**Laboratorio 02. RECO-02**

Angel Nicolas Cuervo Naranjo

Jefer Alexis González Romero

**Introducción**

Por medio de la página web de Cisco se hará un curso introductorio a Paket Tracer que nos permite ver de una forma segura y tangible los elementos, conexiones y procesos que pasan detrás de las redes. Además, veremos otra herramienta, Wireshark, que de igual forma nos permite analizar, solucionar problemas y capturar tráfico de una red. También nos permite hacer análisis de datos y protocolos.

Asimismo, se realizarán algunos Shell los cuales nos permitirán incorporar un lenguaje de programación para controlar procesos y archivos. Por último, utilizaremos una implementación de protocolo de archivos compartidos llamado Samba, que nos permite compartir diversos sistemas de archivos.

**Desarrollo del tema**

**Marco teórico**

Una herramienta que nos permite diseñar redes y realizar simulaciones es Cisco Packet Tracer testeando la funcionalidad y el uso que a este le podemos dar ya en proyectos preconstruidos, topologías de red y diseños. Utilizando visualizadores que nos permiten visualizar los distintos sistemas operativos, en este laboratorio se hace uso de Virtualbox en el cual podemos instalar sistemas operativos cada uno separado por su ambiente virtual, teniendo así la opción de ejecutar de forma remota, también tendremos Wireshark es cual es software libre y nos permitirá realizar análisis de los protocolos en la red y solucionar problemas con las redes de comunicaciones.

Para la edición de archivos se usa del editor *Vi,* el cual es el editor de texto clásico de UNIX, este se puede usar en cualquier tipo de terminal con un mínimo de teclas, lo cual lo hace difícil su uso. A través de este editor se realizarán los Shell Script, que son programas que está creado con instrucciones que son ejecutadas por un shell.

Se hará uso de una implementación del protocolo *SMB,* el cual es un protocolo cliente-servidor que controla el acceso a archivos y directorios enteros, así como otros recursos de la red, como impresoras, routers o interfaces compartidas con la red. La implementación usando es *SAMBA,* el protocolo de archivos compartidos de Windows para sistemas operativos de tipo UNIX.

**Uso y aplicaciones**

Experimentos

**1. Conociendo Packet Tracer**

• Responda las siguientes preguntas

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

Se encuentra disponible la versión ***Packet Tracer 8.2.0***

1. Realicen un video que resumen los cursos. Máximo 5 min.

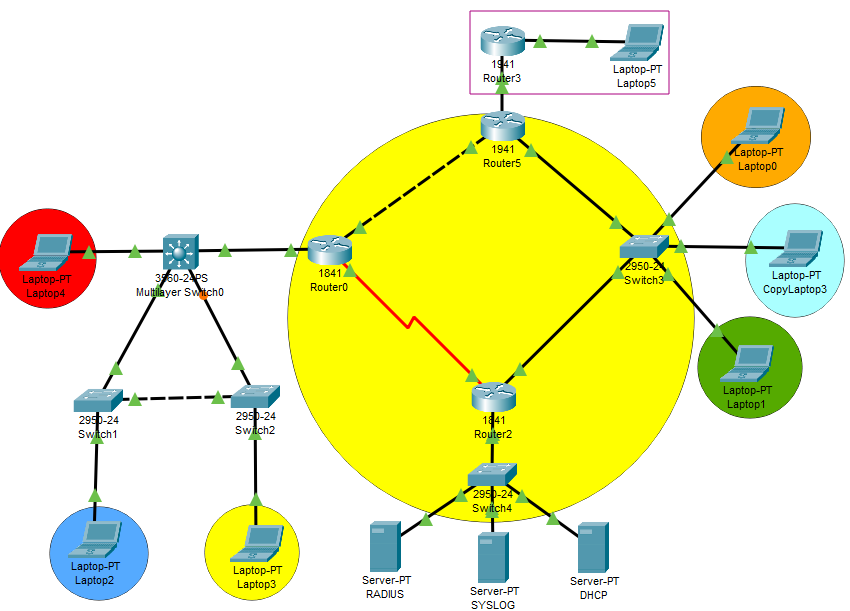
<https://youtu.be/QTvhp7FFQZY>

* Usando Packet Tracer cada estudiante debe hacer el diagrama de red.
* ¿Qué significan las conexiones negras continuas?

Son cables de cobre directos que permiten conectar dos dispositivos que no son del mismo tipo, por ejemplo, ordenador-switch, switch-router, router-ordenador.

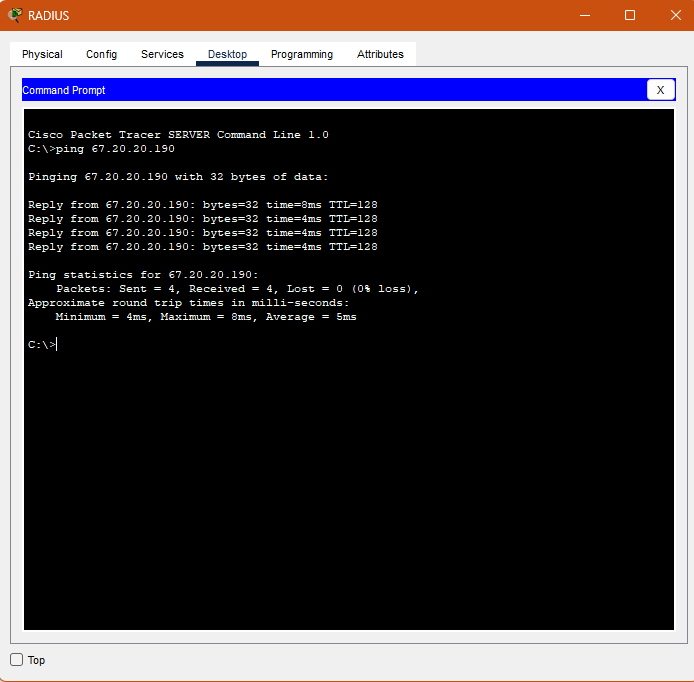
* ¿Qué significan las conexiones negras discontinuas?

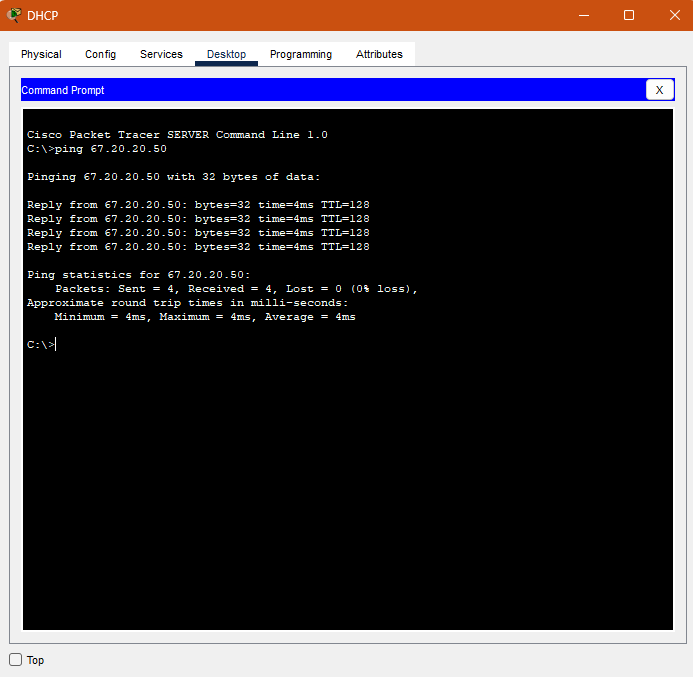
Son cables de cobre cruzado que permiten conectar dos dispositivos del mismo tipo, por ejemplo, dos ordenadores, dos routers o dos switches.



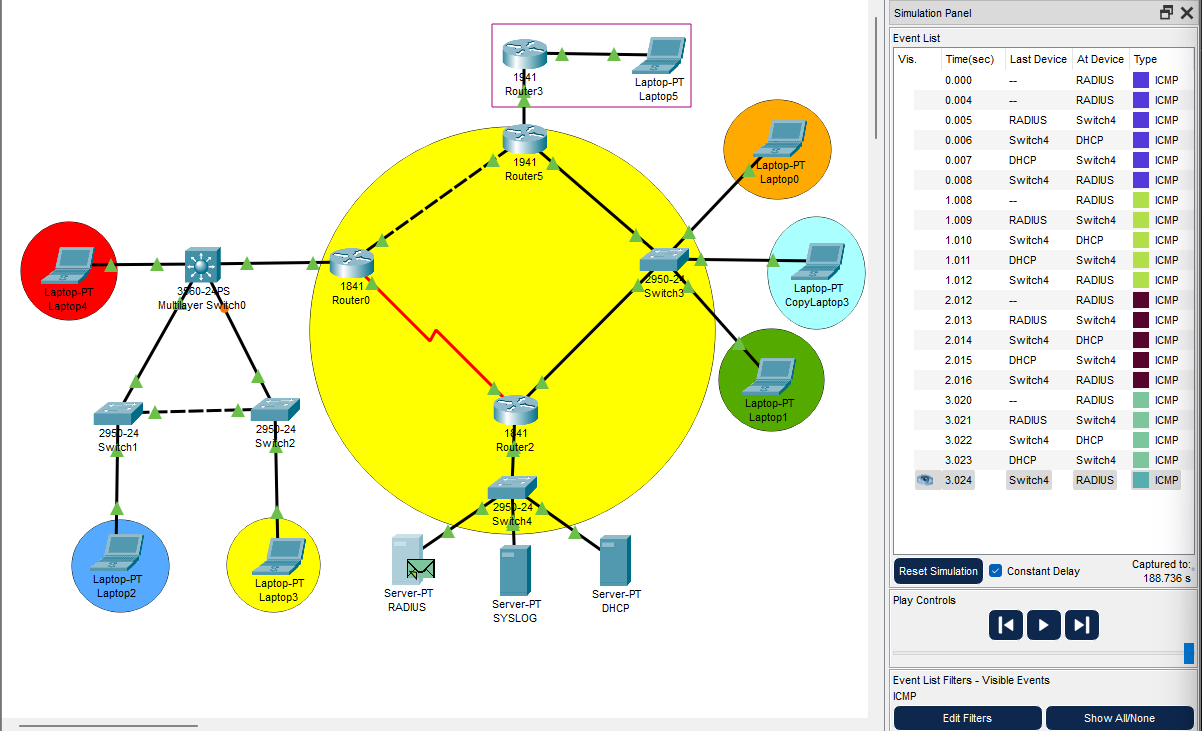
**2. Siguiendo mensajes con Packet tracer**

• Haga ping desde el servidor RADIUS y DHCP desde el modo simulación de packet tracer

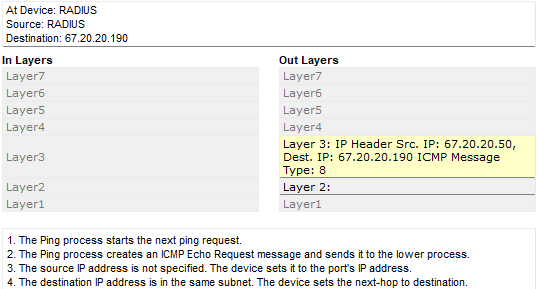




• Ahora, revise los PDUs por capas:



• Revise el contenido de los paquetes capturados. Vea cómo se van construyendo los PDU de cada capa

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamenteInterfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamenteInterfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamenteInterfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

En la red real

**1. Usando Wireshark**

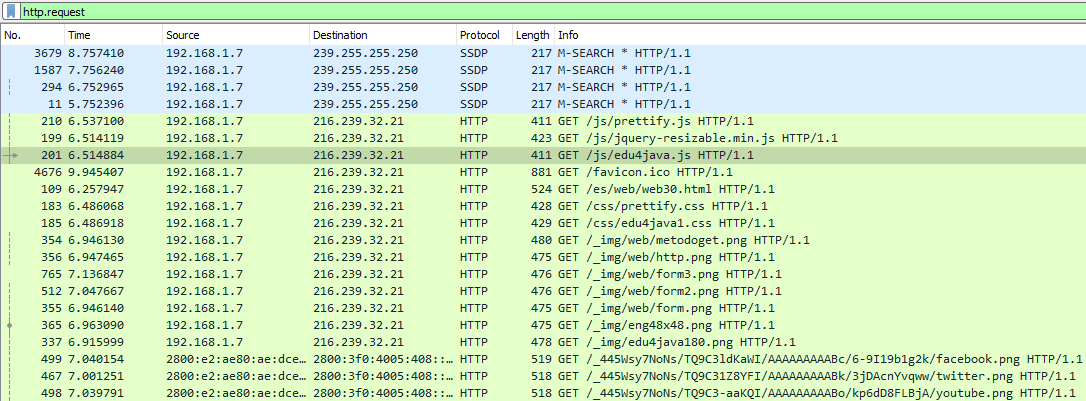
• ¿Qué es Wireshark?

Es un analizador de paquetes de red en tiempo real, permite conocer latencia o actividad maliciosa, se encarga de traducirlo a un formato legible para las personas. (welivesecurity, 2013)

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

Es el modo en el que un dispositivo de red puede interceptar y leer la totalidad de cada paquete de red que le llega. (Kripton, s.f.)

• Realice una consulta web al link http://www.edu4java.com/es/web/web30.html y capture el tráfico generado (para eso, ingrese al browser, inicie la captura con Wireshark y visite a la página indicada, termine la captura). Finalmente, pare la captura.



• Analice los datos encontrados en uno de los paquetes capturados. Mire el encapsulamiento que cada capa hace, revise la información que se puede ver en diferentes áreas de la pantalla de Wireshark y presente capturas del mismo (Para facilitar el análisis, filtre y encuentre un paquete capturado que contenga la palabra GET).

Interfaz de usuario gráfica, Aplicación, Word

Descripción generada automáticamente

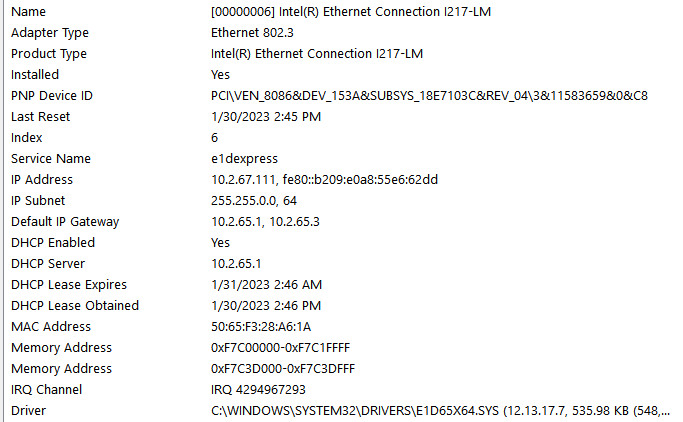
• Haga un video en donde especifique las partes de la interface que lo compone, ¿Cómo generar filtros?, ¿Para qué se usan? De unos ejemplos. Presente su respuesta con un video de máximo 5 min.

<https://www.youtube.com/watch?v=_SOI_wLv-o8>

**2. Tarjetas de red**

Conozca las tarjetas de red de varios dispositivos. Para esto, busque la información de las tarjetas de red de los computadores de la Escuela y de al menos 3 equipos diferentes (computadores, portátiles celulares, tablets, consolas de juegos, etc.) de cada miembro de su equipo de trabajo.

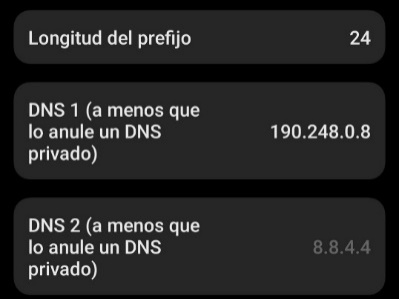
*Computador de la escuela*

Interfaz de usuario gráfica, Tabla

Descripción generada automáticamente

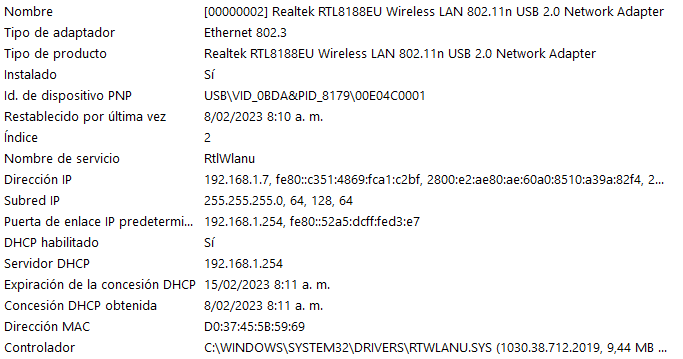
*Celular Alexis*

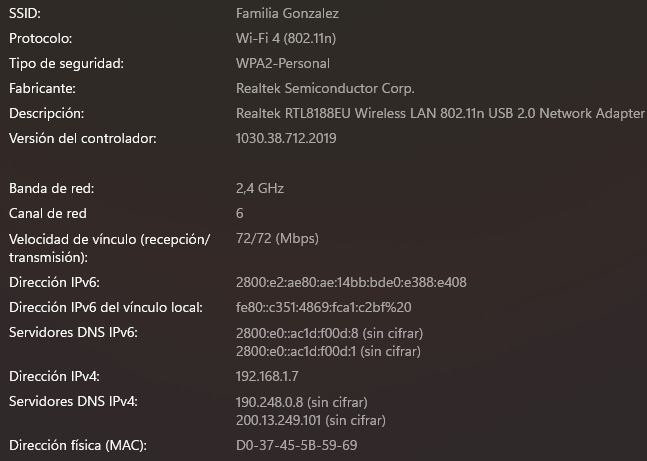






*Computador Alexis*

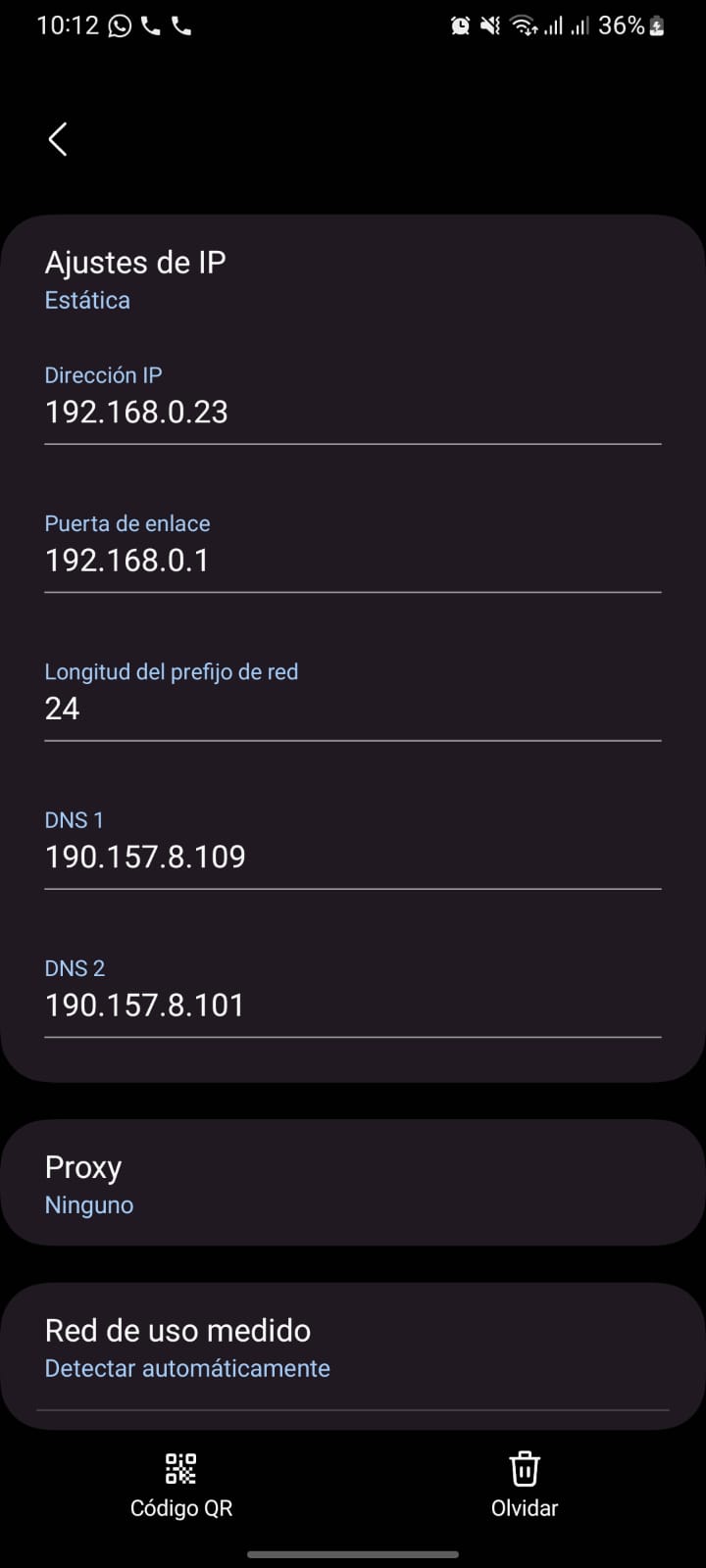




*Celular Angel*









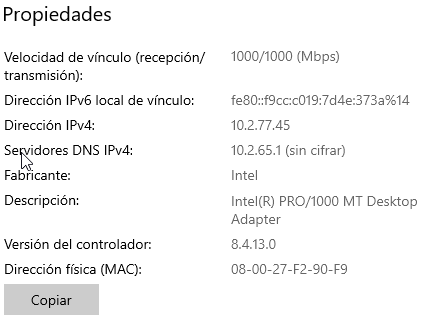
*Computador Angel*





Ahora, revise la misma información para 2 de sus máquinas virtuales y compare la información obtenida con la información de las máquinas anfitrionas.

*Máquina virtual Windows*



*Máquina virtual Slackware*

Texto

Descripción generada automáticamente

**Software base**

**1.** Shell programming- Unix

**Comando ls**

**•** Realice un Shell que liste los archivos en un directorio, inclusive los ocultos, dado y permitan

• Ordenarlo por las diferentes opciones e indicar la cantidad por grupos:

o Más reciente (debe decir cuántos archivos son de la misma fecha)

Texto

Descripción generada automáticamente

***./listar.sh /*** (Opción 1)

Tabla, Escala de tiempo

Descripción generada automáticamente con confianza mediaTexto

Descripción generada automáticamente con confianza media

o Más antiguo (debe decir cuántos archivos son de la misma fecha)

Texto

Descripción generada automáticamente

***./listar.sh /*** (Opción 2)

Escala de tiempo

Descripción generada automáticamenteImagen que contiene Calendario

Descripción generada automáticamente

o Tamaño de mayor a menor (debe decir cuántos archivos son del mismo tamaño)

Texto

Descripción generada automáticamente

***./listar.sh /*** (Opción 3)

Tabla

Descripción generada automáticamente con confianza mediaTexto

Descripción generada automáticamente con confianza media

o Tamaño de menor a mayor (debe decir cuántos archivos son del mismo tamaño)

Texto

Descripción generada automáticamente

***./listar.sh /*** (Opción 4)

Tabla

Descripción generada automáticamente con confianza mediaTexto

Descripción generada automáticamente con confianza media

o Tipo de archivo (Archivo/directorio) (debe decir cuántos archivos son del mismo tipo)



***./listar.sh /*** (Opción 5)

Texto

Descripción generada automáticamente con confianza media

• Que tenga las siguientes condiciones (dar la opción de sólo en el directorio indicado o

en el directorio indicado y sus subdirectorios)

o Inicie con una cadena dada



***./listar.sh /*** (Opción 6 con subdirectorios – cadena “etc”)

Texto

Descripción generada automáticamente



***./listar.sh /*** (Opción 6 sin subdirectorios – cadena “etc”)



o Termine con una cadena dada



***./listar.sh /*** (Opción 7 con subdirectorios – cadena “ios”)

Texto

Descripción generada automáticamente



***./listar.sh /*** (Opción 7 sin subdirectorios – cadena “ios”)



o Contenga una cadena dada



***./listar.sh /*** (Opción 8 con subdirectorios – cadena “srv”)

Texto

Descripción generada automáticamente



***./listar.sh /*** (Opción 8 sin subdirectorios – cadena “srv”)



Y luego, debe presentar un menú con las opciones anteriores (se debe quedar en el menú

hasta que el usuario indique que quiere salir). Debe limpiar pantalla antes de mostrar el

resultado y si es muy extenso el resultado, debe paginar.

Texto

Descripción generada automáticamenteTexto

Descripción generada automáticamenteTexto

Descripción generada automáticamente

**Comandos de búsqueda o visualización de archivos**

• Realice un Shell que desde la línea de comando (dando los parámetros indicados) permita

• Buscar un archivo/parte de un archivo dado una ruta y un nombre/parte de un

nombre de un archivo. La salida será las ubicaciones y nombres de los archivos y al final, la cantidad de veces que se encontró el archivo

Diagrama

Descripción generada automáticamente con confianza media

***./buscar.sh /aplicaciones ext*** (Opción 1)Texto

Descripción generada automáticamente

• Busque una palabra/parte de una palabra en un archivo dado. La salida será la

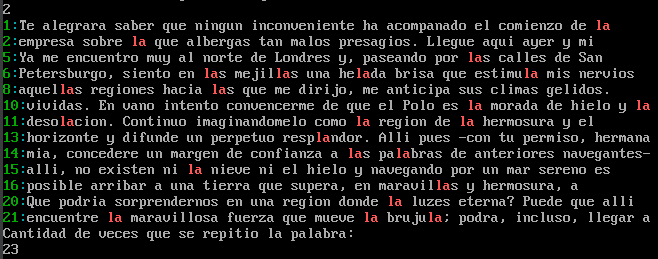
palabra encontrada y las líneas en las que la encontró y al final, la cantidad de

veces que se repitió.

Texto

Descripción generada automáticamente

***./buscar.sh Texto.txt la*** (Opción 2)



• Busque un archivo/parte de un archivo en una ruta dada y cuando lo encuentre,

busque una palabra/parte de una palabra. La salida será, por cada archivo

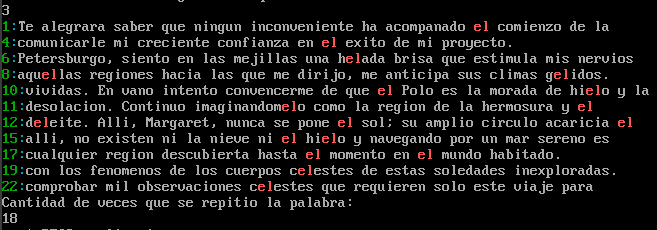
encontrado, la línea en donde se encontró la palabra y al final, la cantidad de

veces que se repitió.

Texto

Descripción generada automáticamente

***./buscar.sh /aplicaciones ext el*** (Opción 3)



• Usando un menú

Texto

Descripción generada automáticamente

Texto

Descripción generada automáticamente

• Cuente la cantidad de líneas de un archivo



***./buscar.sh Texto.txt*** (Opción 4)

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

• Cuente la cantidad de veces que se repite una palabra en el mismo archivo.



***./buscar.sh Texto.txt la*** (Opción 4)

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

**Revisión de log**

Escriba un programa Shell que:

• ¿Qué son los logs?

Son archivos de texto que se encargan de guardar cronológicamente los acontecimientos como cambios, actualizaciones y errores. Lo que ayuda a identificar los problemas que hay.

• ¿Qué tipo de logs encuentra en los sistemas operativos que instaló?

**Slackware:** faillog, lastlog, maillog, cron, debug, syslog, secure, btmp.

**NetBSD:** authlog, cron, lastlog, maillog, messages, rdist, secure, wtmp.

• ¿Qué es syslog? ¿En qué consiste este estándar?, ¿los logs que encontró en los

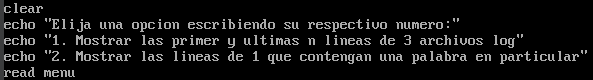
sistemas operativos siguen este estándar?

Syslog es un protocolo de registro basado en la red que utilizan los sistemas informáticos para enviar registros de datos de eventos como errores en contraseña, anomalías y errores de hardware o software a una ubicación central para su almacenamiento, estos se usan para monitorear y solucionar problemas. (sumo logic, s.f.)

Tiene la siguiente estructura: Encabezado (prioridad, versión, marca de tiempo, nombre de host, aplicación, id del proceso y del mensaje), seguido de datos estructurados (SD), seguido de un mensaje.

En los sistemas operáticos si siguen el protocolo syslog.

• Limpie la pantalla



• Despliegue un menú que permita hacer las siguientes actividades

• Muestre las primeras y últimas *n* líneas de 3 archivo de log que contiene los

datos de la actividad general del sistema. *n* es dado por el usuario.

Texto

Descripción generada automáticamente

***./log.sh 4*** (Opción 1)

Texto

Descripción generada automáticamente

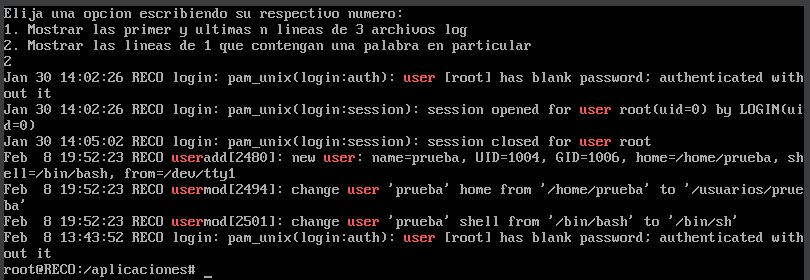
• Muestre, de esas *n* líneas de los mismo archivo, las que contengan una

palabra particular. *n* es dado por el usuario.

Texto

Descripción generada automáticamente

***./log.sh 4 user*** (Opción 2)



**Creación de usuarios**

Escriba un programa Shell que implemente el trabajo que hizo de creación de usuarios,

grupos y permisos del laboratorio anterior. Debe solicitar en la línea de comandos toda la

información requerida. Debe verse del estilo

# newgroup nombre\_grupo ID\_grupo



# newuser nombre grupo descripción directorio Shell permiso\_usuario(en

número) permiso\_grupo(en número) permiso\_otros(en número)

Texto

Descripción generada automáticamente con confianza baja

**NOTA**: Muestre a su profesor la ejecución de sus programas.

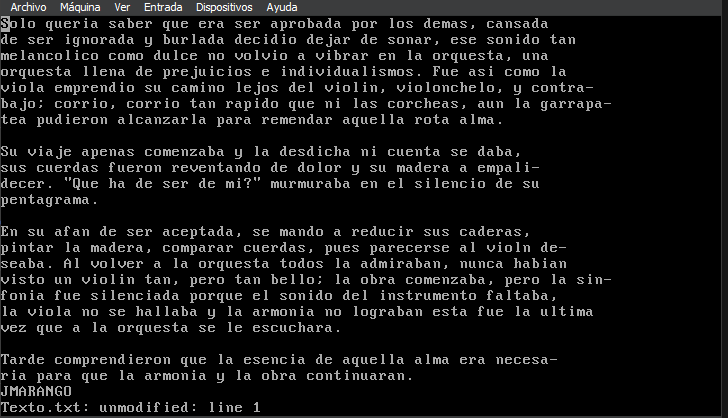
**2. Editor VI en Linux/Unix**

• Utilice el editor VI para crear un archivo. Indique los comandos utilizados.

***vi Texto.txt******→*** Crear un archivo.

• Escrita en un archivo de texto un reporte de lo que hicieron en vacaciones los

miembros del grupo. Debe tener al menos 3 párrafos y 200 palabras.



• Grabe el trabajo realizado sin salir del editor

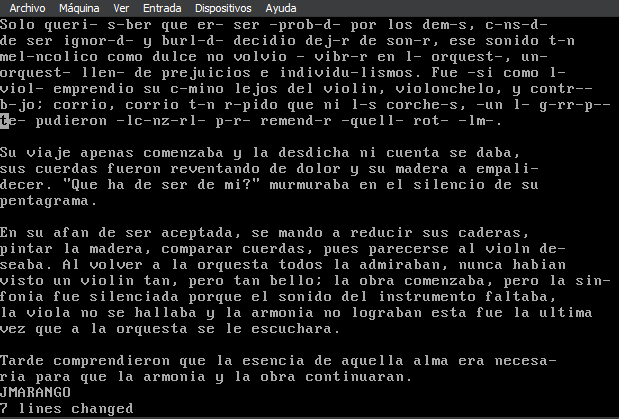
**:*w →*** Guardar el archivo.

Texto

Descripción generada automáticamente

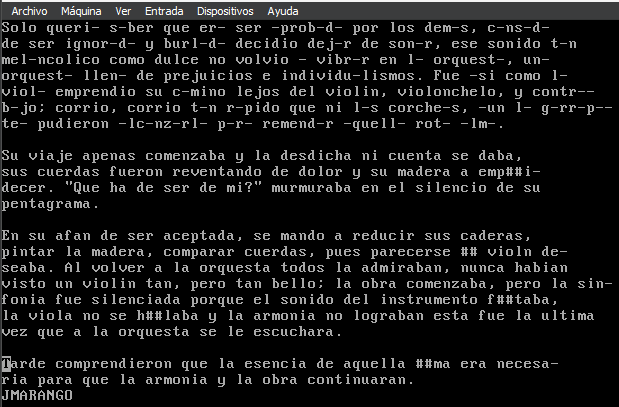
• Cambie las letras ‘a’ del primer párrafo por el símbolo –

**:1,7s/a/-/g *→*** Remplazar la letra a por un guion (-) desde la fila 1 hasta la 7.



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

**:%s/al/##/g *→*** Remplazar la cadena “al” por ## en todo el texto (%).



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

Texto

Descripción generada automáticamente

Se usa el comando ***dw →*** Elimina la palabra “continuaran”, se debe estar encima de la primera letra de la palabra que se quiere borrar.

Texto

Descripción generada automáticamente

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

Texto

Descripción generada automáticamente

***:-3,$d →*** Elimina la las ultimas 4 líneas del archivo.

Texto

Descripción generada automáticamente

• Deshaga el comando anterior.

Texto

Descripción generada automáticamente con confianza media

Se puede deshacer el comando anterior con ***:u*** o ***:undo***

Texto

Descripción generada automáticamente

• Pase a mayúscula la última línea del documento.

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente con confianza media

***:$s/.\*/\U&/ →*** Pasa todas las letras de la última fila a mayúsculas.

Texto

Descripción generada automáticamente

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

Texto

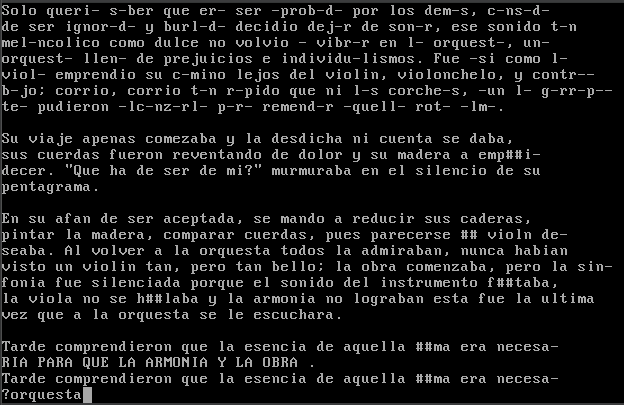
Descripción generada automáticamente

***:-1,$ co $ →*** Copia las dos últimas líneas al final del archivo.

Texto, Aplicación

Descripción generada automáticamente

• Busque la palabra editor dentro del texto



Para buscar se puede usar ***/<palabra>*** ***o ?<palabra>*** para ir a la siguiente coincidencia se oprime la tecla ***n***

Texto

Descripción generada automáticamente

Texto

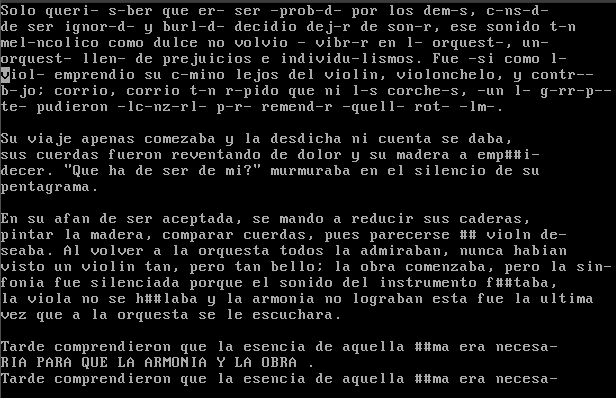
Descripción generada automáticamente

• Ubíquese en la línea 5 del texto usando un comando

Texto

Descripción generada automáticamente

***:5 →*** Va hacia la línea 5 del texo.



• Haga un cuadro resumen con comandos de VI

|  |  |
| --- | --- |
| **Comando** | **Función** |
| ***vi <nombreArchivo>*** | Abre o crea el archivo con el nombre dado |
| *:w* | Guarda el archivo |
| ***:<linea(s)>s/<cadena>/<nuevaCadena>/g*** | Remplaza una cadena por otra en la línea o líneas dadas.  ***<línea(s)>***  $ ***→*** Última línea-  % ***→*** Todas las líneas  . ***→*** Línea actual  n,m ***→*** Desde la línea n hasta la m |
| ***dw*** | Elimina la palabra / Elimina las letras de la palabra desde la letra en que se tiene el cursor. |
| ***:<línea(s)>d*** | Elimina la línea o líneas dadas. |
| ***:u***  ***:undo*** | Deshace la última acción. |
| ***: <línea(s)>s/.\*/\U&/*** | Pasa a mayúscula las letras de la línea o líneas dadas. |
| ***: <línea(s)>s/.\*/\L&/*** | Pasa a minúscula las letras de la línea o líneas dadas. |
| ***:<línea(s)> co <línea>*** | Copia una línea o varias líneas en una línea dada. |
| ***/<palabra>*** (Hacia adelante)  ***?<palabra>*** (Hacia atrás) | Busca una palabra, con la tecla ***n*** se dirige hacia la siguiente coincidencia. |
| ***:<línea>*** | Se ubica en la línea dada. |
| ***:wq*** | Guardar el archivo y salir del editor. |
| ***:q!*** | Sale del editor sin guardar los cambios. |
| ***:q*** | Sale del editor si no se han hecho cambios. |
| ***dd*** | Elimina la línea donde se encuentra el cursor. |
| ***h*** | Mueve el cursor hacia la izquierda. |
| ***j*** | Mueve el cursor hacia abajo. |
| ***k*** | Mueve el cursor hacia arriba. |
| ***l*** | Mueve el cursor hacia la derecha. |
| ***w*** | Mueve el cursor una palabra a la derecha. |
| ***W*** | Mueve el cursor una palabra a la derecha sin tener en cuenta los signos de puntuación. |
| ***b*** | Mueve el cursor una palabra a la izquierda. |
| ***B*** | Mueve el cursor una palabra a la izquierda sin tener en cuenta los signos de puntuación. |
| ***e*** | Mueve el cursor al final de la palabra actual. |

• Grabe el trabajo y salga del editor

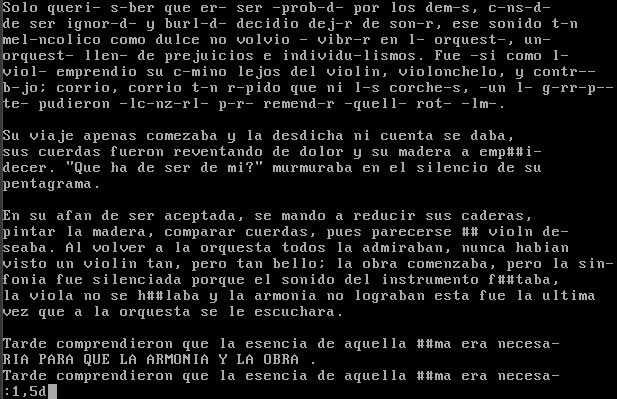
***:wq →*** Guarda el archivo y sale del editor.

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

• Vuelva a entrar y borre las primeras 5 líneas

***vi Texto.txt******→*** Entrar a un archivo si existe.



***:1,5d*** ***→*** Elimina las 5 primeras líneas del texto.

Texto

Descripción generada automáticamente

• Salga del archivo sin grabar

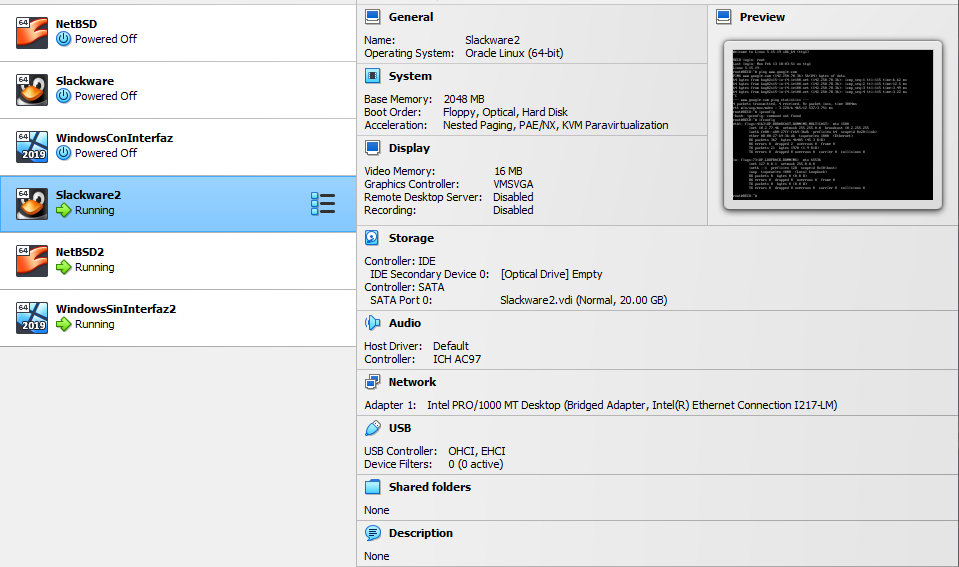
:***q! →*** Sale del archivo sin guardar los cambios.

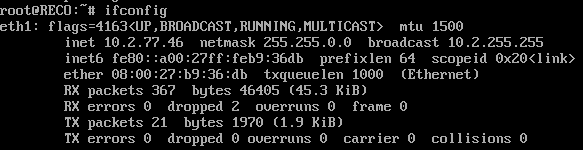
**3. Generación de máquinas**

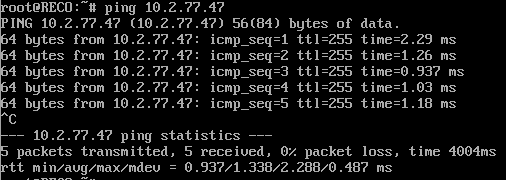
Para el trabajo del semestre se necesitarán 2 máquinas virtuales de cada sistema operativo instalado excepto Windows Server sin GUI y Android. Genere las nuevas máquinas y pruebe que puedan verse entre ellas y hacia internet.

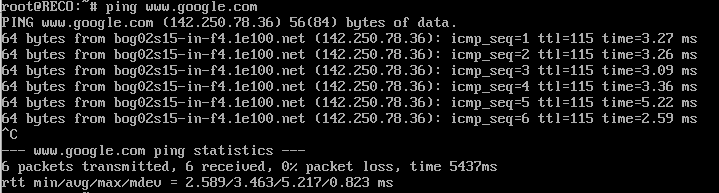
Se realiza el mismo procedimiento realizado en el laboratorio 1 para instalación de máquinas se asignarán las siguientes ip:

* + Slackware2: 10.2.77.46

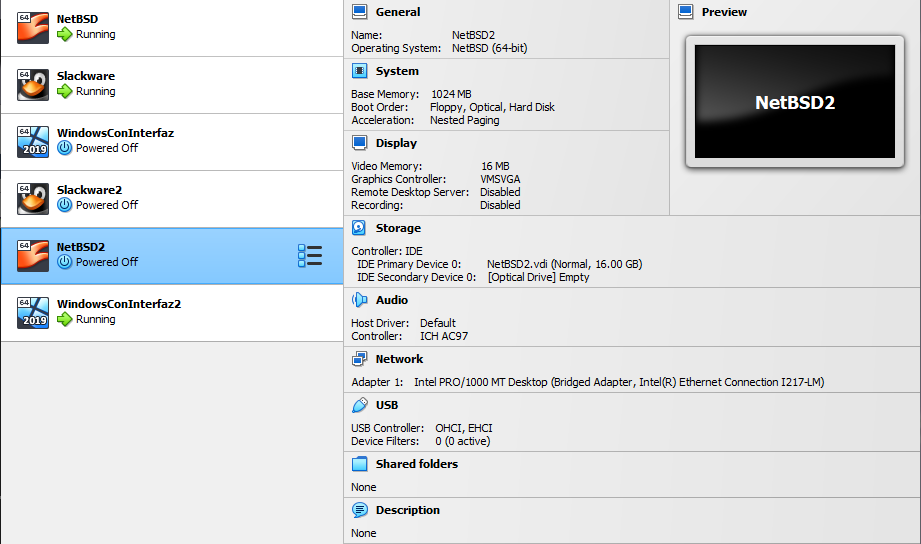




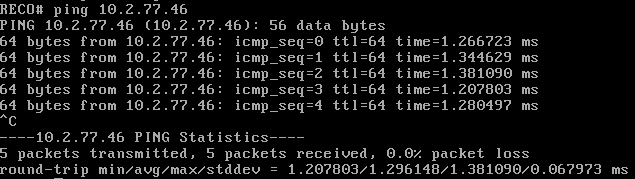


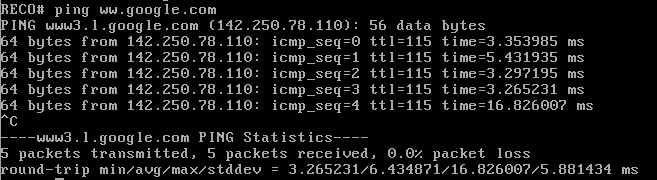


* + NetBSD2: 10.2.77.47

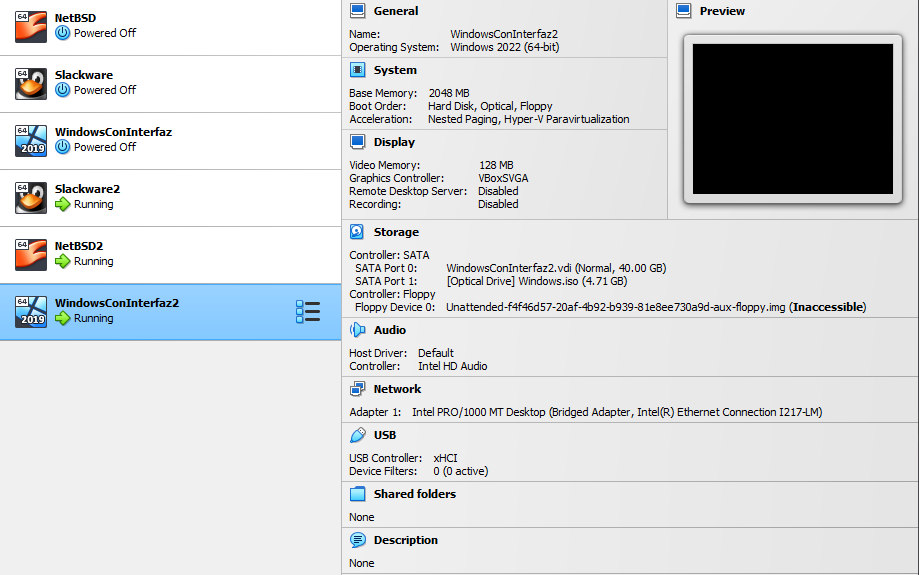


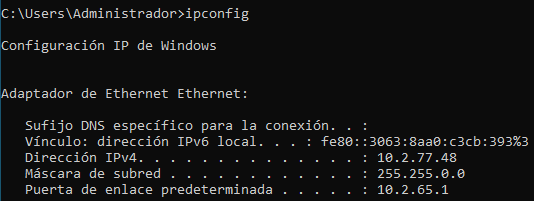


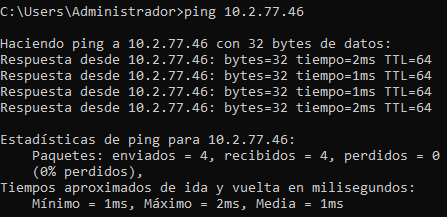


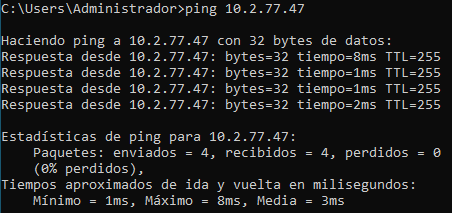


* + WindowsSinInterfaz2: 10.2.77.48







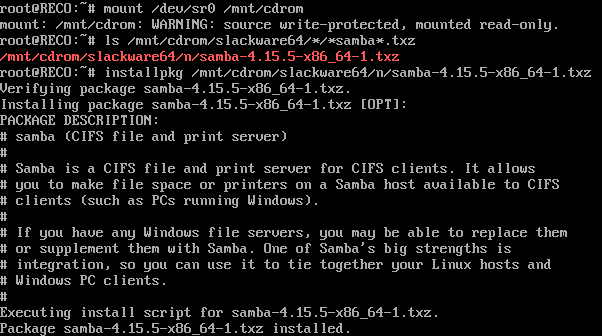


**4. Compartir archivos**

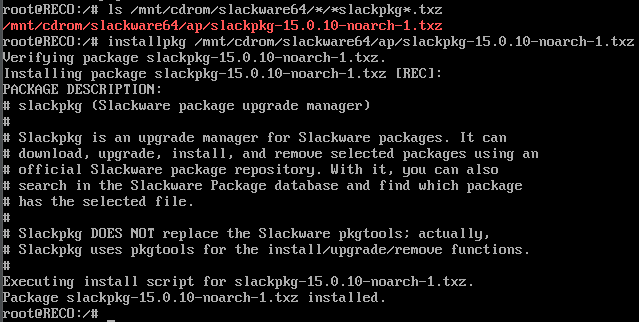
Uno de los servicios claves en un ambiente empresarial son los file system compartidos, en donde las personas de la empresa pueden guardar archivos y compartirlos con un grupo de trabajo. La tarea en esta ocasión consiste en configurar un servidor de archivos en Linux Slackware usando SMB/SAMBA, de tal manera que se permita compartir archivos entre los tres sistemas operativos (Linux Slackware, NetBSD y Windows. Adicionalmente, Centos --> En los grupos de 3).

Slackware

Montamos el disco y buscamos donde se encuentra *samba* para instalarlo.



Miramos donde está el paquete *slackpkg* para instalarlo.

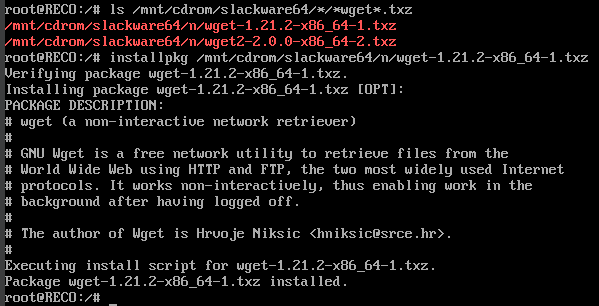


Instalamos el paquete *gnupg*.

Texto

Descripción generada automáticamente

Instalamos el paquete wget.



Abrimos con un editor *vi* el archivo */etc/slackpkg/mirrors* y desconectamos el mirror que se muestra a continuación, después lo instalamos con *slackpkg update*

Texto

Descripción generada automáticamente

Se crea la carpeta que se va a compartir, se copian los shells hechos y se cambia sus permisos.

Texto

Descripción generada automáticamente

Entramos a la carpeta samba y copiamos el archivo *smb.conf-sample a smb.conf* y o editamos con *vi.*



Vamos hacia el final del archivo y escribimos lo siguiente y guardamos el archivo:

Texto

Descripción generada automáticamente

Ahora se creará el usuario y se habilitará en smb, al hacer esto nos pedirá unos paquetes que tendremos que instalar que son:

* talloc
* gnutls
* icu4c
* tevent
* libunwind
* p11-kit
* nettle
* cyrus-sasl
* jansson

Texto

Descripción generada automáticamente

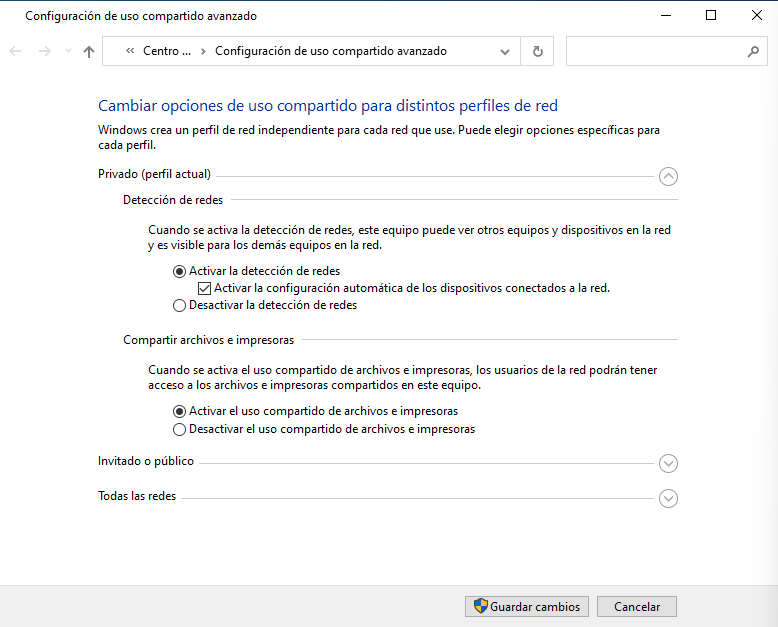
Se inicia el samba con el comando */etc/rc.d/rc.samba start*

Texto

Descripción generada automáticamente con confianza media

Windows

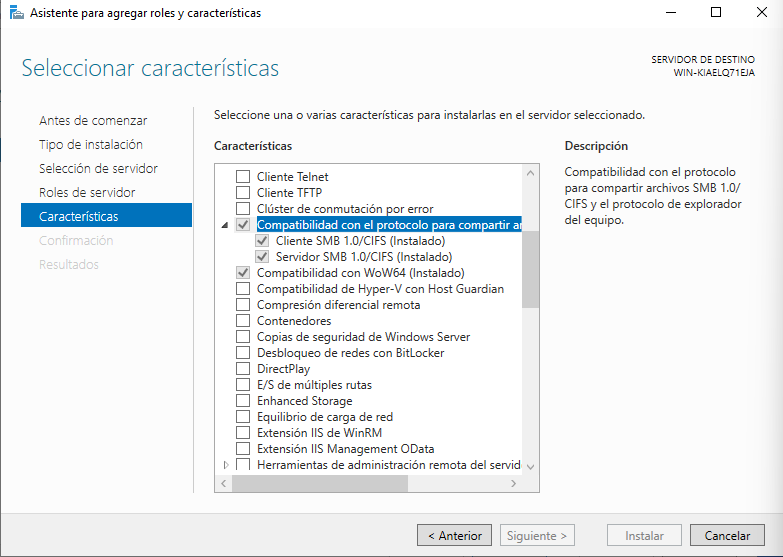
Se activa la dirección de redes y el uso compartido de archivos e impresoras en Privado, invitado y en todas las redes.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente Texto

Descripción generada automáticamente

En la seción de programas de panel de control vamos a *Activar o desactivar las características de Windows,* se activa el protocolo para compartir archivos SMB y se instala.



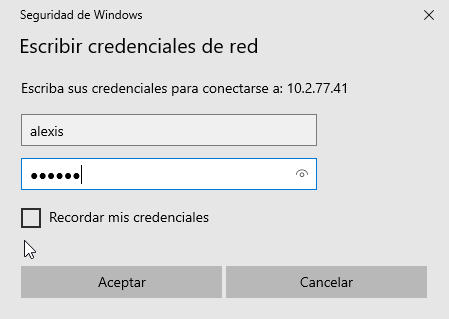
En *Windows Defender Firewall con seguridad avanzada* y se activan las reglas de entrada que comiencen con *Compartir.*

Interfaz de usuario gráfica, Texto

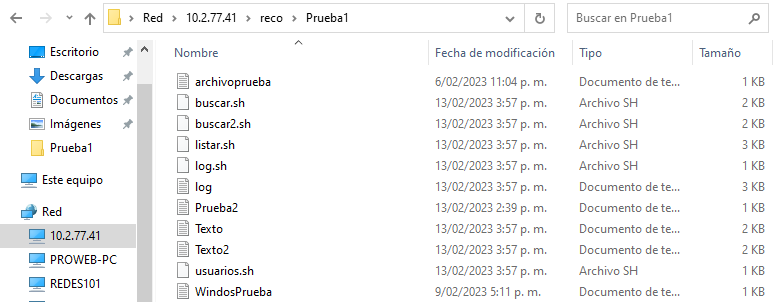
Descripción generada automáticamente

En red se escribe la dirección [\\10.2.77.41\RECO\Prueba1,](file:///\\10.2.77.41\RECO\Prueba1) se ingresa el nombre y la contraseña del usuario habilitado.



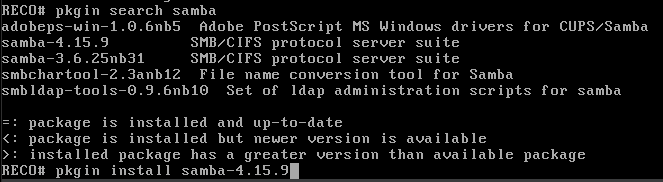


Se confirma que este el archivos que tenía la carpeta compartida esten*.*

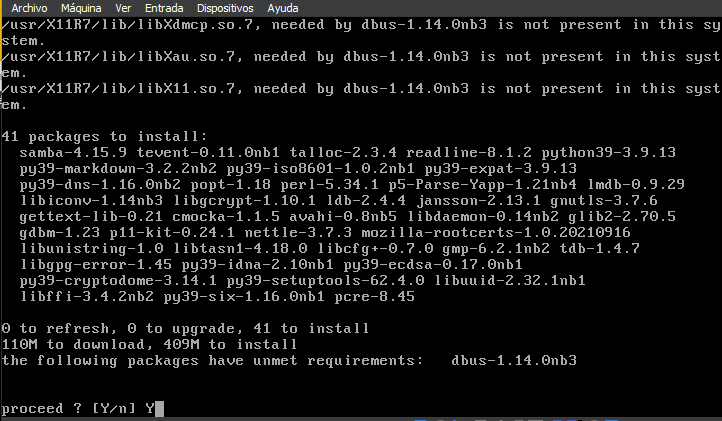


NetBSD

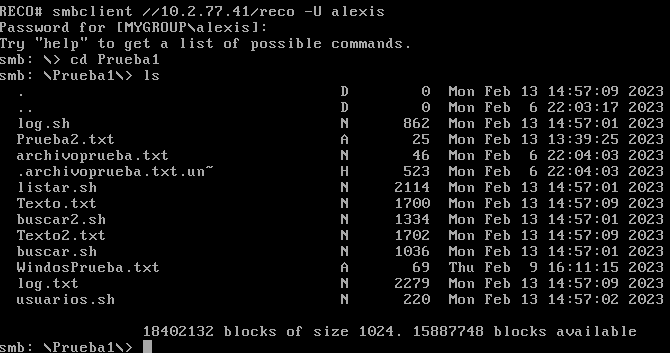
Se busca con el comando *pkgin search samba* cuál versión de samba está disponible para instalarla con *pkgin install samba-4.15.9*



Al hacer esto nos pedirá que instalemos unos paquetes le daremos que sí.



Para entrar al samba se usa el comando *smblient //10.2.77.41/RECO -U alexis*, al estar dentro nos dirigimos a la carpeta *Prueba1* y confirmamos el archivo prueba que habíamos creado esté (*slackware.txt)*.



**Conclusiones**

Ahora sabemos a más profundidad el modo en el cual operan las herramientas de red como Paket Tracer y Wireshark, con los que diseñar y visualizamos diferentes redes y mirar sus protocolos, con Packet Tracer pruebas de conexión y funcionamiento de la red, Wireshark entender información de nuestra red, consultar información de la tarjeta de red de nuestros dispositivos, escribimos distintos shells scripts y realizamos distintas operaciones para optimizar tareas.

Luego de realizar el proceso de instalación y configuración de samba, al compartir archivos, podemos inferir que samba proporciona los recursos para que las máquinas de Unix y Windows puedan coexistir en una misma red.

# **Referencias**

*A Sanchez Corbalán*. (11 de Diciembre de 2021). Obtenido de https://sanchezcorbalan.es/que-es-un-shell-script/#:~:text=Un%20Shell%20Script%20es%20un,que%20cada%20instrucci%C3%B3n%20le%20indica

*CCNA*. (s.f.). Obtenido de https://ccnadesdecero.es/cable-directo-cruzado-y-consola-diferencias/

*Francisconi*. (26 de Abril de 2014). Obtenido de https://francisconi.org/linux/expresiones-regulares#:~:text=Una%20expresi%C3%B3n%20regular%20en%20Linux,caracteres%20

*IBM*. (12 de Abril de 2021). Obtenido de https://www.ibm.com/docs/es/aix/7.2?topic=administration-operating-system-shells

*Kripton*. (s.f.). Obtenido de https://kryptonsolid.com/que-es-el-modo-promiscuo/#:~:text=En%20modo%20promiscuo%2C%20un%20dispositivo,como%20a%20una%20NIC%20inal%C3%A1mbrica.

*sumo logic*. (s.f.). Obtenido de https://www.sumologic.com/syslog/

*welivesecurity*. (28 de Enero de 2013). Obtenido de https://www.welivesecurity.com/la-es/2013/01/28/uso-filtros-wireshark-para-detectar-actividad-maliciosa/