/netplan/01-network-manager-all.yaml + sudo netplan try

Comprobar con ping si se comunica con los de su subred respectivamente y anotar IPs y tarjetas de red

3. Configurar puerta de enlace (IP del router en esa subred) en las máquinas de las subredes para conectarlas entre ellas:

sudo nano /etc/netplan/01-network-manager-all.yaml + sudo netplan try

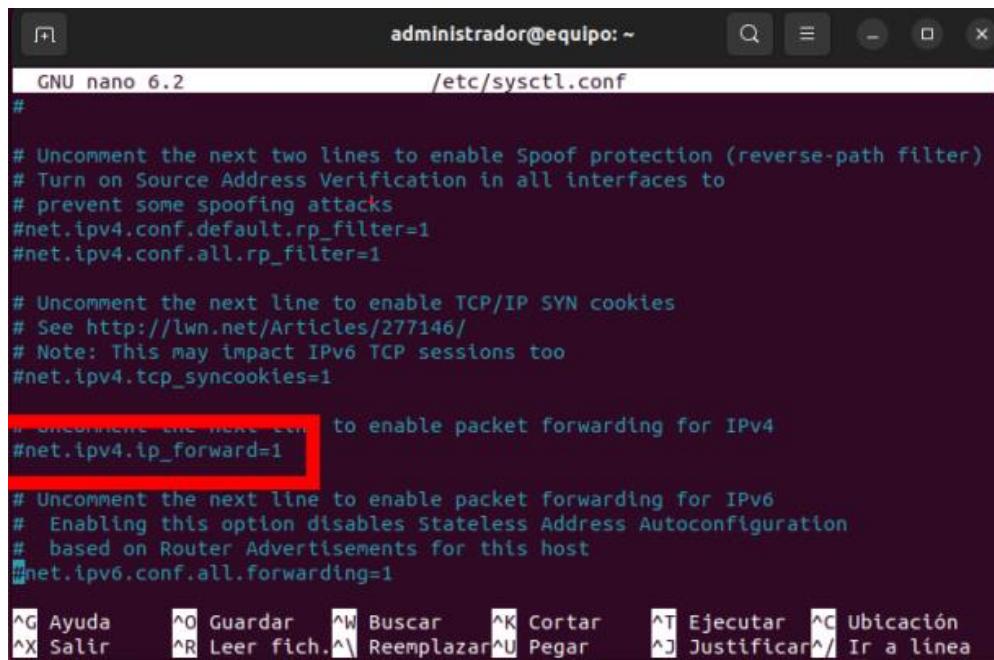


```
GNU nano 6.2          /etc/netplan/01-network-manager-all.yaml *
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    enps03:
      dhcp4: false
      addresses:
        - 192.168.200.25/24
      routes:
        - to: default
          via: 192.168.200.1
```

^G Ayuda ^O Guardar ^W Buscar ^K Cortar ^T Ejecutar ^C Ubicación
^X Salir ^R Leer fich.^A Reemplazar^U Pegar ^J Justificar^/ Ir a línea

4. Habilitar IP Forwarding descomentando “net.ipv4.ip_forward = 1” :

sudo nano /etc/sysctl.conf + sudo sysctl -p



```
GNU nano 6.2          /etc/sysctl.conf
#
# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1

# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
#net.ipv4.ip_forward=1

# Uncomment the next line to enable packet forwarding for IPV6
# Enabling this option disables Stateless Address Autoconfiguration
# based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1
```

^G Ayuda ^O Guardar ^W Buscar ^K Cortar ^T Ejecutar ^C Ubicación
^X Salir ^R Leer fich.^A Reemplazar^U Pegar ^J Justificar^/ Ir a línea

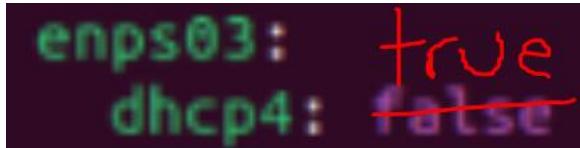
Comprobar con ping si se comunican de una subred a otra

5. Hacer que el router enmascare nuestra IP privada, haga las peticiones por nosotros y nos devuelva las respuestas:

sudo apt install iptables-persistent + sudo iptables -t nat -A POSTROUTING -o tarjeta de red que sale a internet -j MASQUERADE + sudo netfilter-persistent save

6. Activar dhcp4 (true) de la tarjeta de red que sale a internet:

sudo nano /etc/netplan/01-network-manager-all.yaml + sudo netplan try

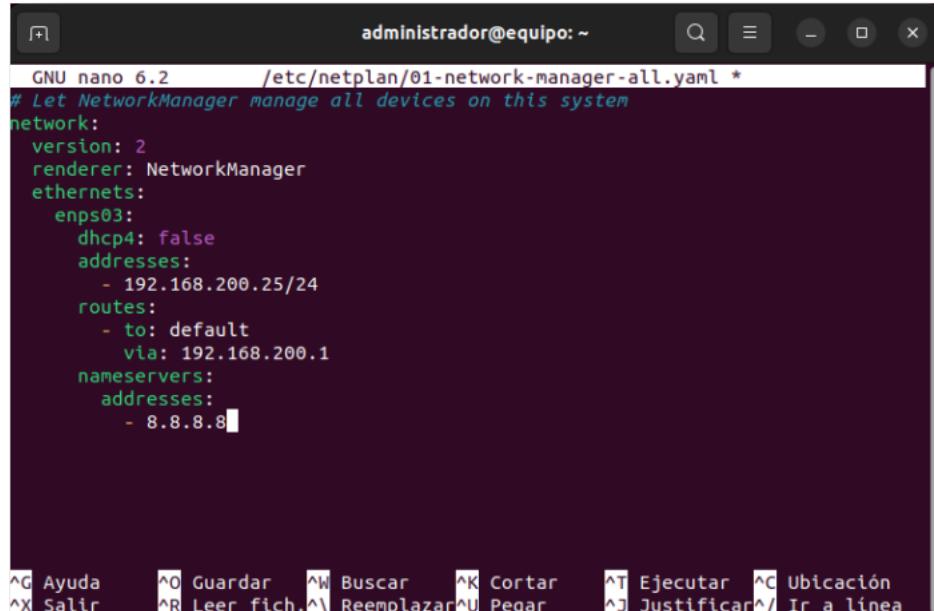


```
enps03: true
  dhcp4: false
```

Comprobar con ping que cualquier ordenador puede acceder a internet (8.8.8.8 ‘Google’)

7. Configurar DNS en todas las máquinas para poder acceder a webs mediante nombres y no IPs:

sudo nano /etc/netplan/01-network-manager-all.yaml + sudo netplan try



```
GNU nano 6.2      /etc/netplan/01-network-manager-all.yaml *
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    enps03:
      dhcp4: false
      addresses:
        - 192.168.200.25/24
      routes:
        - to: default
          via: 192.168.200.1
      nameservers:
        addresses:
          - 8.8.8.8
```

Comprobar con ping que cualquier ordenador puede acceder a una web mediante su nombre ('google.es')