

UNIDAD DE REDES 11.COMPUTER (II)

Los sistemas informáticos
CFGS DAW

Alfredo Oltra / Sergio García

[alfredo.oltra @ ceedcv.e s](mailto:alfredo.oltra@ceedcv.es)

2019/2020

Versión: 190927.1232

Licencia



Reconocimiento - NoComercial - CompartirIgual (by-nc-sa): No permite en sí ONU USO comercial de la obra original, ni de las obras Posibles

Derivadas, La Distribución de las Cuales se Dêbe Hacer con licencia Una Igual a La que regula la Obra originales.

nomenclatura

A lo largo de Este tema se utilizarán Distintos Símbolos para distinguir Elementos Importantes Dentro del contenido. Símbolos Estós hijo:

- Importante

- Atención

- interesante

ÍNDICE

1. Conexión a una red de ordenadores	4
1.1 La asignación dinámica	4
1.1.1 sistemas Linux	4
1.1.2 sistemas Windows	7
1.2 Asignación estática	8
1.2.1 sistemas Linux	8
1.2.2 sistemas Windows	9
2. Localización de recursos en la red	10
2.1 Asignación de su nombre de equipo	10
2.2 Relacionar nombres e IP localmente	10
2.3 DNS	10
3. Seguridad	12
3.1 Firewall	12
3.1.1 sistemas Linux	12
3.1.2 sistemas Windows	14
4. El acceso remoto	15
4.1 ssh	15
4.2 TeamViewer	dieciséis
5. Los recursos compartidos	dieciséis
5.1 SAMBA	dieciséis
6. El material adicional	17
7. Bibliografía	17

UD11. Redes de ordenadores (II)

1. CONEXIÓN equipos a una red

El primer paso para poder utilizar los dispositivos en una red es para conectarlos a la misma, y para ello es necesario conocer las interfaces disponibles (NIC) y asignarles una dirección IP. Hay dos maneras de IPs ceder, ya sea dinámica o estática:

- **Dinámica:** un dispositivo de red (un servidor DHCP) administra la distribución IP, cuando el dispositivo está conectado a esa red, solicita una dirección IP al servidor DHCP que asigna basa en ciertas reglas. De este modo, la incorporación de nuevos dispositivos es más rápida y los posibles conflictos se evitan mediante la asignación de direcciones IP son iguales a los diferentes nodos de la red). Sin embargo, es posible que entre las diferentes conexiones a la red, la dirección IP asignada es diferente
- **Estática:** La IP de cada dispositivo debe asignarse manualmente. Esto complica la adición de nuevos dispositivos y aumenta la probabilidad de conflictos, pero permite que la IP de un ordenador se fija en el tiempo.

1.1 La asignación dinámica

Debido a su simplicidad, es del tipo común la mayor parte de la asignación dentro de una red. Se utiliza cuando nos conectamos con nuestro móvil a una red inalámbrica (Wi-Fi o 4G) o con nuestro escritorio en nuestra red doméstica. En general, el router es el servidor DHCP.

- que es el que está configurado por defecto en la mayoría de los sistemas operativos que funcionan como estaciones de trabajo, por lo que el usuario sólo tiene que conectar el equipo a la red física.

1.1.1 sistemas Linux

El primer paso es saber cuántos y cuáles están disponibles en nuestro ordenador interfaces. Para ello, desde el terminal, se utiliza el ***ifconfig*** mando.

- Uno de los comandos más importantes de Linux (en lo que se refiere a la creación de redes) es, sin duda ***ifconfig***. Con ello, es posible configurar y modificar la configuración de las interfaces de red.

```

> ifconfig -a
lo0: flags = 8049 <UP, LOOPBACK, CONDUCCION, Multicast> MTU 16384
    Opciones = 1203 <RXCSUM, TXCSUM, TXSTATUS, SW_TIMESTAMP> inet 127.0.0.1
    máscara de red 0xFF000000 inet6 :: 1 128 prefixlen

    inet6 fe80 :: 1% lo0 prefixlen 64 ScopeId opciones 0x1 ND6 = 201
    <PERFORMNUD, DAD>
en0: flags = 8863 <UP, BROADCAST, inteligente que funciona, SIMPLEX, Multicast> MTU 1500
    options = 10b <RXCSUM, TXCSUM, VLAN_HWTAGGING, AV> éter 10: 9a: dd:
    71: opciones ND6 c6 = 201 <PERFORMNUD, DAD> medios de comunicación::
    1d autoselect (ninguno) Estado: inactiva

en1: flags = 963 <UP, BROADCAST, inteligente que funciona, promisc, SIMPLEX> MTU 1500
    options = 60 <TSO4, TSO6> éter d2: 00: 1c: 56: cf:
    medios c0: autoselect <full-duplex> Estado: inactiva

fw0: flags = 8863 <UP, BROADCAST, inteligente que funciona, SIMPLEX, Multicast> MTU 4078
    lladdr 70: cd: 60: ss: Fe: C5: 6c: fc = 201 ND6 opciones
    <PERFORMNUD, DAD> medios: selección automática
    <full-duplex> Estado: inactiva

```

Con el - **un** opción, se nos muestra información sobre todas las interfaces que existen en nuestro sistema. Cada uno de ellos se llama con dos o tres letras, seguido de un número (similar a la nomenclatura de disco duro). En el caso mostrado en la figura hay 4 interfaces, 3 de ellos física (es decir, que se refieren a elementos de hardware), y 1 lógico **lo0**, que se refiere a la **bucle de retorno**, al bucle interno (otros pueden aparecer, tal como **vbox**, que se refiere a las interfaces creadas por **caja virtual**).

Una vez que sabemos el nombre de la interfaz a la que queremos asociar una dirección IP dinámica (en nuestro caso elegiremos en1), hay que modificar el archivo

/etc/network/interfaces

```
> sudo nano /etc/network/interfaces
```

Y añadir (o modificar si ya existía) una línea que configura la interfaz. En nuestro caso vamos a modificar el en1 interfaz, por lo que habría que añadir

```
iface en1 inet dhcp
```

El último paso es reiniciar la interfaz. Podemos hacerlo de dos maneras: desactivación y activación de las interfaces directamente con la **ifconfig** mando:

1 en0, en1 referencia a la interfaz de ethernet y fw0 refiriéndose interfaz fuego hilos

- > sudo ifconfig en1 abajo
- > sudo ifconfig en1 hasta

O al detener y arrancar el sistema de red con el guión de arranque del sistema de red ².

- > sudo /etc/init.d/networking parada
- > sudo /etc/init.d/networking inicio

- Hay una manera más sencilla de reiniciar la secuencia de comandos utilizando el parámetro de reinicio, pero en algunos casos puede fallar, por lo que la opción más segura es llevar a cabo el proceso separado

- scripts de arranque son scripts que se ejecutan en el inicio del sistema operativo. Su objetivo es comenzar en unos programas y demonios de forma controlada ³ que realizan tareas en el sistema (por ejemplo un servidor de base de datos o el control de la red).

En los sistemas con interfaz gráfica de usuario, es posible llevar a cabo estas acciones de forma gráfica. La forma exacta depende del sistema en sí, pero en general la idea es la misma. Para ver un ejemplo, en Ubuntu.

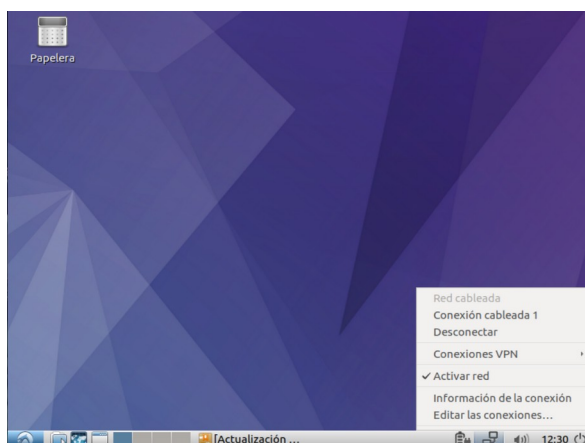


Figura 1. GUI DHCP paso config 1

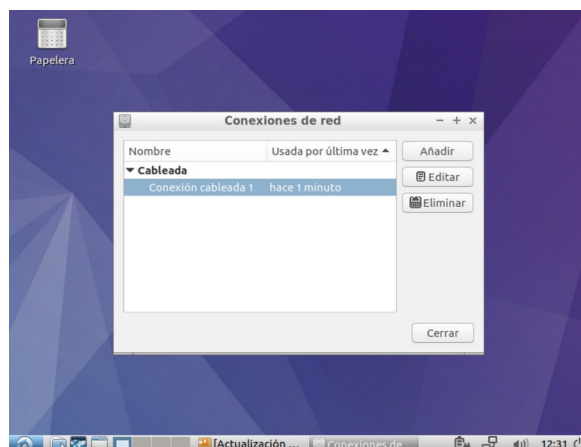


Figura 2. GUI DHCP paso config 2

² Un script es un programa escrito usando el sistema de mando, que por lo general tiene como objetivo automatizar tareas ³ En Linux, un demonio es un servicio, es decir, un programa que se ejecuta en segundo plano, de manera transparente para el usuario. Por ejemplo un antivirus

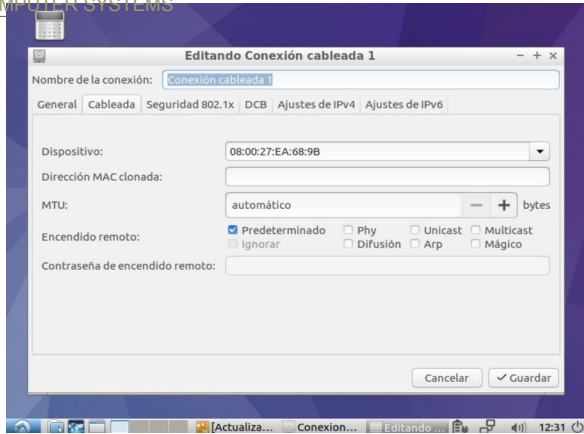


Figura 3. GUI DHCP paso config 3

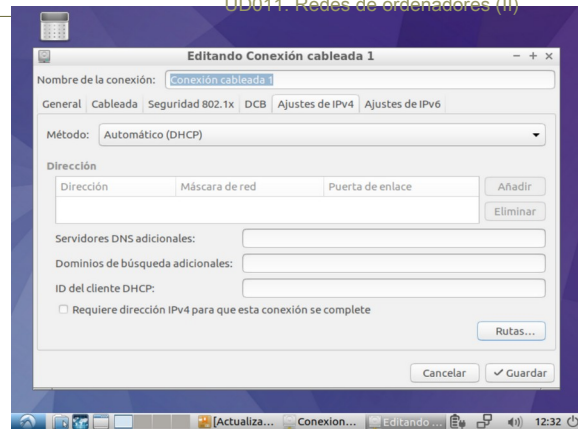


Figura 4. GUI DHCP paso config 4

- Como se puede ver, la dirección del servidor DHCP se indica en ninguna parte. ¿Cómo sabe el equipo que solicite IP? El proceso funciona con una serie de señales de radiodifusión llamada **Descubrir DHCP, DHCP Offer, DHCP requests, acuse de recibo de DHCP**, que se llevan a cabo utilizando la dirección 0.0.0.0 cliente y como un destino 255.255.255.255 (broadcast).

1.1.2 sistemas Windows

Si usted quiere saber cuántos y cuáles son las interfaces están disponibles en nuestro ordenador en un sistema Windows, puede utilizar el comando **ipconfig**.

- > ipconfig
- > ipconfig / all

Puede configurar una dirección IP dinámica en los sistemas Windows siguientes esos pasos:

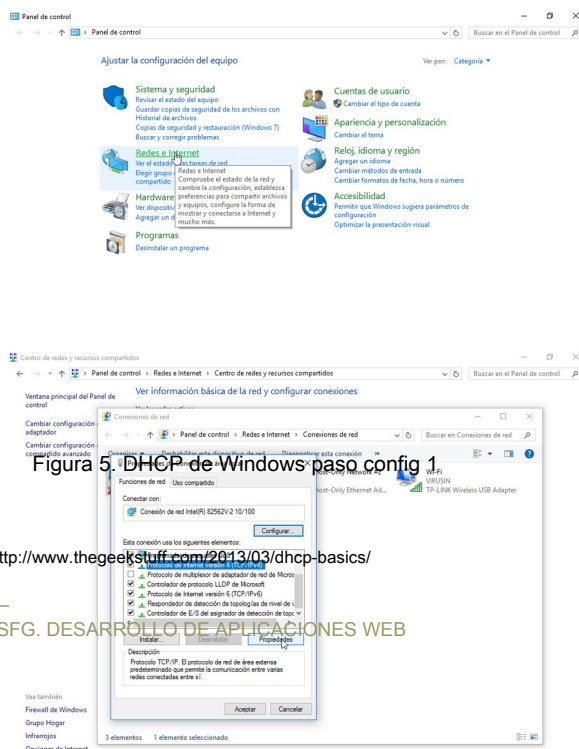


Figura 5. DHCP de Windows paso config 1

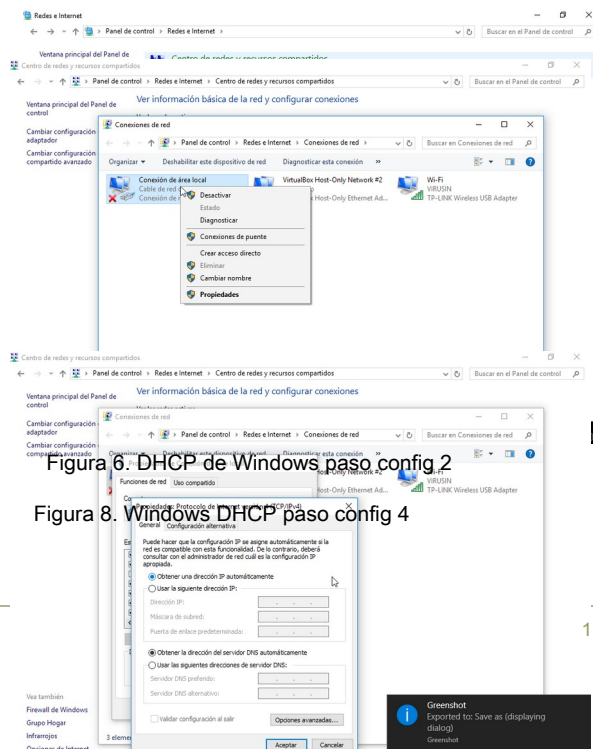


Figura 6. DHCP de Windows paso config 2

Figura 8. Windows DHCP paso config 4

4 <http://www.thegeekstuff.com/2013/03/dhcp-basics/>

Figura 9. DHCP de Windows paso config 5

Figura 10. DHCP de Windows paso config 6

1.2 Asignación estática

La configuración de la dirección IP estática no es muy complejo, pero sí requiere el conocimiento de la topología de la red. Al igual que en la configuración dinámica DHCP maneja todo el trabajo, en este caso es el usuario quien tiene que configurar todos los datos de forma manual.

Los datos que necesitamos son los IP que será asignada (teniendo en cuenta que aún no se ha utilizado por cualquier otro equipo), la máscara de red y la dirección de la puerta de enlace, es decir, el router que es la salida al exterior a esa red.

1.2.1 sistemas Linux

De una manera similar a la asignación dinámica, modificamos el archivo **/etc/network/interfaces** pero en este caso la adición a la información necesaria para la operación estática:

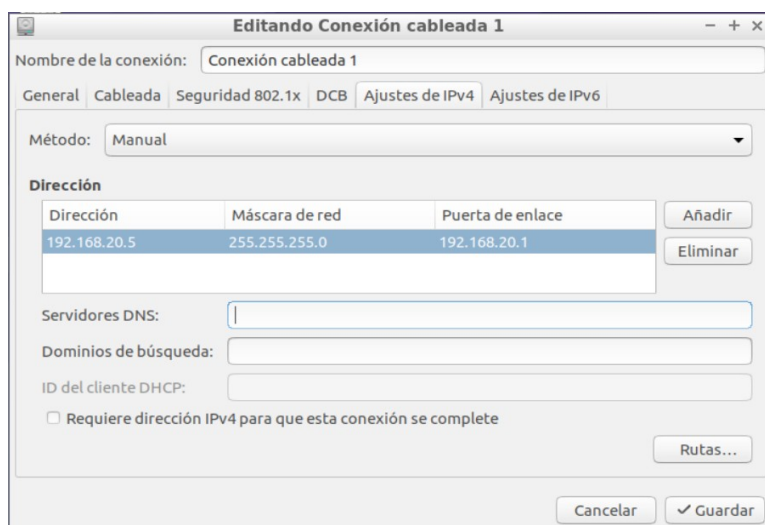
iface de en1 inet estática dirección

192.168.20.5 máscara de red

255.255.255.0 puerta de enlace

192.168.20.1

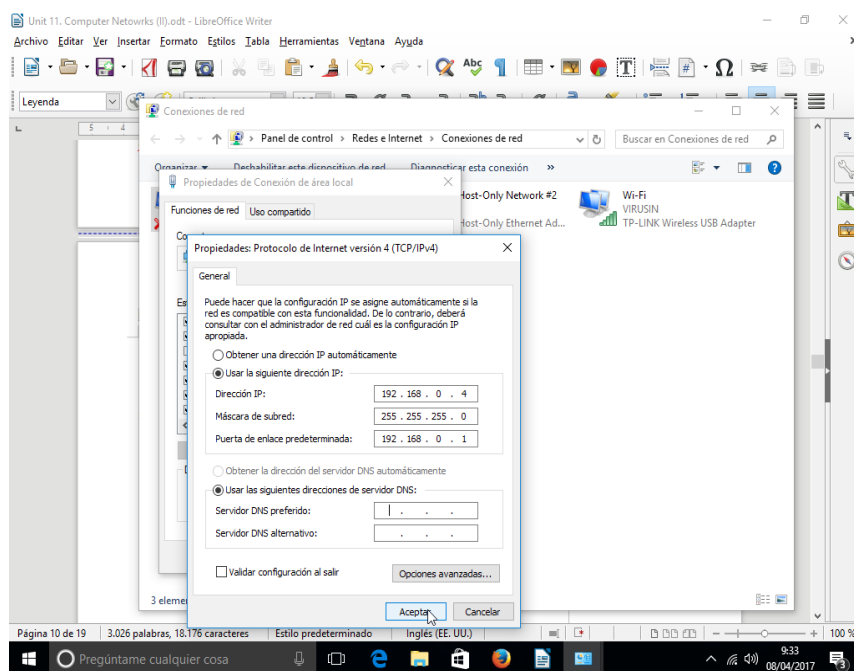
De manera gráfica, tenemos que seleccionar la opción manual y configurar los datos.



config Figura 11. GUI estática IP

1.2.2 sistemas Windows

En los sistemas Windows, para configurar la dirección IP estática que tiene que ir al mismo lugar que usted fue a configurar IP dinámica. En ese lugar, en vez de elegir **Obtener IP automáticamente**, usted debe introducir manualmente IP, máscara de red y puerta de enlace.



config Figura 12. IP estática de Windows

2. LOCALIZACIÓN recursos de la red

Cada dispositivo conectado a una red IP tiene una dirección IP, pero recordando que conjunto de números para ser capaces de comunicarse entre dispositivos es algo que es muy complicado. La resolución de nombres es el proceso de asignar direcciones IP a nombres de host, por lo que es más fácil identificar los recursos en una red. Por ejemplo, es más fácil de recordar www.google.com que 216.58.211.238.

2.1 Asignación de su nombre de equipo

Con el fin de acceder a los dispositivos por su nombre debe asignarse uno. A partir de los sistemas Linux, tenemos que cambiar el archivo `/etc/hostname`.

```
> sudo nano /etc/hostname
```

En los sistemas Windows 10, abierto *ajustes* E ir a **Sistema> Acerca de**

- Se puede utilizar letras, números y guiones, pero no espacios.

2.2 Relacionar nombres e IP local

La forma más fácil de relacionar nombres con IP es el uso de la **Hospedadores** archivo. Este archivo contiene líneas de texto que están hechos de direcciones IP seguido de uno o más nombres de host. Cada campo está separado por espacios en blanco (espacios en blanco o caracteres de tabulación).

192.168.20.6 mortadelo por ordenador

192.168.20.7 Filemon por ordenador

192.168.20.8 Zipi-ordenador

192.168.20.9 zape por ordenador

192.168.20.10 Carpanta por ordenador

Este archivo se encuentra en `/etc/hosts` en sistemas Linux o en `[X]:\Windows\System32\drivers\etc` (donde [X] es el hasta donde el sistema de ventanas se instala, por lo general C).

- En los sistemas Windows la **Hospedadores** archivo no puede ser modificado directamente por razones de seguridad. Para modificar, es necesario hacer una copia en otra carpeta, modificarlo y, a continuación, vuelva a colocar el original con el modificado usando los permisos de administrador

2.3 DNS

El archivo hosts puede resolver el problema de la localización de nombres dentro de un ambiente pequeño y controlado, como una red local, pero cuando tenemos que resolver los nombres de los servidores de Internet, esta solución no es viable.

Para ello, existen los - llamados servidores DNS, que proporcionan un nombre - relación IP. Es evidente que un único servidor no puede resolver todos los nombres de los

toda Internet, por lo que si un servidor no puede resolver, se remitirá la petición a otro.

En general, estos servidores son asignados por el ISP, pero hay otros públicos como Google (8.8.8.8 y 8.8.4.4)

En los sistemas Linux estos servidores se indican mediante el archivo **/etc/resolv.conf**

127.0.0.1 servidor de nombres del servidor de
nombres 172.16.1.254

Tenga cuidado con las modificaciones realizadas en este archivo. En general, el servidor DHCP asignará en sí no sólo la IP, sino también los servidores DNS. Estas modificaciones pueden anular los realizados manualmente. Para mantener estos datos, podemos editar el **/etc/network/interfaces** con la información que queremos añadir a la **resolv.conf** archivo.

íface de en1 inet estática dirección

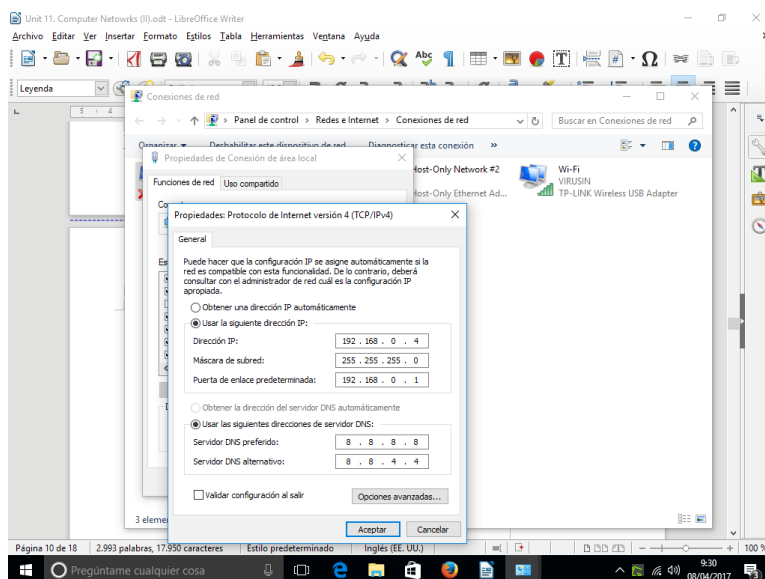
192.168.20.5 máscara de red

255.255.255.0 puerta de enlace

192.168.20.1

servidores de nombres DNS-172.16.1.254,8.8.8.8

En los sistemas Windows, puede configurar el DNS utilizando su interfaz gráfica de usuario:



config Figura 13. DNS de Windows

- En el ejemplo de Windows que estamos utilizando Google DNS público que son 8.8.8.8 y 8.8.4.4. Son fáciles de recordar. Puede encontrar más información en la Wikipedia [Google Public DNS](#).

3. SEGURIDAD

3.1 Firewall

Un firewall es un sistema (que puede ser implementado utilizando software o hardware) que supervisa y controla el tráfico de red entrante y saliente. Ha configurado una serie de reglas de confianza y no de confianza que se aplican a cada paquete de una manera que lo deja pasar, dependiendo de si es o no cumplir cualquiera de esas reglas.

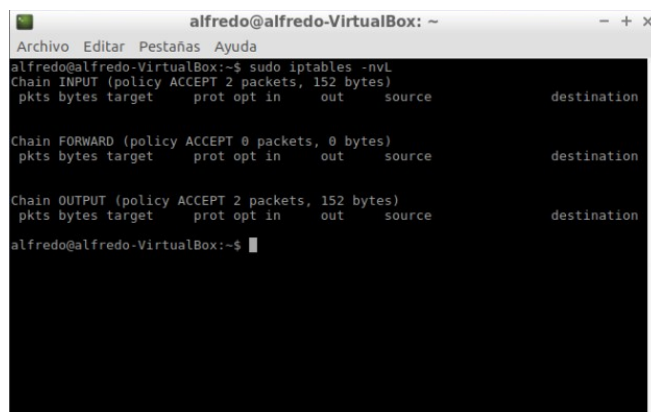
3.1.1 sistemas Linux

Linux incluye un firewall integrado nativo en el interior del núcleo. Dicho servidor de seguridad está controlada por el **iptables** mando. Las tablas IP son un conjunto de tablas que indican al kernel cómo procesar los paquetes entrantes. Cada tabla tiene una función distinta. Por ejemplo, la tabla de filtros (la tabla por defecto) proporciona comandos para filtrar y aceptar o paquetes de caída y esta se comportan manera que un servidor de seguridad. La tabla NAT proporciona comandos para traducir (modificar) direcciones IP de origen o destino, y la tabla mangle proporciona comandos para modificar las cabeceras de los paquetes. Cada tabla contiene **cadenas** que son conjuntos de reglas o políticas de paquetes. La tabla representa qué hacer con los paquetes y la cadena representa en qué etapa de la pila TCP / IP de la operación debe ser realizada. Por ejemplo, la tabla de filtros contiene funciones integradas en las cadenas de llamadas INPUT, FORWARD y OUTPUT, y apoyar las políticas de ACCEPT, DROP y REJECT (y otros). Una regla para paquetes DROP configurado por debajo de la cadena INPUT dirigirá el kernel para descartar los paquetes que se reciben en una interfaz determinada.

- En nuestro caso, sólo funcionará con la tabla de filtros, que es la opción por defecto **iptables** mesa. Para elegir la mesa de trabajo con, debe utilizar el **-t** opción

Para una lista de la tabla de filtros:

`iptables -nvL`



```
alfredo@alfredo-VirtualBox: ~
Archivo  Editor  Pestañas  Ayuda
alfredo@alfredo-VirtualBox:~$ sudo iptables -nvL
Chain INPUT (policy ACCEPT 2 packets, 152 bytes)
 pkts bytes target     prot opt in     out     source            destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source            destination

Chain OUTPUT (policy ACCEPT 2 packets, 152 bytes)
 pkts bytes target     prot opt in     out     source            destination
alfredo@alfredo-VirtualBox:~$
```

Figura 14. iptables -nvL

- Por defecto, no hay reglas se definen y la política predeterminada para cada cadena es aceptar, por lo que la **iptables** permiten todos los paquetes pasen a través del kernel

Una forma más segura de trabajo es cambiar el modo por defecto de ACCEPT a la baja, al menos cuando se trata de los paquetes entrantes. Para hacerlo:

```
sudo iptables -P GOTA DE ENTRADA
```

este cambio de mando de la política por defecto ENTRADA (-P) a caer. De esta manera, cuando la lista de la tabla de nuevo:

A partir de este momento en nuestro ordenador rechazará todos los paquetes entrantes. Esta solución puede ser drástica ya que la comunicación con el exterior puede ser imposible si no se permite la entrada de cualquier paquete. Lo interesante es añadir reglas que se están abriendo elementos de acuerdo a nuestras necesidades. Esta apertura se puede hacer de varias maneras:

- abierto una interfaz

```
iptables -A entrada LO -i -j ACCEPT
```

append (A) una regla a la cadena INPUT. La política es aceptar y la regla se aplica a la loopback (lo) de interfaz (-i).

- por protocolo

```
iptables -A ENTRADA -i eth1 -p udp --sport 68 --dport 67 -j ACCEPT
```

append (A) una regla a la cadena INPUT. La política es aceptar y la regla se aplica a la ethernet1 (eth1) interfaz (-i) para el protocolo (-p) udp. Además, el cliente envía el paquete de de port (-deporte) 68 y el servidor es escuchar para el puerto (-dport) 68

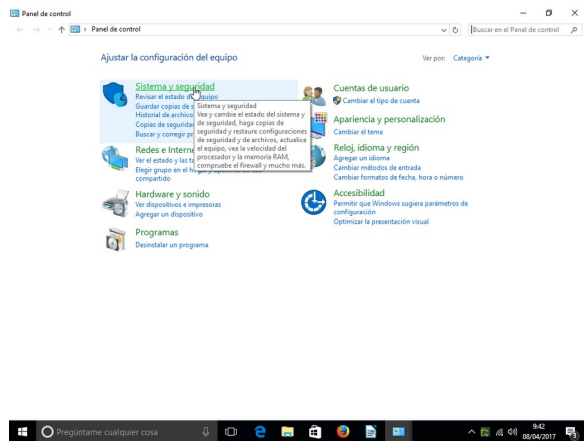
- por estado

```
iptables -A ENTRADA -i eth0 -m --state estado ESTABLISHED, RELATED -j ACCEPT
```

iptables puede controlar el estado de la conexión, es decir, se pueden agrupar los paquetes en las conexiones de acuerdo con sus direcciones IP y puertos de origen / destino y entender si la conexión está siendo iniciado por el equipo local o un equipo remoto. En el ejemplo añadimos (A) una regla a la cadena INPUT. La política es aceptar y la regla se aplica a la ethernet1 (eth1) interfaz (-i) si el estado (-m) se establece (c onexiones que hemos originado) o relacionados (creado por las conexiones establecidas existentes)

3.1.2 sistemas Windows

cortafuegos por defecto en los sistemas Windows es muy limitada en comparación con iptables en Linux, pero para configuraciones sencillas que podría ser útil. Se puede configurar utilizando la interfaz gráfica de usuario de Windows



paso Figura 15. Firewall Windows 1

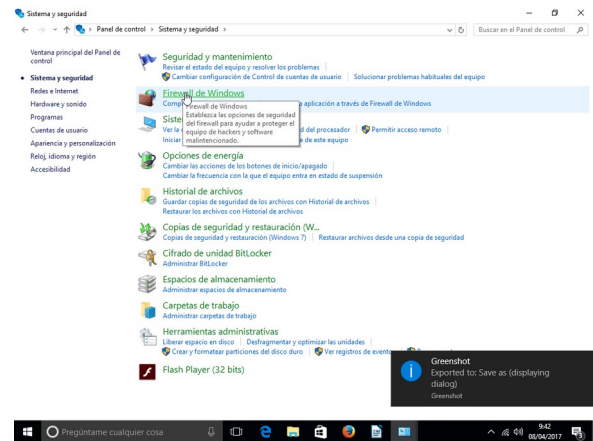


Figura 16. Firewall Windows Paso 2

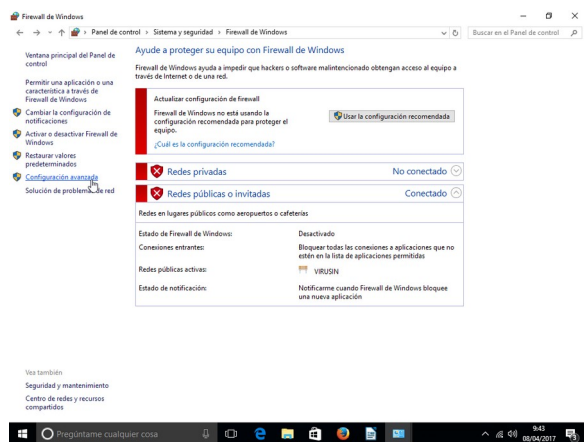
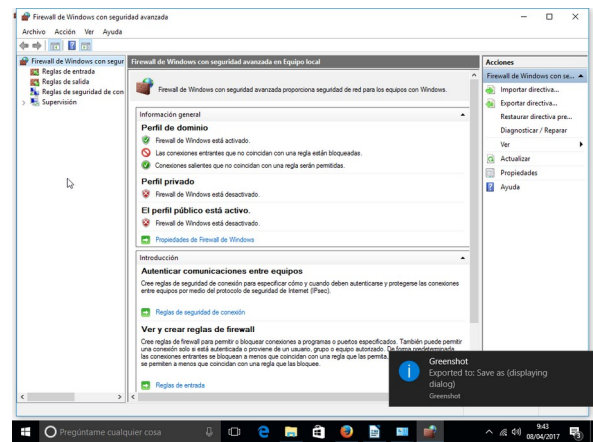


Figura 17. Firewall Windows Paso 3



paso Figura 18. Firewall Windows 4

4. ACCESO REMOTO

A nivel administrativo, una de las primeras ventajas de las redes es la posibilidad de gestionar un equipo de forma remota. Hay muchas opciones, pero nos centraremos en dos de los más utilizados.

- Una dirección IP podría tener una gran cantidad de servicios. Para distinguir qué servicio nos estamos conectando, cada servicio tiene un puerto diferente. La mayoría de los puertos comunes son 80 para servidores web, 22 para ssh, 25 para SMTP, ... Más información

[https://en.wikipedia.org/wiki/Port_\(computer_networking\)](https://en.wikipedia.org/wiki/Port_(computer_networking))

4.1 ssh

La primera opción era existente **telnet**. **Telnet** es un programa que permite conectar a través del terminal con otro sistema. Basta con indicar la IP y, con las credenciales adecuadas, se les permite trabajar de forma remota en el terminal del otro equipo. sin embargo **telnet** Ya no se utiliza porque tiene varios problemas de seguridad, el ser más importante que la conexión no está encriptada de manera que se pudieron obtener datos tales como contraseñas. Para resolver este problema parece que el **Cubierta segura (SSH)** protocolo de la familia de herramientas para controlar a distancia o la transferencia de archivos entre ordenadores de una manera segura. Entre las herramientas de la familia son la conexión remota (el estilo de telnet, pero seguro) o la copia de seguridad. El sistema consiste en un demonio (**sshd**) en el equipo al que queremos acceder a un cliente y en la función del tipo de acceso que se utiliza (**ssh** para el control remoto, **SCP** copiar ...).

- En el servidor (la computadora a la que quiere acceder) que necesitamos:

1. Instalar el servidor SSH daemon

```
sudo apt-get install openssh-server
```

2. Abra el puerto correspondiente para recibir paquetes. En este caso, el protocolo es TCP y el puerto por defecto es 22

```
iptables -A ENTRADA -i eth1 -p tcp --dport 22 -j ACCEPT
```

- En el cliente necesitamos nstall el cliente ssh

```
sudo apt-get install openssh-client
```

Para conectar, desde el cliente

```
> ssh user@192.145.6.23
```

Usted recibirá un mensaje de advertencia preguntando si confía en la firma digital de la computadora remota. Si confía en él, la firma se almacena en un archivo oculto llamado. **ssh / known_hosts** y usted no recibirá más advertencias cuando se conecta a

este servidor que el futuro a menos que la huella digital de los cambios en el servidor remoto, que puede ser una señal de que alguien está interceptando su conexión. A continuación, el programa le preguntará por su contraseña⁵ en el equipo remoto y una sesión se iniciará.

4.2 Visor de equipo

TeamViewer es una de las herramientas más comunes de terceros para la administración remota. En este caso, su funcionalidad no es directa desde un ordenador a otro, pero la conexión se realiza a través de los servidores de la TeamViewer. Que no requiere casi de configuración, sólo tiene que instalar el programa en ambos equipos un entonces cada ordenador se conectará a los servidores del visor de equipo en Internet y se creará una cuenta de gestión cuyo ID y contraseña se visualizará en la pantalla. Usted tendrá que escribir las credenciales cuando se desea conectar a cada equipo de forma remota.

Puede ver un video sobre el proceso en el curso de Moodle.

5. RECURSOS COMPARTIDOS

En el nivel de usuario de las grandes ventajas de las redes es la posibilidad de compartir recursos, especialmente los archivos e impresoras. Como siempre, hay varias opciones para realizar este intercambio, con NFS, pero en esta unidad vamos a trabajar con SAMBA un sistema que nos permita compartir recursos entre los sistemas Linux y Windows

5.1 SAMBA

Hoy en día gran parte de la funcionalidad de SAMBA es transparente para el usuario final: un usuario de Linux puede abrir un explorador de archivos en la red, buscar ordenadores Windows y acceso a aquellos elementos que se han compartido desde Windows. Aun así, en muchas situaciones no vamos a ser capaces de utilizar la interfaz gráfica o requerir una configuración más detallada. En la plataforma se vinculan dos videos ([1](#) y [2](#)) Acerca de la instalación y configuración de SAMBA⁶

⁵ Hay varias formas de autenticación: Logina y contraseña, clave privada / pública ...

⁶ El servidor Linux Formación de vídeo 101 se basa en una distribución CentoOS, no Ubuntu. En términos generales, el proceso es

el mismo, excepto que el proceso de instalación se lleva a cabo con el instalador yum (no con apt-get) y los directorios de algunas configuraciones pueden ser diferentes.

6. MATERIAL ADICIONAL

[1] Glosario. [2]

Ejercicios

7. BIBLIOGRAFÍA

[1] Como Funciona ONU servicio DHCP

[http:// windowserver.wordpress.com/2013/09/20/cmo-funciona-el-servicio-dhcp-incluye-Capturas-de-rojo /](http://windowserver.wordpress.com/2013/09/20/cmo-funciona-el-servicio-dhcp-incluye-Capturas-de-rojo/)

[2] Las redes de ordenadores. S. Tanenbaum Andrew. Pearson. 2010 [3] ¿Cómo cambiar el nombre de los ordenadores en Windows 10