LABORATORIO 2

Aislamiento S.O, Shell y software de apoyo en redes

Elaborado por

Santiago Cárdenas Amaya

Juan Pablo Fonseca Cárdenas

RECO

Bogotá, 2022

# Introducción

Los usuarios día a día se conectan a internet sin embargo no llegan a imaginarse que es lo que realmente pasa cuando escriben [www.google.com](http://www.google.com) en este laboratorio vamos a usar distintas herramientas que nos ayudaran a entender que es lo que pasa a nivel lógico cuando ingresamos a una página. También a entender cómo funciona el envío de paquetes en la red y los subprocesos que esta hace. Entenderemos cómo funciona uno de los editores que manejan los sistemas Linux como lo es vi y manejo básico de Shell. E indagaremos en un protocolo público de Windows que nos permite compartir archivos por red.

# Marco teórico

Para este laboratorio iremos definiendo a lo largo de él los softwares packetracer y wireshare. A continuación, se encuentra el concepto que nos ayuda a familiarizarnos con el laboratorio.

**SAMBA:** Samba es una implementación libre del protocolo de archivos compartidos de Microsoft Windows para sistemas de tipo UNIX. De esta forma, es posible que computadoras con GNU/Linux, Mac OS X o Unix en general se vean como servidores o actúen como clientes en redes de Windows.

**PAQUETE:** En redes, un paquete es un pequeño segmento de un mensaje más grande. Los datos enviados a través de redes informáticas, como Internet, se dividen en paquetes. Estos paquetes los vuelve a combinar el ordenador o el dispositivo que los recibe.

# Uso y aplicaciones

Por un lado, Packetracer nos ayuda a entender más fácil el cómo se comunican la red en general mientras que wireshare nos ayudara a ver lo que realmente está pasando en tiempo real en la red. Mientras que el entendimiento de samba nos permitirá compartir archivos entre las diferentes máquinas virtuales, lo cual nos servirá a lo largo del semestre.

# Conociendo Packet Tracer

## Preguntas generales

### ¿Qué versión de Packet Tracer se encuentra disponible en la plataforma de Cisco?

8.2

### ¿Qué significan las conexiones negras continuas?

Se trata de un cable Ethernet estándar que se utiliza para conectar dos dispositivos que operan en diferentes capas del modelo OSI (como el hub al router y el switch al PC). Puede utilizarse con los tipos de puerto Ethernet, Fast Ethernet y Gigabit Ethernet.

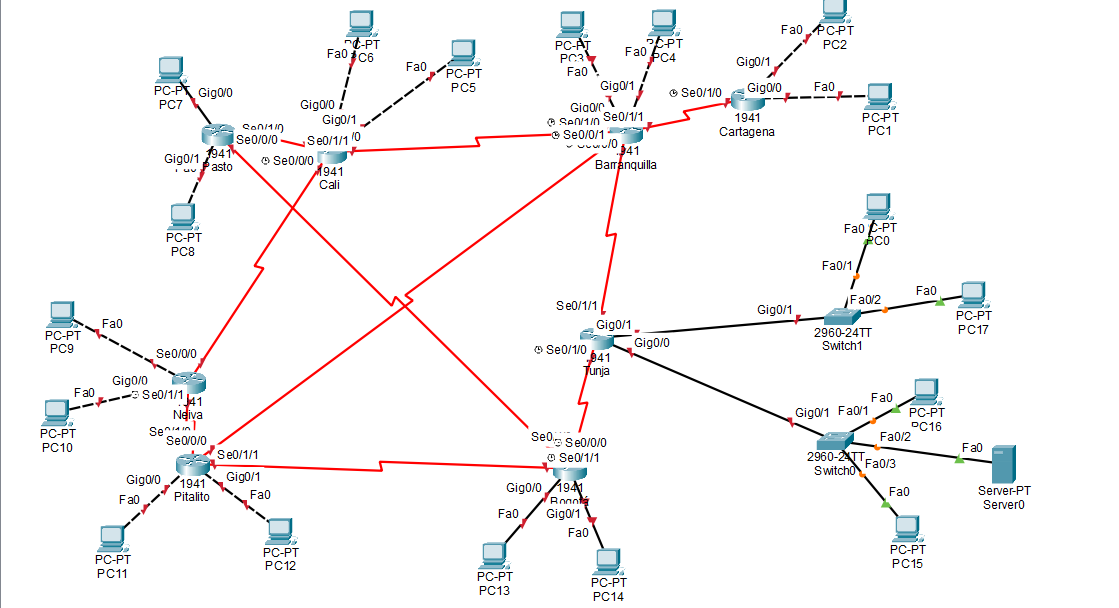
### ¿Qué significan las conexiones negras discontinuas?

Este cable Ethernet conecta dispositivos que funcionan en la misma capa OSI (como hub a hub, PC a PC, PC a router y PC a impresora). Este cable también puede utilizarse con los tipos de puerto Ethernet, Fast Ethernet y Gigabit Ethernet.

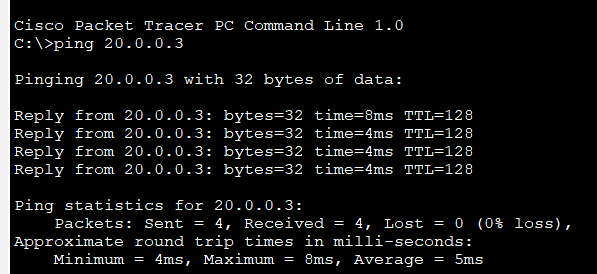
### El video se llama “Pablo va a cancelar.mp4”

## Packet Tracer Juan Pablo

### Imagen diagrama de red



### ping desde el PC15 o PC16 al servidor Webserver desde el modo simulación de packet tracer.



Eventos capturados

Tabla

Descripción generada automáticamente

Tabla

Descripción generada automáticamente

### Revise el contenido de los paquetes capturados

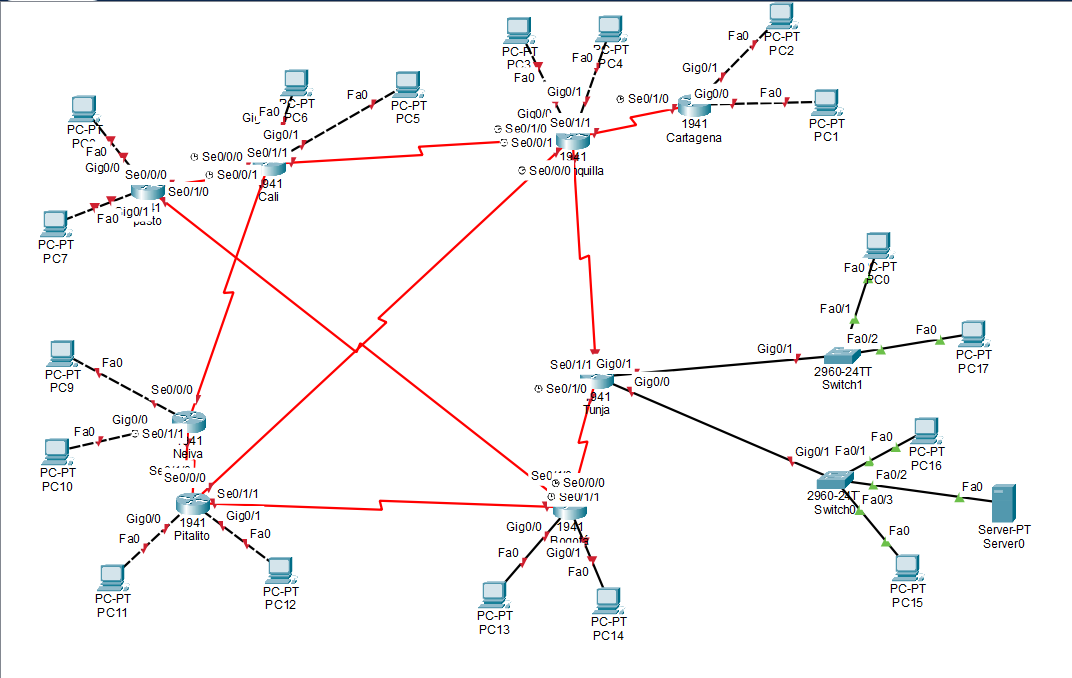
Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Dentro de lo poco que se entiende, en la parte inferior se aprecia un breve resumen indicando que sucedió en ese evento, y así sucede con todos. Un resumen

## Packet Tracer Santiago

### Imagen diagrama de red



### ping desde el PC15 o PC16 al servidor Webserver desde el modo simulación de packet tracer.

Texto

Descripción generada automáticamente

Tabla

Descripción generada automáticamente

### Revise el contenido de los paquetes capturados

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Este es el ultimo evento capturado, el cual indica que la capa 3 desencapsula el paquete donde viene la IP address. Al clickear las otras partes se ve que la capa 1 recibe el frame, y la 2 relaciona la dirección MAC con el puerto por donde se emitió el broadcast.

## ¿Qué es Wireshark?

Es un software gratuito que permite visualizar y analizar el trafico de la red en tiempo real. Este coge la información que uno podría captar normalmente con comandos como tracerroute, pero este software hace que la visualización de toda esta información sea mucho mas legible, esto sumado a que permite filtrar el trafico en la red

## ¿Qué significa que la tarjeta queda en modo promiscuo?

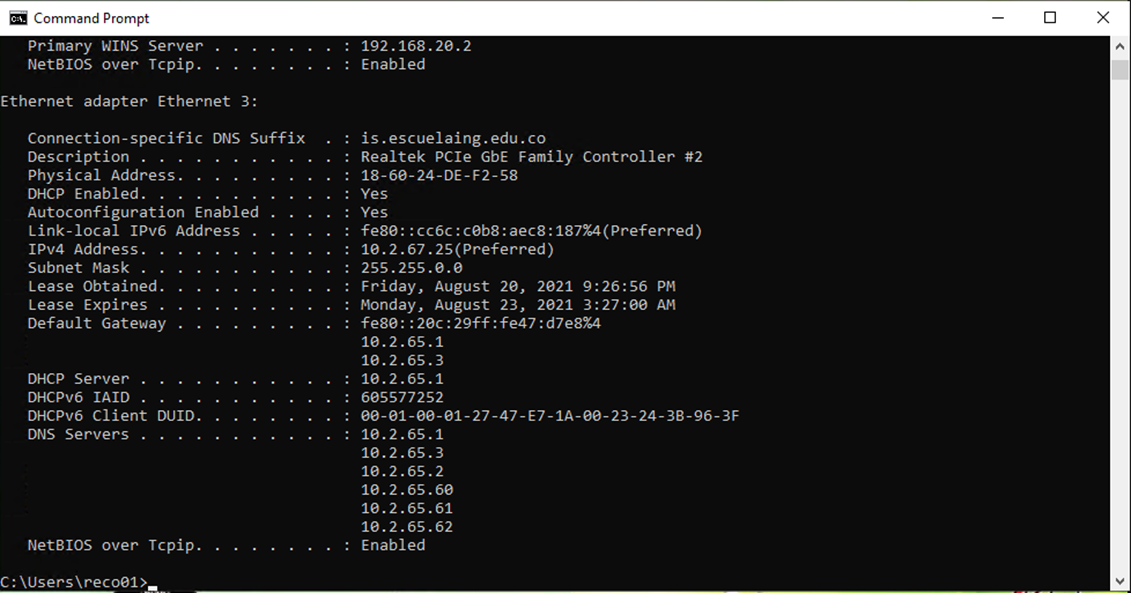
Es un modo de wireshark que permite que la tarjeta de red pueda interceptar todos los paquetes que circulan en toda nuestra red, es decir que también puedo capturar el trafico de otros dispositivos, siempre y cuando estén relacionados a mi red.

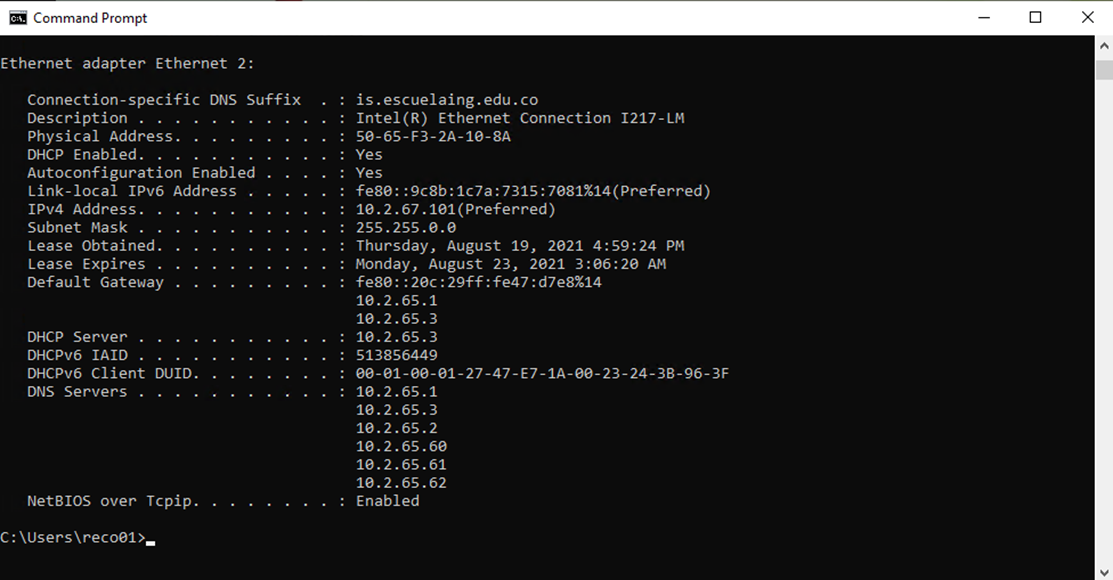
## Video wireshark

El video se llama “Profe entiendanos.mp4”

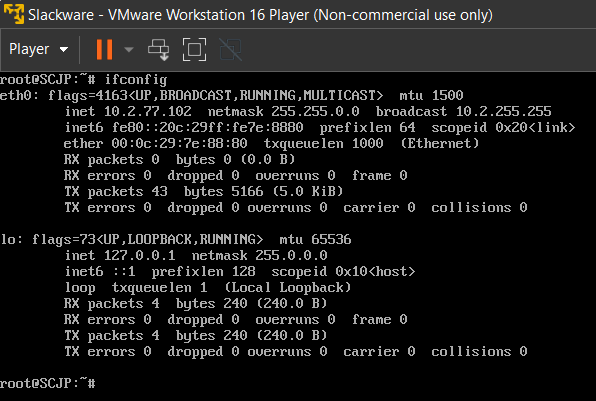
# Tarjetas de red

## Tarjeta de red computador de la escuela

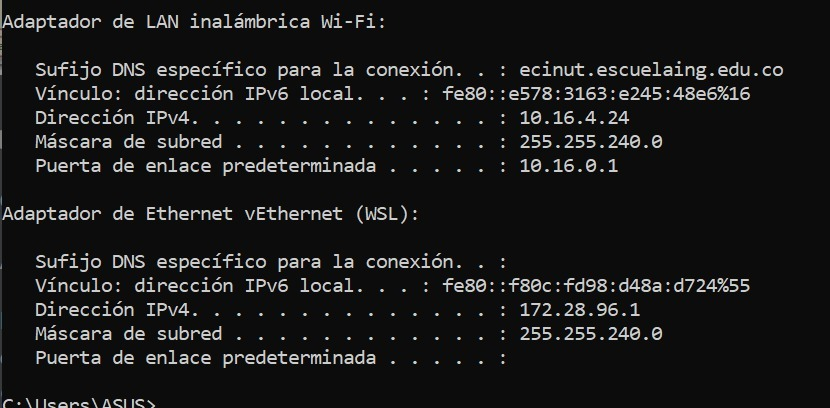




## Tarjetas de red maquinas virtuales



## Tarjetas de Red dispositivos Juan Pablo



Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

proveedor:Microsoft

version:10.0.19041.1

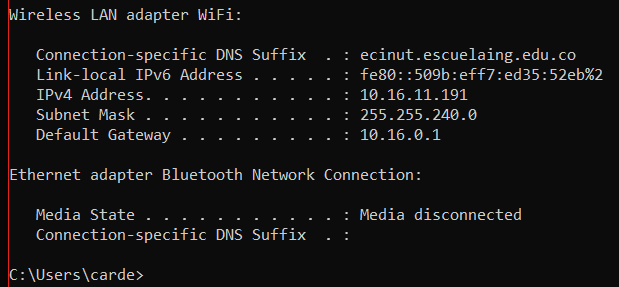
MAC Address:255.255.255.0

IPv4 Address:192.168.0.4

IPv6 Address: fe80::807e:84c0:2b06:81b8%11

cantidad de bytes transmitidos y recibidos:

## Tarjetas de Red Santiago



## Comparación de información de las maquinas virtuales respecto a las máquinas anfitrionas

Las máquinas virtuales usan una tarjeta de red que genera el virtualizador en este caso VM Ware lo que es una copia de la tarjeta física de la maquina host. Mientras que desde las maquinas anfitrionas la información es mucho más detallada.

# Shell programming Unix

Las shell’s programadas quedaron dentro de la carpeta que se compartio por samba llamada “Slackware”

# Edito VI / en Linux /Unix

**Grabe el trabajo realizado sin salir del editor**

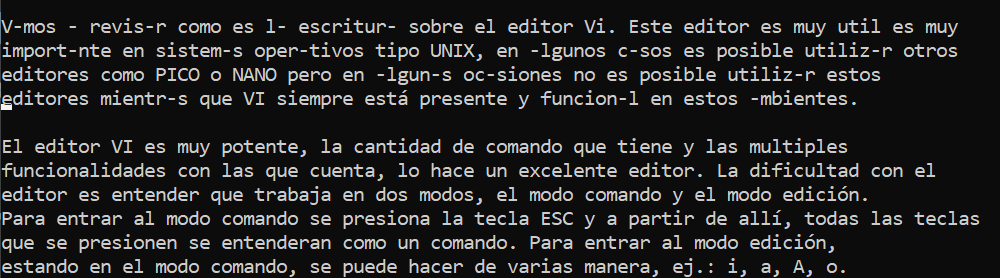
:w

Texto

Descripción generada automáticamente

**Cambie las letras ‘a’ del primer párrafo por el símbolo –**

:1,5s/a/-/g



**Cambie las palabras “al” en todo el texto por los símbolos ##**

:%s/al/##/g

Texto

Descripción generada automáticamente

**¿Qué comando se puede usar para borrar una palabra en VI?**

Uno se posiciona en la palabra a borrar y escribe dw

**Borre la última 4 línea del documento con un solo comando.**

:9,9d

Texto

Descripción generada automáticamente

**Deshaga el comando anterior.**

u

Texto

Descripción generada automáticamente

**Pase a mayúscula la última línea del documento**

Nos posicionamos en la última línea del documento y escribimos gUU

**Copie las últimas 2 líneas del segundo párrafo al final del archivo.**

Nos ubicamos en la línea y escribimos nyy, donde n es el numero de líneas a copiar.

Luego los ubicamos en la línea donde de va a pegar y se presiona la p.

Texto

Descripción generada automáticamente

**Busque la palabra editor dentro del texto**

/editor

**Ubíquese en la línea 5 del texto usando un comando**

:5

**Haga un cuadro resumen con comandos de VI**

|  |  |
| --- | --- |
| Uso | Comando |
| Guardar cambios | :w |
| Cambiar un string por otro | :{línea\_0},{línea\_1}s/{string\_0}/{string\_a}/g |
| Borrar una palabra | dw |
| Borrar líneas | :{línea\_0},{línea\_1}d |
| Deshacer comandos | u |
| Cambiar a edición | a, i etc. |
| Cambiar a modo comando | Esc |
| Convertir línea a upperCase | gUU |
| Copiar líneas | {numLineas}yy |
| Pegar | p |
| Buscar una palabra | /{word} |
| Ubicarme en una determinada línea | :{numLinea} |

**Grabe el trabajo y salga del editor**

:wq

**Vuelva a entrar y borre las primeras 5 líneas**

:1,5d

Texto

Descripción generada automáticamente

**Salga del archivo sin grabar5**

:q!

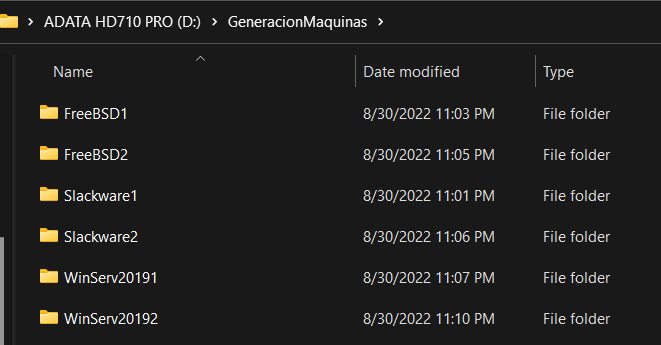
Al entrar de nuevo:

Texto

Descripción generada automáticamente

# Generación máquinas

Dentro del disco creamos la carpeta “GeneracionMaquinas” y dentro de ella creamos las 6 maquinas que se pide en este punto, 2 de slackware, 2 de freeBSD y 2 de windows server 2019 con GUI

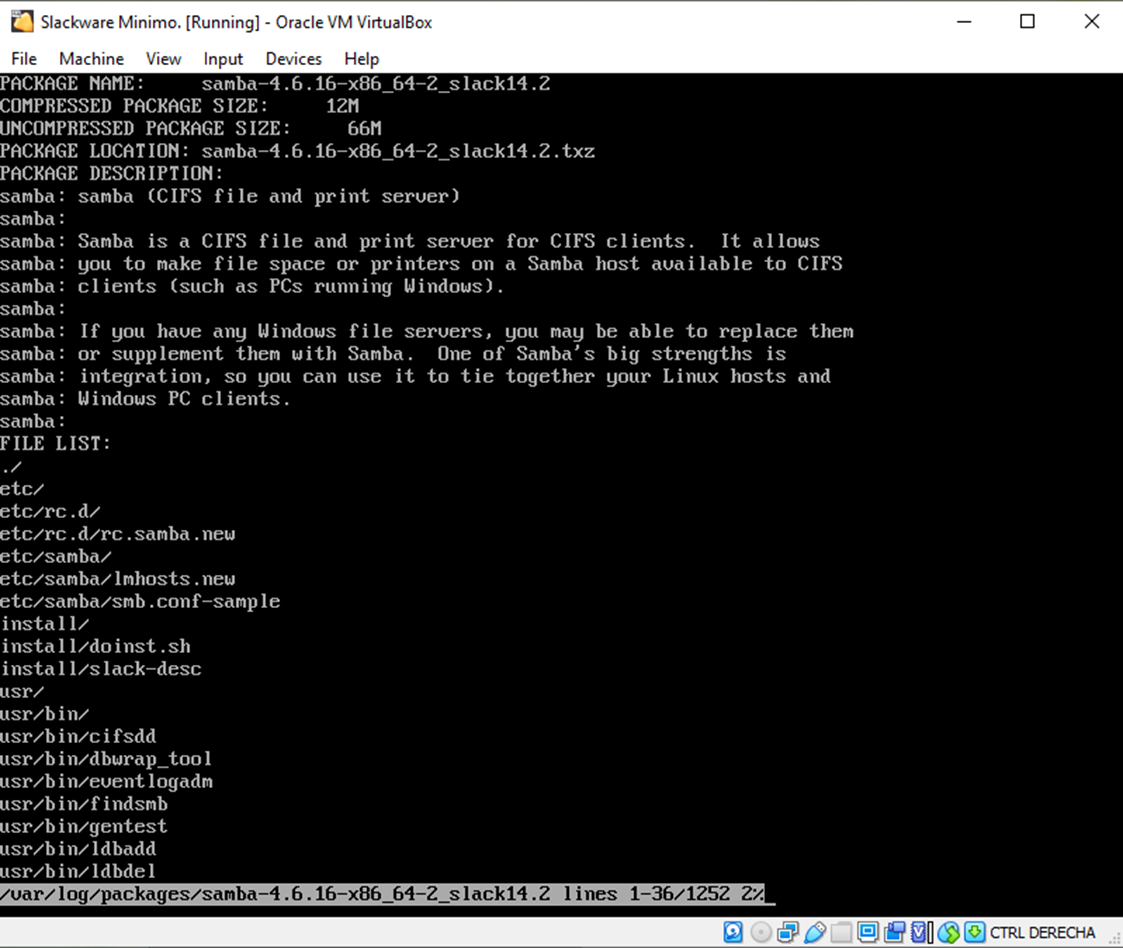


# Compartir archivos

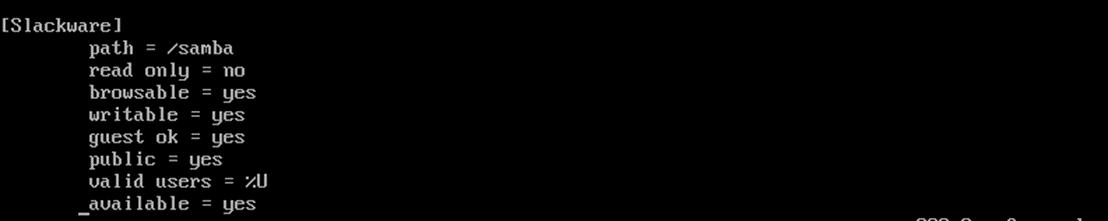
Lo primero sera instalar samba en slackware por lo que usaremos el comando “Get” y la url que hayamos encontrado en este caso <https://slackware.uk/slackware/slackware64-14.2/slackware64/n/samba-4.4.4-x86_64-3.txz>

Luego pasaremos a realizar la instalacion con el comando “upgradepkg --install-new samba-4.4.4-x86\_64-3.txz”

Una vez hecho este verificamos que haya quedado instalado con el comando “less /var/log/packages/samba\*”



Ahora con cualquier editor en este caso vi abrimos el archivo smb.conf y lo editamos de la siguiente forma



Se crea un usuario que sera con el que se ingrese a los archivos desde otras maquinas



Luego usamos el comnado “smbpasswd -a” y el nombre del usuario creado en este caso “scjp”

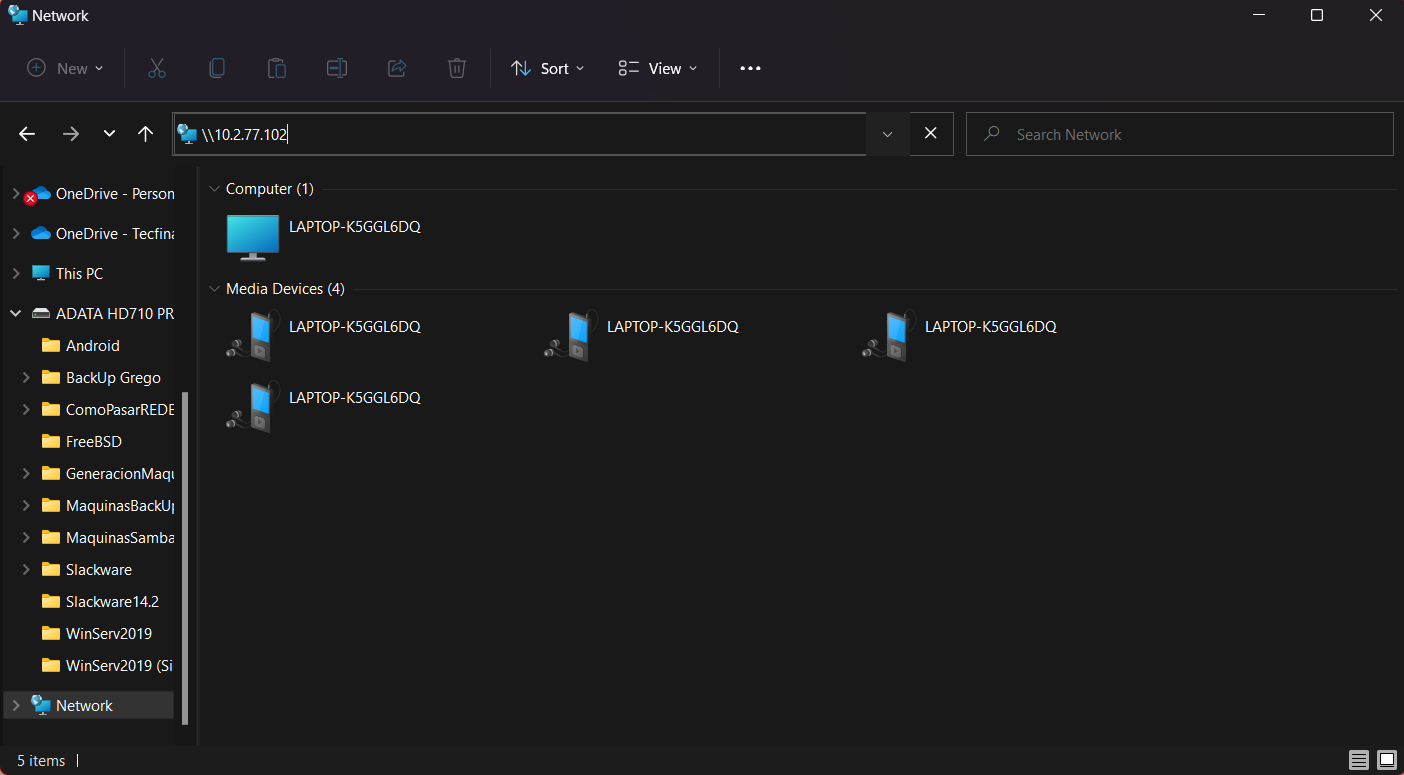
Con mkdir creamos la carpeta que se va a compartir “Slackware” y dejamos un archivo adrentro de ella con “touch” nombre del archivo

Damos permisos 755 sobre la carpeta y el archivo rc.samba

Luego iniciamos samba con el comando “/etc/rc.d/rc.samba start”



Para probar si funciono en sistemas windows no hace falta mas que conectar con la red desde el explorador de archivos



Para probar si funciono en sistemas unix/linux (debemos tener instalado samba) usamos el comando “smbclient // [Direccion de la maquina]// [Carpeta a la que se quiere acceder] -U [Nombre del usuario creado] ”

Para este caso “smbclient //10.2.77.102//Slackware -U scjp” luego de ingresar la clave deberia dejar ver los archivos

# Conclusiones

Se aprendió el correcto uso del software de simulación “packetracer” y el software de monitorio de red “Wireshark” adicional a ello se aprendió el correcto uso y manejo de shell’s. También se aprendió a configurar samba y su uso a la hora de enviar archivos por medio de la red.

# Bibliografía

A. (2008, 24 marzo). *Análisis de red con Wireshark. Filtros de captura y visualización.* Seguridad y Redes. https://seguridadyredes.wordpress.com/2008/03/24/analisis-de-red-con-wireshark-filtros-de-captura-y-visualizacian/

colaboradores de Wikipedia. (2022, 12 agosto). *Samba (software)*. Wikipedia, la enciclopedia libre. https://es.wikipedia.org/wiki/Samba\_(software)

*Packages for Linux and Unix*. (2021). Slackware. https://slackware.pkgs.org/14.2/slackware-x86\_64/samba-4.4.4-x86\_64-3.txz.html

*¿Qué es Wireshark? Así funciona la nueva tendencia esencial en seguridad*. (2018, 19 septiembre). IDG Communications S.A.U. https://cso.computerworld.es/tendencias/que-es-wireshark-asi-funciona-la-nueva-tendencia-esencial-en-seguridad