

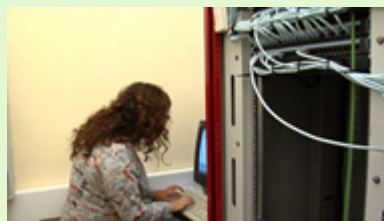
Administración de la red (Linux III).



Caso práctico

María visita a Juan.

-Juan, vamos a mejorar la red de la empresa y para eso necesito que utilices un 📁 **servidor** para que actúe como router y le proporcione a la empresa los servicios más importantes. 📁 **Encaminamiento** y 📁 **DHCP**, y luego le instalaremos más servicios.



-Muy bien María, he visto por Internet que Linux funciona muy bien con redes. De hecho su máxima potencia se utiliza para actuar como servidor. Ahora mismo me pongo a configurar el servidor.



Materiales formativos de FP Online propiedad del Ministerio de Educación, Cultura y Deporte.

[Aviso Legal](#)

1.- Esquema básico de red.



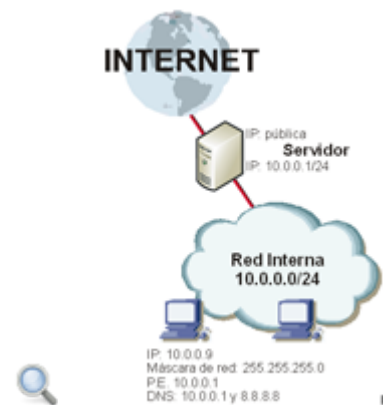
Caso práctico

Juan se dispone a diseñar la red, pero antes de empezar, va a hacer un esquema de red, ya que este esquema le será de utilidad, para mantener la red y para cuando tenga que hacer cambios en la misma.



Con la fuerte expansión que ha tenido Internet se ha generalizado la utilización de redes en las empresas y en nuestros hogares. Hoy en día para un empresa es totalmente necesario disponer de una red interna que le permita compartir información, conectarse a Internet e incluso, ofrecer sus servicios en Internet.

En esta unidad aprenderás a configurar el sistema GNU/Linux para convertirlo en un potente router que provea a la red de los servicios necesarios: encaminamiento, DHCP y DNS. Para poder aprender mejor a administrar el sistema nuestro objetivo es configurar la infraestructura de red que se muestra en la siguiente figura y que puede utilizarse en una empresa o domicilio.



Esquema básico de red.

A la hora de configurar la red hay que tener en cuenta los siguientes objetivos:

- ✓ Configurar iptables para darle acceso a Internet a los clientes de la red interna.
- ✓ Configurar el servidor DHCP para que asigne de forma automática las direcciones que van desde la 10.0.0.100 a la 10.0.0.254. Las demás direcciones las asignará el administrador de la red de forma manual.
- ✓ Además, se dispone de una impresora de red que tiene la dirección MAC (AA:BB:CC:DD:EE:FF) a la que se le quiere asignar siempre la IP 10.0.0.254.
- ✓ Configurar el servidor de nombres para que administre el dominio miempresa.com. Además, se tiene que crear los siguientes registros: www.miempresa.com y ftp.miempresa.com apuntan a la IP 10.0.0.1; mail.miempresa.com es equivalente a www.miempresa.com; y el servidor de correo electrónico se encuentra en mail.miempresa.com.
- ✓ Por último, se configuran los servicios Web y FTP para que la empresa tenga su propio servidor de páginas web y FTP.

1.1.- Configuración de la red.

Una vez que tienes claro el esquema de red que vas a implementar, el primer paso que debes realizar es configurar correctamente las diferentes interfaces de red de nuestro servidor (que actúa como router) y de los clientes.

Básicamente existen dos formas de configurar las tarjetas de red de nuestro equipo: manualmente o dinámicamente a través de un servidor DHCP. A continuación se van a ver ambos métodos de configuración.



1.1.1.- Configuración de la red cableada.

Para configurar una interfaz de red es necesario asignarle una dirección IP con su respectiva máscara de red. El comando más utilizado para configurar la red es ifconfig (Interface Configuration). Por ejemplo:

```
# ifconfig eth0 192.168.1.2 netmask
255.255.255.0 up
```

```
root@ubuntu-vm:~# ifconfig
eth0: flags=4096<UP,BROADCAST,MULTICAST> mtu=1500
    inet 192.168.1.2 netmask 255.255.255.0 broadcast 192.168.1.255
    ether 08:00:27:1d:1d:1d txqueuelen 1000
    RX packets 0 errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 errors 0 dropped 0 overruns 0 carrier 0
    collisions 0
    Interrupt:0
    RX bytes 0 (0.0 KB) TX bytes 0 (0.0 KB)

eth1: flags=4096<UP,BROADCAST,MULTICAST> mtu=1500
    inet 192.168.1.3 netmask 255.255.255.0 broadcast 192.168.1.255
    ether 08:00:27:1d:1d:1d txqueuelen 1000
    RX packets 0 errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 errors 0 dropped 0 overruns 0 carrier 0
    collisions 0
    Interrupt:0
    RX bytes 0 (0.0 KB) TX bytes 0 (0.0 KB)

lo: flags=73<UP,LOOPBACK,RUNNING> mtu=65536
    inet 127.0.0.1 netmask 255.0.0.0
    ether 00:00:00:00:00:00 txqueuelen 1000
    RX packets 0 errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 errors 0 dropped 0 overruns 0 carrier 0
    collisions 0
    Interrupt:0
    RX bytes 0 (0.0 KB) TX bytes 0 (0.0 KB)

root@ubuntu-vm:~#
```

Comando ifconfig.

En este caso estas configurando la interfaz eth0 (primera tarjeta de red detectada) con la dirección IP 192.168.1.2 y con máscara de red 255.255.255.0. El parámetro up indica que la tarjeta debe activarse, pero puede omitirse puesto que al asignarle los parámetros de red la tarjeta se activará por defecto. Para desactivar una interfaz de red ejecuta:

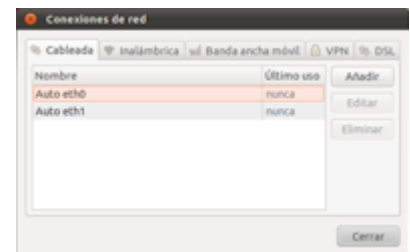
```
# ifconfig eth0 down
```

Para activar una interfaz de red ejecuta:

```
# ifconfig eth0 up
```

Para comprobar la configuración de las interfaces de red ejecuta el comando ifconfig. Tal y como puedes ver en la siguiente figura la interfaz eth0 tiene la dirección 192.168.118.142 (la ha obtenido de forma automática) y la interfaz eth1 tiene la dirección IP 10.0.0.1.

Para que el equipo pueda conectarse a una red diferente de la que se encuentra (por ejemplo, Internet) necesita establecer la puerta de enlace. La puerta de enlace es el equipo que permite comunicar varias redes. Por ejemplo, si el equipo se encuentra conectado a la red 192.168.0.0/24 en la interfaz eth0 y la puerta de enlace es 192.168.0.1, debes ejecutar el siguiente comando:



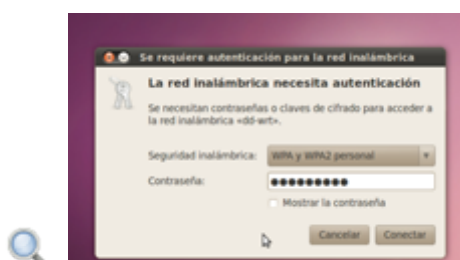
Configuración de red.

```
# route add -net 0/0 gw 192.168.0.1 eth0
```

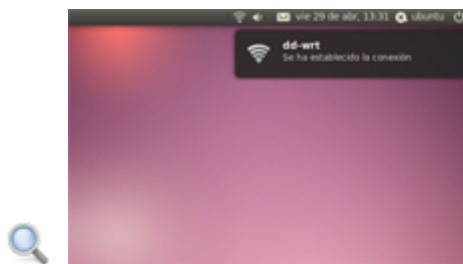
Si quieres puedes realizar la configuración mediante el entorno gráfico xWindows. Para ello, en el menú Sistema > Preferencias ejecuta la herramienta Conexiones de red.

1.1.2.- Configuración de la red inalámbrica.

Desde los sistemas GNU/Linux es posible configurar la red inalámbrica a través del comando iwconfig o a través del asistente de Conexión. Para acceder a la red inalámbrica de forma gráfica, en el menú de herramientas superior, pulsa en el icono de la red inalámbrica y selecciona la red a la que deseas conectarse. Si la red inalámbrica requiere autenticación, indica la contraseña WEP o WPA y pulsa el botón Conectar.



Automáticamente, el asistente establece la conexión a la red inalámbrica y muestra en pantalla un mensaje de que el proceso se ha realizado correctamente.



Establecida conexión inalámbrica

1.1.3.- Ficheros de configuración.

El problema de configurar las interfaces de red con ifconfig es que no se guardan los datos de configuración en ningún fichero, al reiniciar el equipo se pierde la configuración. A continuación se van a ver los diferentes ficheros de configuración que intervienen en la configuración de la red del equipo.



La configuración de las interfaces de red se guarda en el fichero `/etc/network/interfaces`. Siguiendo el esquema de red propuesto anteriormente, la interfaz de red `eth0` es la encargada de conectarse a Internet mientras que la interfaz `eth1` pertenece a la red interna. Los parámetros de configuración de `eth0` los tiene que facilitar el proveedor de Internet o los puedes obtener automáticamente utilizando DHCP.

Fichero `/etc/network/interfaces`.

```
auto eth0 iface eth0 inet dhcp auto eth1
iface eth1 inet static address 10.0.0.1
netmask 255.255.255.0 network
10.0.0.0 broadcast 10.0.0.255 #
gateway 10.0.0.1
```

Aunque lo normal es que `eth0` obtenga la dirección IP de forma automática al iniciar el equipo puedes hacerlo manualmente ejecutando:

```
# dhclient eth0
```

Configuración del nombre del equipo.

Para configurar el nombre del equipo hay que modificar el fichero `/etc/hostname` e indicar el nombre del equipo.

Configuración del servidor DNS.

Existen dos formas para la resolución de nombres: de forma local o a través de un servidor de nombres (DNS). Para la resolución de nombres de forma local se utiliza el fichero `/etc/hosts` en

donde se guarda el nombre y la dirección IP de las máquinas locales. Por ejemplo:

```
127.0.0.1 localhost.localdomain localhost 193.147.0.29 www.mec.es
```

Para establecer los servidores de resolución de nombres (DNS) debes editar el fichero `/etc/resolv.conf`. Por ejemplo:

```
nameserver 8.8.8.8 nameserver  
150.214.156.2
```

Actualizar los cambios.

Una vez realizada la configuración del sistema para que se apliquen los cambios en las interfaces de red hay que reiniciar el servicio o hacer un reload ejecutando:

```
# /etc/init.d/networking force-reload
```



Autoevaluación

Indica la opción incorrecta.

En el archivo `/etc/resolv.conf` se guardan los servidores de nombres.

El comando `ifconfig` es la única forma de configurar la red.

En el fichero `/etc/network/interfaces` se guarda la configuración de las interfaces de red.

El servicio DHCP permite obtener la configuración IP de forma automática.

1.1.4.- Comprobación.

Para comprobar la conexión a Internet puedes ejecutar el comando `ping` indicando como parámetro cualquier dirección de Internet. Por ejemplo:

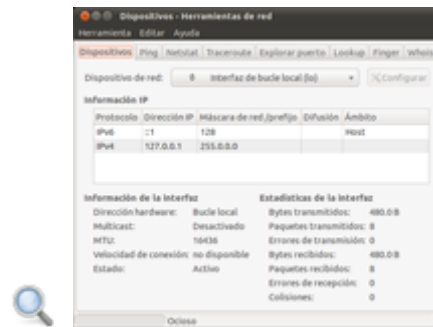
```
$ ping www.google.es
```

```
[root@localhost ~]# ping www.google.es  
PING www.l.google.com (66.249.92.104): 56(84) bytes of data:  
64 bytes from 66.249.92.104: icmp_seq=1 ttl=120 time=31.5 ms  
64 bytes from 66.249.92.104: icmp_seq=2 ttl=120 time=39.7 ms  
64 bytes from 66.249.92.104: icmp_seq=3 ttl=120 time=43.2 ms  
64 bytes from 66.249.92.104: icmp_seq=4 ttl=120 time=39.7 ms  
64 bytes from 66.249.92.104: icmp_seq=5 ttl=120 time=42.9 ms  
^C  
--- www.l.google.com ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4525ms  
rtt min/avg/max/mdev = 39.729/43.451/51.527/4.330 ms  
[root@localhost ~]#
```

Comando ping.

Si al realizar el ping se recibe respuesta entonces la comunicación se está realizando correctamente. Si por el contrario indica que todos los paquetes se han perdido (100% packet loss) debes comprobar la configuración de red o los parámetros de configuración. En la figura anterior puedes ver como el servidor `www.google.es` responde correctamente al comando ping.

Para comprobar la configuración de la red de forma gráfica es posible utilizar las Herramientas de red. Para ello en el menú Sistema > Administración ejecuta la aplicación Herramientas de red.



Herramientas de red.

La aplicación Herramientas de red incluye información relacionada con nuestros dispositivos de red. Permite realizar ping a un determinado host. Incluye la posibilidad de ver el estado de las conexiones de mi equipo, utilizando netstat. Permite utilizar traceroute para ver la ruta entre mi equipo y un equipo remoto. Tiene una pestaña para explorar puertos, que me permite analizar y/o visualizar los puertos que están abiertos o cerrados de un determinado equipo. Tiene un herramienta de búsqueda. Usando finger se puede autenticar los usuarios que están siendo usados en un determinado host de la red. Finalmente con whois se pueden identificar todos los detalles de la adquisición de un determinado dominio.

1.2.- iptables.

La tecnología de firewall de GNU/Linux ha evolucionado desde sencillos filtros de paquetes lineales hasta los motores actuales de inspección de paquetes de estado. Los núcleos de Linux 2.0 emplean una implementación de reglas de filtrado de paquetes que utilizan tres pilas: INPUT (tráfico de entrada), OUTPUT (tráfico de salida) y FORWARD (paquetes que se reenvían a otro equipo). Los paquetes llegan a la parte superior de las pilas y se filtran a través de las reglas hasta que exista una coincidencia. En este punto, cada paquete se puede aceptar, descartar, rechazar o reenviar. Si el paquete no coincide con ninguna de las reglas, pasa a la directiva predeterminada, que normalmente descarta el paquete.



Aunque la capacidad nativa de firewall de los núcleos de Linux 2.0 era más que adecuada para generar firewalls, en la siguiente versión del núcleo 2.2 apareció Iptables que incorporó nuevas y eficaces características: permite la definición de nuevas pilas y mejora la administración de las reglas de una pila.

A partir del desarrollo del núcleo 2.3, los programadores de Linux comenzaron a trabajar en iptables (también llamado netfilter). Iptables mejoró las ventajas de administración de conjuntos de reglas al permitir la capacidad de crear y anular asociaciones de conjunto de reglas con sesiones existentes. Con iptables, el firewall se puede programar para asociar el tráfico devuelto generado a partir de una regla INPUT anterior. El tráfico que entra correctamente en el host puede salir automáticamente del host al ser devuelto, indicando simplemente que genere dinámicamente una regla de devolución.

Las ventajas de la tecnología de inspección de paquetes de estado (SPI, State Packet Inspection) no se limitan a la eficacia de las reglas. Iptables no permite diferenciar la "verdadera naturaleza" del tráfico de la red. Por ejemplo, un firewall iptables programado para permitir el tráfico FTP de salida también tendrá una regla INPUT asociada para permitir la devolución de paquetes. Si un atacante puede fabricar paquetes FTP devueltos, Iptables permite su entrada.

Con SPI no existe ninguna sesión para asociar estos paquetes falsificados y, por tanto, el firewall los rechazaría.



Adobe Flash Player is no longer supported

Resumen textual alternativo

O si lo prefieres puedes descargarte el documento explicando la configuración de iptables.

1.2.1.- Resolución del supuesto práctico.

A continuación se va a configurar el cortafuegos para que permita que la red Interna pueda conectarse a Internet.

Para establecer que el sistema actúe como router hay que ejecutar:

```
# echo "1" >/proc/sys/net/ipv4/ip_forward
```



✓ Limpia la configuración del cortafuegos:

```
# iptables -F # iptables -t nat -F
```

✓ Indica que la red interna tiene salida al exterior por NAT:

```
# iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -d 0/0 -j MASQUERADE
```


- ✓ Se permite todo el tráfico de la red interna y todo lo demás se deniega:

```
# iptables -A FORWARD -s 10.0.0.0/24 -j ACCEPT # iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT # iptables -A FORWARD -j DROP
```

- ✓ Guarda la configuración del cortafuegos ejecutando:

```
# iptables-save >/etc/iptables.rules
```

- ✓ Y modifica el fichero /etc/sysctl.conf para establecer la variable net.ipv4.ip_forward=1.

Para comprender mejor iptables se va a realizar una mejora del supuesto en la que la red interna sólo tiene acceso al exterior para ver páginas web (puerto 80/TCP) y para la resolución de nombres (53/UDP y 53/TCP). Además, se va a publicar un servidor web interno que se encuentra en la dirección 10.0.0.100.

Limpia la configuración del cortafuegos:

```
# iptables -F # iptables -t nat -F
```

Indica que la red interna tiene salida al exterior por NAT.

```
# iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -d 0/0 -j MASQUERADE
```

Se permite sólo el tráfico web (80/tcp) y DNS (53/udp y 53/tcp). Todo lo demás se deniega:

```
# iptables -A FORWARD -s 10.0.0.0/24 -p TCP --dport 80 -j ACCEPT # iptables -A FORWARD -s 10.0.0.0/24 -p TCP --dport 53 -j ACCEPT # iptables -A FORWARD -s 10.0.0.0/24 -p UDP --dport 53 -j ACCEPT # iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT # iptables -A FORWARD -j DROP
```

Redirige el tráfico web que entra por la interfaz externa (eth0) al servidor de la red interna:

```
# iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to 10.0.0.100:80
```

Guarda la configuración del cortafuegos ejecutando:

```
# iptables-save >/etc/iptables.rules
```


Finalmente, modifica el fichero `/etc/network/interfaces` y escribe al final:

```
pre-up iptables-restore </etc/iptables.rules
```

1.3.- DHCP.

El mantenimiento y la configuración de la red en los equipos de una red pequeña es relativamente fácil. Sin embargo, cuando se dispone de una red grande con equipos heterogéneos, la administración y asignación de direcciones IPs así como la configuración de los equipos, se convierte en una tarea compleja de difícil mantenimiento y gestión. Cualquier cambio en la configuración de red, el servidor de nombres, la dirección IP asignada, la puerta de enlace, etcétera, conlleva un excesivo tiempo para ejecutar la tarea.



Por otra parte, en entornos con equipos móviles, la gestión y asignación de direcciones supone una tarea compleja que, aunque puede resolverse con la asignación de direcciones IP estáticas, conlleva la asociación fija de una dirección IP al mismo equipo, para evitar conflictos, y la imposibilidad de su reutilización si un portátil no está conectado a la red local en un momento determinado.

Éste es el mismo problema que se presenta en el entorno de trabajo de un ISP: o se dispone de un sistema de asignación dinámica y flexible que permita reutilizar las direcciones de tal forma que sólo los equipos conectados en un momento determinado a la red tienen asignada una dirección IP, o se dispone de una dirección IP distinta por cada cliente es inviable con el número de usuarios conectados a Internet. El servidor DHCP surge ante la necesidad de realizar la asignación dinámica y automática de las direcciones IP de una red.

El servidor DHCP se encarga de gestionar la asignación de direcciones IP y de la información de configuración de la red en general. Para ello, necesita de un proceso (`dhcpcd`) y un fichero de configuración (`/etc/dhcpd.conf`) que proporciona la información necesaria al proceso.

Los datos mínimos que un servidor de DHCP proporciona a un cliente son: dirección IP, máscara de red, puerta de enlace (gateway) y servidor DNS.

El protocolo DHCP incluye dos métodos de asignación de direcciones IP:

- ✓ Asignación dinámica. Asigna direcciones IPs libres de un rango de direcciones establecido por el administrador en el fichero `/etc/dhcpd.conf`. Es el único método que permite la reutilización dinámica de las direcciones IP.
- ✓ Asignación por reservas. Si quieres que un dispositivo o equipo tenga siempre la misma dirección IP entonces la mejor forma es establecer una reserva. Para ello, en el fichero de configuración para una determinada dirección MAC se asignará una dirección IP. Este método es muy útil para aquellos dispositivos que no cambian de dirección IP. Por ejemplo, es deseable que una impresora en red tenga siempre la misma dirección IP ya que si cambia de dirección IP debes configurar nuevamente la impresora en todos los equipos clientes que la utilicen.

En el fichero `/etc/dhcpd.conf` se almacena toda la información referente a la asignación de direcciones IPs a los clientes. Esta información incluye:

- ✓ Rango de direcciones IP a otorgar a los clientes.
- ✓ Asociación fija de direcciones IP a clientes, mediante el uso de la dirección MAC.
- ✓ Periodo de validez de las asignaciones.
- ✓ Servidores de nombres y wins.
- ✓ Si tienen o no autoridad para asignar direcciones IP.

1.3.1.- Resolución del supuesto práctico.

En primer lugar, es necesario realizar la instalación del servidor DHCP ejecutando:

```
# apt-get install dhcp3-server
```



Configurar el servidor DHCP para la asignación dinámica de direcciones IP, de tal forma que se preste servicio a la red 10.0.0.0/24 y, por otro lado, realizar una reserva al portátil con dirección MAC (AA:BB:CC:DD:EE:FF) para que se le asigne siempre la dirección IP 10.0.0.254.

Para comenzar con la configuración, debes indicar los parámetros generales del servidor y comunes a los equipos de la red, la información necesaria para que éste sepa cómo comportarse. Así, si el servidor dhcp.ejemplo.es es el que tiene la autoridad sobre la zona, se quiere que el tiempo máximo de asignación de una dirección IP sea de una semana (max-lease-time). Para ello el fichero /etc/dhcp3/dhcpd.conf debe tener el siguiente contenido:

```
authoritative; one-lease-per-client on; server-  
identifier 10.0.0.1; default-lease-time 604800;  
max-lease-time 604800; ddns-update-style ad-  
hoc;
```

Posteriormente, se deben introducir los parámetros generales que se transmitirán a los clientes de la red. La red 10.0.0.0 con la máscara de red 255.255.255.0 tiene como puerta de enlace la dirección IP 10.0.0.1 y quiere utilizar los servidores de nombres 8.8.8.8 y 194.224.52.36. Además, hay que tener en cuenta el rango de direcciones IP que desea asignar por DHCP que en el ejemplo es desde la dirección 10.0.0.100 a la 10.0.0.254.

A partir de estos parámetros de configuración debes escribir en el fichero la siguiente configuración:

```
subnet 10.0.0.0 netmask 255.255.255.0 { range 10.0.0.100 10.0.0.254; option  
subnet-mask 255.255.255.0; option broadcast-address 10.0.0.255; option  
routers 10.0.0.1; option domain-name-servers 8.8.8.8, 194.224.52.36; option  
domain-name "miempresa.com"; }
```

Como se desea realizar la reserva de la dirección IP 10.0.0.254 para el portátil con la dirección MAC AA:BB:CC:DD:EE:FF debes añadir las siguientes líneas:

```
host portatil { hardware ethernet AA:BB:CC:DD:EE:FF; fixed-  
address 10.0.0.254; }
```

Para comprobar que la configuración del servidor dhcpd se ha realizado correctamente ejecuta:

```
# dhcpd3 eth1
```

Siendo eth1 la interfaz de red donde quiere que el servidor dhcpd ofrezca sus servicios.

Una vez configurado correctamente el servidor, inicia el servicio ejecutando:

```
# service dhcp3-server start
```

Finalmente, configura el sistema para que se inicie automáticamente el servicio dhcp al iniciar el equipo:

```
# chkconfig dhcp3-server on
```

De esta forma el servidor dhcpd irá asignando automáticamente las direcciones IP a los equipos que se conecten a la red. Para comprobar las asignaciones que se han realizado puedes consultar el fichero /var/lib/dhcp3/dhcpd.leases donde, como puedes ver a continuación, se muestran los datos de cada concesión de dirección IP:

Datos más importantes del servicio DHCP.

Nombre del servicio:	dhcp3-server
Fichero de configuración:	/etc/dhcp3/dhcpd.conf
Concesiones de direcciones:	/var/lib/dhcp3/dhcpd.releases
Comandos más utilizados:	dhcpd3 dhclient



Autoevaluación

¿Qué función NO realiza el servicio DHCP?

Permite que los clientes obtengan la dirección IP de forma automática.

Permite realizar reservas de direcciones IP.

Permite optimizar las direcciones IP de la red.
Permite dar una mayor seguridad.

2.- Compartir archivos e impresoras (Samba).



Caso práctico

Ana y Juan están cada uno utilizando su ordenador.

-Juan, tengo aquí todos los documentos que me pediste pero ocupan mucho espacio y no tengo USB ¿cómo te los paso?

-Muy fácil, vamos a compartir una carpeta por red y me lo pasas.

-Así de fácil ¿cómo se hace?



Samba es el método más utilizado para permitir la integración entre sistemas, ya que permite que los equipos Windows y GNU/Linux puedan compartir carpetas e impresoras entre sí.



Samba es una colección de programas que hacen que Linux sea capaz de utilizar el protocolo SMB (Server Message Block) que es la base para compartir ficheros e impresoras en una red Windows. Los posibles clientes para un servidor SMB incluyen Windows y otros sistemas GNU/Linux.

Samba esta compuesto por tres paquetes: samba-common (archivos comunes), samba-client (cliente) y samba (que es el servidor). Por lo tanto, los paquetes que necesitas instalar dependen del uso que quieras darle al equipo.

Para instalar el cliente y servidor de samba es necesario ejecutar:

```
# apt-get install samba4 smbclient
```

A continuación, inicia el servicio ejecutando:

```
# service samba4 start
```


2.2.- Compartir carpetas.

Para compartir una carpeta hay que modificar el fichero de configuración de samba /etc/samba/smb.conf. En la siguiente tabla puedes ver las opciones más importantes para compartir carpetas.

El ejemplo más sencillo que se puede realizar es compartir una carpeta de forma pública para todos los usuarios. Para ello añade:

```
[publico] path = /publico public = yes read  
only = yes
```



Opciones más utilizadas de smb.conf.

Opción.	Comentario.
[recurso]	Nombre del recurso compartido.
browseable	Indica si se puede explorar dentro del recurso. Los posibles valores son no y yes.
comment	Proporciona información adicional sobre el recurso (no afecta a su forma de operar).
create mode	Especifica los permisos por defecto que tienen los ficheros creados.
directory mode	Especifica los permisos por defecto que tienen los directorios creados.
force user	Especifica el usuario propietario que tienen los ficheros y carpetas que se crean.
force group	Especifica el grupo propietario que tienen los ficheros y carpetas que se crean.
guest ok	Indica si se permite el acceso a usuarios anónimos. Los posibles valores son no y yes.
path	Carpeta a compartir.
public	Indica si el directorio permite el acceso público. Los posibles valores son no y yes.
read only	Indica que el directorio es sólo lectura. Los posibles valores son no y yes.
valid users	Indica los usuarios que pueden acceder a la carpeta. Para añadir un grupo entonces hay que poner el nombre del grupo precedido de la @.
writable	Indica que se puede modificar el contenido de la carpeta.

write list

Indica los usuarios que pueden modificar el contenido.

O si lo prefieres, puedes establecer que el recurso sea accesible solamente por unos determinados usuarios:

```
[miscosas] path = /datos/ comment = "Datos y aplicaciones" valid  
users = juan,encarni,@master
```

Lógicamente los usuarios se han tenido que crear previamente y el grupo master debe existir en el fichero /etc/group.

```
master:x:502:juan,encarni
```

A continuación se amplía el ejemplo pero estableciendo el permiso de escritura para el usuario juan y el permiso de lectura para el usuario encarni y el grupo master. Además, cuando un usuario crea un fichero o carpeta éste se crea en el sistema con un propietario (juan:juan) y unos determinados permisos (770).

```
[miscosas] path = /datos/ comment = "Datos y aplicaciones" valid  
users = juan, encarni,@master writeable = yes write list = juan  
read list = juan,@master force user = juan force group = juan  
create mode = 770 directory mode = 770
```

Cuando se comparte una carpeta es necesario establecer los permisos en el fichero de configuración y en el sistema de ficheros. Para ello puedes utilizar los comandos: chmod, chown y chgrp.

Finalmente, para que se apliquen los cambios reinicia el servicio:

```
# service samba4 restart
```

2.3.- Compartir impresoras.

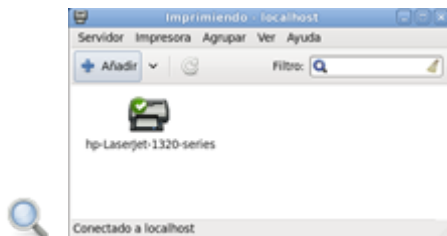
Existen dos formas de compartir las impresoras que se encuentran conectadas al equipo para que las puedan utilizar todos los clientes de la red: a través de la herramienta gráfica system-config-printer o utilizando samba.

Existen impresoras con tarjeta de red que permiten a los clientes imprimir

directamente sin necesidad de ningún servidor.

system-config-printer

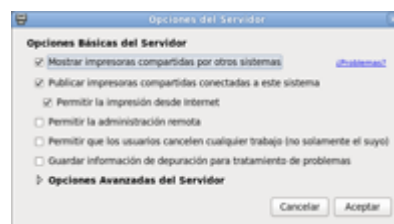
La herramienta Impresoras, que se encuentra dentro del menú Sistema > Administración, permite compartir las impresoras del sistema de una forma gráfica. Al iniciar la herramienta, el sistema muestra las impresoras activas.



Impresoras.

Las tareas más frecuentes que se pueden realizar son:

- ✓ Compartir las impresoras a través de Internet. Para que otros equipos puedan utilizar las impresoras del servidor ve al menú Servidor y selecciona Configuración. En la ventana que se muestra activa la casilla Publicar impresoras compartidas y Permitir la impresión desde Internet.
- ✓ Compartir una impresora. Selecciona la impresora que deseas compartir, pulsa el botón derecho, seleccione Propiedades y en la pestaña Control de acceso indica los usuarios que pueden utilizar la impresora.
- ✓ Administrar los grupos de impresión. Permite que varias impresoras formen un mismo grupo, de forma que cuando se envía un trabajo se procese en la impresora que se encuentre disponible.
- ✓ Para gestionar los trabajos de la impresora selecciona la impresora, pulsa el botón derecho y selecciona Ver la cola de impresión. En la ventana que aparece permite ver y administrar todos los trabajos de la impresora.



Opciones del servidor.

Samba

Para compartir una impresora hay que añadir en el fichero de configuración de Samba /etc/samba/smb.conf un nuevo recurso siguiendo la siguiente estructura:

```
[printers] comment = All printers path =  
/var/spool/samba browseable = no printable =  
yes public = no writable = no create mode =  
0700
```

El acceso a las impresoras GNU/Linux desde Windows funciona de la misma forma que los directorios. El nombre compartido es el nombre de la impresora Linux en el fichero printtab. Por ejemplo, para acceder a la impresora HP_laserjet, los usuarios de Windows deberá acceder a \\smbserv\HP_laserjet.

A modo de resumen, en la tabla se muestran los parámetros utilizados en la sección [printers].

Opciones más utilizadas de smb.conf (sección printers).

Parámetro.	Comentario.
------------	-------------


```
# apt-get install gksu python-gtk2 python-glade2
```



system-config-samba

2.5.- Cliente.

Además de actuar como servidor de ficheros, el equipo puede utilizarse como cliente para acceder a los recursos compartidos que hay en otros servidores.

Existen varias formas para acceder desde GNU/Linux a carpetas e impresoras compartidas. La forma más sencilla es mediante dos programas cliente que vienen en la instalación de Samba: smbclient y smbprint. Aunque esta solución funciona, está algo limitada, particularmente en el acceso a ficheros. Smbclient proporciona una forma similar a un servidor FTP para acceder a un recurso remoto compartido. No permite el uso de comandos normales de Unix como cp y mv para manipular los ficheros y, por lo tanto, no permite acceder a los recursos compartidos de otras aplicaciones (a diferencia de los sistemas de ficheros remotos montados con NFS, que aparecen para las aplicaciones GNU/Linux como sistemas de ficheros locales).



Este problema se puede evitar montando el sistema de ficheros compartidos samba en GNU/Linux, como se hace con sistemas de ficheros NFS y locales.

La forma más sencilla de acceder a un recurso compartido de Samba es montarlo en una carpeta y así poder acceder al contenido del recurso de la misma forma que lo haces con cualquier otra carpeta del sistema.

Para montar el recurso primero hay que crear la carpeta donde se va a montar el recurso y luego ejecuta el comando mount.

```
$ mkdir /prueba $ mount -t cifs -o user=usuario,pass=contrasena //10.0.0.1/recurso /pru
```

Donde:

- ✓ -t cifs. Indica el tipo de ficheros que se va a utilizar que en este caso es cifs.
- ✓ -o user=usuario,pass=contrasena. Indica el nombre del usuario y la contraseña con la quiere acceder.
- ✓ //10.0.0.1/recurso. Indica la dirección IP y el nombre del recurso al que quieres acceder.
- ✓ /prueba. Es el directorio donde se va a montar el recurso compartido.

Para ver si se ha montado correctamente el recurso puedes ejecutar el comando mount o entrar en la carpeta y ver su contenido.

Para que el recurso se monte automáticamente al iniciar el equipo hay que añadir al fichero /etc/fstab la siguiente línea:

```
//10.0.0.1/recurso /prueba cifs rw,username=login,password=pass 0 0
```

Donde username y password especifican el nombre y la contraseña del usuario con el que acceder al servidor.

Datos más importantes del servicio Samba.

Nombre del servicio:	samba4
Fichero de configuración:	/etc/samba/smb.conf
Comandos más utilizados:	smbpasswd smbclient pdbedit mount
Puertos utilizados:	137/UDP, 138/UDP, 139/TCP y 445/TCP

3.- NFS.



Caso práctico

Ana visita a Juan porque tiene un problema

-Juan, tengo que hacer que dos servidores compartan información entre sí y he pensado en utilizar SAMBA tal y como me enseñaste hace poco. ¿Es la mejor opción?

-Samba esta pensado para compartir carpetas e impresoras entre equipos Windows. Si ambos equipos son GNU/Linux lo mejor es que utilices NFS que es un servicio mucho más seguro. Mira te enseño a utilizarlo, ¡es muy fácil!



NFS (Network File System) es un servicio que permite que los equipos GNU/Linux puedan compartir carpetas entre sí. El servicio NFS se basa en el modelo cliente/servidor de forma que un servidor comparte una carpeta para que los clientes puedan utilizarla. De esta forma, una vez que un cliente monta una carpeta compartida puede utilizarla normalmente; como si se tratara de una carpeta del sistema de ficheros local.



Para instalar el servicio nfs debes ejecutar:

```
# apt-get install nfs-kernel-server nfs-common portmap
```

Antes de iniciar la configuración hay que iniciar el servicio ejecutando:

```
# service nfs-kernel-service start
```

3.1.- Compartir una carpeta.

Para indicar los directorios que se desean compartir hay que modificar el fichero `/etc/exports` de la siguiente forma:

```
<directorio> <IP>(permisos) <IP>(permisos)...
```

Los permisos que se pueden establecer son: `rw` (lectura y escritura) y `ro` (lectura). Por ejemplo, para compartir la carpeta `/datos` para que el equipo `192.168.20.9` pueda acceder en modo lectura y escritura, y el equipo `192.168.20.8` tan sólo pueda acceder en modo lectura se escribe:

```
/datos 192.168.20.9(rw) 192.168.20.8(ro)
```

La carpeta se comparte solamente a la IP establecida en el fichero `/etc/exports` por el usuario `nfsnobody`.

De forma que la carpeta que estas compartiendo tiene que tener los permisos para el usuario `nfsnobody`. Para establecer los permisos ejecuta:

```
# chmod 660 /datos -R # chown nfsnobody  
/datos -R # chgrp nfsnobody /datos -R
```

Como el usuario `nfsnobody` tiene un UID y GID diferente en cada equipo es recomendable asignarle el mismo identificador modificando los ficheros `/etc/passwd` y `/etc/groups` tanto en los equipos clientes como servidores.

Una vez compartida la carpeta, reinicia el servicio ejecutando:

```
# service nfs-kernel-service restart
```

3.2.- Configuración del cliente.



Para acceder al directorio que comparte el servidor hay que montarlo, ya sea manualmente, o automáticamente al iniciar el equipo.



Para montar el sistema de ficheros en el cliente hay que ejecutar:

```
# mount 192.168.20.100:/datos /prueba
```

Donde:

- ✓ 192.168.20.100:/datos es la carpeta que se ha compartido en el servidor en el fichero /etc/exports.
- ✓ /mnt/trabajo es la carpeta donde se monta la carpeta compartida.

Si deseas montar la carpeta automáticamente al iniciar el sistema, hay que modificar el fichero /etc/fstab añadiendo la siguiente línea:

```
192.168.20.100:/datos /prueba nfs rw,hard,intr 0 0
```

Donde:

- ✓ rw. Indica que se monta el directorio en modo lectura/escritura. Para montarlo sólo en modo lectura escriba ro.
- ✓ hard. Indica que si al copiar un fichero en la carpeta compartida se pierde la conexión con el servidor se vuelva a iniciar la copia del fichero cuando el servidor se encuentre activo.
- ✓ intr. Evita que las aplicaciones se queden "colgadas" al intentar escribir en la carpeta si no se encuentra activa.

Datos más importantes del servicio NFS.

Nombre del servicio:	nfs
Carpetas compartidas:	/etc/exports
Comandos más utilizados:	mount
Puertos:	2049/TCP y 2049/UDP



Autoevaluación

¿Qué servicios permite compartir datos con otro equipo Linux?

Telnet.
Samba.
NFS.

4.- Acceso remoto al sistema.



Caso práctico

-Pufff, Hemos puesto el servidor en la planta de arriba y cada vez que tengo que instalar algo tengo que subir a realizar la tarea. ¡Estoy cansada de tantas escaleras!

-¿Por qué no lo haces de forma remota?

-¿Cómo se hace eso?

-Muy fácil, nos conectamos por ssh o por vnc al equipo y lo utilizamos directamente desde cualquier ordenador. Cuando terminemos el café, vamos y te enseño.



Los servicios más utilizados para acceder de forma remota a un sistema GNU/Linux son:

- ✓ Telnet. Permite acceder al sistema de forma remota de una manera no segura.
- ✓ Open SSH. Permite acceder al sistema por terminal, pero de forma segura ya que se cifran las comunicaciones.
- ✓ VNC. Mientras que los servicios telnet y SSH permiten conectarse al servidor por medio de un terminal, el servidor VNC permite utilizar el servidor utilizando el escritorio instalado en el sistema: GNOME o KDE.

4.1.- SSH.

SSH es un protocolo que permite conectarse de forma segura a un servidor para poder administrarlo. En realidad, es más que eso, ya que se ofrecen más servicios como la transmisión de ficheros, el protocolo FTP seguro e, incluso, se puede usar como transporte de otros servicios.

El protocolo SSH garantiza que la conexión se realiza desde los equipos deseados (para lo que usa certificados) y establece una comunicación cifrada entre el cliente y el servidor, mediante un algoritmo de cifrado robusto (normalmente con 128 bits) que se utilizará para todos los intercambios de datos.



Página oficial openSSH.

A continuación vas a ver cómo instalar y configurar el servicio OpenSSH por ser el servidor SSH más utilizado.

Al ser SSH el mecanismo más frecuente para acceder a un servidor, OpenSSH se instala por defecto al realizar la instalación del sistema. No obstante puedes realizar la instalación de OpenSSH ejecutando:

```
# apt-get install ssh
```


E iniciar el servicio ejecutando:

```
# service ssh start
```

Finalmente, si deseas que el servicio se ejecute automáticamente al iniciar el sistema ejecutarás:

```
# chkconfig ssh on
```



Para saber más

Para evitar los ataques de fuerza bruta, una de las mejores soluciones es utilizar fail2ban. Si utilizas fail2ban cuando se realizan 5 intentos fallidos de autenticación en el sistema, fail2ban se comunica con el cortafuegos iptables y bloquea tu dirección IP.

fail2ban.



Adobe Flash Player is no longer supported

Resumen textual alternativo

4.1.1.- Configuración.

El servidor openSSH utiliza el fichero de configuración `/etc/ssh/sshd_config` y normalmente no es necesario modificarlo. Los parámetros más importantes son:



- ✓ Port y ListenAddress. Por defecto el servicio ssh trabaja en el puerto 22 y responde por todas las interfaces del sistema. Los siguientes parámetros permiten cambiar el puerto y la dirección, en las que atenderá peticiones:

```
Port 22 ListenAddress 0.0.0.0
```

- ✓ PermitRootLogin. Establece si se permite o no el acceso del usuario root al servidor.

```
PermitRootLogin no
```

- ✓ AllowUsers. Permite restringir el acceso a los usuarios del sistema. Al utilizar el parámetro AllowUsers indica los usuarios que puedan acceder al sistema.

```
AllowUsers cesar sonia
```

También es posible indicar el equipo anfitrión desde el que pueden conectarse. En el siguiente ejemplo sólo los usuarios cesar y sonia pueden conectarse al servidor desde el equipo 10.0.0.2.

```
AllowUsers cesar@10.0.0.2 sonia@10.0.0.2
```

- ✓ Mensajes de entrada y conexión:

```
PrintMotd yes Banner /etc/issue.net
```

- ✓ Configuración de seguridad y control de acceso:

```
IgnoreUserKnownHosts no GatewayPorts  
no AllowTcpForwarding yes
```

- ✓ Uso de subsistemas para otras aplicaciones, como por ejemplo, FTP.

```
Subsystem sftp /usr/lib/openssh/sftp-server
```

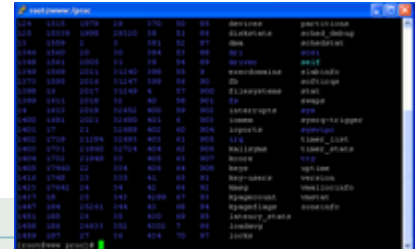
Una vez configurado el servidor, para que se apliquen los cambios, debes ejecutar:

```
# /etc/init.d/ssh restart
```

4.1.2.- Cliente ssh.

Cuando se trabaja con servidores lo normal es administrarlos de forma remota a través de SSH o Webmin. Si utilizas un equipo Linux y quieres conectarte al servidor tan sólo hay que ejecutar:

```
$ ssh <equipo>
```



Conexión remota por SSH con PuTTY.

Donde equipo puede indicar el nombre del equipo o la dirección IP del mismo.

Si utilizas Windows y quieres conectarte al servidor en GNU/Linux lo mejor es utilizar la aplicación PuTTY.

Putty.

El comando scp permite copiar ficheros en equipos remotos a través de ssh scp /etc/passwd 10.0.0.2:/root.



Para saber más

Es posible configurar el servidor para permitir la utilización de los comandos ssh y scp sin necesidad de escribir la contraseña. Para más información visita la siguiente página.

SSH y SCP sin contraseña.

Datos más importantes del servicio SSH.

Nombre del servicio:	sshd
Fichero de configuración:	/etc/ssh/sshd_config
Host a los que se les permite el acceso:	/etc/hosts.allow

Equipos autorizados para acceder por SSH sin contraseña:	\$HOME/.ssh/authorized_keys
Comandos más utilizados:	ssh, scp y sftp
Puerto utilizado:	22/TCP

4.2.- VNC.

VNC es un programa con licencia GPL que utiliza el modelo cliente/servidor y permite acceder a un equipo remoto utilizando su entorno gráfico.

Para realizar la instalación del servidor vnc debes realizar los siguientes pasos:

- ✓ Instala el servidor de vnc ejecutando:

```
# apt-get install tightvncserver
```

- ✓ Indica la contraseña del servidor vnc ejecutando el comando:

```
# vncpasswd
```

- ✓ Ejecuta el siguiente comando para crear automáticamente los ficheros de configuración e iniciar el servicio:

```
# vncserver
```



Datos más importantes del servicio VNC.

Nombre del servicio:	vncserver
Fichero de configuración:	/etc/sysconfig/vncservers
Comandos más importantes:	vncpasswd vncserver
Puertos:	6000/tcp, 6001/tcp, 6002/tcp y 6003/tcp.

4.2.1.- Cliente.

Para acceder al servidor puede utilizar cualquier cliente VNC. Por ejemplo, en sistemas GNU/Linux puede utilizar Vinagre y en sistemas Windows puede utilizar tightVNC.

Vinagre (GNU/Linux).

Si quieres acceder desde un equipo GNU/Linux a un servidor VNC, la mejor opción es utilizar el cliente vinagre. Para utilizar vinagre primero debes instalarlo ejecutando.

```
# apt-get install vinagre
```



Acceso al servidor por VNC con Vinagre.

Ve al menú Aplicaciones, Internet y ejecuta la aplicación Remote Desktop Viewer. Pulsa el botón Connect, indica la dirección del servidor VNC (por ejemplo, 10.0.0.1:5901) y pulsa Connect para acceder al servidor VNC.

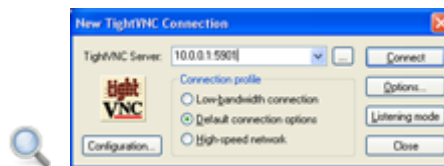
tightVNC (Windows).

tightVNC es un cliente/servidor VNC que se encuentra licenciado bajo GPL. Para acceder desde Windows al servidor VNC debe realizar los siguientes pasos:

- ✓ Descárgate tightVNC.

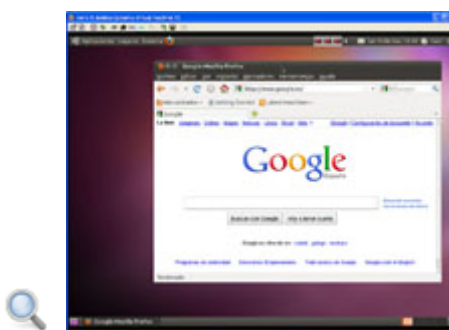
tightVNC.

- ✓ Instala en el equipo el visor tightVNC.
- ✓ Ejecuta tightVNC Viewer que puedes encontrar dentro del menú de aplicaciones tightVNC.
- ✓ En tightVNC Server indica la dirección IP del servidor y el puerto (por ejemplo, 10.0.0.1:5901).



tightVNC conexión.

- ✓ Finalmente, pulsa el botón Connect, introduce la contraseña del servidor VNC establecida durante el proceso de instalación y ya tienes acceso al escritorio del servidor.



Acceso al servidor VNC con tightVNC viewer.



Adobe Flash Player is no longer supported

Resumen textual alternativo



Autoevaluación

Indica la opción incorrecta.

- El servicio SSH permite el acceso remoto a través de un terminal.
- El servicio VNC permite conectarme a un equipo de forma gráfica.
- El servicio Telnet es seguro.
- El programa tightVNC permite conectarme a un equipo Windows.

5.- Servidor Web.



Caso práctico

-Para mejorar la imagen de la empresa vamos a tener nuestro propio servidor web. Hasta ahora estábamos utilizando un servidor externo pero como vamos a incorporar muchos nuevos servicios, vamos a utilizar el nuestro. Juan necesito que hagas tú esa tarea.

-De acuerdo, pero he visto que hay muchos servidores web ¿Cuál utilizo?

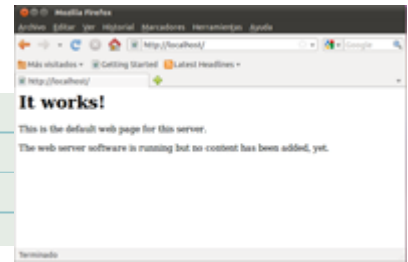
-Aunque hay muchos servidores web, con diferencia, el más utilizado es Apache. Así que lo mejor es instalar Apache en el servidor. Además, es muy sencillo y permite



realizar un montón de tareas con él.

Para instalar el servidor Apache fácilmente desde repositorios ejecuta el comando:

```
# apt-get install apache2
```



Página web de prueba de Apache .

El servicio se inicia automáticamente:

```
# chkconfig apache2 on
```

Para iniciar ahora el servicio:

```
# service apache2 start
```

Una vez instalado, apache publica automáticamente el contenido del directorio /var/www. De esta forma, para publicar una página web debes crearla en dicho directorio.

Para acceder a la web principal del servidor escribe en la barra de direcciones `http://localhost/` o `http://dirección_ip/`:



Adobe Flash Player is no longer supported

Resumen textual alternativo

5.1.- Instalar módulo php.

PHP es un lenguaje de programación interpretado por el servidor de páginas web de forma que éstas se pueden generar de forma dinámica. PHP no sólo se utiliza para este propósito, sino que además se puede utilizar desde una interfaz de línea de comandos o para la creación de aplicaciones con interfaces gráficas.



Para saber más

En la dirección web oficial del proyecto puedes encontrar una amplia documentación sobre el lenguaje: manuales, sintaxis utilizada, interfaz para la programación de las aplicaciones, etcétera.

Sitio oficial de PHP.

Para instalar PHP automáticamente ejecuta:

```
# apt-get install php5
```



Ejecución de phpinfo().

Para comprobar que PHP se ha instalado con éxito puedes crear un fichero php y ubicarlo en el directorio raíz del servidor web. Por ejemplo para mostrar toda la información útil disponible y detalles sobre la instalación actual de PHP, edita el fichero `/var/www/info.php`.

```
# nano /var/www/info.php
```

El contenido del fichero incluye una sentencia para ejecutar la función `phpinfo()` que permite obtener la información sobre el módulo php.

```
<?php phpinfo(); ?>
```

Así, al ejecutar el fichero en una petición HTTP el servidor lanza la sentencia y muestra el contenido solicitado, de forma dinámica. Antes de probar a ejecutar este fichero reinicia el servidor Apache:

```
# service apache2 restart
```

Ahora sí, inicia un navegador web y escribe en la barra de direcciones `http://localhost/info.php`. Como puedes ver en la siguiente figura, PHP se encuentra correctamente instalado. Si observas

con detenimiento la información mostrada puedes ver, por ejemplo, que trabaja a través de Apache, los módulos actualmente habilitados, etcétera.

5.2.- Configuración.

La configuración de apache se almacena en el directorio de configuración /etc/apache2. A continuación se van a ver las opciones de configuración más utilizadas para cada uno de los ficheros:

- ✓ /etc/apache2/ports.conf. Permite establecer los puertos de escucha para las comunicaciones http normales (puerto 80) y las comunicaciones seguras https (puerto 443).

```
Listen *:80 Listen *:443
```



- ✓ /etc/apache2/apache2.conf. Una de las opciones más importantes es que se puede establecer el usuario y grupo al que pertenecen los procesos que ejecuta el servidor:

```
User www-data Group www-data
```

Apache almacena en la carpeta /etc/apache2/sites-available la configuración de cada uno de los sitios web de apache. Por defecto se encuentran los sitios default y default-ssl. Cada sitio tiene la siguiente estructura:

```
<VirtualHost *:80> ServerAdmin servermaster@localhost # Servername
www.miempresa.com # comentado en default DocumentRoot /var/www
DirectoryIndex index.html default.html </VirtualHost>
```

Donde:

- ✓ ServerAdmin es el correo electrónico del administrador del sitio web.
- ✓ Servername es el nombre FQDN del sitio web. Para el dominio default no se indica ningún nombre, pero para atender peticiones específicas de dominios (por ejemplo, www.miempresa.com) sí se debe establecer.
- ✓ DocumentRoot. Indica la ubicación donde se encuentra las páginas web del sitio.
- ✓ DirectoryIndex. Indica el nombre de los ficheros que envía por defecto el servidor web.

Nuevo sitio

Por defecto el servidor web publica el directorio /var/www/ para todos los dominios pero es posible personalizar de forma independiente cada dominio. Por ejemplo, para añadir el dominio www.miempresa.com que se aloja en la carpeta /portales/miempresa hay que crear el fichero /etc/apache2/sites-available/miempresa.com con el siguiente contenido:

```
<virtualhost *:80> ServerName www.miempresa.com  
DocumentRoot /portales/miempresa </virtualhost>
```

Activar el sitio

```
# a2ensite miempresa.com
```

Y reiniciar el servidor web

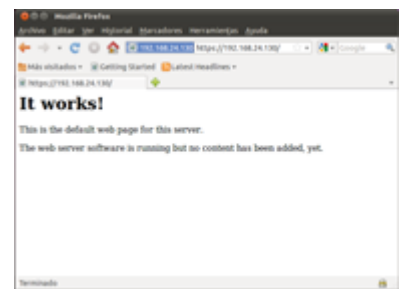
```
# service apache2 restart
```

Lógicamente para que el servidor web atienda un determinado dominio la entrada DNS (por ejemplo, www.miempresa.com) debe apuntar al servidor web.

Sitio seguro (https).

Con el auge de los negocios en Internet se ha popularizado el uso de comunicaciones cifradas entre los clientes y el servidor Web, siendo la tecnología de encriptación más utilizada el Security Socket Layer (SSL).

Para poder utilizar una página segura bajo https hay que realizar los siguientes pasos:



Acceso al servicio https.

- ✓ Activar el módulo ssl:a1
- ✓ Activar el sitio default-ssl aunque si quieres puedes crear un nuevo sitio web:a2
- ✓ Reiniciar el servidor web:a3

Una vez finalizado el proceso, accede a un navegador web y escribe https://IP_Servidor.

Puedes generar tu propio certificado de seguridad utilizando el comando open-ssl.



Para saber más

Para aprender a realizar más operaciones sobre Apache es recomendable que consultes la web www.adminso.es

www.adminso.es

Por último, para iniciar y parar el servidor web puedes utilizar el comando service de forma que si quieres iniciar el servicio ejecuta:

```
# service apache2 start
```

Además, puedes parar el servicio (stop), reiniciarlo (restart) o volver a cargar la configuración (reload).

Datos más importantes del servidor Apache.

Nombre del servicio:	apache2 (Ubuntu)
Fichero de configuración:	/etc/httpd/conf/httpd.conf
Directorio web:	/var/www (Ubuntu)
Comandos más utilizados:	htpasswd
Puertos:	80/tcp y 443/tcp

6.- Servidor FTP.



Caso práctico

Carlos va a ver a Juan porque tiene un problema.

-Hoja Juan, mira, tengo un problema y es que ya he hecho la web de la empresa pero no sé cómo subirla al servidor. ¿Cómo se hace? ¿Te la mando por correo?

-No, no hace falta el correo. ¡Es mucho más fácil! Mira, voy a instalar el servidor FTP y así podrás conectarte y actualizar la web de la empresa cuando quieras,

-Genial, ¡vamos a ver cómo lo haces!



Vsftpd (Very Secure FTP) es un servidor FTP muy pequeño y seguro. Para instalar el servidor FTP en el sistema debes de instalar el paquete vsftpd (Demonio FTP muy seguro). Puedes realizar la instalación a través de la línea de comandos o a través de synaptic.



```
# apt-get install vsftpd
```

Una vez instalado el paquete debes iniciar el servicio ejecutando:

```
# service vsftpd start
```

Para comprobar que el servidor está funcionando correctamente puedes conectarte al servidor:

```
$ ftp localhost Connected to localhost (127.0.0.1). 220 (vsFTPd 2.3.0) Name  
(localhost:root): usuario 331 Please specify the password. Password: 230 Login success  
Have fun. Remote system type is UNIX. Using binary mode to transfer files. ftp> ls 200  
PORT command successful. Consider using PASV 150 Here comes the directory listing.  
rw-r--r-- 1 1003 1003 179 Mar 15 18:00 examples.desktop 226 Directory send OK. ftp> c  
221 Goodbye.
```

Si el servidor está correctamente instalado pero no permite el acceso desde el exterior, es muy posible que no tengas el router configurado para dejar pasar el tráfico del servidor FTP.



Para saber más

Para aprender a configurar y a proteger el servidor vsftpd es recomendable que consultes la web www.adminso.es.

www.adminso.es

Nunca configures el servidor FTP para permitir el acceso anónimo ni permitas la escritura sin enjaular a los usuarios del sistema.

Datos más importantes del servidor VSFTP.

Nombre del servicio:	vsftpd
Fichero de configuración:	/etc/vsftpd.conf

Puerto utilizado:

21/tcp



Adobe Flash Player is no longer supported

Resumen textual alternativo



Autoevaluación

Indica la opción incorrecta.

El servidor Apache trabaja normalmente en los puertos 80 y 443.

El servidor FTP trabaja normalmente en el puerto 21.

El servidor Apache trabaja normalmente en los puertos 80 y 445.

El servidor FTP puede trabajar en el puerto 44.

Anexo I.- Configuración de iptables.

Iptables puede manejar varias tablas, pero las más importantes son:

- ✓ **Filter.** Es la tabla predeterminada que permite el filtrado de las comunicaciones. La tabla Filter está compuesta por tres pilas:
 - **INPUT.** Referencia el tráfico de entrada.
 - **OUTPUT.** Referencia el tráfico de salida.
 - **FORWARD.** Referencia el tráfico que el router reenvía a otros equipos.
- ✓ **NAT.** El servicio que permite dar acceso a Internet a una red interna. Esta tabla permite definir el tipo de comunicaciones entre la red externa y las redes internas. La tabla NAT tiene dos pilas:
 - **POSTROUTING.** Permite establecer las comunicaciones desde la red interna al exterior. Por ejemplo, para hacer que la red interna tenga Internet.
 - **PREROUTING.** Permite establecer las comunicaciones desde la red externa a la red interna. Por ejemplo, se utiliza para que desde el exterior se tenga acceso a un servidor interno.

Los comandos básicos de iptables son:

- ✓ iptables -L. Muestra el estado de la tabla predeterminada (filter). Si quiere ver el estado de la tabla NAT ejecuta iptables -t nat -L.
- ✓ iptables -A <parámetros> -j <acción>. Permite añadir una regla para que el cortafuegos realice una acción sobre un tráfico determinado.
- ✓ iptables -D <parámetros> -j <acción>. Permite quitar una regla del cortafuegos.
- ✓ iptables -F. Limpia la tabla de cortafuegos. Si quieres limpiar la tabla NAT ejecuta iptables -t nat -F.
- ✓ iptables -P <cadena> <acción>. Permite establecer por defecto una acción determinada sobre una pila. Por ejemplo, si quieres que por defecto el router deniegue todo el tráfico de la pila FORWARD ejecuta el comando iptables -P FORWARD DROP.

Como se ha comentado antes, con el comando iptables -A <parámetros> -j <acción> puedes definir la acción que quieras que realice el cortafuegos con un determinado tráfico. En la tabla 10-1 puedes ver los parámetros que se utilizan para especificar el tráfico.

Las acciones que se pueden realizar en la tabla FILTER son:

- ✓ -j ACCEPT. Acepta el tráfico.
- ✓ -j DROP. Elimina el tráfico.
- ✓ -j REJECT. Rechaza el tráfico e informa al equipo de origen.
- ✓ -j LOG --log-prefix "IPTABLES_L". Registra el tráfico que cumple los criterios en /var/log.

Las acciones que se pueden realizar en la tabla NAT son:

- ✓ -j MASQUERADE. Hace enmascaramiento del tráfico (NAT) de forma que la red interna sale al exterior con la dirección externa del router.
- ✓ -j DNAT --to <ip>. Se utiliza para que desde el exterior se tenga acceso a un servidor que se encuentra en la red interna.

Tabla 10.1. Parámetros para especificar las reglas de iptables.

Tabla 10.1. Parámetros para especificar las reglas de iptables.

Elemento.	Sintaxis.	Ejemplo.	Descripción.
Interfaz.	-i <interfaz>	-i eth0	Interfaz de entrada.
	-o <interfaz>	-o eth1	Interfaz de salida.
Dirección.	-s <dir_red>	-s 10.0.0.0/24	Red de origen.
	-d <dir_red>	-d 0/0	Red de destino.
Puerto.	-p <tipo>	-p TCP	Tipo de protocolo. Las opciones son: TCP, UDP o ICMP.
	--dport <puerto>	-p TCP --dport 80	Indica el puerto de destino. En el ejemplo de hace referencia al puerto de destino http (80/TCP).
	--sport <puerto>	-p UDP --sport 53	Indica el puerto de origen. En el ejemplo se hace referencia al puerto de destino

			DNS (53/UDP).
Estado.	-m state --state <tipo>	-m state --state ESTABLISHED	Indica el estado de la conexión. Los posibles estados son: NEW, INVALID, RELATED y ESTABLISHED.
Acción.	-j <acción>	-j ACCEPT	Indica la acción que se va a realizar con un determinado tráfico. Las posibles acciones son: ACCEPT, DROP, REJECT, LOG, DNAT y MASQUERADE.

De esta forma puedes "jugar" con los parámetros de una determinada regla para poder especificar la acción que se aplica. A continuación puedes ver tres reglas, para permitir el tráfico que reenvía el router, que van desde la más general a la más específica:

- ✓ iptables -A FORWARD -j ACCEPT. Permite todo el tráfico.
- ✓ iptables -A FORWARD -s 192.168.0.0/24 -j ACCEPT. Permite sólo el tráfico de la red interna 192.168.0.0/24.
- ✓ iptables -A FORWARD -s 192.168.0.0/24 -p TCP -dport 80 -j ACCEPT. Permite sólo el tráfico de la red interna 192.168.0.0/24 en el puerto 80.



Para saber más

Si deseas bloquear comunicaciones por su país de origen te recomiendo que visites la página web ipinfodb.com.

ipinfodb.com

Una vez configurado el cortafuegos para guardar la configuración ejecuta:

```
# iptables-save >/etc/iptables.rules
```

Donde el fichero /etc//iptables.rules guarda la configuración de iptables. Si lo deseas puedes modificarlo directamente y cargar su configuración ejecutando:

```
# iptables-restore < /etc/iptables.rules
```

Finalmente, modificamos el fichero /etc/network/interfaces y escribimos al final:

```
pre-up iptables-restore </etc/iptables.rules
```

Además de configurar iptables mediante comandos o a través del fichero de configuración, existen interfaces gráficas que facilitan el proceso de configuración. En la siguiente tabla se muestra un listado de las interfaces más utilizadas entre las que destaca Webmin.

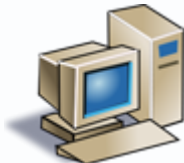

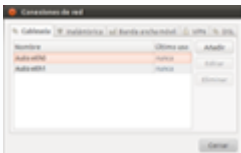
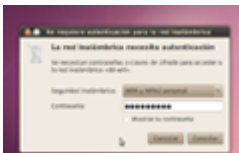
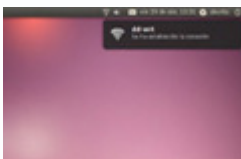

Tabla 10.2. Interfaces gráficas para la configuración del firewall.

Tabla 10.2. Interfaces gráficas para la configuración del firewall.










Dwall.	http://dag.wieers.com/home-made/dwall/
FireHOL.	http://firehol.sourceforge.net/
Firestarter.	http://www.fs-security.com/
Firewall Builder.	http://www.fwbuilder.org/
Guarddog.	http://www.simonzone.com/software/guarddog/
KMyFirewall.	http://kmyfirewall.sourceforge.net/
Shorewall.	http://shorewall.net/
Webmin.	http://www.webmin.com

Anexo.- Licencias de recursos.

Licencias de recursos utilizados en la Unidad de T

Recurso (1)	Datos del recurso (1)	Recurso (2)	
	Autoría: rgtaylor_csc. Licencia: GPL. Procedencia: http://openclipart.org/detail/17668/net-computer-by-rgtaylor_csc		Autoría: Licenc Proce termin Ubuntu
	Autoría: Ubuntu. Licencia: GNU/GPL. Procedencia: Captura de pantalla de la herramienta de configuración de red de Xwindows, propiedad de Ubuntu.		Autoría: Licenc Proce herran inalám Ubuntu
	Autoría: Ubuntu. Licencia: GNU/GPL. Procedencia: Captura de pantalla del escritorio de Ubuntu, propiedad de Ubuntu.		Autoría: Licenc Proce http://c page-i

	<p>Autoría: Ubuntu. Licencia: GNU/GPL. Procedencia: Captura de pantalla del terminal mostrando el comando ping, propiedad de Ubuntu.</p>		<p>Autoría: Licencia: Procedencia: herramienta de propiedad de</p>
	<p>Autoría: HASH(0x89c79d4) / Anonymous. Licencia: GPL. Procedencia: http://openclipart.org/detail/24075/firewall-by-anonymous-24075</p>		<p>Autoría: Licencia: Procedencia: http://openclipart.org/detail/24075/firewall-by-anonymous-24075</p>
	<p>Autoría: isc.org. Licencia: GPL. Procedencia: Captura de pantalla de www.isc.org.</p>		<p>Autoría: Licencia: Procedencia: www.isc.org</p>
	<p>Autoría: warszawianka. Licencia: GPL. Procedencia: http://openclipart.org/detail/35347/tango-system-users-by-warszawianka</p>		<p>Autoría: Licencia: Procedencia: http://openclipart.org/detail/35347/tango-system-users-by-warszawianka</p>
	<p>Autoría: Ubuntu. Licencia: GNU/GPL. Procedencia: Captura de pantalla de la herramienta Imprimiendo propiedad de Ubuntu.</p>		<p>Autoría: Licencia: Procedencia: herramienta de Ubuntu</p>
	<p>Autoría: swat. Licencia: GNU/GPL. Procedencia: Captura de pantalla de la herramienta swat propiedad de SAMBA.</p>		<p>Autoría: Licencia: Procedencia: herramienta de www.samba.org</p>
	<p>Autoría: Ubuntu. Licencia: GNU/GPL. Procedencia: Captura de pantalla de la herramienta Configuración del servidor de Samba propiedad de Ubuntu.</p>		<p>Autoría: Licencia: Procedencia: http://openclipart.org/detail/24075/firewall-by-anonymous-24075</p>
	<p>Autoría: Blog del sensei. Licencia: GPL. Procedencia: Montaje sobre: http://josejuanlt.ipower.com/blogsensei/?p=763</p>		<p>Autoría: Licencia: Procedencia:</p>
	<p>Autoría: Andrew Fitzsimon / Anonymous. Licencia: GPL. Procedencia: http://openclipart.org/detail/25528/text-page-icon-by-anonymous-25528</p>		<p>Autoría: Licencia: Procedencia: aplicación de</p>

	<p>Autoría: tightVNC Software. Licencia: GNU/GPL. Procedencia: http://www.tightvnc.com/</p>		<p>Autoría: Licencia: Procedencia: aplicación</p>
	<p>Autoría: tightVNC. Licencia: GNU/GPL. Procedencia: Captura de pantalla de la aplicación tightVNC, propiedad de tightVNC.</p>		<p>Autoría: Licencia: Procedencia: aplicación tightVNC</p>
	<p>Autoría: Firefox y Apache. Licencia: GNU/GPL. Procedencia: Captura de pantalla del navegador Firefox, propiedad de firefox.</p>		<p>Autoría: Licencia: Procedencia: http://c page-i</p>
	<p>Autoría: Firefox y PHP.org. Licencia: GNU/GPL. Procedencia: Captura de pantalla del navegador Firefox, propiedad de firefox .</p>		<p>Autoría: Licencia: Procedencia: navegador</p>
	<p>Autoría: vsftpd. Licencia: GNU/GPL. Procedencia: vsftpd.beasts.org/.</p>		