

## 1. CONECTAR COMPUTADORAS A UNA RED

El primer paso para poder utilizar dispositivos en una red es conectarlos a ella, y para ello necesitamos

para conocer las interfaces disponibles (NIC) y asignarles una dirección IP. Hay dos formas de asignar

IP, ya sea de forma dinámica o estática:

- Dinámico: un dispositivo de red (un servidor DHCP) gestiona la distribución de IP, cuando el dispositivo

conectado a esa red, solicita una IP al servidor DHCP que la asigna en base a

algunas reglas. De esta forma se agiliza la incorporación de nuevos dispositivos y se evitan posibles conflictos.

evitado asignando IPs iguales a diferentes nodos de la red). Sin embargo, es posible que entre diferentes conexiones a la red, la 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 una computadora

permanecer fijo en el tiempo.

### 1.1 Asignación dinámica

Debido a su simplicidad, es el tipo de asignación más común dentro de una red. Esta usado cuando nos conectamos con nuestro móvil a una red inalámbrica (wifi o 4g) o con nuestro escritorio en nuestro

red domestica. En general, el enrutador es el servidor DHCP.

es el que viene configurado por defecto en la mayoría de sistemas operativos

que funcionan como estaciones de trabajo, por lo que el usuario solo tiene que conectar el equipo a

la red físicamente.

Sistemas Linux

El primer paso es saber cuántas y qué interfaces están disponibles en nuestro equipo. Para hacer esto,

desde la terminal, usamos el comando `ifconfig`.

☐ Uno de los comandos de Linux más importantes (en lo que a redes se refiere)

es definitivamente `ifconfig`. Con él, es posible configurar y modificar la configuración de las interfaces de red.

```

> ifconfig -a
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
    options=1203<RXCSUM, TXCSUM, TXSTATUS, SW_TIMESTAMP>
    inet 127.0.0.1 netmask 0xff000000
    inet6 ::1 prefixlen 128
    inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
    nd6 options=201<PERFORMNUD,DAD>
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=10b<RXCSUM, TXCSUM, VLAN_HWTAGGING, AV>
    ether 10:9a:dd:71:1d:c6
    nd6 options=201<PERFORMNUD,DAD>
    media: autoselect (none)
    status: inactive
en1: flags=963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX> mtu 1500
    options=60<TSO4,TSO6>
    ether d2:00:1c:56:cf:c0
    media: autoselect <full-duplex>
    status: inactive
fw0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 4078
    lladdr 70:cd:60:ff:fe:c5:6c:fc
    nd6 options=201<PERFORMNUD,DAD>
    media: autoselect <full-duplex>
    status: inactive

```

Con la opción -a, se nos muestra información sobre todas las interfaces que existen en nuestro sistema.

Cada uno de ellos se nombra con dos o tres letras, seguidas de un número (similar al disco duro

nomenclatura). En el caso que se muestra en la figura existen 4 interfaces, 3 de ellas físicas<sup>1</sup> (eso es,

se refieren a elementos de hardware), y 1 lo0 lógico, que se refiere al loopback, al interno loop (pueden aparecer otros, como vbox, que se refiere a interfaces creadas por virtual box).

Una vez que sepamos el nombre de la interfaz a la que queremos asociar una ip dinámica (en nuestro caso

elegiremos en1), debemos modificar el archivo / etc / network / interfaces

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

Y añadiendo (o modificando si ya existía) una línea que configura la interfaz. En nuestro caso nosotros

modificará la interfaz en1, por lo que agregaríamos

```
iface en1 inet dhcp
```

El último paso es reiniciar la interfaz. Podemos hacer esto de dos maneras: deshabilitando y habilitando el

interactúa directamente con el comando ifconfig:

> sudo ifconfig en1 abajo

> sudo ifconfig en1 arriba

1 en0, en1 se refiere a la interfaz ethernet y fw0 se refiere a la interfaz de cable de fuego

O deteniendo y arrancando el sistema de red con el script de arranque del sistema de red2

.

> sudo /etc/init.d/networking stop

> sudo /etc/init.d/networking start

☐ Existe una forma más sencilla de reiniciar el script utilizando el parámetro de reinicio, pero en

en algunos casos puede fallar, por lo que la opción más segura es realizar el proceso por separado

☐ Los scripts de inicio son scripts que se ejecutan al inicio del sistema operativo.

Su objetivo es iniciar de forma controlada programas y demonios3

que realizan

tareas en el sistema (por ejemplo, un servidor de base de datos o el control de la red).

En sistemas con GUI es posible realizar estas acciones gráficamente. La forma exacta depende de

el sistema en sí, pero en general la idea es la misma. Para ver un ejemplo, en LUbuntu.

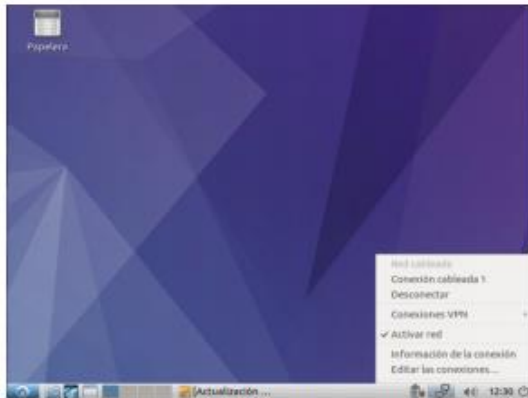


Figure 1. GUI DHCP config step 1

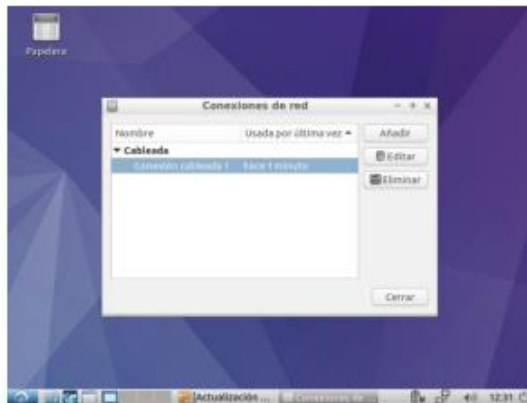


Figure 2. GUI DHCP config step 2

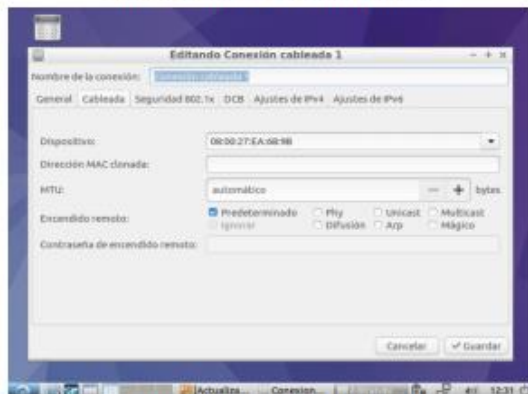


Figure 3. GUI DHCP config step 3

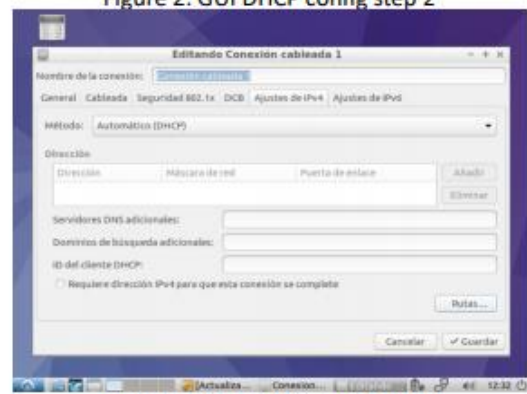


Figure 4. GUI DHCP config step 4

2 Un script es un programa escrito usando un sistema de comando, que generalmente tiene como objetivo automatizar tareas.

3 En Linux, un daemon es un servicio, es decir, un programa que se ejecuta en segundo plano, de forma transparente al

usuario. Por ejemplo un antivirus

❑ Como puede ver, la dirección del servidor DHCP no se indica en ninguna parte. Cómo la computadora sabe a quien solicitar IP? El proceso funciona con una serie de transmisiones señales llamadas DHCP Discover, DHCP Offer, DHCP Requests, DHCP ack4

que son

realizado utilizando la dirección del cliente 0.0.0.0 y como destino 255.255.255.255 (transmisión).

### 1.1.2 Sistemas Windows

Si desea saber cuántas y qué interfaces están disponibles en nuestro equipo en una sistema, puede utilizar el comando ipconfig.

> ipconfig

> ipconfig / todos

Puede configurar una IP dinámica en sistemas Windows siguiendo estos pasos:



Figure 5. Windows DHCP config step 1



Figure 6. Windows DHCP config step 2

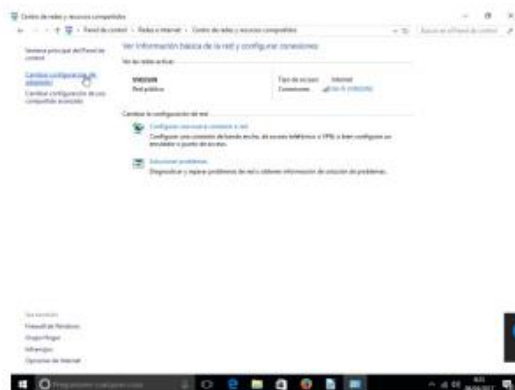


Figure 7. Windows DHCP config step 3

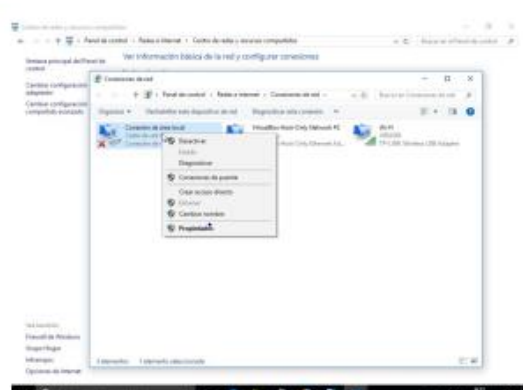


Figure 8. Windows DHCP config step 4

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

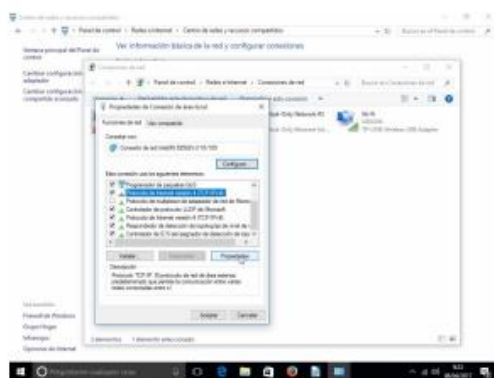


Figure 9. Windows DHCP config step 5

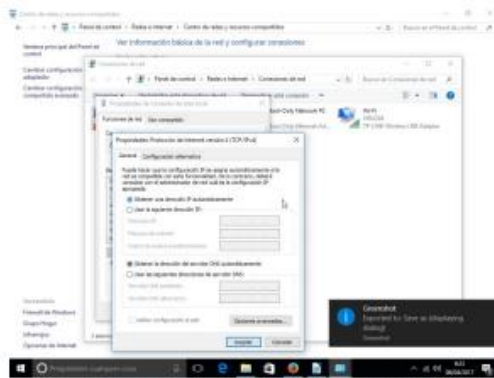


Figure 10. Windows DHCP config step 6

## 1.2 Asignación estática

La configuración de la IP estática no es muy compleja, pero requiere conocimientos sobre la topología de la red. Como en la configuración dinámica DHCP maneja todo el trabajo, en este caso

es el usuario que tiene que configurar todos los datos manualmente.

Los datos que necesitamos son la IP que se va a asignar (teniendo en cuenta que aún no la utiliza ningún

otros equipos), la máscara de red y la dirección de la puerta de enlace, es decir, el enrutador que generará

el exterior a esa red.

### 1.2.1 sistemas Linux

De manera similar a la asignación dinámica, modificamos el archivo / etc / network / interfaces pero en este

caso añadiendo a la información necesaria para la operación estática:

iface en1 inet estático

dirección 192.168.20.5

máscara de red 255.255.255.0

puerta de enlace 192.168.20.1

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



Figure 11. GUI static IP config

### 1.2.2 Sistemas Windows

En los sistemas Windows, para configurar una IP estática debes ir al mismo lugar al que fuiste configurar IP dinámica.

En ese lugar, en lugar de elegir Obtener IP automáticamente, debe introducir manualmente la IP,

máscara de red y puerta de enlace.

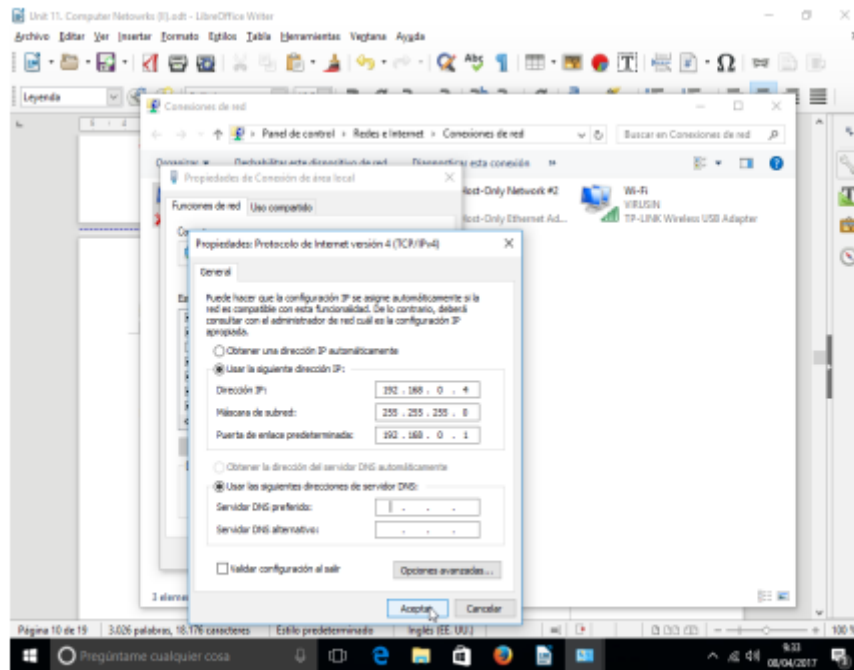


Figure 12. Windows static IP config

## 2. LOCALIZACIÓN DE RECURSOS EN LA RED

Cada dispositivo conectado a una red IP tiene una dirección IP pero recuerda ese conjunto de números

Poder comunicarse entre dispositivos es algo muy complicado. La resolución de nombres es el proceso de mapeo de direcciones IP a nombres de host, lo que facilita la identificación de recursos en un

la red. Por ejemplo, es más fácil recordar [www.google.com](http://www.google.com) que 216.58.211.238.

### 2.1 Asignar el nombre de su computadora

Para acceder a los dispositivos por su nombre, se le debe asignar uno. Desde los sistemas Linux, tenemos que

cambie el archivo / etc / hostname.

> sudo nano / etc / nombre de host

En los sistemas Windows 10, abra Configuración y vaya a Sistema> Acerca de

☐ Puede utilizar letras, números y guiones, pero no espacios.

### 2.2 Relacionar nombres e IP localmente

La forma más sencilla de relacionar nombres con IP es utilizando el archivo hosts. Este archivo contiene líneas de texto que

están formados por direcciones IP seguidas de uno o más nombres de host. Cada campo está separado por blanco

espacio (espacios en blanco o caracteres de tabulación).

192.168.20.6 mortadelo-computadora

192.168.20.7 filemon-computadora

192.168.20.8 zipi-computadora

192.168.20.9 zape-computadora

192.168.20.10 carpanta-computadora

Este archivo se encuentra en / etc / hosts en sistemas Linux o en [X]: \ Windows \ System32 \ Drivers \ etc (donde

[X] es el hasta donde se instala el sistema de Windows, generalmente C.

☒ En los sistemas Windows, el archivo de hosts no se puede modificar directamente por motivos de seguridad.

razones. Para modificarlo es necesario hacer una copia en otra carpeta, modificarlo y luego, reemplace el original con el modificado usando los permisos de administrador

### 2.3 DNS

El archivo hosts puede resolver el problema de la ubicación de los nombres dentro de un pequeño y controlado

entorno como una red local, pero cuando necesitamos resolver los nombres de los servidores de Internet, esto

la solución no es factible.

Para ello, existen los denominados servidores DNS, que proporcionan una relación nombre-IP. Obviamente

un solo servidor no puede resolver todos los nombres de todo Internet, por lo que si un servidor no puede resolver,

Reenviará la solicitud a otro

En general estos servidores los asigna 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

servidor de nombres 127.0.0.1

servidor de nombres 172.16.1.254

Tenga cuidado con las modificaciones realizadas en este archivo. En general, el propio servidor DHCP no asignará

sólo la IP pero también los servidores DNS. Estas modificaciones pueden anular las realizadas manualmente.

Para mantener estos datos, podemos editar el / etc / network / interfaces con la información que queremos agregar a



el archivo resolv.conf.

iface en1 inet estático

dirección 192.168.20.5

máscara de red 255.255.255.0

puerta de enlace 192.168.20.1

dns-nameservers 172.16.1.254,8.8.8.8

En los sistemas Windows, puede configurar DNS usando su GUI:

ems, you can configure DNS using its GUI.

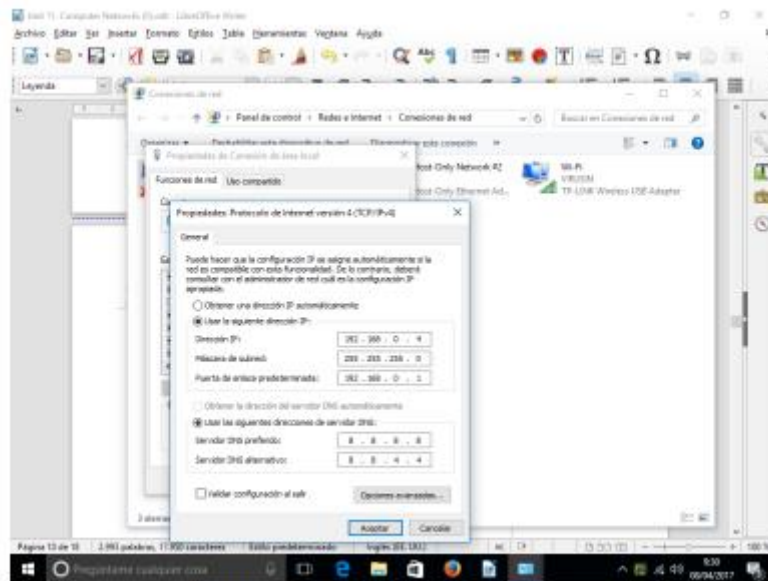


Figure 13. Windows DNS config

En el ejemplo de Windows, estamos usando DNS públicos de Google que son 8.8.8.8 y 8.8.4.4. Son fáciles de recordar. Puedes encontrar más información en la wikipedia.

DNS público de Google.

### 3. SEGURIDAD

#### 3.1 Cortafuegos

Un firewall es un sistema (se puede implementar mediante software o hardware) que monitorea y

controla el tráfico de red entrante y saliente. Ha configurado una serie de reglas de confianza y no confianza que se aplican a cada paquete de una manera que lo deja pasar dependiendo de si

cumplir cualquiera de esas reglas.

##### 3.1.1 Sistemas Linux

Linux incluye un firewall nativo construido dentro del kernel. Ese firewall está controlado por iptables

mando. Las tablas de IP son un conjunto de tablas que le dicen al kernel cómo procesar los paquetes entrantes.

Cada mesa tiene una función distinta. Por ejemplo, la tabla de filtros (la tabla predeterminada) proporciona

comandos para filtrar y aceptar o descartar paquetes y de esta manera se comportan como un firewall. La tabla NAT

proporciona comandos para traducir (modificar) direcciones IP de origen o destino, y la tabla de mangle

proporciona comandos para modificar los encabezados 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 de TCP / IP la operación debe

estar hecho. Por ejemplo, la tabla de filtros contiene cadenas integradas llamadas INPUT, FORWARD y OUTPUT,

y respaldar las políticas ACCEPT, DROP y REJECT (y otras). Una regla DROP de paquetes configurada

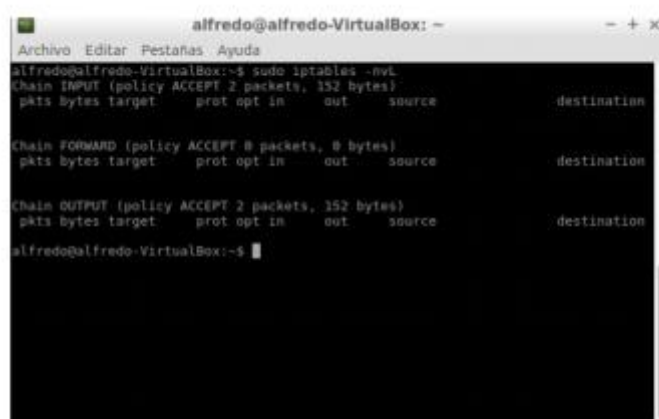
debajo de la cadena INPUT dirigirá el kernel a los paquetes DROP que se reciben en una determinada

interfaz.

❑ En nuestro caso solo trabajaremos con la tabla de filtros que también es la predeterminada tabla de iptables. Para elegir la tabla con la que trabajar, debe usar la opción -t

Para enumerar la tabla de filtros:

iptables -nvL



```
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: ~$
```

Figure 14. iptables -nvL

❑ Por defecto, no se definen reglas y la política por defecto para cada cadena es ACEPTAR,

por lo que las iptables permiten que todos los paquetes pasen por el kernel

Una forma más segura de trabajar es cambiar el modo predeterminado de ACEPTAR a DROP, al menos cuando

llega a los paquetes entrantes. Para hacerlo:

```
sudo iptables -P INPUT DROP
```

este comando cambia la política de ENTRADA predeterminada (-P) a DROP. De esta manera, cuando enumera la tabla

otra vez:

A partir de este momento nuestra computadora rechazará todos los paquetes entrantes.

Esta solución puede resultar drástica ya que la comunicación con el exterior puede resultar imposible si lo hacemos

No permitir la entrada de ningún paquete. Lo interesante es agregar reglas que son elementos de apertura.

según nuestras necesidades. Esta apertura se puede realizar de varias formas:

- abrir una interfaz

```
iptables -A ENTRADA -i lo -j ACEPTAR
```

anexar (A) una regla a la cadena INPUT. La política se ACEPTA y la regla se aplica al interfaz loopback (lo) (-i).

- por protocolo

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

anexar (A) una regla a la cadena INPUT. La política se ACEPTA y la regla se aplica al ethernet1 (eth1) interfaz (-i) para el protocolo (-p) udp. Además, el cliente envía el paquete. para el puerto (-sport) 68 y el servidor está a la escucha del puerto (-dport) 68

- por estado

```
iptables -A ENTRADA -i eth0 -m estado --estado ESTABLECIDO, RELACIONADO -j ACEPTAR
```

iptables puede controlar el estado de la conexión, es decir, puede agrupar los paquetes en conexiones

de acuerdo con sus direcciones IP y puertos de origen / destino y comprender si el

la conexión está siendo iniciada por la máquina local o una máquina remota. En el ejemplo nosotros

anexar (A) una regla a la cadena INPUT. La política se ACEPTA y la regla se aplica al ethernet1 (eth1) interfaz (-i) si el estado (-m) está ESTABLECIDO (conexiones que tenemos

originado) o RELACIONADO (creado por las conexiones ESTABLECIDAS existentes)

### 3.1.2 Sistemas Windows

El firewall predeterminado en los sistemas Windows es muy limitado en comparación con iptables en Linux, pero para configuraciones podría ser útil.

Puede configurarlo usando la GUI de Windows

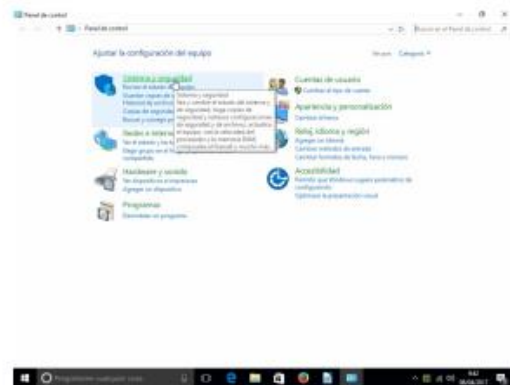


Figure 15. Firewall Windows step 1

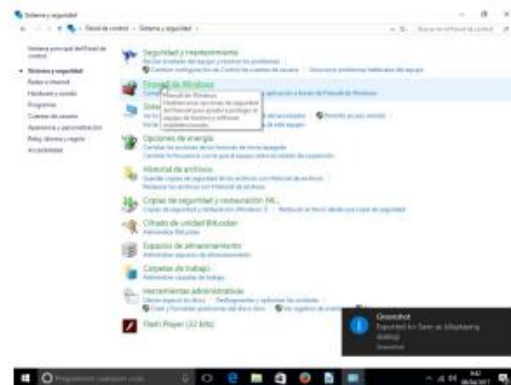


Figure 16. Firewall Windows step 2

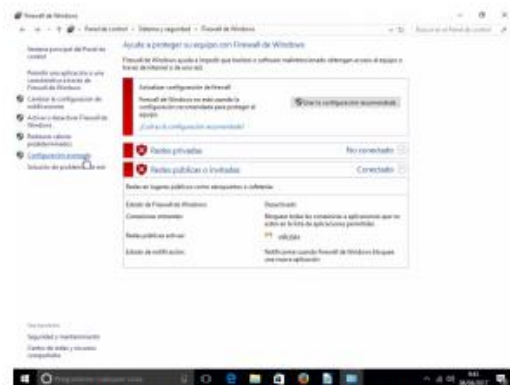


Figure 17. Firewall Windows step 3

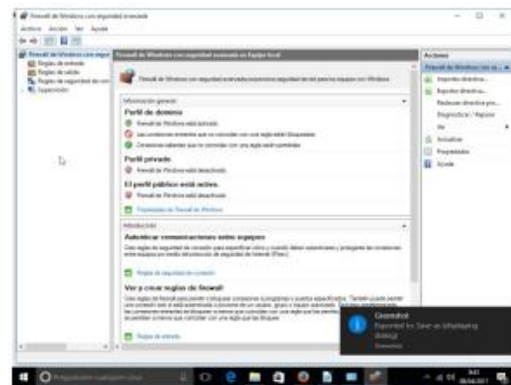


Figure 18. Firewall Windows step 4

## 4. ACCESO REMOTO

A nivel administrativo, una de las primeras ventajas de las redes es la posibilidad de gestionar un

computadora de forma remota. Hay muchas opciones, pero nos centraremos en dos de las más utilizadas.

☐ Una dirección IP podría tener muchos servicios. Para distinguir que servicio somos

conectando, cada servicio tiene un puerto diferente. Los puertos más comunes son 80 para web

servidores, 22 para ssh, 25 para SMTP,...

Más información en [https://en.wikipedia.org/wiki/Port\\_\(computer\\_networking\)](https://en.wikipedia.org/wiki/Port_(computer_networking))

#### 4.1 ssh

La primera opción existente fue telnet. Telnet es un programa que permite conectarse vía terminal con

otro sistema. Simplemente indique la IP y, con las credenciales adecuadas, podrá trabajar de forma remota en el terminal de otra computadora.

Sin embargo, telnet ya no se usa porque tiene varios problemas de seguridad, el más importante

siendo que la conexión no está encriptada para que se puedan obtener datos como contraseñas.

Para resolver este problema, aparece la familia de herramientas del protocolo Secure Shell (SSH) para

controlar o transferir archivos entre ordenadores de forma segura. Entre las herramientas de la familia se encuentran

la conexión remota (al estilo de telnet pero segura) o la copia segura. El sistema consta de un daemon (sshd) en el equipo al que queremos acceder y un cliente en la función del tipo de acceso que se utiliza (ssh para control remoto, scp para copiar ...).

- En el servidor (el ordenador al que queremos acceder) necesitamos:

1. Instale el servidor demonio ssh

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

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

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

- En el cliente necesitamos instalar el cliente ssh

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

Para conectarse, desde el cliente

```
> ssh user@192.145.6.23
```

Recibirá un mensaje de advertencia que le preguntará si confía en la firma digital de la computadora remota. Si

confía en él, la firma se almacenará en un archivo oculto llamado `.ssh / known_hosts` y no obtendrá

más advertencias cuando se conecte a este servidor en el futuro a menos que la huella digital del control remoto

cambios en el servidor, lo que puede ser una señal de que alguien está interceptando su conexión. Entonces el

El programa le pedirá su contraseña

en la computadora remota y se iniciará una sesión.

#### 4.2 Visor de equipo

TeamViewer es una de las herramientas de terceros más comunes para la gestión remota. En este caso es

La funcionalidad no es directa de una computadora a otra, pero la conexión se realiza a través del

Servidores de TeamViewer.

No requiere casi configuración, simplemente instale el programa en ambas computadoras y luego

cada computadora se conectará a los servidores de Team Viewer en Internet y creará un cuenta de administración cuyo ID y contraseña se mostrarán en la pantalla. Tendrás que escribir

esas credenciales cuando desee conectarse a cada computadora de forma remota.

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

### 5. RECURSOS COMPARTIDOS

A nivel de usuario una de las grandes ventajas de las redes es la posibilidad de compartir recursos,

especialmente archivos e impresoras. Como siempre, existen varias opciones para realizar este intercambio, con NFS,

pero en esta unidad trabajaremos con SAMBA un sistema que nos permitirá compartir recursos entre

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, busque computadoras con Windows y acceda a los elementos que se han

compartido desde Windows.

Aun así, en muchas situaciones no podremos utilizar la interfaz gráfica o requeriremos una mayor

configuración detallada.

En la plataforma se enlazan dos videos (1 y 2) sobre la instalación y configuración de SAMBA

5 Hay varias formas de autenticarse: login y contraseña, clave privada / pública ...

6 El video Linux Server Training 101 se basa en una distribución de CentoOS, no en Ubuntu. En términos generales, el proceso es

lo mismo, excepto que el proceso de instalación se realiza con el instalador yum (no con apt-get) y el

los directorios de algunas configuraciones pueden ser diferentes.