

CONEXIÓN Y

RECURSOS DE RED

Prof. Manuel Enguidanos
SISTEMES INFORMÀTICS

Cicle Formatiu de Grau Superior de Desenvolupament d'Aplicacions Web

Índice

| | |
|---------------------|----|
| Actividad 6.1 | 3 |
| Actividad 6.2 | 5 |
| Actividad 6.3 | 8 |
| Actividad 6.4 | 10 |
| Practica 1 | 12 |

Actividad 6.1

Actividad resuelta 6.1

Comprueba si en Linux está instalado el cortafuegos **ufw**. Si no es así, instálalo. Actívalo y examina las aplicaciones disponibles que tienes para aplicar. Cambia la política predeterminada a permitir. Muestra el estado del cortafuegos de forma detallada.

Solución

```
dpkg -s ufw
sudo apt update
sudo apt install ufw
sudo ufw status
sudo ufw enable
sudo ufw app list
sudo ufw default allow
sudo ufw status verbose
```

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:

```
richard@richard-VirtualBox:~$ dpkg -s ufw
Package: ufw
Status: install ok installed
Priority: optional
Section: admin
Installed-Size: 830
Maintainer: Jamie Strandboge <jdstrand@ubuntu.com>
Architecture: all
Version: 0.36.1-4ubuntu0.1
Depends: iptables, lsb-base (>= 3.0-6), ucf, python3:any, debconf (>= 0.5) | debconf-2.0
Suggests: rsyslog
Conffiles:
/etc/default/ufw a921dd9d167380b04de4bc911915ea44
/etc/init.d/ufw 4156943ab8a824fcf4b04cc1362eb230
/etc/logrotate.d/ufw 969308e0ddfb74505f0da47b49ada218
/etc/rsyslog.d/20-ufw.conf 98e2f72c9c65ca8d6299886b524e80d1
/etc/ufw/sysctl.conf 7723079fc108eda8f57eddab3079c70a
Description: program for managing a Netfilter firewall
The Uncomplicated FireWall is a front-end for iptables, to make managing a
Netfilter firewall easier. It provides a command line interface with syntax
similar to OpenBSD's Packet Filter. It is particularly well-suited as a
host-based firewall.
Homepage: https://launchpad.net/ufw
```

```
richard@richard-VirtualBox:~$ sudo ufw status
Estado: inactivo
richard@richard-VirtualBox:~$ sudo ufw enable
El cortafuegos está activo y habilitado en el arranque del sistema
richard@richard-VirtualBox:~$ sudo ufw status
Estado: activo
richard@richard-VirtualBox:~$ sudo ufw app list
Aplicaciones disponibles:
  CUPS
richard@richard-VirtualBox:~$ sudo ufw default allow
La política incoming predeterminada cambió a «allow»
(asegúrese de actualizar sus reglas consecuentemente)
richard@richard-VirtualBox:~$ sudo ufw status verbose
Estado: activo
Acceso: on (low)
Predeterminado: allow (entrantes), allow (salientes), disabled (enrutados)
Perfiles nuevos: skip
```

Actividad 6.2

Actividad resuelta 6.2

Comprueba en Windows el estado del cortafuegos. Actívalo si no lo está. Comprueba las reglas que tiene habilitadas, las que no y las que estén habilitadas para la conexión activa.

Solución

Para consultar el estado del *firewall* en Windows, puedes ir a **Panel de control → Firewall de Windows Defender**. En la red donde aparezca **Conectado**, puede ser una red privada o una pública, comprueba si en **Estado de Firewall de Windows Defender** aparece la palabra **Activado**.

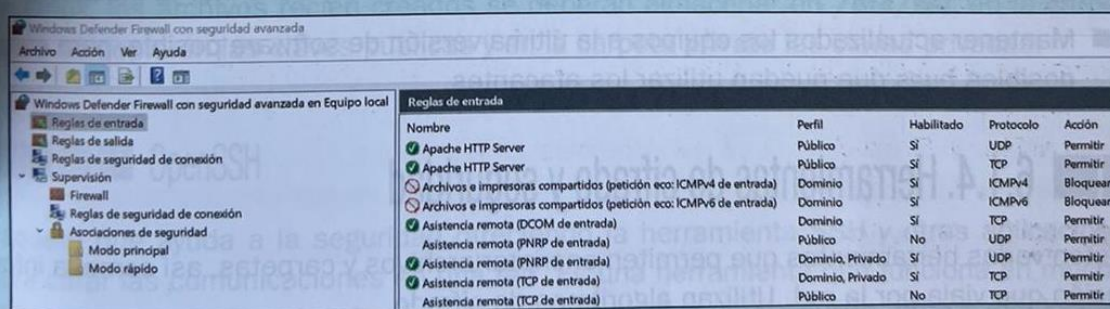
También puedes obtener la información si vas a PowerShell o al Símbolo del sistema y escribes:

```
netsh advfirewall show allprofiles state
```

En este caso también te muestra la información del perfil de dominio (cuando estás en una red con un controlador de dominio), privado (red privada detrás de un *firewall* o un *router*) y público (red pública como la que se suele encontrar en los lugares públicos).

Si aparece **Desactivado**, ve a activar o desactivar el Firewall de Windows Defender y marca las opciones **Activar Firewall de Windows Defender**, tanto en **Configuración de red privada** como en **Configuración de red pública**.

Para ver las reglas que tiene activadas, ve a **Configuración avanzada**. Allí podrás ver las reglas de entrada y las de salida. De cada regla puedes ver si está habilitada o deshabilitada, dependiendo de si tiene icono de permitida o no delante del nombre. Si no aparece el icono es que no está habilitada. En el perfil verás si la regla se aplica para el perfil público, privado o de dominio. En **Habilitado** puedes ver si está habilitada o no lo está. También puedes ver el protocolo, si se va a permitir esa regla, se va a bloquear o solo se va a permitir cuando la conexión sea segura (Figura 6.8). Otra información que puedes ver es el número de puerto, el protocolo, los programas, etcétera.

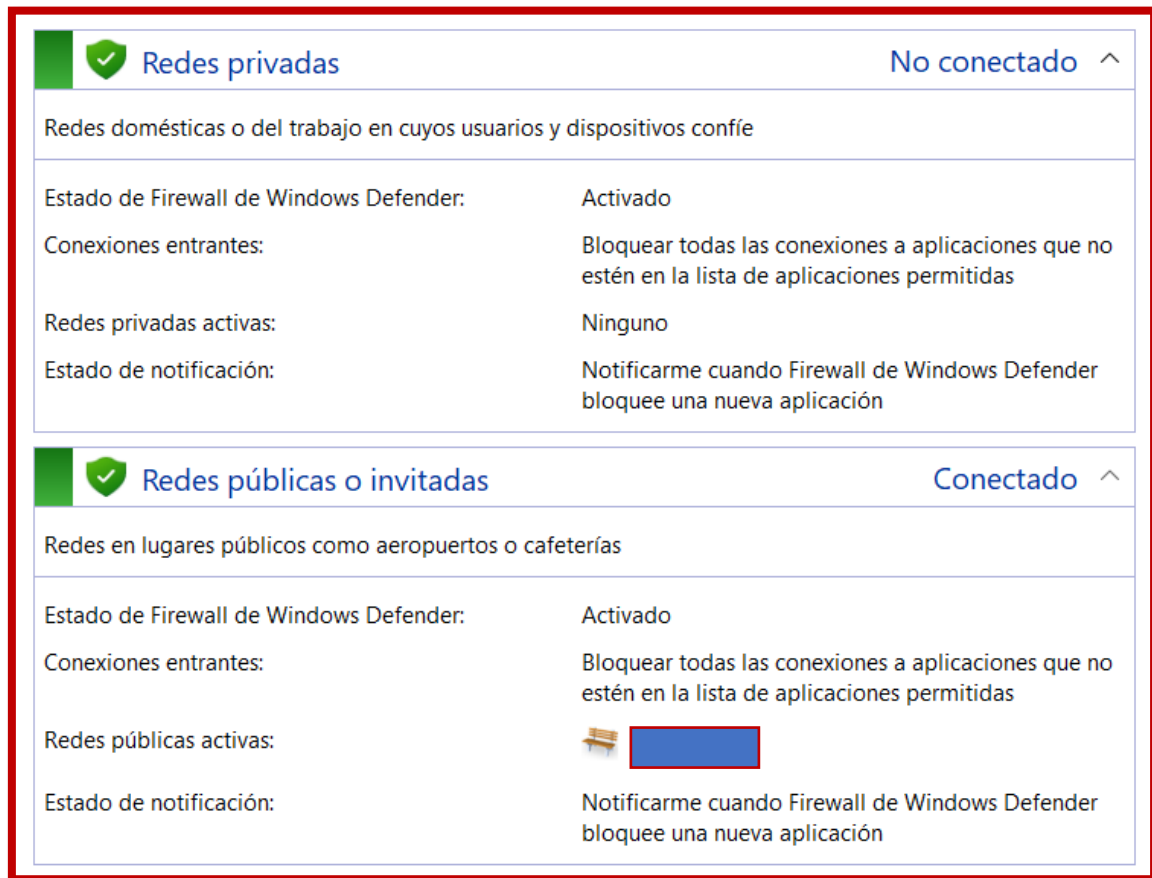


| Nombre | Perfil | Habilitado | Protocolo | Acción |
|---|------------------|------------|-----------|----------|
| Apache HTTP Server | Público | Si | UDP | Permitir |
| Apache HTTP Server | Público | Si | TCP | Permitir |
| Archivos e impresoras compartidos (petición eco: ICMPv4 de entrada) | Dominio | Si | ICMPv4 | Bloquear |
| Archivos e impresoras compartidos (petición eco: ICMPv6 de entrada) | Dominio | Si | ICMPv6 | Bloquear |
| Asistencia remota (DCOM de entrada) | Dominio | Si | TCP | Permitir |
| Asistencia remota (PNRP de entrada) | Público | No | UDP | Permitir |
| Asistencia remota (PNRP de entrada) | Dominio, Privado | Si | UDP | Permitir |
| Asistencia remota (TCP de entrada) | Dominio, Privado | Si | TCP | Permitir |
| Asistencia remota (TCP de entrada) | Público | No | TCP | Permitir |

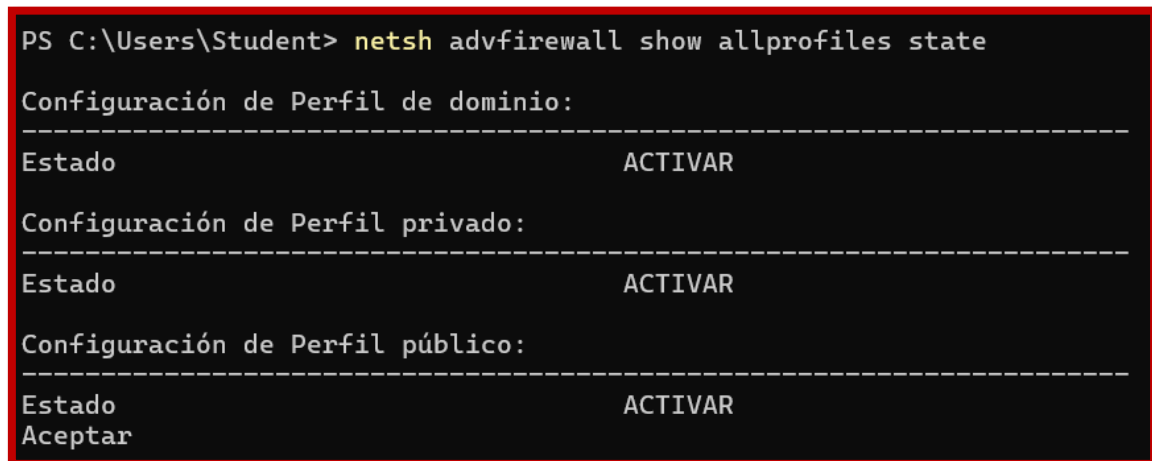
Figura 6.8. Firewall de Windows Defender con seguridad avanzada. Reglas de entrada si están habilitadas y permitidas, habilitadas y no permitidas, o no habilitadas.

Si vas a **Supervisión → Firewall** puedes monitorizar las reglas de entrada y de salida que estén habilitadas en la conexión activa.

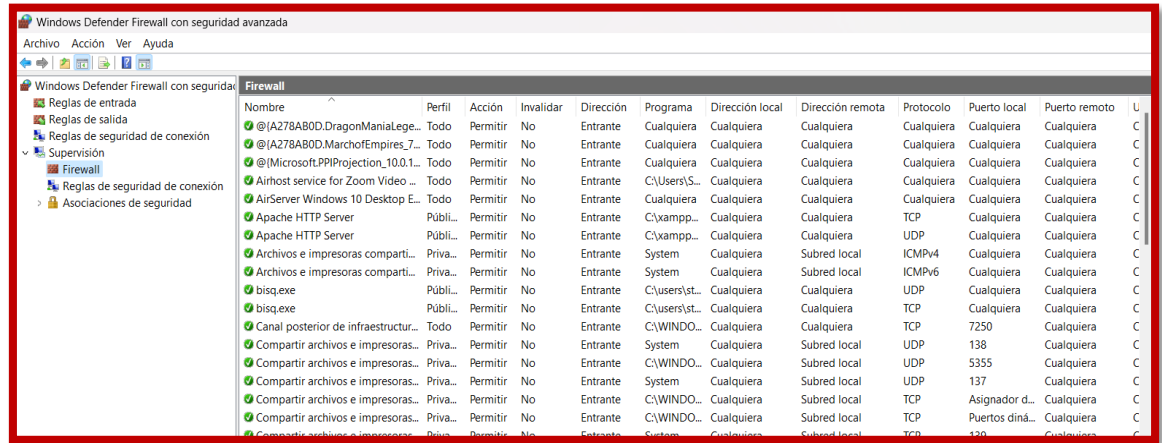
Podemos comprobar que el firewall de Windows está ACTIVADO:
Panel de control >> Firewall de Windows Defender



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:



| Firewall | | | | | | | | | | | | |
|-------------------------------------|----------|----------|----------|-----------|----------------|-----------------|------------------|------------|-----------------|---------------|---|--|
| Nombre | Perfil | Acción | Invaldar | Dirección | Programa | Dirección local | Dirección remota | Protocolo | Puerto local | Puerto remoto | U | |
| Reglas de entrada | | | | | | | | | | | | |
| Reglas de salida | | | | | | | | | | | | |
| Reglas de seguridad de conexión | | | | | | | | | | | | |
| Supervisión | | | | | | | | | | | | |
| Firewall | | | | | | | | | | | | |
| Reglas de seguridad de conexión | | | | | | | | | | | | |
| Asociaciones de seguridad | | | | | | | | | | | | |
| Nombre | Perfil | Acción | Invaldar | Dirección | Programa | Dirección local | Dirección remota | Protocolo | Puerto local | Puerto remoto | U | |
| @(A278AB0D.DragonManiaLege... | Todo | Permitir | No | Entrante | Cualquiera | Cualquiera | Cualquiera | Cualquiera | Cualquiera | Cualquiera | C | |
| @(A278AB0D.MarchofEmpires_7... | Todo | Permitir | No | Entrante | Cualquiera | Cualquiera | Cualquiera | Cualquiera | Cualquiera | Cualquiera | C | |
| @(Microsoft.PPIProjection_10.0.1... | Todo | Permitir | No | Entrante | Cualquiera | Cualquiera | Cualquiera | Cualquiera | Cualquiera | Cualquiera | C | |
| Airhost service for Zoom Video ... | Todo | Permitir | No | Entrante | C:\Users\S... | Cualquiera | Cualquiera | Cualquiera | Cualquiera | Cualquiera | C | |
| AirServer Windows 10 Desktop E... | Todo | Permitir | No | Entrante | Cualquiera | Cualquiera | Cualquiera | Cualquiera | Cualquiera | Cualquiera | C | |
| Apache HTTP Server | Públi... | Permitir | No | Entrante | C:\xampp... | Cualquiera | Cualquiera | TCP | Cualquiera | Cualquiera | C | |
| Apache HTTP Server | Públi... | Permitir | No | Entrante | C:\xampp... | Cualquiera | Cualquiera | UDP | Cualquiera | Cualquiera | C | |
| Archivos e impresoras comparti... | Priva... | Permitir | No | Entrante | System | Cualquiera | Subred local | ICMPv4 | Cualquiera | Cualquiera | C | |
| Archivos e impresoras comparti... | Priva... | Permitir | No | Entrante | System | Cualquiera | Subred local | ICMPv6 | Cualquiera | Cualquiera | C | |
| bisq.exe | Públi... | Permitir | No | Entrante | C:\users\st... | Cualquiera | Cualquiera | UDP | Cualquiera | Cualquiera | C | |
| bisq.exe | Públi... | Permitir | No | Entrante | C:\users\st... | Cualquiera | Cualquiera | TCP | Cualquiera | Cualquiera | C | |
| Canal posterior de infraestrucur... | Todo | Permitir | No | Entrante | C:\WINDO... | Cualquiera | Cualquiera | TCP | 7250 | Cualquiera | C | |
| Compartir archivos e impresoras... | Priva... | Permitir | No | Entrante | System | Cualquiera | Subred local | UDP | 138 | Cualquiera | C | |
| Compartir archivos e impresoras... | Priva... | Permitir | No | Entrante | C:\WINDO... | Cualquiera | Subred local | UDP | 5355 | Cualquiera | C | |
| Compartir archivos e impresoras... | Priva... | Permitir | No | Entrante | System | Cualquiera | Subred local | UDP | 137 | Cualquiera | C | |
| Compartir archivos e impresoras... | Priva... | Permitir | No | Entrante | C:\WINDO... | Cualquiera | Subred local | TCP | Asignador d... | Cualquiera | C | |
| Compartir archivos e impresoras... | Priva... | Permitir | No | Entrante | C:\WINDO... | Cualquiera | Subred local | TCP | Puertos diná... | Cualquiera | C | |
| Compartir archivos e impresoras... | Priva... | Permitir | No | Entrante | System | Cualquiera | Subred local | TCP | 139 | Cualquiera | C | |

Actividad 6.3

Actividad resuelta 6.3

Comprueba en Windows y en Linux los certificados que tengas instalados en tus equipos.

Solución

En Linux ve a la ruta **/etc/ssl/certs**. Allí puedes ver todos los certificados que tienes instalados en el equipo.

En Windows, con el botón derecho del ratón sobre **Inicio**, selecciona **Ejecutar** y escribe:

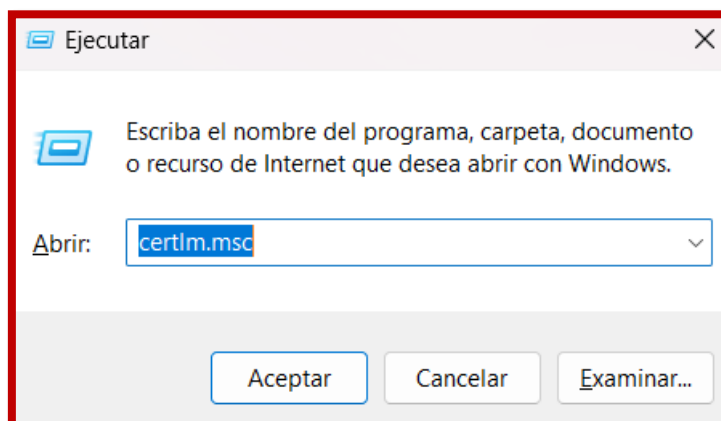
certlm.msc

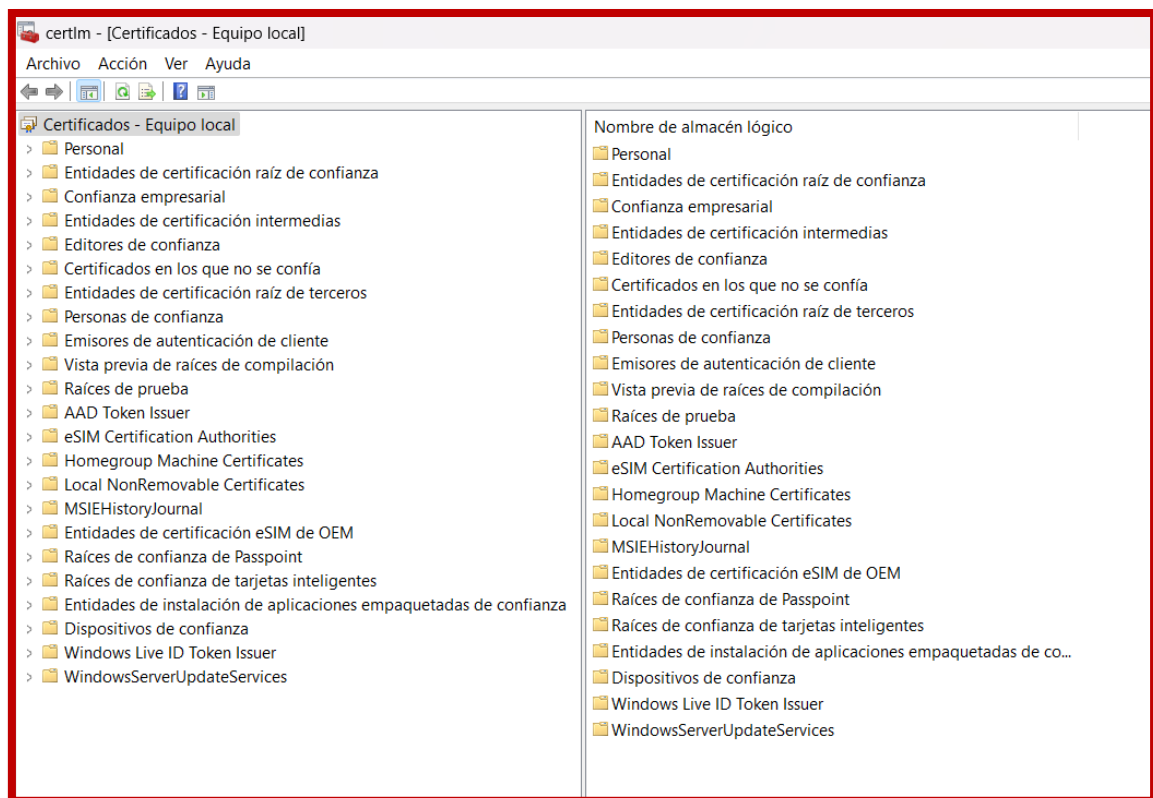
Después pulsa **Aceptar**. Cuando te pregunte si quieres permitir que el programa realice cambios en el equipo, responde que sí. En **Entidades de certificación**, en **Certificados**, puedes ver los certificados que se han ido instalando en el equipo con información de para quién se emitió, el emisor, la fecha de expiración y el propósito para el que se emitió, entre otra información.

Certificados en Linux:

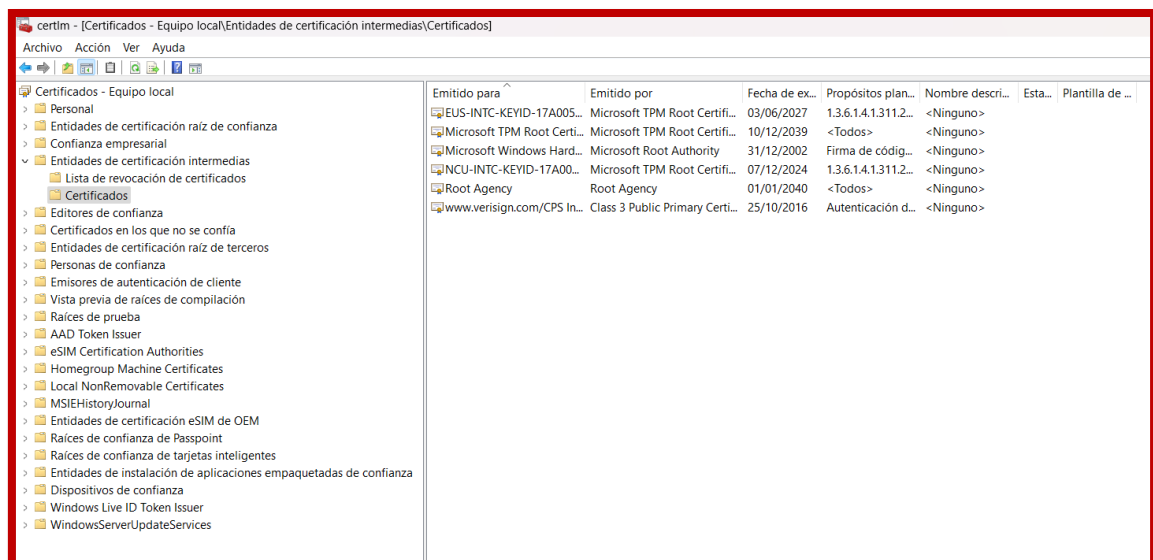
```
richard@richard-VirtualBox:~$ ls /etc/ssl/certs/  
002c0b4f.0  
02265526.0  
062cdee6.0  
064e0aa9.0  
06dc52d5.0  
08063a00.0
```

Certificados en Windows:





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



Actividad 6.4

Actividad resuelta 6.4

Consulta la dirección IP de tu *router* y comprueba si puedes entrar. Comprueba desde el Símbolo del sistema con el comando **tracert** la ruta que siguen los paquetes que salen por la IP de la puerta de enlace. Comprueba con **netstat** las conexiones abiertas y los puertos de escucha.

Solución

Se puede obtener de varias formas. En un equipo Windows abre el Símbolo del sistema y escribe **ipconfig**. En la conexión que tengas activa, mira el valor de puerta de enlace predeterminada. Para poder acceder, en un navegador web escribe la dirección IP anterior. Te deberá pedir un nombre de usuario y una contraseña para acceder. Si puedes acceder, dependiendo de sus características, podrás cambiar y configurar las diferentes propiedades. Los menús y dónde está cada opción varían de un *router* a otro.

Para comprobar la puerta de enlace, escribe en una terminal de Windows:

```
ipconfig
```

En la información que te muestra, mira cuál es la dirección IP de la puerta de enlace predeterminada. A continuación escribe:

```
tracert google.es
```

Y verás que la primera línea te muestra que el paquete sale por esa dirección IP.

En el sistema operativo Linux, para ver la dirección IP de la puerta de enlace deberás escribir:

```
ip route
```

La dirección IP de la puerta de enlace o *gateway* la puedes ver en la línea que empieza por:

```
default via <dir_ip_enlace>
```

Si la utilidad **traceroute** no está instalada, puedes instalarla escribiendo:

```
sudo apt install traceroute
```

A continuación, para ver la ruta que siguen los paquetes que salen por la IP de la puerta de enlace, escribe:

```
traceroute google.es
```

(En ambos casos puedes cambiar el destino **google.es** por cualquier otro para ver la ruta de los paquetes hacia él).

Para utilizar el comando **netstat**, en Windows puedes escribirlo en una terminal. En el sistema operativo Linux, si no está instalado, puedes instalarlo mediante el paquete:

```
sudo apt install net-tools
```

Después, para ver las conexiones abiertas y los puertos de escucha, puedes escribir:

```
netstat -an
```

Si la información es demasiado larga, puedes paginarla escribiendo:

```
netstat -an | more
```

Con este comando puedes ver si hay una conexión con tu equipo de la que no eres consciente. Para conocer las conexiones abiertas y en ejecución utilizarás el comando anterior. Te indica los protocolos (TCP o UDP), la IP local, la IP remota, los números de puertos y el estado de la conexión.

Con **ip config** vemos lo siguiente:

```
Sufijo DNS específico para la conexión. . . :  
Vínculo: dirección IPv6 local. . . : fe80::2765:cf39:8619:5bba%8  
Dirección IPv4. . . . . : 192.168.0.103  
Máscara de subred . . . . . : 255.255.255.0  
Puerta de enlace predeterminada . . . . . : 192.168.0.1
```

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

```
C:\Users\Student>tracert google.es  
  
Traza a la dirección google.es [142.250.201.67]  
sobre un máximo de 30 saltos:  
  
 1  2 ms    2 ms    2 ms  router [192.168.0.1]  
 2  4 ms    4 ms    3 ms  83.red-81-46-38.customer.static.ccgg.telefonica.net [81.46.38.83]  
 3  3 ms    3 ms    3 ms  201.red-81-46-69.customer.static.ccgg.telefonica.net [81.46.69.201]  
 4 17 ms    8 ms    8 ms  217.red-81-46-69.customer.static.ccgg.telefonica.net [81.46.69.217]  
 5  8 ms   11 ms    8 ms  97.red-80-58-106.staticip.rima-tde.net [80.58.106.97]  
 6  9 ms    9 ms    8 ms  176.52.253.93  
 7 11 ms    8 ms    9 ms  5.53.1.74  
 8  9 ms   11 ms    9 ms  142.250.213.243  
 9  8 ms    8 ms    8 ms  74.125.37.87  
10 12 ms    8 ms   41 ms  mad07s25-in-f3.1e100.net [142.250.201.67]  
  
Traza completa.
```

Comprobamos lo mismo en Linux:

```
richard@richard-VirtualBox:~$ ip route  
default via 192.168.0.1 dev enp0s3 proto dhcp metric 100  
169.254.0.0/16 dev enp0s3 scope link metric 1000  
192.168.0.0/24 dev enp0s3 proto kernel scope link src 192.168.0.151 metric 100  
richard@richard-VirtualBox:~$  
richard@richard-VirtualBox:~$ traceroute google.es  
traceroute to google.es (142.250.200.131), 30 hops max, 60 byte packets  
 1  gateway (192.168.0.1) 3.567 ms 3.192 ms 2.863 ms  
 2  83.red-81-46-38.customer.static.ccgg.telefonica.net (81.46.38.83) 8.161 ms 7.879 ms 7.284 ms  
 3  201.red-81-46-69.customer.static.ccgg.telefonica.net (81.46.69.201) 11.154 ms 9.840 ms 12.791 ms  
 4  * * 217.red-81-46-69.customer.static.ccgg.telefonica.net (81.46.69.217) 23.418 ms  
 5  * * *  
 6  * 176.52.253.93 (176.52.253.93) 10.470 ms 10.169 ms  
 7  5.53.1.82 (5.53.1.82) 11.633 ms 5.53.0.176 (5.53.0.176) 9.881 ms 5.53.1.82 (5.53.1.82) 11.348 ms  
 8  192.178.110.71 (192.178.110.71) 9.565 ms 192.178.110.89 (192.178.110.89) 17.275 ms 192.178.110.71 (192.178.110.71) 16.718 ms  
 9  142.251.51.141 (142.251.51.141) 16.593 ms 142.251.51.143 (142.251.51.143) 16.425 ms 142.251.51.141 (142.251.51.141) 16.286 ms  
10  mad41s14-in-f3.1e100.net (142.250.200.131) 16.163 ms 15.256 ms 15.586 ms
```

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

```
richard@richard-VirtualBox:~$ netstat -an  
Conexiones activas de Internet (servidores y establecidos)  
Proto Recib Envíad Dirección local Dirección remota Estado  
tcp 0 0 127.0.0.1:631 0.0.0.0:* ESCUCHAR  
tcp 0 0 127.0.0.53:53 0.0.0.0:* ESCUCHAR  
tcp 0 0 192.168.0.151:60216 91.189.91.83:80 TIME_WAIT  
tcp6 0 0 :::631 :::* ESCUCHAR  
udp 0 0 127.0.0.53:53 0.0.0.0:*  
udp 0 0 192.168.0.151:68 192.168.0.1:67 ESTABLECIDO  
udp 0 0 0.0.0.0:631 0.0.0.0:*  
udp 0 0 0.0.0.0:5353 0.0.0.0:*  
udp 0 0 0.0.0.0:47910 0.0.0.0:*  
udp6 0 0 fe80::e9:185d:941b::546 :::*  
udp6 0 0 :::5353 :::*  
udp6 0 0 :::35498 :::*  
raw6 0 0 :::58 :::*  
  
Sockets activos de dominio UNIX (servidores y establecidos)  
Proto RefCnt Flags Type State I-Node Ruta  
unix 3 [ ] FLUJO CONECTADO 22628 /run/dbus/system_bus_socket  
unix 3 [ ] FLUJO CONECTADO 24803 /run/user/1000/bus  
unix 3 [ ] FLUJO CONECTADO 26294 /run/user/1000/bus  
unix 3 [ ] FLUJO CONECTADO 26270 /run/user/1000/bus  
unix 3 [ ] FLUJO CONECTADO 22547  
unix 3 [ ] FLUJO CONECTADO 27134 /run/user/1000/bus  
unix 3 [ ] FLUJO CONECTADO 26145 /run/dbus/system_bus_socket  
unix 3 [ ] FLUJO CONECTADO 26414  
unix 3 [ ] FLUJO CONECTADO 27124 /run/systemd/journal/stdout  
unix 2 [ ] DGRAM CONECTADO 22624
```

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.

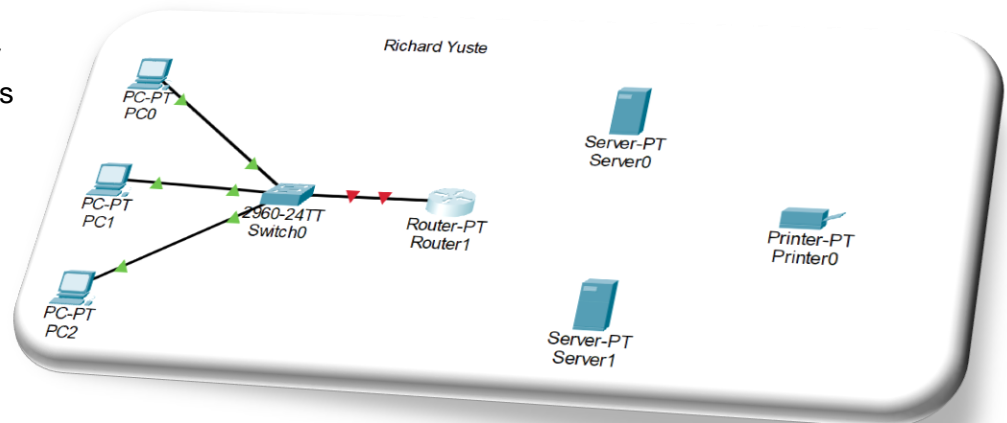
La entrega será una explicación del proceso seguido en las configuraciones de los equipos. Sobre todo, aquellos donde se repite el mismo no es necesario realizar capturas.

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:

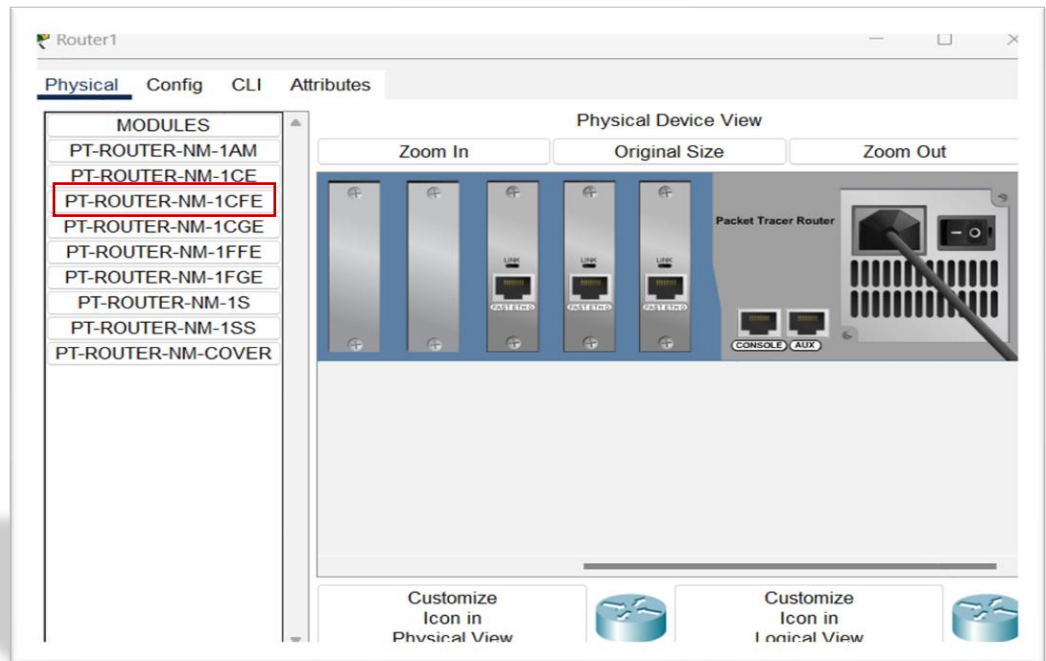
<https://youtu.be/JtgEgtOoco?si=Rt7PQValeEUETweGx>

Creamos una red sencilla con:

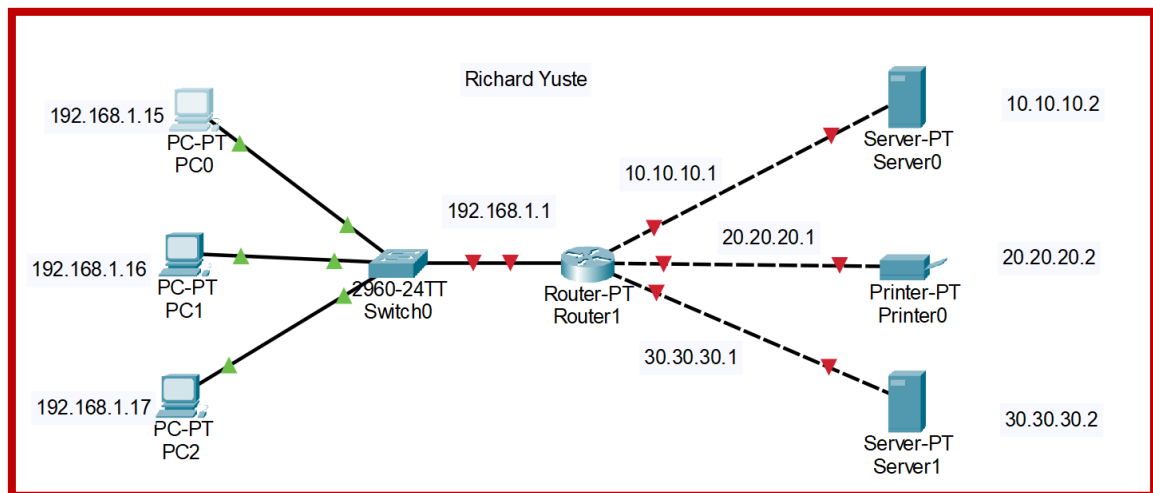
- 3 PCs
- 1 Switch
- 1 Router
- 2 Servers
- 1 Printer



Ahora configuramos el Router añadiéndole más conexiones FastEthernet:



Procedemos a configurar las siguientes IPs:



Primero los PCs:

Gateway/DNS IPv4

☐ DHCP

☒ Static

Default Gateway 192.168.1.1

DNS Server

IP Configuration

☐ DHCP

☒ Static

IPv4 Address 192.168.1.5

Subnet Mask 255.255.255.0

Ahora el router:

- FA0/0:

| | |
|------------------|---------------|
| IP Configuration | |
| IPv4 Address | 192.168.1.1 |
| Subnet Mask | 255.255.255.0 |

- FA1/0:

| | |
|------------------|------------|
| IP Configuration | |
| IPv4 Address | 10.10.10.1 |
| Subnet Mask | 255.0.0.0 |

- FA2/0:

| | |
|------------------|------------|
| IP Configuration | |
| IPv4 Address | 20.20.20.1 |
| Subnet Mask | 255.0.0.0 |

- FA3/0:

| | |
|------------------|------------|
| IP Configuration | |
| IPv4 Address | 30.30.30.1 |
| Subnet Mask | 255.0.0.0 |

Seguimos con los servers:

| | |
|---|------------|
| Gateway/DNS IPv4 | |
| <input type="radio"/> DHCP | |
| <input checked="" type="radio"/> Static | |
| Default Gateway | 10.10.10.1 |
| DNS Server | |

| | |
|---|------------|
| IP Configuration | |
| <input type="radio"/> DHCP | |
| <input checked="" type="radio"/> Static | |
| IPv4 Address | 10.10.10.2 |
| Subnet Mask | 255.0.0.0 |

Y por último la impresora:

Gateway/DNS IPv4

☐ DHCP

☒ Static

Default Gateway

DNS Server

IP Configuration

☐ DHCP

☒ Static

IPv4 Address

Subnet Mask

Configuramos los servidores para DNS, WEB y DHCP:

- DNS:

DNS y WEB

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS**
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DNS

DNS Service ☒ On ☐ Off

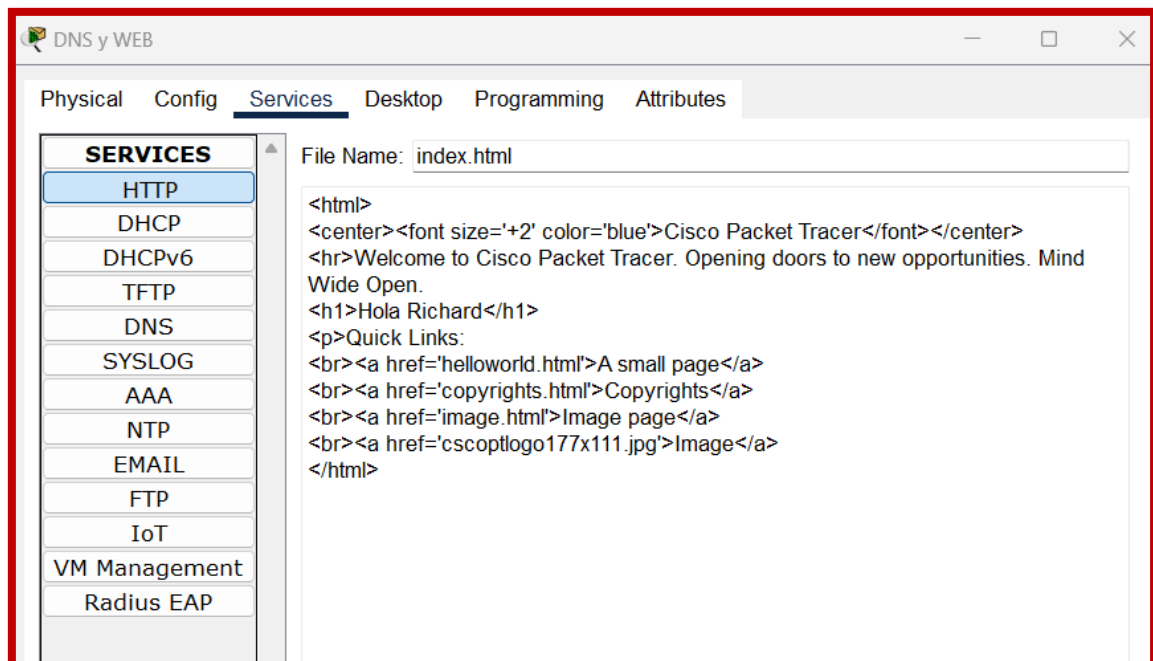
Resource Records

Name Type

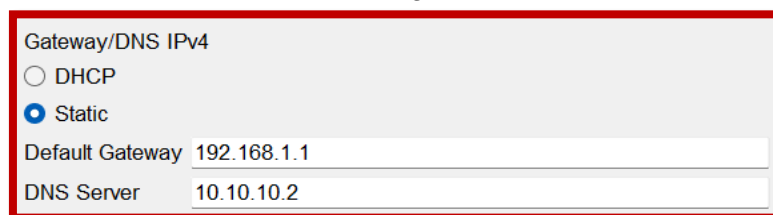
Address

| No. | Name | Type | Detail |
|-----|------|------|--------|
|-----|------|------|--------|

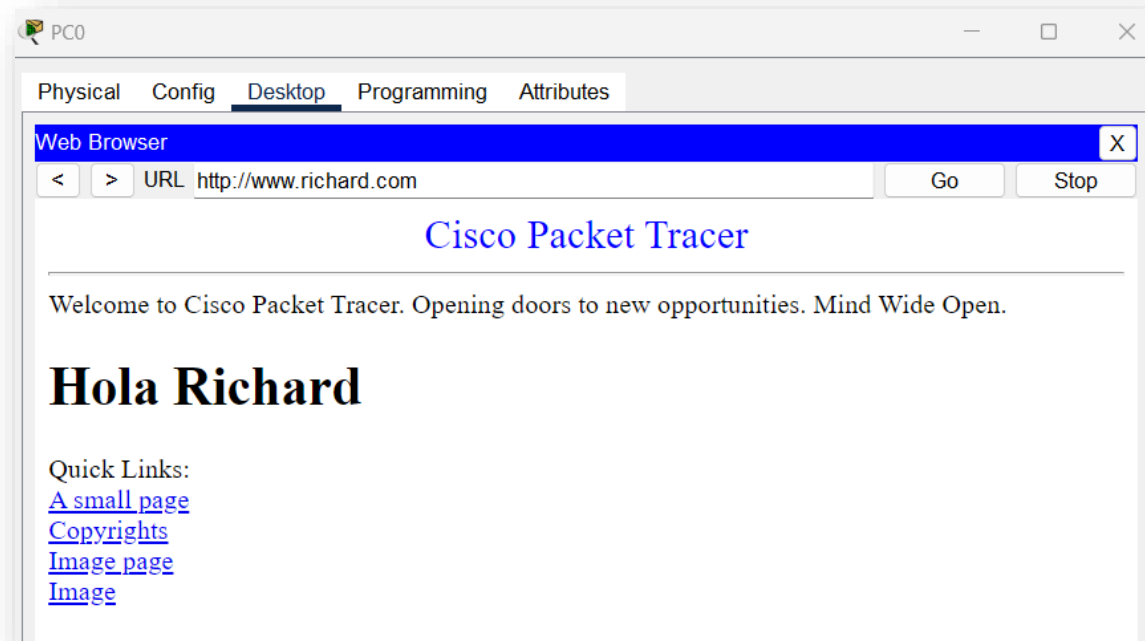
- HTTP:
 - o Editamos el index:



- o Modificamos el DNS en la configuración del PC1:



- o 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

SERVICES

- HTTP
- DHCP**
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DHCP

Interface: FastEthernet0 Service: ☒ On ☐ Off

Pool Name: serverPool

Default Gateway: 30.30.30.1

DNS Server: 10.10.10.2

Start IP Address: 30 30 30 30

Subnet Mask: 255 0 0 0

Maximum Number of Users: 100

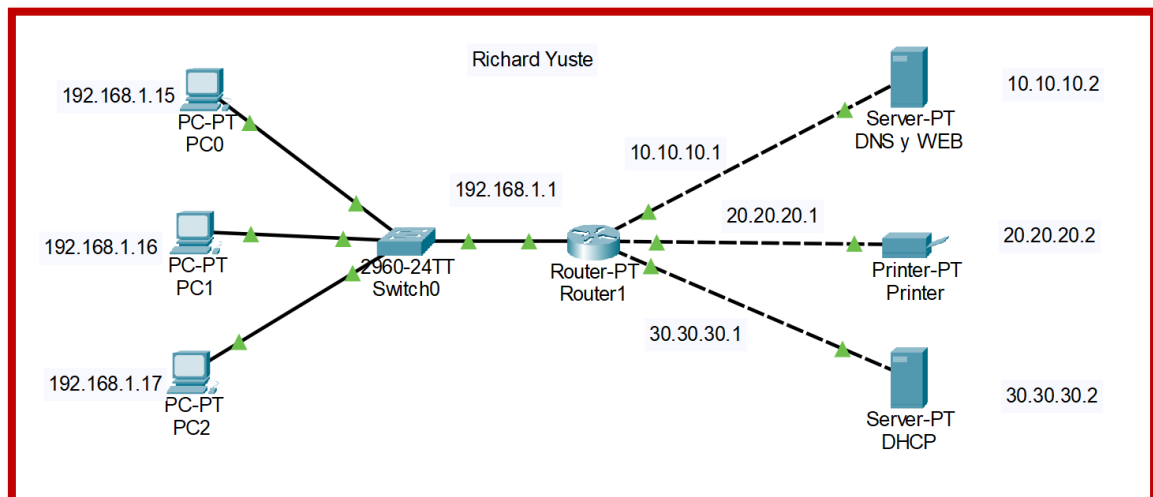
TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Buttons: Add Save Remove

| Pool Name | Default Gateway | DNS Server | Start IP Address | Subnet Mask | Max User | TFTP Server | WLC Address |
|------------|-----------------|------------|------------------|-------------|----------|-------------|-------------|
| serverPool | 30.30.30.1 | 10.10.10.2 | 30.30.30.30 | 255.0.0.0 | 100 | 0.0.0.0 | 0.0.0.0 |

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
```

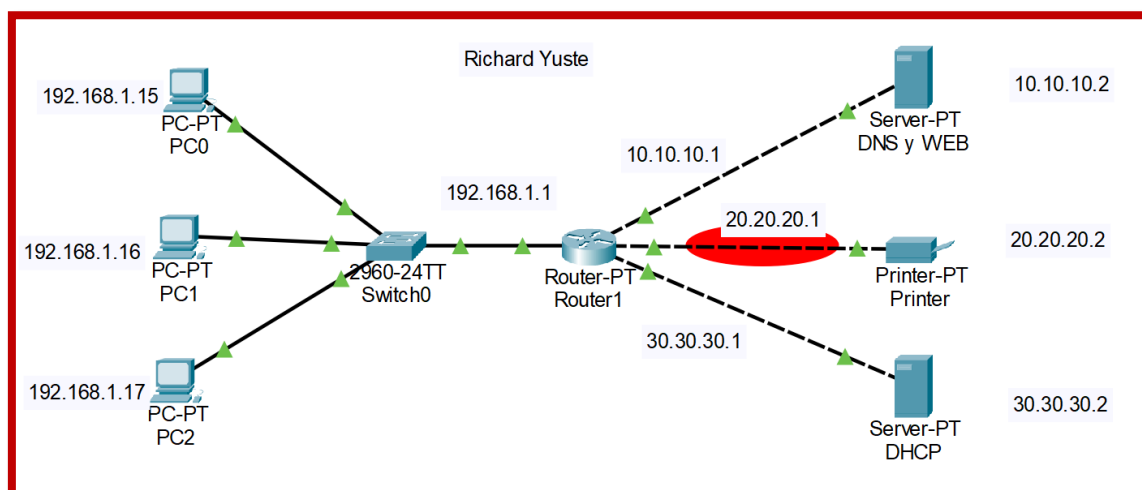
```
Router(config)#interface fastethernet 2/0
```

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

```
Router(config-if)#exit
```

```
Router(config)#exit
```

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
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
Router#
%SYS-5-CONFIG I: Configured from console by console
```



Si hacemos ping hacia la impresora no nos dejará:

| Fire | Last Status | Source | Destination | Type | Color | Time(sec) | Periodic | Num | Edit | Dek |
|------|-------------|---------|-------------|------|-------|-----------|----------|-----|--------|-------|
| | Successful | Router1 | DNS y WEB | ICMP | | 0.000 | N | 14 | (edit) | (del) |
| | Failed | Router1 | Printer | ICMP | | 0.000 | N | 15 | (edit) | (del) |
| | Successful | Router1 | DHCP | ICMP | | 0.000 | N | 16 | (edit) | (del) |

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.