CONEXIÓN

Y

RECURSOS DE RED

Prof. Manuel Enguidanos SISTEMES INFORMÀTICS

Cicle Formatiu de Grau Superior de Desenvolupament d’Aplicacions Web

Prof. Manuel Enguidanos SISTEMES INFORMÀTICS

Cicle Formatiu de Grau Superior de Desenvolupament d’Aplicacions Web

Índice

[**Actividad 6.1** 3](#_Toc165057817)

[**Actividad 6.2** 5](#_Toc165057818)

[**Actividad 6.3** 8](#_Toc165057819)

[**Actividad 6.4** 10](#_Toc165057820)

[**Practica 1** 12](#_Toc165057821)

# **Actividad 6.1**

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

dpkg -s ufw: Comprueba el estado de instalación del paquete UFW.

sudo apt update: Actualiza la lista de paquetes y versiones disponibles.

sudo apt install ufw: Instala el paquete UFW.

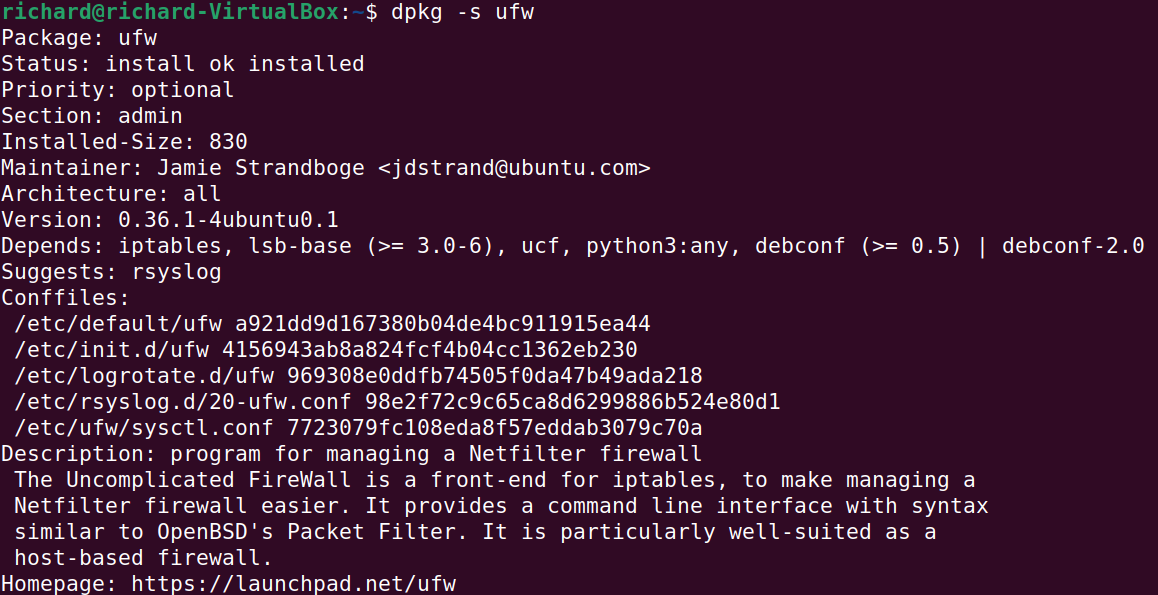
sudo ufw status: Muestra el estado actual de UFW (activo o inactivo).

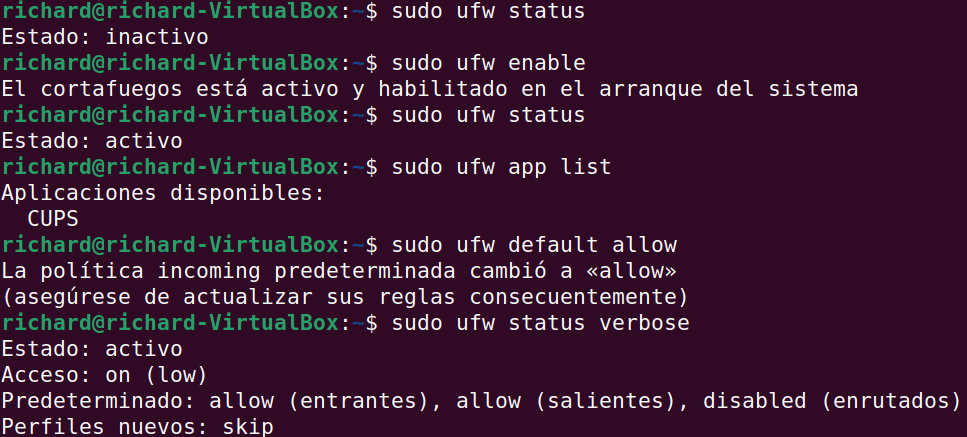
sudo ufw enable: Activa UFW para que se inicie en el arranque.

sudo ufw app list: Lista las aplicaciones con perfiles de UFW disponibles.

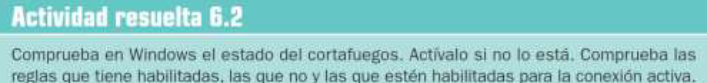
sudo ufw default allow: Establece la política predeterminada para permitir todas las conexiones entrantes.

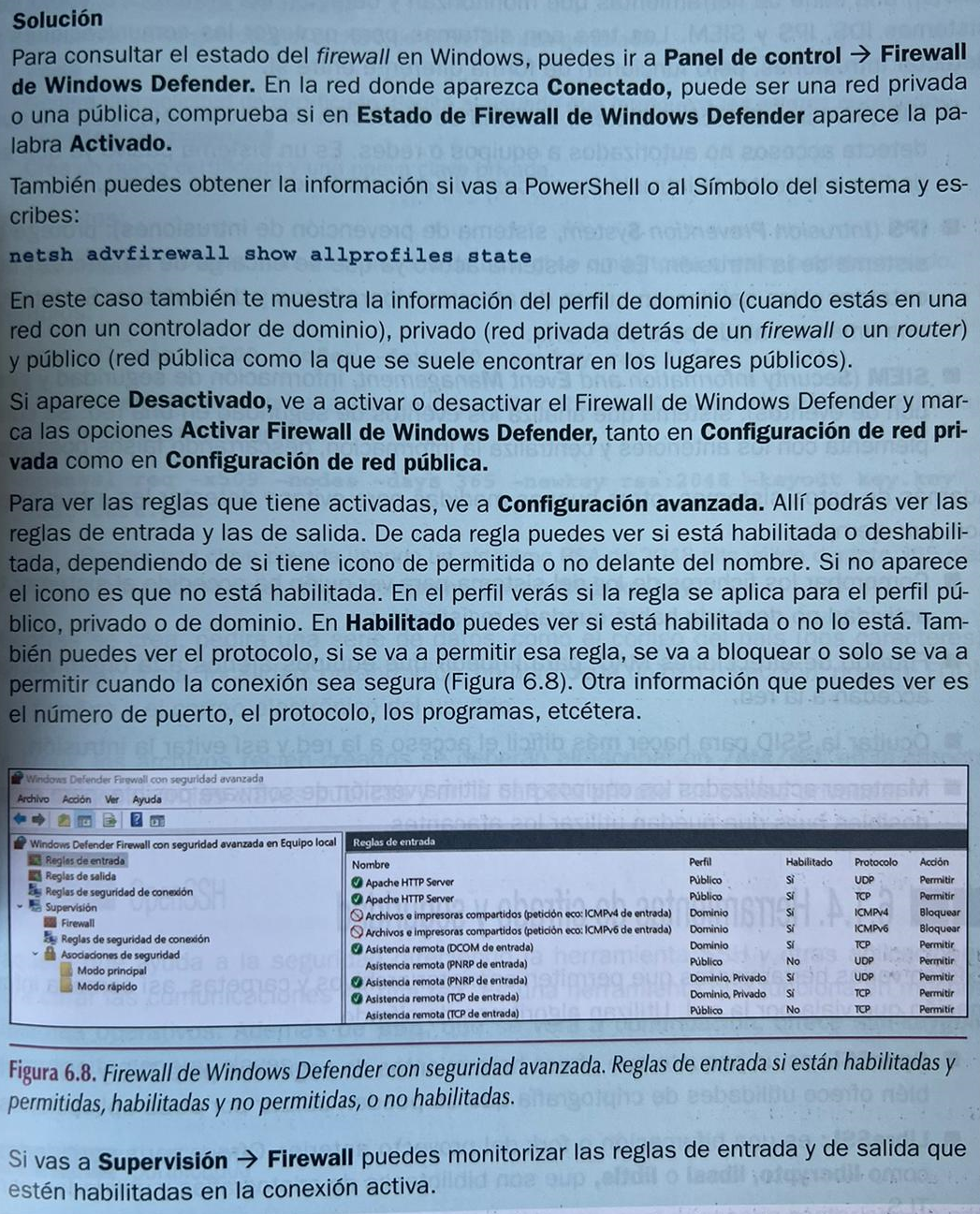
sudo ufw status verbose: Muestra un estado detallado de UFW incluyendo reglas y políticas.

En este caso nosotros lo tenemos instalado en el sistema ya que Ubuntu lo trae por defecto:  




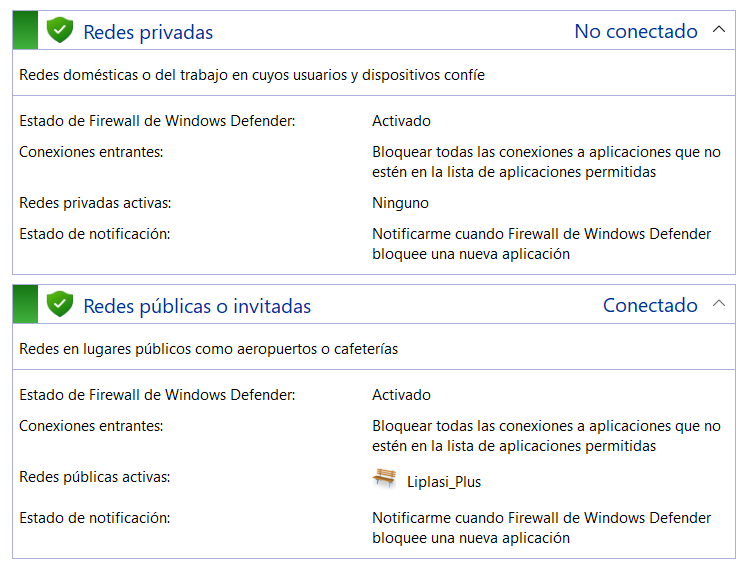
# **Actividad 6.2**

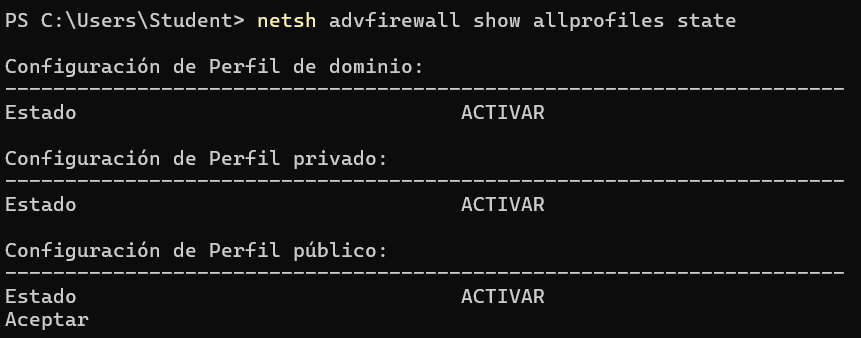




Podemos comprobar que el firewall de Windows está ACTIVADO:

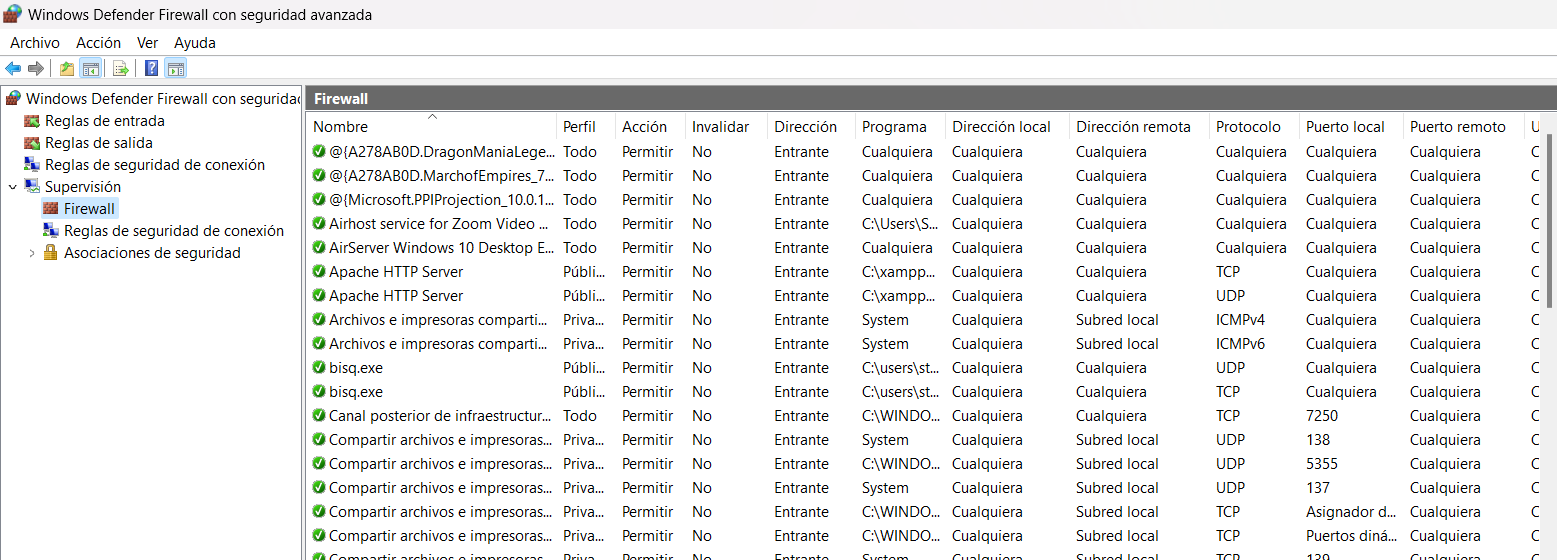
Panel de control >> Firewall de Windows Defender



A través de PowerShell también se puede comprobar:  


En la configuración avanzada podemos ver todas las reglas de entrada y de salida.

Y en Supervisión >> Firewall podemos monitorear las que estén activas:

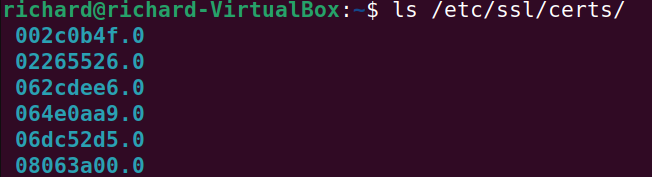


# **Actividad 6.3**

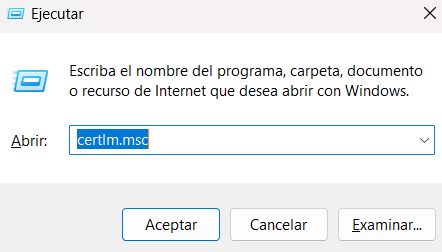
Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

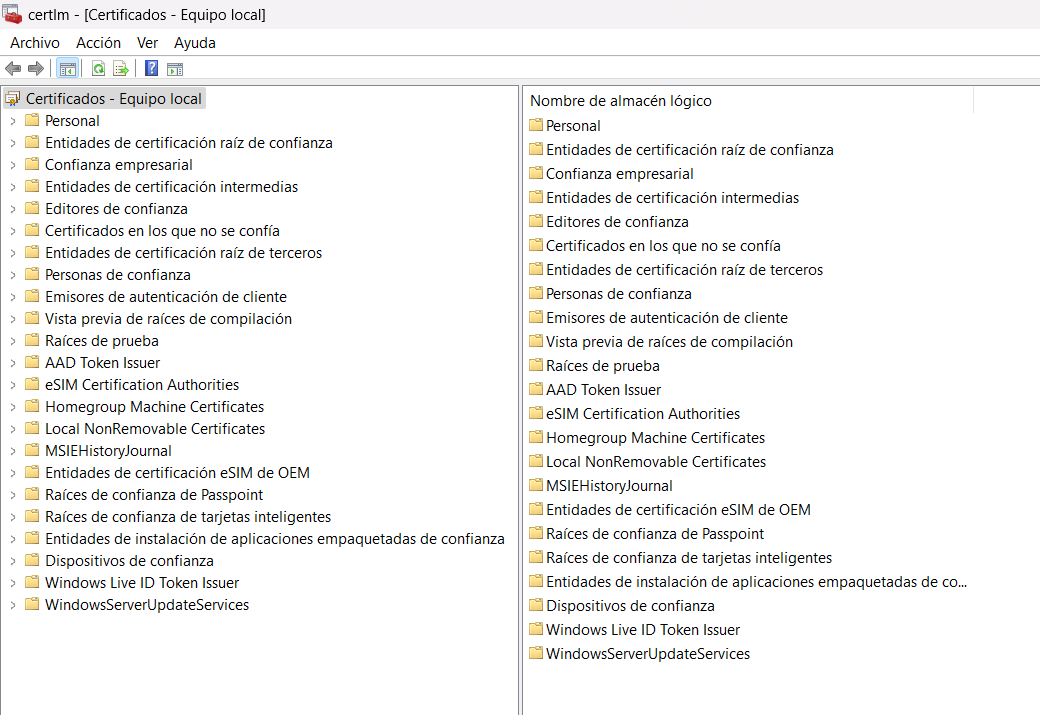
Descripción generada automáticamente

Certificados en Linux:

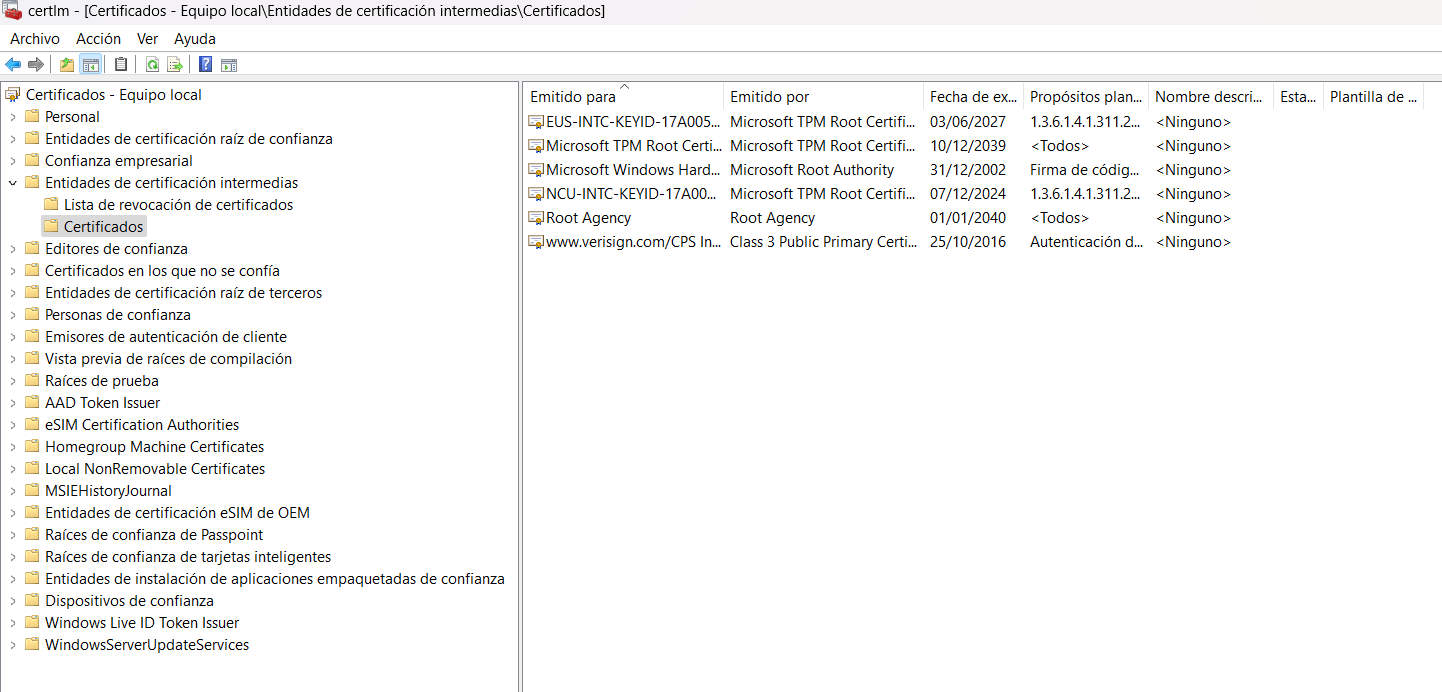


Certificados en Windows:

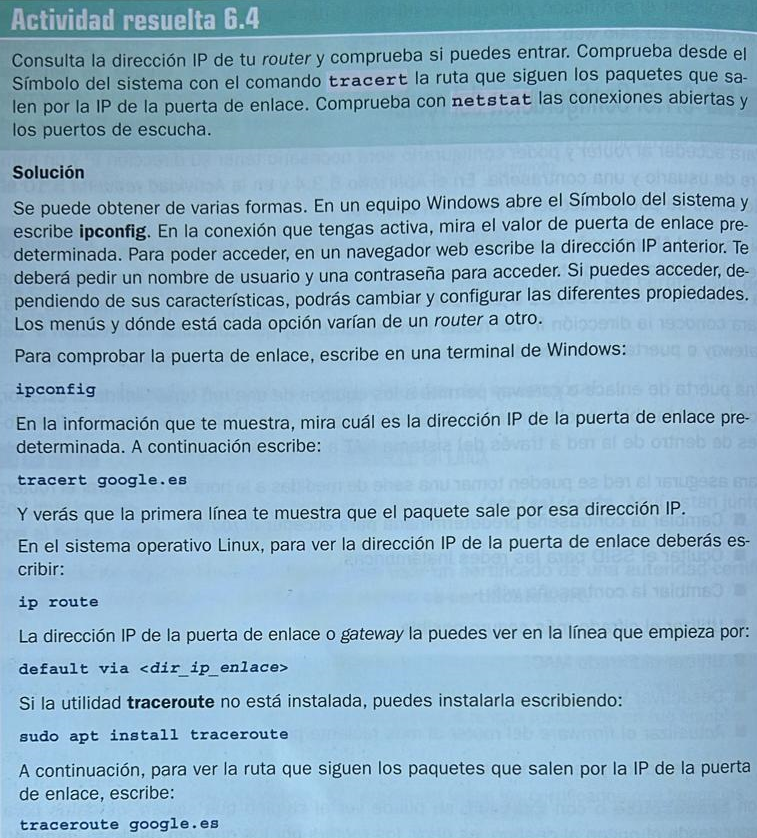


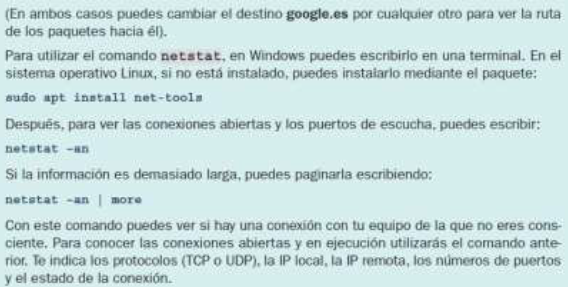


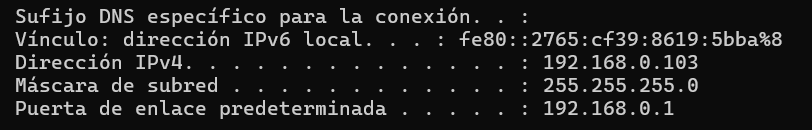
En Entidades de certificación >> Certificados podemos ver los certificados instalados en nuestro dispositivo:



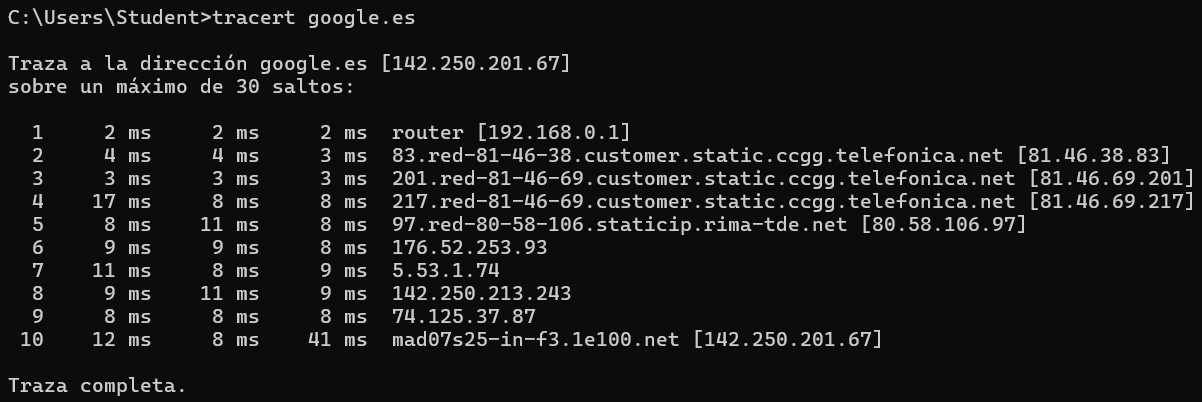
# **Actividad 6.4**

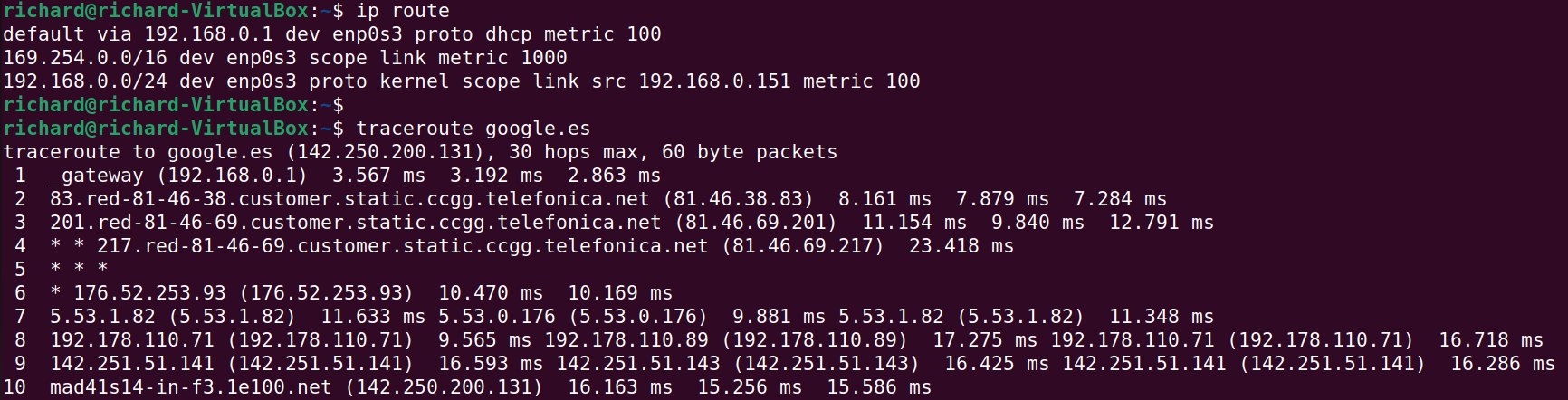




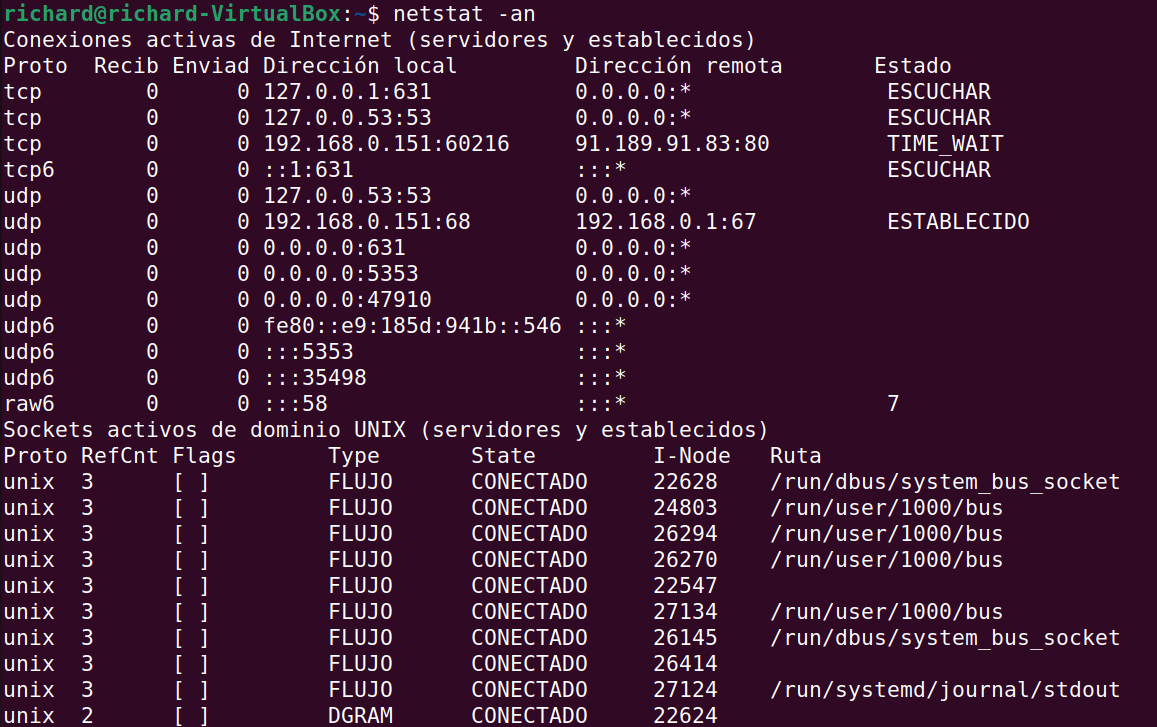
Con ip config vemos lo siguiente:  


Con tracert google.es comprobamos que la primera IP es la de nuestra puerta de enlace:



Comprobamos lo mismo en Linux:  


Con netstat -an podemos ver las conexiones abiertas y en ejecución:



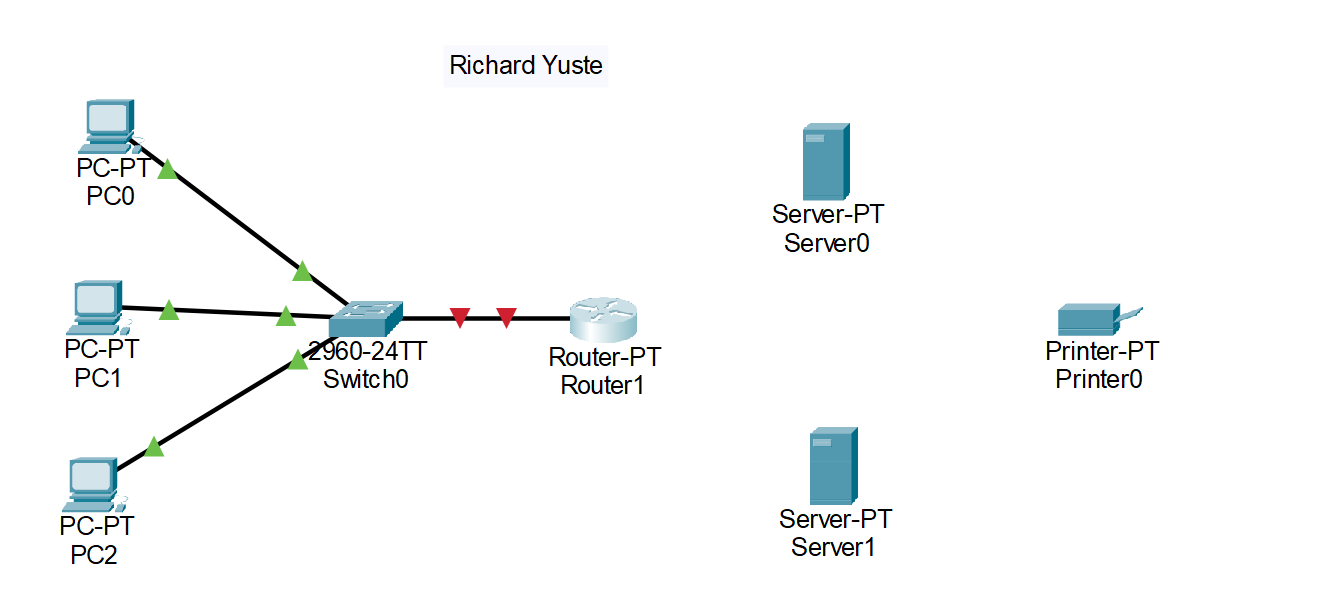
# **Practica 1**

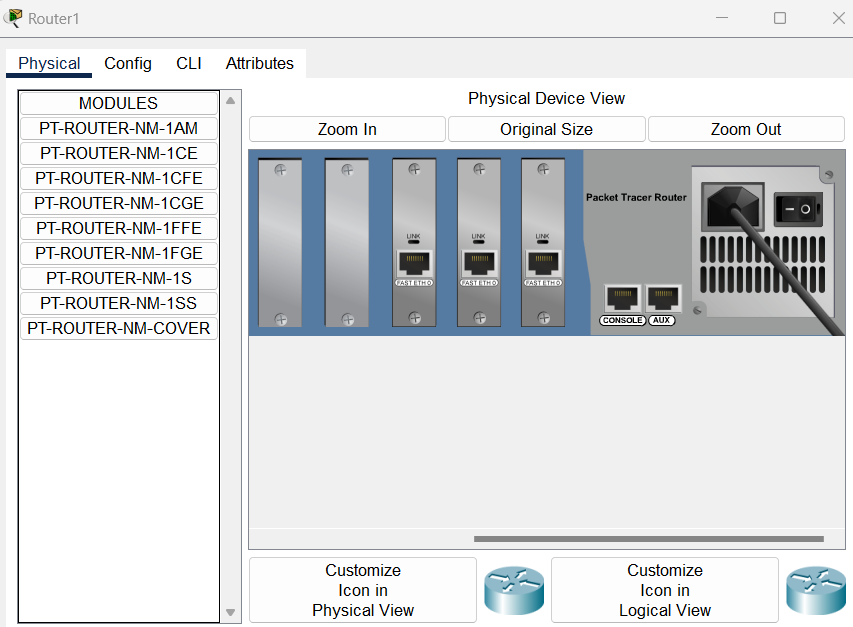
**Realiza el ejercicio del vídeo que te dejé a continuación dónde vas a crear un Firewall entre 2 redes: una interna y una externa.**

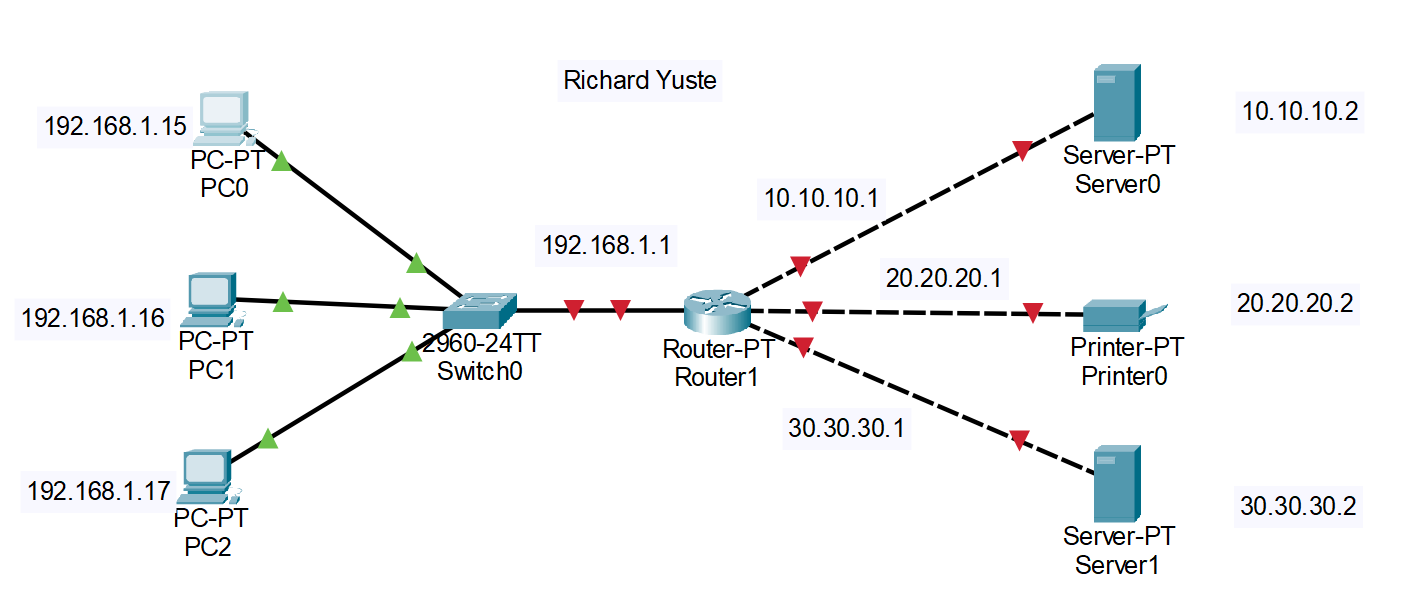
**La entrega será una explicación del proceso seguido en las configuraciones de los equipos. Sobre todo, aquellos donde se repite el mismo no es necesario realizar capturas.**

**En la práctica se tiene que ver tu nombre y apellidos y el nombre de las redes (SSID) será la primera inicial de tu nombre y primero apellido. El enlace es:** <https://youtu.be/JtgEgtO_oco?si=Rt7PQVaIEUETweGx>

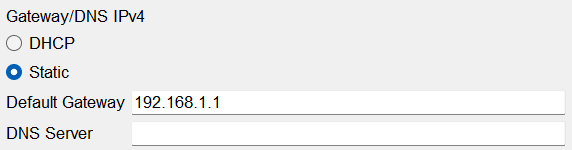
Creamos una red sencilla con:

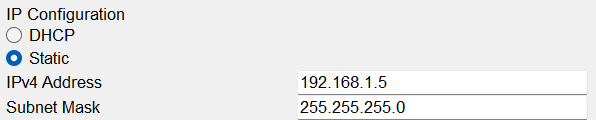
* 3 PCs
* 1 Switch
* 1 Router
* 2 Servers
* 1 Printer

Ahora configuramos el Router añadiéndole más conexiones FastEthernet: 

Procedemos a configurar las siguientes IPs:  


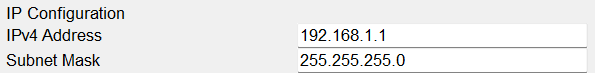
Primero los PCs:



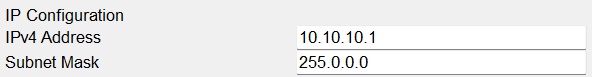


Ahora el router:

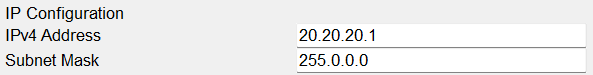
* FA0/0:



* FA1/0:



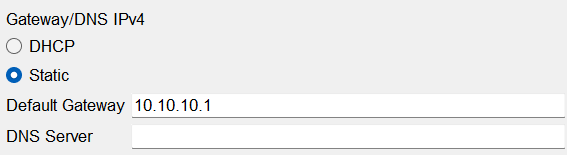
* FA2/0:

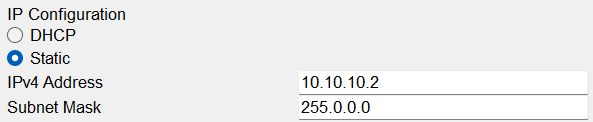


* FA3/0:

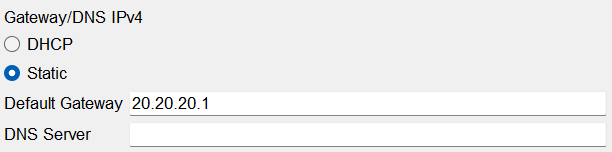


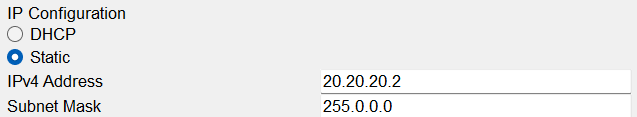
Seguimos con los servers:





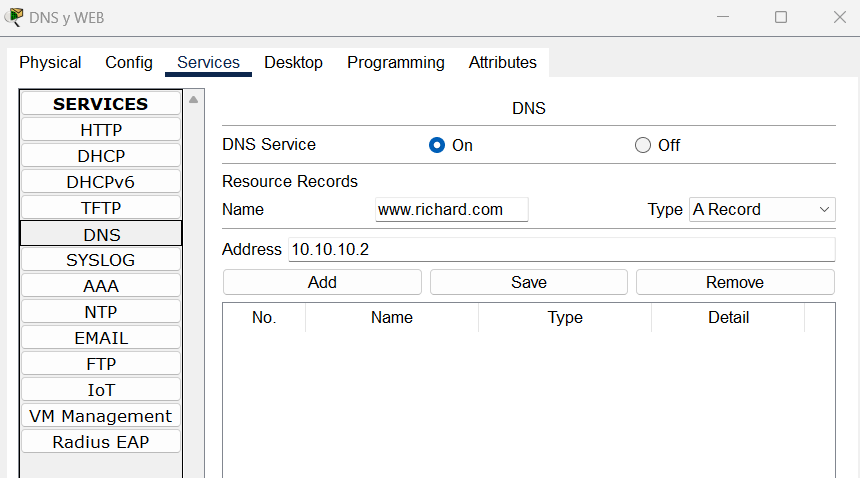
Y por último la impresora:



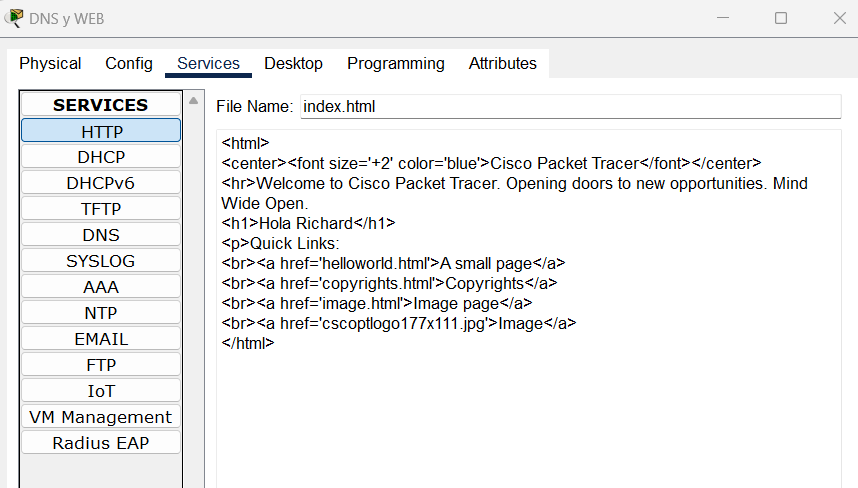


Configuramos los servidores para DNS, WEB y DHCP:

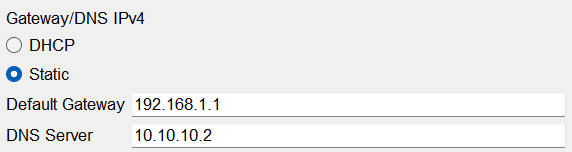
* DNS:



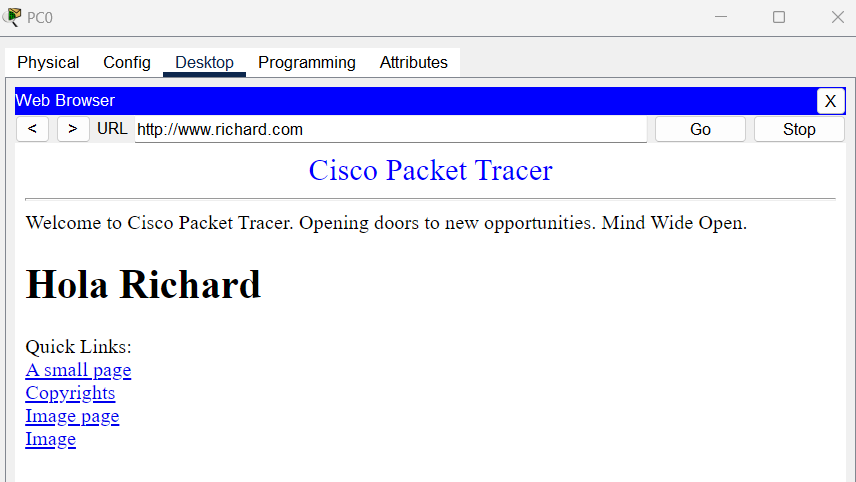
* HTTP:
  + Editamos el index:



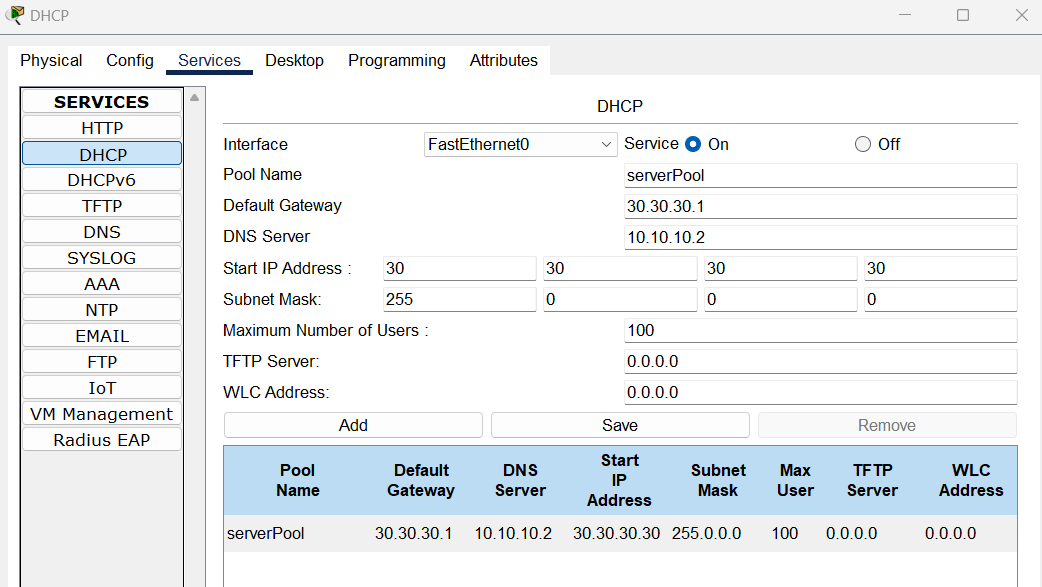
* + Modificamos el DNS en la configuración del PC1:



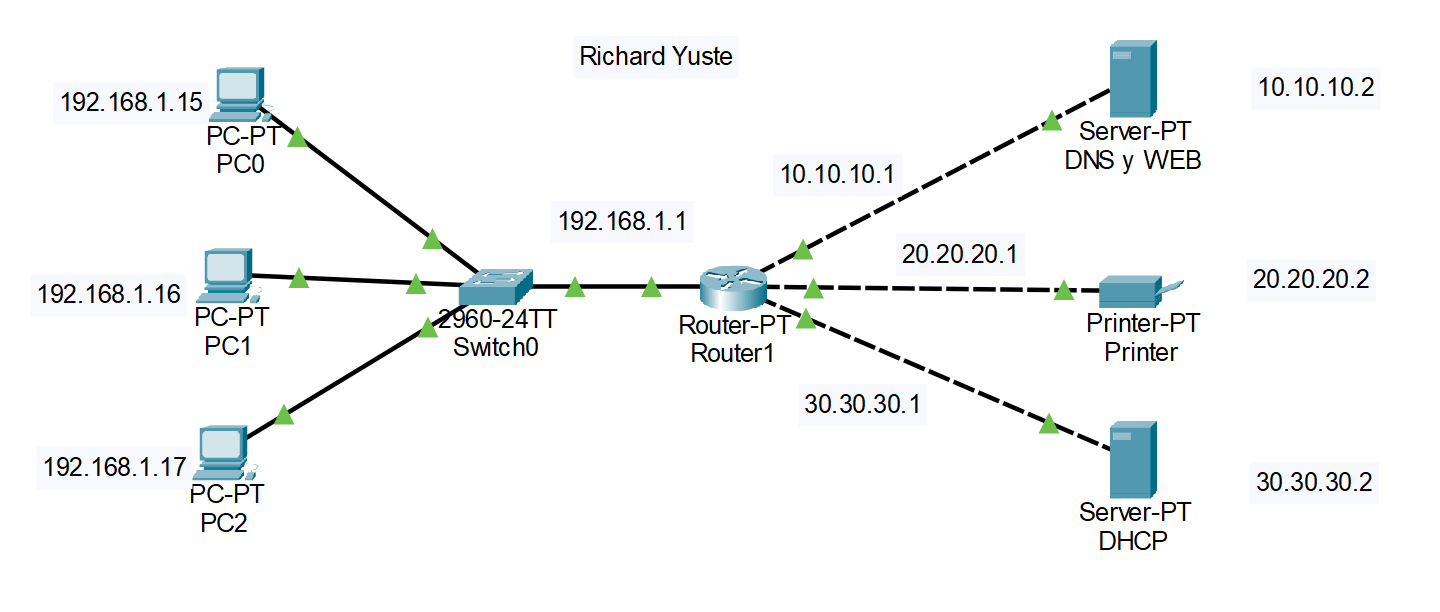
* + Comprobamos que se visualiza la web a través del navegador:



* DHCP:
  + Default Gateway: 30.30.30.1
  + DNS Server: 10.10.10.2
  + Rango de IPs desde la 30.30.30.30
  + Número total de IPs para hosts: 100



Ya tenemos toda la configuración de red corriendo correctamente:



Si creamos una ACL en el router simulamos lo que haría un firewall, impidiendo que pudiéramos hacer ping a través de la interfaz FA2/0:

Router>enable

Router#configure terminal

Router(config)#access-list 101 deny icmp any any host-unreachable

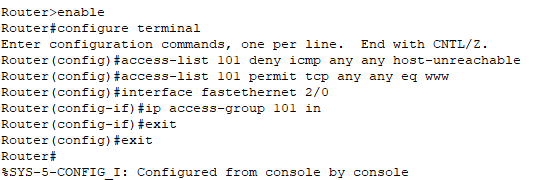
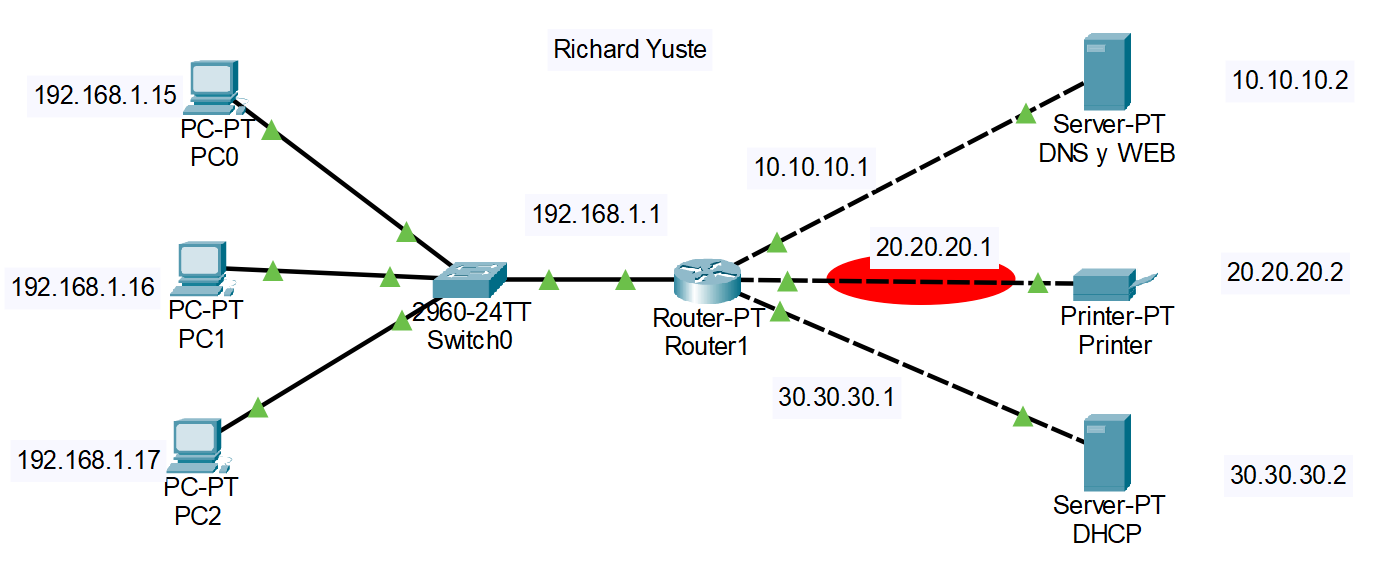
Router(config)#access-list 101 permit tcp any any eq www

Router(config)#interface fastethernet 2/0

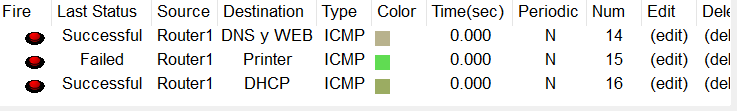
Router(config-if)#ip access-group 101 in

Router(config-if)#exit

Router(config)#exit

Si hacemos ping hacia la impresora no nos dejará:



Explicación de la línea de comandos:

1. Router>enable: Este comando cambia del modo de usuario (Router>) al modo privilegiado (Router#), que proporciona más comandos y capacidades para la configuración.
2. Router#configure terminal: Se entra al modo de configuración global desde el modo privilegiado, donde se pueden ejecutar comandos que afectan la configuración del dispositivo.
3. Router(config)#access-list 101 deny icmp any any host-unreachable: En el modo de configuración global, se crea o modifica la lista de acceso numerada 101 para denegar el tráfico ICMP (ping, por ejemplo) de cualquier origen a cualquier destino cuando la respuesta sería "host-unreachable", es decir, no se puede alcanzar el host destino.
4. Router(config)#access-list 101 permit tcp any any eq www: Se agrega otra regla a la ACL 101 que permite el tráfico TCP desde cualquier origen hacia cualquier destino en el puerto equivalente a 'www' (puerto 80, que es el utilizado para HTTP).
5. Router(config)#interface fastethernet 2/0: Se ingresa al modo de configuración de la interfaz específica FastEthernet 2/0.
6. Router(config-if)#ip access-group 101 in: Se aplica la ACL 101 a la interfaz FastEthernet 2/0 para filtrar el tráfico entrante según las reglas definidas en la ACL.
7. Router(config-if)#exit: Se sale del modo de configuración de la interfaz y se vuelve al modo de configuración global.
8. Router(config)#exit: Se sale del modo de configuración global y se regresa al modo privilegiado.