Requisitos previos

☒Disponer de los conocimientos sobre redes explicados en el capítulo La red.

☒Disponer de los conocimientos de administración explicados en el capítulo Las tareas administrativas.

☒Tener acceso como root.

☒Estar conectado a una red.

☒Tener la posibilidad de probar los accesos desde otra máquina de la red.

Objetivos

Al final de este capítulo, será capaz de:

☒Manejar/trabajar con las bases de seguridad.

☒Controlar los permisos SUID/SGID.

☒Comprobar la integridad de un sistema de paquetes.

☒Modificar la política de las contraseñas.

☒Gestionar las conexiones y límites de los usuarios.

☒Probar las contraseñas y la presencia de rootkits.

☒Buscar y erradicar virus.

☒Recibir boletines de seguridad.

☒Efectuar actualizaciones de seguridad.

☒Controlar la seguridad de la red con nmap.

☒Parar los servicios inútiles.

☒Proporcionar mayor seguridad a los servicios con los tcp wrappers.

☒Configurar un firewall básico con Netfilter ufw y firewalld.

A. Bases de seguridad

1. Seguridad informática

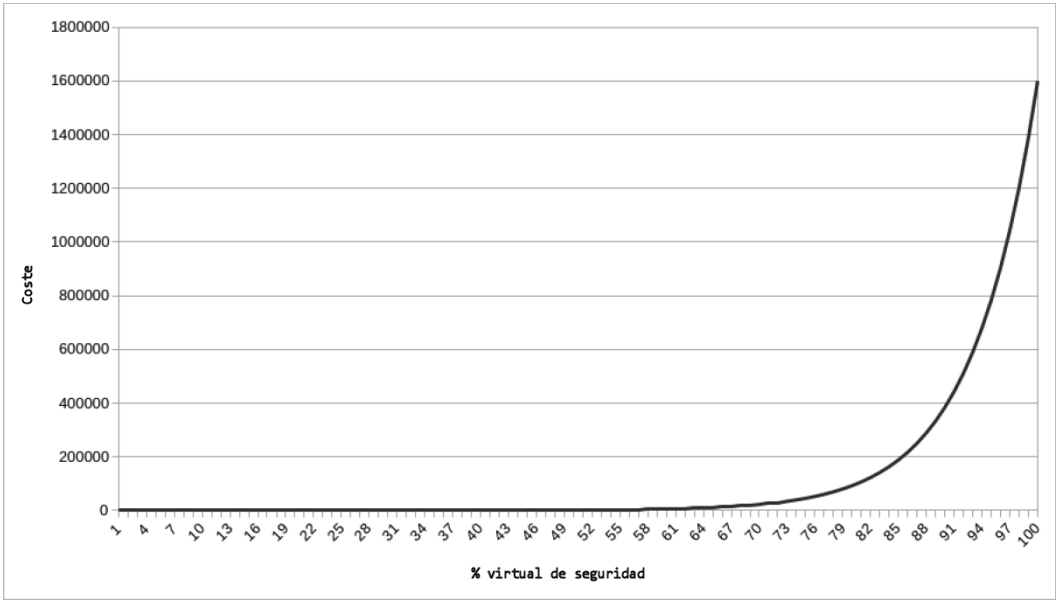
Los principales objetivos de la seguridad informática conciernen a:

- **La seguridad de la conexión**: se trata de controlar que los usuarios que se conectan dispongan efectivamente de la autorización para ello y de prohibirles el acceso al sistema en caso contrario.
- **La integridad de los datos**: se trata de conseguir que los archivos y las bases de datos no estén corruptas y de mantener la coherencia entre los datos.
- **La confidencialidad de los datos**: el acceso a los datos para consulta y modificación se debe limitar únicamente a usuarios autorizados.

Dispone de varios medios:

- La autentificación de los usuarios mediante contraseña.
- El cifrado de los datos.
- La seguridad física controlando el acceso de las personas a las salas informáticas, mediante circuitos físicos inviolables.
- La información relativa a los riesgos penales en los que se incurre en caso de infracción. Un "atraco" informático es un delito, no un juego.
- El control frecuente de los permisos de acceso a los archivos y bases de datos.
- El control de acceso a los servidores y al software.
- El control de los «checksum» de los archivos para asegurar su integridad.
- La copia de seguridad regular de los datos.
- El control de los principales eventos del sistema.
- La instalación de cortafuegos (*firewall*) que controlan los accesos al sistema informático desde el exterior y evitan que los usuarios accedan a servicios externos sin querer o sin necesitarlo y, de esa manera, limitar el riesgo de propagación de virus.
- El uso de firewall de aplicaciones para analizar el tráfico de datos, por ejemplo para detectar los ataques a los servidores web.
- El uso de herramientas de detección y prevención de intrusiones (por correlación de trazas) y el filtrado de direcciones o personas pertinentes.
- El uso de puntos de control para un mejor filtrado de los accesos.
- La instalación de un antivirus, incluso en Linux, si el servidor trata datos desde sistemas operativos susceptibles de tener virus y hacia ellos.
- La instalación de herramientas antispams y antispywares, según el mismo principio, con el fin de evitar una intrusión y la saturación de los servidores de correo electrónico.
- Iniciar únicamente los servicios realmente útiles en el servidor y el cliente.
- Y muchos otros…

La seguridad es también una cuestión de la relación coste/riesgo. Los costes no son proporcionales al nivel deseado, son más bien exponenciales. El gráfico siguiente expone de manera simplificada el problema:



Informe coste/eficacia de la seguridad

La seguridad perfecta no existe. Cuanto mayor sea el nivel de seguridad que se deba obtener, mayor será su coste. Esto implica el tiempo para configurarlo, los productos hay que comprar, las personas hay que emplear y formar…. Debemos encontrar un punto intermedio, usando el sentido común, y por último ser un poco peor que el pirata o el hacker básico. ¿Qué quiere proteger? ¿Opera con datos personales, sensibles, bancarios, de bolsa? ¿O es un simple sitio internet público sin datos sensibles ni acceso a su sistema de información? ¿Debemos caer en la paranoia?

Aquí nos limitaremos a la seguridad que los componentes del sistema nos pueden ofrecer.

Algunos métodos sencillos permiten limitar los riesgos de acceso al sistema, sin un coste significativo:

- Puede definir un valor de umask restrictivo (p. ej.: 077) para extender a continuación los permisos de acceso de algunos archivos.
- No debe apartarse del terminal sin desconectarse o bloquearlo (una buena broma en caso contrario consiste en utilizar el cliente de correo de la persona en cuestión para que le traigan una pizza; después de algún tiempo, el resultado es radical…).
- Hay que prestar atención a las fechas de los últimos inicios de sesión logrados e infructuosos que aparecen en cada conexión.
- No permitir nunca el acceso, incluso en modo de sólo lectura, a los archivos de sesión como .profile.
- Nunca poner el "." en primera posición del PATH, y controlar sus rutas.
- Si los servicios lo autorizan, emplee un entorno de tipo chroot.

- Si es posible, piense en compartimentar (containers docker).
- Verifique las fuentes del software y las firmas de los paquetes.
- Evite fuentes de instalación dudosas.
- Evite las herramientas de crack y hack (generadores de números de serie…) vectores de virus, spyware y otros.
- Utilice un antivirus, de igual forma en Linux.
- Verifique con regularidad los logs de acceso a los equipos.
- Actualice su distribución regularmente.
- Active el firewall por defecto.
- Utilice una contraseña fuerte.
- Favorezca los protocolos seguros (SSH, HTTPS…).
- Utilice claves complejas.

2. Controlar los privilegios especiales

Los privilegios especiales de ejecución (bits SUID y SGID) suelen ser causa de inseguridad en el sistema. En efecto, un usuario malintencionado, aprovechando la falta de atención o la ausencia de un compañero o un administrador que no está desconectado de su consola, puede modificar los permisos de ciertos comandos a su favor. El ejemplo más habitual es el de reescribir un shell como un programa poco usado (por ejemplo sx) y darle los privilegios SUID. Al iniciar este comando, se puede convertir en root.

Obtener el permiso de listar todos los archivos:

```
# chmod u+s cat
```

Obtener un shell root:

```
# cp /bin/sh /bin/sx
# chmod u+s /bin/sx
...
$ sx
# ...
```

El comando siguiente permite buscar todos los archivos que disponen de los bits SUID o SGID:

```
# find / -type f \( -perm -4000 -o -perm -2000 \)
# find / -type f \( -perm -4000 -o -perm -2000 \)
/bin/su
/bin/umount
/bin/eject
/bin/mount
/bin/ping
/bin/ping6
/sbin/unix2_chkpwd
/sbin/unix_chkpwd
/usr/bin/expiry
/usr/bin/write
```

```
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/gnotski
/usr/bin/mahjongg
/usr/bin/chfn
/usr/bin/yset
/usr/bin/wall
/usr/bin/crontab
/usr/bin/v4l-conf
/usr/bin/gnomine
/usr/bin/same-gnome
/usr/bin/gnotravex
/usr/bin/gnobots2
...
```

En la lista anterior, hay un intruso: **`/usr/bin/yset`**, que permite modificar las configuraciones de un servidor de sonido y que no necesita para nada disponer del privilegio SUID. Hay un problema.

```
# ls -l /usr/bin/yset
-rwsr-sr-x 1 root root 604040 may 19 21:28 /usr/bin/yset
# md5sum /usr/bin/yset
04ff72010ff1cf1c14d7706159cdf8bf  /usr/bin/yset
# ls -l /bin/bash
-rwxr-xr-x 1 root root 604040 jan 22  2016 /bin/bash
# md5sum /bin/bash
04ff72010ff1cf1c14d7706159cdf8bf  /bin/bash
```

Alguien ha vuelto a escribir un shell con otro nombre. Éste es un caso experimentado por el autor.

3. Comprobar los paquetes

El capítulo Instalación de Linux y de los paquetes de software ha tratado sobre toda la gestión de los paquetes de software. Entre las diversas opciones, algunas permiten controlar la autenticidad de un paquete. El sistema de paquetería RPM contiene, además del nombre del archivo, su tipo (configuración, binario, etc.) y en algunos casos (binario) la suma de control (checksum) MD5 del archivo. No existe un comportamiento equivalente para dpkg.

Según el ejemplo anterior, ¿cómo restaurar el archivo yset? En tres etapas:

➢Encontrar el paquete de origen:

```
# rpm -qf /usr/bin/yset
yiff-2.14.5-0.pm.1
```

➢Controlar el estado del paquete instalado:

```
# rpm -V yiff
SM5....T    /usr/bin/yset
```

- S: el tamaño no es el correcto
- M: se han modificado los permisos
- 5: la suma de control MD5 es diferente

- T: la fecha de modificación no es la correcta.

➢Vuelva a instalar el paquete de origen según las modalidades propias de su distribución.

4. Política de la contraseñas

Las contraseñas son la base de la autenticación de un usuario. Deben ser seguras. Sin embargo, suele ser la asignatura pendiente, tanto en el trabajo como en casa, e incluso en Internet:

- contraseña escrita en un post-it;
- uso de un gestor de contraseña automático, a su vez sin contraseña;
- misma contraseña para todos los sitios web y software;
- contraseña nunca cambiada;
- misma contraseña o cuenta para a toda la familia/servicio;
- contraseña demasiado sencilla;
- etc.

No sirve de nada caer en la paranoia. Tiene que encontrar un término medio. Si pide a los usuarios que modifiquen su contraseña demasiado a menudo, o si es demasiado difícil, tienden a apuntarla. Si es demasiado fácil y deja pasar demasiado tiempo, ya no es seguro.

Los usuarios deben elegir una buena contraseña, evitando la sencillez o más bien lo evidente: nombres de los hijos, de la esposa, de lugares, fecha de nacimiento y, en general, todo lo que importa y que es conocido del entorno profesional o personal.

Un término medio puede ser modificar las reglas de cambio de contraseña con chage (o passwd), de forma que se establezca una duración para la validez de la contraseña de 40 días. Se han presentado los comandos de modificación de la política de gestión de las contraseñas en el capítulo Las tareas administrativas - Administración de los usuarios.

```
root@ubuntu:~# chage -l jolivares
Último cambio de contraseña                                    : ago 04, 2017
La contraseña caduca                                           : mar 18, 2018
Contraseña inactiva                                            : mar 18, 2018
La cuenta caduca                                               : ene 01, 2019
Número de días mínimo entre cambio de contraseña               : 7
Número de días máximo entre cambio de contraseña               : 4
Número de días de aviso antes de que caduque la contraseña     : 10
```

Los módulos PAM influyen en la política de gestión de las contraseñas, obligando en algunos casos a elegir uno más o menos complejo. Aunque parezca una paradoja, una contraseña debe ser fácil de recordar por un usuario, lo que no implica forzosamente que sea fácil de piratear (por John the Ripper, por ejemplo). Existen contraseñas que se pueden recordar por medios mnemotécnicos. También puede generar contraseñas de manera automática con la herramienta **pwgen**.

```
$ pwgen
uash6She lohJo7ae Ohphab3i ouRik9ie uM4va3im Neer7Eit eib3Hauy xo9Iuy5p
ahSiW0uf AhG6wail Yai6neeh phae4ioV deeL3aip Uz5ahzaa aiV5phee Aegaiy7x
ioPh1ahn Ong6Baib Eish4rip eik9Gie1 ien3Iepe xohduj7U aiP2keov So5ovaht
Voh9oxoe ahs2Meeg Ooch5xix Phe3yiuz eeCa5ohv aig9Ai3o Go4Ateeh Hee6thei
Rai6Daeh aid8ieNg Thah6ien daphaiG0 Iefai5oh Pheife6i Poora8ah Coh5Aida
```

```
ViC7ieth hohG5sei Aa9Jeilu eopoX8Si jooh3Eif dooPhai1 chohqu1G ieNgae3o
wiCeiSi3 aej6Piev eoTha1Fu ieR2yeeb Eireili6 saiGhie2 XohRoo1a cahb2Yah
Guungah0 ube3vo0D oshol3Op Pui6agh5 Ao7baeN1 foTek9Ei aeM3lala Ene2baol
geloV9ai Weeyu2ie Uvae2Vie dei0euL7 Xee9uaza ed8Eeghu eebiu2Ka zey0Liuh
be6Ailoi eiph8Ohb Yahpahr4 aij4dahG oQu2chae Fe5eeg9c Hoosh6oh Iip8eiwe
AuPie0um Ahxai9eo Dae5oquu Ie7Viek8 pa2aew8B fohham7A fah1Oogi ieH9vee8
```

Estas contraseñas son pseudoaleatorias. Si habla inglés (y geek/leet), estas contraseñas representan una pronunciación. Por ejemplo:

```
dooPhai1: Do you fail?
```

Puede pedir que se generen contraseñas totalmente aleatorias con una longitud dada, en este caso de 16 caracteres con al menos un carácter especial:

```
$ pwgen -sy -1 16
"%Eie*0s3KKUa_@T
```

5. Almacenar las contraseñas

¡Ni se le ocurra ponerlas bajo el teclado ni en un post-it pegado a la pantalla! Usted no pone las llaves de su casa debajo de la alfombra o en la maceta que hay junto a la puerta, ¿no es verdad?

Se vuelve complicado recordar todas las contraseñas tanto de los servidores como de los servicios en línea (foros, sitios de comercio electrónico, redes sociales…). Existen herramientas para ayudarle. Los administradores de contraseñas, llamados Password Managers, llaveros, portallaves, monederos, pueden almacenar de forma segura todas sus contraseñas en un solo lugar, a través de una clave, una contraseña maestra o un archivo codificado.

Por lo general, podemos considerar los llaveros proporcionados por los sistemas operativos como relativamente seguros, por supuesto con la condición de que su formato sea codificado, que proporcione una contraseña y que su sesión sea protegida de la misma forma. KDE o Gnome proporcionan estos llaveros.

En entornos empresariales, contar con un puesto de trabajo en Linux es todavía poco frecuente. Se trata por lo general de puestos Windows o Mac OS X. En ese caso, las herramientas de tipo keepass y sus derivados (**keepassx** por ejemplo) son una buena alternativa ya que están disponibles para todos los sistemas operativos.

6. Prohibir las conexiones

a. /bin/false

Algunas cuentas no deben ser interactivas: se deben prohibir las conexiones desde una consola. Se pueden asignar estas cuentas a una aplicación, a un servicio, a una conexión FTP, etc., pero se debería rechazar la conexión: ¡no shell!

En las lista de los shells autorizados, uno llama la atención:

```
$ cat /etc/shells
/bin/ash
/bin/bash
/bin/bash1
/bin/csh
```

Requisitos

Los conocimientos necesarios para la certificación LPIC-1:

☒Nociones de base de redes IPv4 (arquitectura, protocolos y subnetting).

☒Comandos de base de uso de los servicios de red.

Objetivos

Al final de este capítulo, deberá poder:

☒Configurar una interfaz de red, Ethernet o wifi, en IPv4 e IPv6.

☒Implementar diferentes métodos de autenticación de red.

☒Configurar y administrar un sistema con distintas redes.

☒Identificar y resolver los problemas de red más corrientes.

A. Configuración de red

Este tema está dividido en tres partes con pesos diferentes.

1. Configuración básica de redes

Peso	3
Objetivos	Configurar una interfaz de red conectada a una red local, por cable o wifi, o a una red extendida. En particular, configurar subredes en IPv4 e IPv6.

a. Competencias principales

- Configurar y administrar tarjetas Ethernet.
- Configuración básica de redes wifi.

b. Elementos empleados

- `ip`
- `ifconfig`
- `route`
- `arp`
- `iw`
- `iwconfig`
- `iwlist`

2. Configuración avanzada de redes

Peso	4
Objetivos	Implementar diferentes métodos de autenticación de conexión de red. Configurar un sistema incluido en diferentes redes y resolver diferentes problemas de comunicación.

a. Competencias principales

- Gestión de las tablas de enrutamiento.
- Herramientas de configuración y de gestión de interfaces de red Ethernet.
- Herramientas de análisis del estado de las interfaces de red.
- Herramientas de supervisión y de análisis del tráfico TCP/IP.

b. Elementos empleados

- `ip`
- `ifconfig`
- `route`
- `arp`

- ss
- netstat
- lsof
- ping, ping6
- nc
- tcpdump
- nmap

3. Resolución de problemas de red

Peso	4
Objetivos	Identificar y resolver problemas de red corrientes, para ello se necesitará un buen conocimiento de los distintos archivos de configuración y de los comandos de red básicos.

a. Competencias principales

- Archivos de configuración del control de acceso.
- Herramientas de configuración y de gestión de las interfaces de red Ethernet.
- Herramientas de administración de las tablas de enrutamiento.
- Herramientas de supervisión del estado de la red.
- Herramientas de monitoreo de la configuración de red.
- Método para determinar los periféricos de red reconocidos por el sistema operativo y su uso.
- Archivos de configuración de la inicialización del sistema (systemd y init System V).
- Apropiación de NetworkManager y de su rol en la configuración de redes.

b. Elementos empleados

- ip
- ifconfig
- route
- ss
- netstat
- /etc/network/, /etc/sysconfig/network-scripts/
- ping, ping6
- traceroute, traceroute6
- mtr
- hostname
- Registros del sistema como /var/log/syslog, /var/log/messages y el registro systemd
- dmesg

- /etc/resolv.conf
- /etc/hosts
- /etc/hostname, /etc/HOSTNAME
- /etc/hosts.allow, /etc/hosts.deny

B. Configuración básica de redes

Linux es un sistema operativo particularmente orientado a redes. La mayoría de los protocolos de redes modernos se encuentran implementados en él, y la mayoría de los servidores de aplicaciones de red corren hoy día Linux.

Este tema de la certificación versa sobre la configuración básica de red de un sistema Linux, con conexiones de tipo Ethernet y wifi en IPv4 e IPv6.

Para conectar una tarjeta de interfaz de red en una red IP hay que especificar, como mínimo, dos o tres parámetros: una dirección IP, una máscara de red y una pasarela por defecto (excepto si se trata de una red estrictamente local).

1. Direcciones IPv4 e IPv6

Existen dos versiones utilizadas del protocolo IP:

- IPv4, la más antigua, con direcciones en 32 bits.
- IPv6, con direcciones en 128 bits.

Un sistema Linux puede trabajar con las dos versiones del protocolo y tener una o varias direcciones para cada uno de los protocolos.

Por otra parte, independientemente de la versión del protocolo IP, puede haber distintas combinaciones entre dirección IP, interfaz de red y sistema:

- Un sistema puede tener una interfaz de red y una dirección IP.
- Un sistema puede tener distintas interfaces de red y distintas direcciones IP.
- Una interfaz de red puede tener una sola dirección IP.
- Una interfaz de red puede tener varias direcciones IP.
- Distintas interfaces de red pueden utilizar solamente una dirección IP.

☞*Tradicionalmente se usa el término dirección IP de host (host address). Este término puede llevar a confusión porque una máquina puede tener distintas interfaces de red, en distintas redes IP, y presentar, por lo tanto, direcciones IP de host diferentes. Se debería decir más bien dirección IP de interfaz de red, aunque, en algunos casos, distintas interfaces de red pueden usar la misma dirección IP.*

2. Configuración básica de una conexión IPv4

a. Red/subred

El protocolo IP (*Internet Protocol*) permite conectar distintas redes entre ellas. Para ello, es necesario disponer de equipos (de hardware o software) que estén integrados en distintas redes y sean capaces de transferir un paquete IP de una red a otra (función de enrutamiento).

Las redes IP están organizadas en tres clases, A, B y C, caracterizadas por el tamaño de su identificador de red: 1 byte para la clase A, 2 bytes para la clase B y 3 bytes para la clase C.

Dos redes IP pueden comunicarse entre ellas si están conectadas por, al menos, un router y atravesando, opcionalmente, una serie de redes y de routers intermediarios.

Cuando el número de redes interconectadas comenzó a ser importante, se tuvo que extender la noción de red para permitir que las organizaciones puedan dividir su red en conjuntos interconectados: las subredes. Estas son las reglas que aseguran la comunicación entre las subredes:

- Las subredes son transparentes para las otras redes, que solamente necesitan conocer el identificador de red y del host de destino en su red para comunicarse con él, sea cual sea su subred.
- Dos subredes de una misma red no pueden comunicarse entre ellas si no están conectadas por, al menos, un router, atravesando opcionalmente una serie de subredes y de routers intermediarios.

Para identificar las diferentes subredes, se usa una parte del identificador de red del host además de su identificador de red. Por lo tanto, leyendo una dirección IP no se puede saber a qué subred pertenece. Hay que configurar un dato suplementario: el número de bits de la parte de red/subred de la dirección. Este parámetro se llama **máscara de subred** (*subnet mask*).

En la documentación se pueden encontrar distintos términos para máscara de red (*net mask*) o máscara de subred (*subnet mask*). Son equivalentes, el primero es más antiguo y viene de la época en que las subredes se utilizaban muy poco.

☞*Más generalmente, también se pueden agregar distintas redes entre ellas, para organizar una especie de subred, división lógica en redes. En ese caso se habla de direcciones CIDR (Classless Inter Domain Routing).*

b. Dirección IP

Se trata de la dirección IP clásica, en 32 bits. Está dividida en dos partes: la dirección de red/subred, seguida de la dirección del host. La dirección de red/subred identifica la red/subred en la que está integrado el host, la dirección de red de host identifica de manera única un elemento de red que está integrado en una red/subred.

El reparto de los 32 bits de la dirección de red entre la parte de red/subred y la parte host es variable y está definido por la máscara de subred.

Se puede especificar una dirección IPv4 usando la sintaxis siguiente:

```
w.x.y.z[/NúmbitsMáscara]
```

Se trata de cuatro valores enteros en notación decimal separados por un punto (notación decimal punteada), especificando la dirección de red propiamente dicha, seguidos, si fuera necesario, de un carácter / y del número de bits de la parte de red/subred, notación llamada CIDR (*Classless Internet Domain Routing*).

c. Máscara de subred

La máscara de subred permite determinar la parte de la dirección de red que identifica la red/subred a la que pertenece la dirección de red.

Se puede escribir de dos maneras:

Notación clásica «máscara de subred» (*subnet mask*): todos los bits del identificador red/subred valen 1, los del identificador del host valen 0.

Notación CIDR: se indica el identificador de red/subred, todos los bits del identificador del host en cero, seguido de un / y del número de bits del identificador de red/subred.

Ejemplo

Para un identificador de red/subred en `10.1`:

Identificador de red/subred: `10.1.0.0` y máscara de subred: `255.255.0.0`

Notación CIDR: `10.1.0.0/16`

d. Pasarela por defecto

Si la red/subred no está conectada a otras redes/subredes, no habrá pasarela por defecto. En caso contrario, la pasarela por defecto designa la dirección IP hacia la que se enviarán los paquetes IP dirigidos hacia otra red/subred. Si este parámetro no está especificado, el host no podrá comunicar a través de esta tarjeta de red con otros hosts de otras redes/subredes.

3. Configuración básica de una conexión IPv6

a. Dirección IPv6

La versión 6 del protocolo IP tiene como objetivo aumentar las funcionalidades del protocolo y atenuar algunas de sus limitaciones. El paso a una dirección de 128 bits permite, en particular, responder al riesgo de escasez de direcciones IP en Internet.

Representación de una dirección IPv6

Una dirección IPv6 tiene un tamaño de 128 bits, es decir 16 bytes. Se representa generalmente bajo la forma de ocho elementos de 2 bytes. El valor de cada elemento está expresado en hexadecimal, y cada elemento está separado por el carácter `:`.

Una simplificación en su escritura consiste en reemplazar una única serie de campos con cero en la dirección de red por dos caracteres de dos puntos seguidos `::` .

Ejemplo

Observemos la dirección IPv6 de un servidor Google:

```
host www.google.com
www.google.com has address 216.58.215.36
www.google.com has IPv6 address 2a00:1450:4007:80c::2004
```

La dirección IPv6 mostrada corresponde a la dirección de red completa siguiente:

2a00:1450:4007:080c:0000:0000:0000:2004

Estructura de una dirección IPv6

Una dirección IPv6 se compone de tres partes, de izquierda a derecha:

- Un prefijo, compuesto por 6 bytes.
- Un identificador de subred, compuesto por 2 bytes.
- Un identificador de host, compuesto por 8 bytes.

Ejemplo

Observemos la dirección IPv6 de un servidor Google:

```
host www.google.com
www.google.com has address 216.58.215.36
www.google.com has IPv6 address 2a00:1450:4007:80c::2004
```

La dirección IPv6 presenta la siguiente estructura:

Prefijo: `2a00:1450:4007`

Identificador de subred: `80c`

Identificador de host: `0000:0000:0000:2004`

Los seis primeros bytes constituyen el prefijo de sitio, e identifican la red dentro de su red.

El campo siguiente, de dos 2 bytes, identifica una subred dentro de su red.

Los ocho últimos bytes identifican el host dentro de su subred.

También se usa esta división:

- Topología pública: está constituida por los seis primeros bytes de la dirección, está definida en relación a una autoridad externa que administra las redes (a menudo se trata del proveedor de acceso a la organización). Una dirección global de red, es decir, enrutable a través de las redes interconectadas, tiene un prefijo de red que empieza por 2 o 3.
- Topología privada: se trata de los diez últimos bytes de la dirección de red y están definidos por la organización responsable de la red interna, que gestiona la división en subredes (prefijo de subred) que reagrupan los hosts.

Identificador de host

La parte del host de la dirección de red (llamada también *token* o identificador de interfaz), compuesta por ocho bytes, se puede definir de distintas maneras:

- Automáticamente a partir de la dirección de red MAC de la interfaz de red que corresponde al host.
- Manualmente, a partir del plan de direccionamiento IP definido por la red privada.

Mapping de una dirección IPv4 en una dirección IPv6

Se puede generar una dirección IPv6 a partir de una dirección IPv4, con el objetivo de facilitar la integración de redes IPv4 en el interior de una IPv6. Esta técnica consiste en crear automáticamente una dirección IPv6, que corresponderá a una dirección IPv4.

Para ello se usa un prefijo particular, seguido de los cuatro bytes de la dirección IPv4:

Los 80 primeros bits de la dirección de red se fijan a 0, los 16 siguientes a 1, lo que nos da: `::ffff:wx:yz` donde `w`, `x`, `y` y `z` representan el valor en hexadecimal de los 4 bytes de la dirección IPv4.