

UNIDAD DIDÁCTICA 5

CONEXIÓN DE SISTEMAS EN RED

**MÓDULO PROFESIONAL:
SISTEMAS INFORMÁTICOS**



CESUR
Tu Centro Oficial de FP

Índice

Resumen introductorio	2
Introducción.....	2
Caso introductorio.....	3
1. Configuración del protocolo TCP/IP en un cliente de red. Direcciones IP. Máscaras de subred. IPv4. IPv6. Configuración estática. Configuración dinámica automática.	4
2. Ficheros de configuración de red.....	8
3. Gestión de puertos.....	16
4. Resolución de conectividad en sistemas operativos en red. Herramientas de diagnóstico.....	18
4.1. Herramientas gráficas y comandos utilizados en sistemas operativos libres y propietarios.	18
4.2 Herramientas gráficas de diagnóstico de red.	20
5. Monitorización de redes.....	23
6. Protocolos TCP/IP	25
7. Configuración de redes	26
7.1. Configuración de los adaptadores de red en sistemas operativos libres y propietarios.....	27
7.2. Interconexión de redes: Adaptadores de red y dispositivos de interconexión. Enrutamiento.....	29
7.3. Redes cableadas. Tipos y características. Adaptadores de red. Conmutadores, enrutadores, entre otros. Seguridad	33
7.4. Redes inalámbricas. Tipos y características. Adaptadores. Dispositivos de interconexión. Seguridad	37
8. Seguridad de comunicaciones.....	40
9. Tecnologías de acceso a redes de área extensa	46
Resumen final	49

RESUMEN INTRODUCTORIO

A lo largo de esta unidad vamos a ver el protocolo de red TCP/IP, desde su concepto a sus características y sus distintos tipos de configuración, así como los ficheros de configuración de red y la gestión de puertos.

Dentro de la conectividad de sistemas operativos en red, estudiaremos su importancia y cómo disponemos de herramientas de diagnóstico que nos facilitan la tarea de comprobar su conectividad y en caso de problemas, resolverlos. Este tipo de herramientas los encontramos tanto en sistemas operativos libres como sistemas operativos propietarios.

Y, en relación con lo anterior, centraremos un apartado al tema de monitorización de redes, conocer su rendimiento y funcionamiento es fundamental, además de haber comprobado su conectividad.

Dentro de los protocolos TCP/IP, que debemos conocer, entraremos en la parte más práctica de como configurar una red, conociendo la configuración de los adaptadores de red y la interconexión de redes con estos dispositivos y las posibilidades de enrutamiento. Diferenciando entre lo que son redes cableadas y redes inalámbricas.

Para finalizar, hablaremos del tema de seguridad de comunicaciones dentro de la interconexión de redes y de las distintas tecnologías de acceso a redes de área extensa, con su concepto y características.

INTRODUCCIÓN

En la Unidad 1 ya tuvimos un primer contacto con las redes de ordenadores, describiendo sus principales componentes, los tipos de redes existentes, sus topologías, los mapas físicos y lógicos... Pero fue simplemente una visión genérica, sin entrar en terreno práctico.

Esta Unidad viene a aportar esa componente práctica. En ella se verá cómo se estructura una red siguiendo unos modelos que permitan interconectarla con otras redes diferentes, cómo se configuran dichos modelos en un dispositivo concreto, sea cual sea su sistema operativo, cómo se gestionan las conexiones de red para sacarles el máximo rendimiento, y cómo se pueden detectar y solucionar los posibles problemas de conectividad que pudieran ir surgiendo.

Todos estos conceptos, tanto teóricos como prácticos, deben ser asimilados por cualquier desarrollador, ya que, hoy en día, prácticamente no se concibe una aplicación

que no esté conectada de algún modo: bien en su propia operativa, bien en su instalación, bien en sus actualizaciones.

CASO INTRODUCTORIO

Te contratan para realizar una aplicación de gestión para una pequeña empresa, y al realizar un primer estudio de necesidades detectas que sus ordenadores no están conectados en red, sino que cada uno de ellos trabaja de forma independiente. Lógicamente quieres que tu aplicación esté diseñada para trabajar en red, así que, tras mostrar a la empresa las ventajas de esta opción, le ofreces como servicio complementario la instalación y configuración de una red local que conecte sus equipos.

Al finalizar la unidad conocerás, las características principales del modelo TCP/IP y serás capaz de configurar una red utilizando este modelo, podrás gestionar los puertos que necesitan sus aplicaciones, y serás capaz de detectar y solucionar, utilizando las herramientas más adecuadas para ello, los posibles problemas que pueden darse en una red de ordenadores.

1. CONFIGURACIÓN DEL PROTOCOLO TCP/IP EN UN CLIENTE DE RED. DIRECCIONES IP. MÁSCARAS DE SUBRED. IPV4. IPV6. CONFIGURACIÓN ESTÁTICA. CONFIGURACIÓN DINÁMICA AUTOMÁTICA.

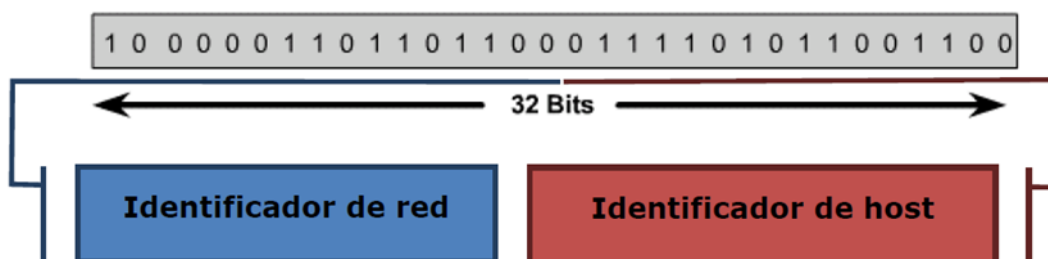
Tras tu propuesta, la empresa ha decidido la instalación de una red informática con los actuales ordenadores, para lo que deberás realizar la configuración del protocolo TCP/IP en los distintos equipos de red donde debes tener en cuenta las direcciones IP, máscaras de subred, etc.

Principales protocolos del modelo TCP/IP.

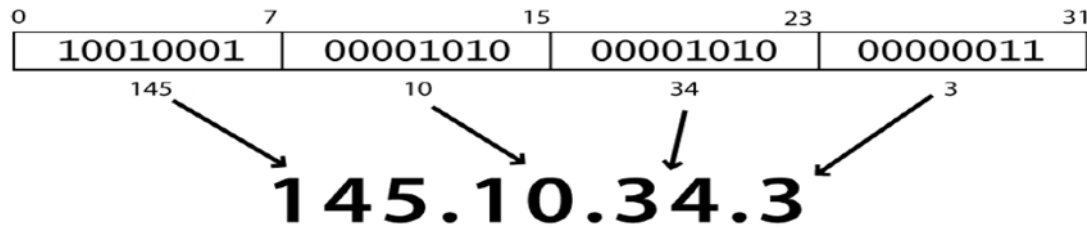
Una **dirección IP** es un número que identifica a un dispositivo (normalmente un ordenador, pero también un teléfono, una tableta, una impresora...) dentro de una red TCP/IP. Dicho número no debe confundirse con la dirección MAC, que es un número hexadecimal fijo asignado al dispositivo de red por el fabricante.

Una dirección IP clásica (**IPv4**) tiene una longitud de 32 bits y consta de dos campos:

- Un campo identificador de red (netid), que identifica la red a la que está conectado el host.
- Un campo identificador de host (hostid), que asigna un identificador único a cada host de una red específica.



Para simplificar su representación, estos 32 bits se dividen en cuatro octetos, que se expresan en sistema decimal separados por puntos. Esta forma de escribir una dirección se conoce como formato decimal con puntos o punteado. El valor decimal de cada octeto puede ir desde 0 a 255.



Dirección IPv4 en formato punteado.

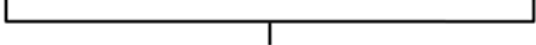
IPv4 se ha venido utilizando con éxito desde los inicios de Internet. Pero en los últimos años ha planteado un grave problema: su **capacidad de direccionamiento** no puede soportar el ritmo de crecimiento de la Red. Hay que tener en cuenta que con 32 bits (dejando aparte el hecho de que no todas las posibles direcciones obtenibles se pueden utilizar, ya que algunas de ellas están reservadas), apenas se pueden direccionar 4000 millones de dispositivos (2^{32}). Se emplean técnicas que permiten ampliar esta capacidad, pero aun así el problema del direccionamiento con IPv4 no se soluciona.


Es por eso que IPv4 se está sustituyendo progresivamente por la nueva versión del protocolo, **IPv6**, que proporciona direcciones de 128 bits. Esto supone una capacidad de direccionamiento de 2^{128} dispositivos, lo que debería resolver el problema por bastantes años.

Las direcciones IPv6 también tienen un formato abreviado, aunque en este caso no se emplean números decimales, sino hexadecimales. Así una dirección IPv6 consta de 8 grupos de 4 dígitos hexadecimales, separados por el signo ":". Cada grupo puede tomar valores entre 0 y FFFF. Los grupos formados únicamente por ceros se pueden omitir, indicándolo con "::".

Una dirección IPv6 (en hexadecimal)

2001:0DB8:AC10:FE01:0000:0000:0000:0000

↓ ↓ ↓ ↓ 
2001:0DB8:AC10:FE01:: Se pueden omitir los ceros


1000000000000001:0000110110111000:1010110000010000:1111111000000001:
0000000000000000:0000000000000000:0000000000000000:0000000000000000

Ejemplo de dirección IPv6.

Fuente: Wikipedia



ENLACE DE INTERÉS

Conoce una visión general del estándar IPV6:



Máscara de subred, puerta de enlace y DNS.

La máscara de subred nos indica qué parte de la dirección IP pertenece a la red, y cuál al equipo. Es por ello por lo que determina el número máximo de equipos de la red. En sistemas de tamaño pequeño se suele utilizar la máscara 255.255.255.0 que corresponde a un rango de 256 direcciones IP (suficientes para cualquier pequeña empresa), en los que todos los dispositivos tienen los tres primeros números de la IP iguales (sería la parte de la red) y solo cambia el último. Lo normal es que todos los equipos de nuestra red tengan configurada la misma máscara de subred.

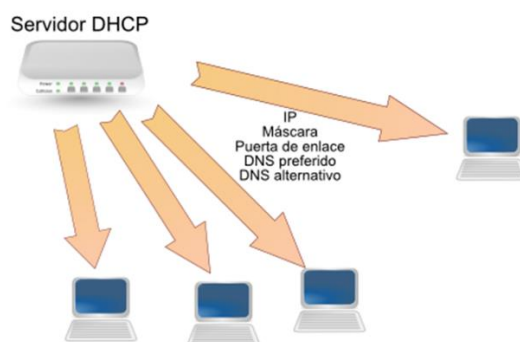
La puerta de enlace es un dispositivo que sirve de enlace entre dos redes. En nuestro caso, entre la red local e Internet. Cuando un dispositivo de una red local quiere acceder a Internet, habrá que indicarle la dirección de la puerta de enlace, que deberá ser una IP del rango ya que, de lo contrario, nuestro PC no será capaz de comunicarse con ella. Lo normal es que todos los PCs de nuestra red tengan configurada la misma puerta de enlace. Si no sabemos la IP de nuestra puerta de enlace, podemos verla en otro PC en el que funcione correctamente la conexión de Internet.

El DNS (servidor de nombres de dominio) es un equipo que se encarga de convertir las direcciones que escribimos cuando queremos acceder a un recurso, por ejemplo, en un navegador web, en las correspondientes direcciones IP de los servidores que contienen dicho recurso. Los DNS preferido y alternativo nos los debe proporcionar la compañía que presta el servicio de Internet. Telefónica, por ejemplo, usa el 80.58.0.33 y el 80.58.32.97. Lo normal es que todos los PCs de nuestra red tengan configurados los mismos DNS así que, como en el caso anterior, si no sabemos la IP de los DNS podemos consultarla en otro PC en que funcione correctamente la conexión de Internet.

DCHP.

Para que los equipos de una red puedan comunicarse es necesario configurar en cada uno de ellos la dirección IP, la máscara de subred, la puerta de enlace, el DNS preferido y el DNS alternativo. Pero si el número de dispositivos de nuestra red es elevado, existe la posibilidad de configurar las direcciones IP de forma automática.

Para que el equipo pueda obtener una dirección IP automáticamente, es necesario que alguien se la proporcione. Ese alguien es un servidor DHCP. La mayoría de los routers ADSL actuales disponen de servidor DHCP. Si activamos dicha función, podríamos configurar IPs de nuestra red de forma automática:



Funcionamiento de un servidor DHCP.



ENLACE DE INTERÉS

Si quieres conocer información adicional sobre DHCP, consulta este enlace:



2. FICHEROS DE CONFIGURACIÓN DE RED

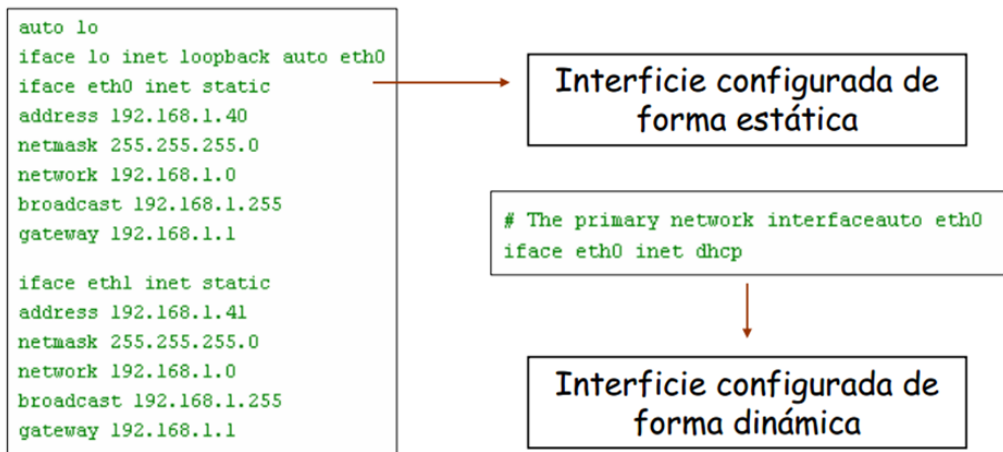
En la configuración de la red en la que estás trabajando, y ante la no disponibilidad de herramientas gráficas para la configuración de la misma, deberás realizar mediante los comandos y ficheros que sean necesarios para un funcionamiento correcto.

Aunque lo habitual es realizar todos los procesos de configuración de una red mediante entorno gráfico, los sistemas operativos disponen de una serie de ficheros en los que se almacena la información de dicha configuración. Conocer estos ficheros resulta muy útil, bien para consultar los datos de nuestras redes, bien para modificarlos de forma manual si queremos agilizar el proceso.

A continuación, se describen los principales archivos de configuración para sistemas Linux.

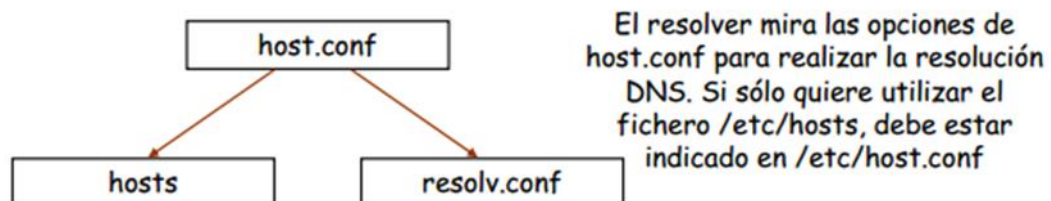
- **ARCHIVO /etc/network/interfaces**

Contiene la información necesaria para configurar las interfaces de red del host al arrancar el sistema. También permite establecer las rutas estáticas hacia otras redes.



Contenido del archivo interfaces.

- **ARCHIVO /ETC/HOSTNAME** contiene el nombre del equipo que adopta el S.O. al iniciar el equipo.
- **FICHERO /ETC/HOST.CONF** indica al sistema de resolución qué servicios debe usar y en qué orden. El fichero host.conf indica el orden de las fuentes que utilizará el resolver del S.O. para obtener las resoluciones DNS que necesiten las aplicaciones del equipo. Tiene dos opciones:
 - Buscarlas dentro: fichero /etc/hosts.
 - Buscarlas fuera: fichero /etc/resolv.conf



Los nombres de las diferentes máquinas accesibles se encuentra aquí

Resolución de servidores.

- **FICHERO /ETC/HOSTS** representa un mecanismo simple de resolución de nombres. Contiene un registro por línea, consistente en una dirección IP, un nombre de máquina y de forma opcional, una lista de alias para esa máquina. Los campos se separan por tabuladores o espacios y el campo con la @ IP debe empezar en la primera columna.

```
# archivo /etc/hosts
#
# IP            FQDN            aliases
#
# definición del bucle local.
127.0.0.1      localhost
#
172.16.1.1     web.dominio.local    web
172.16.1.2     gate.dominio.local   gate
#
172.16.2.1     mail.dominio.local    mail
172.16.2.2     host.dominio.local    host
```

Tanto el nombre con cualificación completa (oficial) como el nombre local se deben registrar en el fichero /etc/hosts, para ser referidos al resolver su dirección IP.

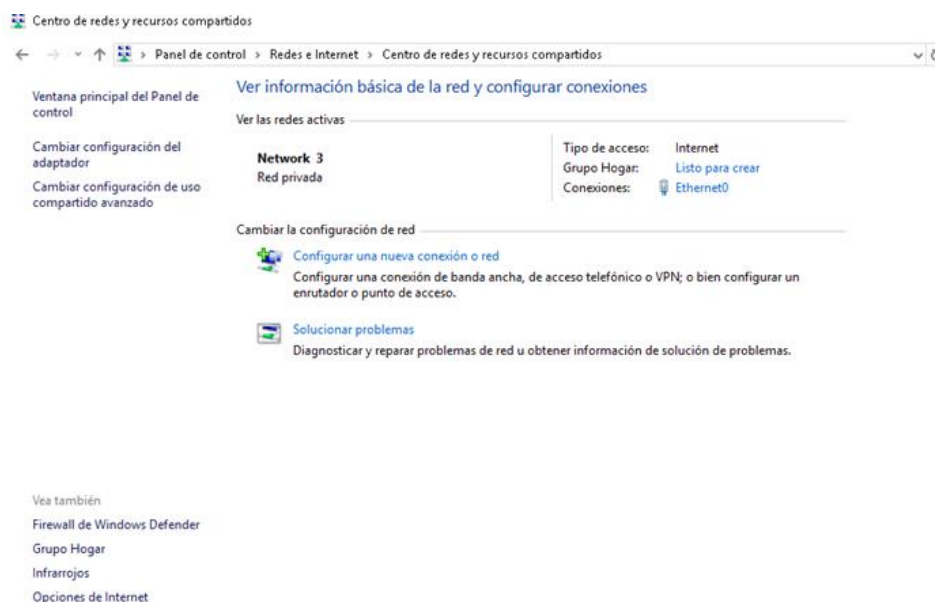
Contenido del archivo hosts.

- **FICHERO /ETC/RESOLV.CONF** contiene las direcciones IP de las máquinas que pueden ofrecer servicios DNS a nuestro host. La instrucción nameserver apunta a servidores DNS que puede utilizar el host para realizar sus resoluciones. El fichero /etc/hosts tiene un compañero llamado /etc/networks, que asocia nombres de red con los números correspondientes y viceversa.

Configuración de TCP/IP en sistemas Windows.

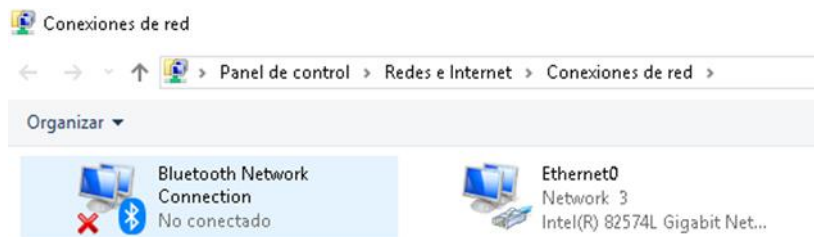
Para establecer los parámetros de TCP/IP anteriormente comentados en un sistema Windows, se deben seguir estos pasos:

1. Desde el Panel de control, en la sección Redes e Internet, se accede al **Centro de redes y recursos compartidos**.



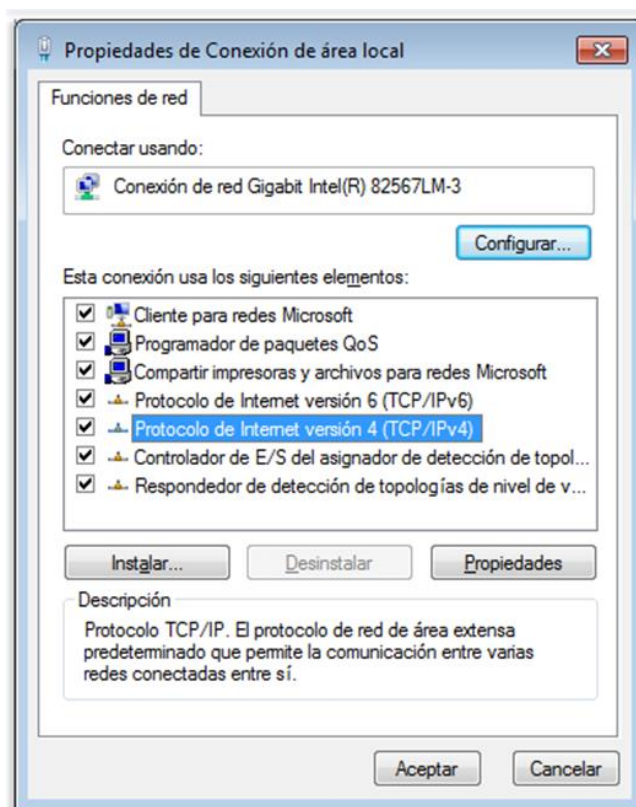
Centro de redes y recursos compartidos en Windows 10.

2. Se elige la opción **“Cambiar configuración del adaptador”** para acceder a las Conexiones de red de nuestro equipo.



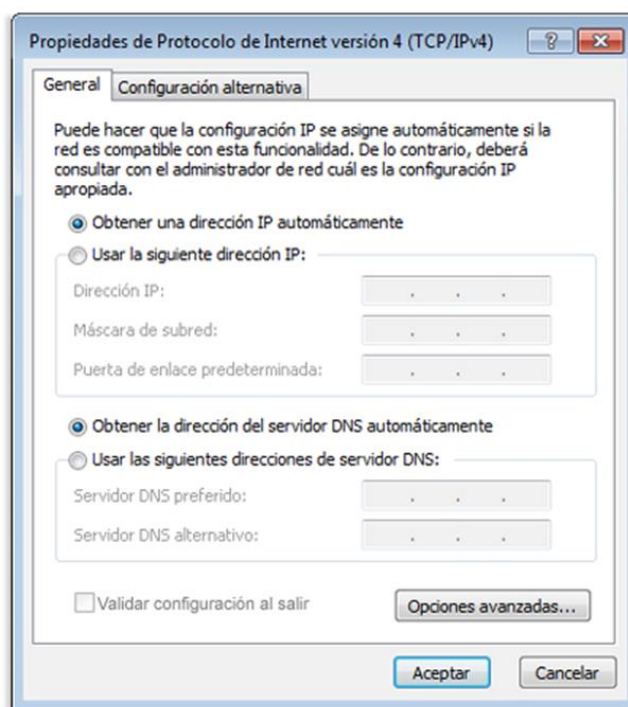
Conexiones de red.

3. Se pulsa con el botón derecho sobre la conexión que se desea cambiar y, a continuación, se elige la opción **Propiedades**. Si se solicita una contraseña de administrador o una confirmación, se escribe la contraseña o se proporciona la confirmación.
4. En la ventana que se muestra se ofrece toda la información acerca de la conexión elegida. Para la configuración que deseamos realizar se utilizan los elementos **Protocolo de Internet versión 4 (TCP/IPv4)** o **Protocolo de Internet versión 6 (TCP/IPv6)**, en función de la versión del protocolo con la que se desee trabajar. Seleccionada dicha versión, se pulsa el botón **Propiedades**.



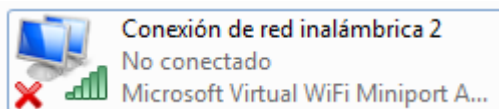
Propiedades de la conexión de red.

5. Para especificar la configuración de una dirección IPv4 (el proceso con IPv6 sería muy similar), tenemos dos opciones:
 - Para obtener la configuración de TCP/IP de forma automática, utilizando DHCP, se marca la opción **Obtener una dirección IP automáticamente**.
 - Para especificar una dirección IP de forma manual, se elige la opción **Utilizar la siguiente dirección IP** y se rellenan los campos **Dirección IP**, **Máscara de subred** y **Puerta de enlace predeterminada**, atendiendo a las indicaciones facilitadas en apartados anteriores.
6. Para especificar la configuración de los servidores DNS, igualmente tenemos dos opciones:
 - Para obtener la dirección de servidor DNS automáticamente, se marca la opción **Obtener la dirección del servidor DNS automáticamente**.
 - Para especificar manualmente una dirección de servidor DNS (o dos, si también proporcionamos el servidor alternativo), se selecciona **Usar las siguientes direcciones de servidor DNS** y, en **Servidor DNS preferido** y **Servidor DNS alternativo**, se escriben las direcciones de los servidores DNS principal y secundario, respectivamente.



Configuración del Protocolo de Internet versión 4 (IPv4)

En el caso de **redes inalámbricas**, el procedimiento de configuración es muy similar. Simplemente tendremos que seleccionar en el paso 3 nuestro dispositivo inalámbrico, y a partir de aquí la operativa es la misma.



Configuración de dispositivo inalámbrico.



ENLACE DE INTERÉS

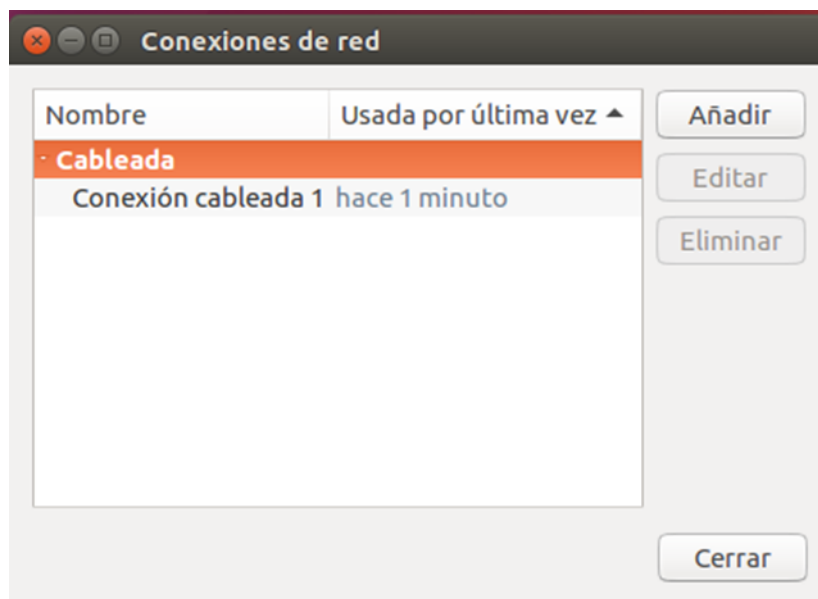
Visualiza este detallado tutorial sobre la configuración de una red inalámbrica en un sistema Windows:



Configuración de TCP/IP en sistemas Linux.

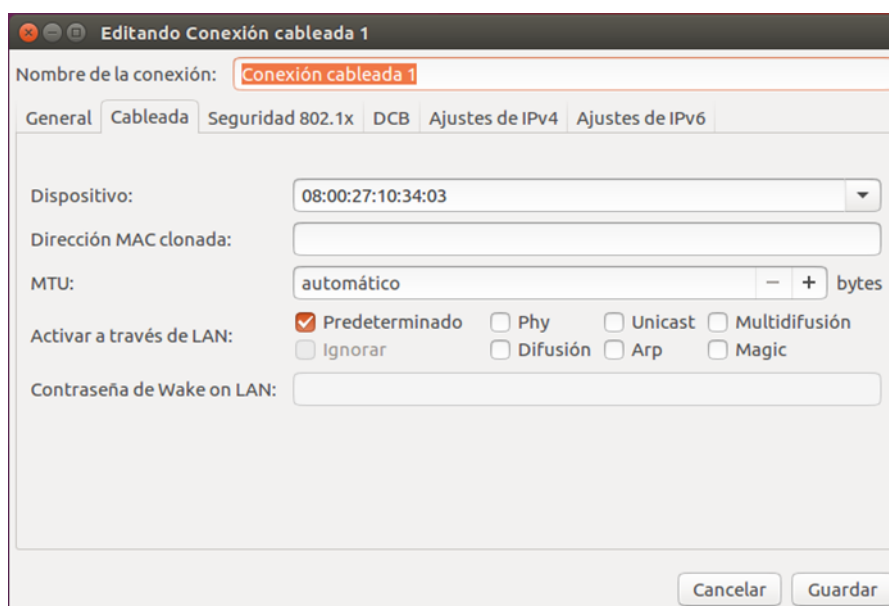
En sistemas Linux, la configuración del protocolo TCP/IP se hace de forma muy similar a la descrita anteriormente para los sistemas Windows.

En este caso se hace uso de las **Conexiones de red**, herramienta a la que podemos acceder desde el buscador de Unity.



Conexiones de red en Ubuntu.

Se selecciona la conexión que se desea configurar, y se pulsa el botón Editar.



Configuración de la conexión seleccionada.

Como puede apreciarse en la imagen anterior, se dispone de pestañas para configurar tanto IPv4 como IPv6. Si se elige la primera de ellas, por ejemplo, se ve como la opción por defecto es aplicar una configuración automática, mediante DHCP.

The screenshot shows the 'Editando Conexión cableada 1' window. The 'Nombre de la conexión' field is 'Conexión cableada 1'. The 'Método' dropdown is set to 'Automático (DHCP)'. The 'Dirección' section contains a table with columns 'Dirección', 'Máscara de red', and 'Puerta de enlace', which is currently empty. Below the table are input fields for 'Servidores DNS adicionales:', 'Dominios de búsqueda adicionales:', and 'ID del cliente DHCP:'. There is a checkbox labeled 'Requiere dirección IPv4 para que esta conexión se complete' which is unchecked. A 'Rutas...' button is located at the bottom right of the configuration area. At the very bottom of the window are 'Cancelar' and 'Guardar' buttons.

Dirección	Máscara de red	Puerta de enlace
-----------	----------------	------------------

Configuración automática de IPv4.

Se puede cambiar el Método a **Manual**, y de ese modo introducir a mano los valores deseados para la dirección IP, máscara de subred...

The screenshot shows the 'Editando Conexión cableada 1' window with the 'Método' dropdown set to 'Manual'. The 'Dirección' section contains a table with columns 'Dirección', 'Máscara de red', and 'Puerta de enlace'. The first row of the table is highlighted in orange and contains the values '192.168.1.10', '255.255.255.0', and '192.168.1.1'. Below the table are input fields for 'Servidores DNS:', 'Dominios de búsqueda:', and 'ID del cliente DHCP:'. There is a checkbox labeled 'Requiere dirección IPv4 para que esta conexión se complete' which is unchecked. A 'Rutas...' button is located at the bottom right of the configuration area. At the very bottom of the window are 'Cancelar' and 'Guardar' buttons.

Dirección	Máscara de red	Puerta de enlace
192.168.1.10	255.255.255.0	192.168.1.1

Configuración manual de IPv4.

3. GESTIÓN DE PUERTOS

Dentro de la configuración de red, a la hora de establecer las conexiones de distintas aplicaciones, deben gestionarse los puertos de modo correcto. Por este motivo, deberás establecer qué puertos van a ser utilizados y con qué finalidad en la red de la empresa.

Como hemos visto en el apartado anterior, cada dispositivo conectado a una red TCP/IP debe tener una dirección IP que lo identifique. Pero dado que el ancho de banda de las conexiones actuales es cada vez mayor, se puede obtener un mejor rendimiento permitiendo que ese dispositivo pueda ejecutar simultáneamente varias aplicaciones mediante una misma conexión. Por ejemplo, pueden abrirse diferentes navegadores de manera simultánea o navegar por páginas HTML mientras se descarga un archivo de un servidor FTP.

Para conseguirlo, a cada una de esas aplicaciones se le asigna una dirección única que se denomina puerto.

Los puertos se codifican con 16 bits, por lo que existen 65536 posibilidades distintas. Es por ello por lo que la IANA (Internet Assigned Numbers Authority) estableció una codificación estándar para ellos.

Los puertos del 0 al 1023 son los "puertos bien conocidos" o reservados. En términos generales, están reservados para procesos del sistema o programas que emplean protocolos bien conocidos, como HTTP (puerto 80) o FTP (puerto 21).

Los puertos del 1024 al 49151 son los "puertos registrados". Pueden ser usados por cualquier aplicación.

Los puertos del 49152 al 65535 son los "puertos dinámicos o privados". Suelen utilizarse por aplicaciones P2P (peer to peer).



ENLACE DE INTERÉS

Consulta una lista de los números de puerto más conocidos y utilizados y para qué sirve cada uno de ellos:



Como se ha dicho, la dirección IP sirve para identificar de manera única un equipo en la red mientras que el número de puerto especifica la aplicación a la que se dirigen los datos. Así, cuando el equipo recibe información que va dirigida a un puerto, los datos se envían a la aplicación relacionada. Si se trata de una solicitud enviada a la aplicación, la aplicación se denomina aplicación servidor. Si se trata de una respuesta, entonces hablamos de una aplicación cliente.



PARA SABER MÁS

En un dispositivo determinado, la combinación de *dirección IP + puerto* es una dirección única en el mundo denominada socket.

4. RESOLUCIÓN DE CONECTIVIDAD EN SISTEMAS OPERATIVOS EN RED. HERRAMIENTAS DE DIAGNÓSTICO

Una vez terminada la configuración de la red informática de tu empresa, llega la hora de comprobar su funcionamiento a nivel de conexión con el sistema operativo en el que se ha implementado. Para ello podrá utilizar las distintas herramientas de diagnóstico que posee el mismo sistema operativo o alguna herramienta de terceros existente en el mercado.

En muchas ocasiones, pese a aplicar las técnicas descritas en apartados anteriores, se producen problemas de conectividad que impiden que los dispositivos puedan acceder de forma correcta a las redes.

Los sistemas operativos en red proporcionan una serie de herramientas que nos ayudan con la gestión y mantenimiento de redes. Herramientas a las que hay que sumar un buen número de utilidades adicionales, tanto gratuitas como de pago.

4.1. Herramientas gráficas y comandos utilizados en sistemas operativos libres y propietarios.

A continuación, se describen algunos de los comandos más utilizados para la verificación de una red, en entornos Linux, destacando que la mayor parte de ellos tienen sus equivalentes en los sistemas Windows (algunos incluso funcionan en ambos sistemas).

- **hostname**

Sintaxis: `hostname [hostname]`

Si no se especifica ningún nombre de equipo la orden proporciona el nombre del equipo. Si se especifica el nombre del equipo en `hostname` la orden cambia el nombre local de la máquina.

- **host**

Sintaxis: `host hostname | IP_address`

Interroga al sistema para obtener la dirección IP del equipo especificado en `hostname` o el nombre del equipo que tiene una IP especificada en `IP_address`

- **dig**

Sintaxis: `dig hostname`

La orden `dig` proporciona información de los servidores DNS que gestionan el nombre de dominio especificado en `hostname`.

- **ifconfig**

Sintaxis: `ifconfig interface parameters`

La orden `ifconfig` permite crear y configurar las interfaces de red. Si no se indican parámetros la orden muestra la configuración de la interface especificada. Si tampoco se indica la interface la orden muestra la configuración de todas las interfaces de red del sistema.

Parámetros:

- Dirección: Configura la dirección IP de la interface de red especificada.
- `netmask mascara`: Configura la máscara de red de la interface de red especificada.
- `broadcast dirección`: Configura la dirección IP de broadcast. `up/down` Activa/desactiva la interface de red especificada.

- **route**

Sintaxis: `route options`

`route [add|del] [-net|-host] destino`

Permite mostrar la tabla de encaminamiento IP del sistema. También permite añadir o eliminar una entrada en la tabla de encaminamiento. Target puede ser una dirección IP numérica o un nombre de equipo o el nombre default. La orden `route` permite establecer las rutas de encaminamiento estáticas de la red.

Opciones y Parámetros:

- `-net` Especifica que el target especificado es una red.
- `-host` Especifica que el target especificado es un equipo.

- **netstat**

Sintaxis: `netstat options`

En función de la opción la orden `netstat` muestra las interfaces de red, los PID asociados a cada interface.

Opciones:

- -c Operación continua. Renueva la información cada segundo hasta que se cancela la orden mediante ctrl-c.
 - -i Muestra una lista con todos los interfaces de red.
 - -p Muestra una lista de los PID.
 - -r Muestra la información de la tabla de encaminamiento.
 - -t Muestra las conexiones activas a puertos TCP.
 - -u Muestra las conexiones activas a puertos UDP. Si se incluye "a" se mostrarán también los puertos que estén esperando una conexión (que estén escuchando).
- **Ping**
Sintaxis: ping hostname
La orden ping envía una petición de eco del protocolo ICMP al equipo especificado en hostname y muestra el tiempo transcurrido hasta recibir la confirmación del eco. En Windows la opción por defecto envía 4 mensajes. Con el modificar "-t" envía mensajes indefinidamente hasta que se cancela la orden mediante ctrl-c. En Linux por defecto envía mensajes de forma indefinida hasta que se cancele.
 - **tracert**
Sintaxis: tracert hostname

Muestra la ruta que los paquetes siguen hasta alcanzar la destinación, mostrando todos las gateways y routes del camino.

4.2 Herramientas gráficas de diagnóstico de red.

Son herramientas que nos permiten escanear y analizar una red, pudiendo identificar en el caso de que se produzca algún tipo de bloqueo para el aviso mediante mensajes, reduciendo de forma considerable la carga de trabajo que supondría una revisión manual periódica de la red.

A continuación, veremos dos de las más utilizadas.

Auvik

Solución que trabaja desde la nube y permite la supervisión y mantenimiento de la conectividad de recursos de una red de empresa en tiempo real, dando protección a los usuarios. Dispone de un mecanismo por defecto que supervisa los eventos y alertas para informar al administrador de la red, sondeando de manera continua la red y aportando

métricas en tiempo real, centralizando el protocolo de registro de los dispositivos de red.

Entre sus características destacan:

- Alertas preconfiguradas para la supervisión de puntos críticos, que pueden ser personalizadas según las necesidades propias de la red.
- Amplia oferta de archivos de datos que incluyen análisis y solución de problemas.
- Dispone del análisis Syslog de los dispositivos de red para llegar al origen del problema de red.
- Revisión de conexiones VPN para la detección de incapacidades de conexión y reducción de tiempos de espera.
- Detección de problemas con el ISP en cuanto a conectividad con internet.

Wireshark

Herramienta de carácter gratuito y colaborativo, que permite el análisis de paquetes de red, muy utilizada en el análisis y soluciones de problemas de red, al nivel de profundizar en el problema llegando a su origen exacto y error.

Entre sus características, destacamos:

- Inspección de un gran número de protocolos, que aumentan a medida que se van necesitando.
- Revisión de registros, con incorporación de los necesarios.
- Recopilación en directo y posibilidad de extracción para su análisis.
- Multiplataforma, compatible con distintos sistemas operativos.
- Integrada con potentes filtros de visualización.
- Permite un análisis rápido e intuitivo con la utilización de reglas de colores.



EJEMPLO PRÁCTICO

Un equipo de nuestra empresa tiene problemas con la conexión a Internet. Como primera medida queremos comprobar que tiene acceso a la puerta de enlace de nuestra red.

SOLUCIÓN

Se ejecuta el comando PING con la dirección IP de la puerta de enlace:

PING 192.168.1.1

```
cesur@cesur-VirtualBox: ~  
cesur@cesur-VirtualBox:~$ ping 192.168.1.1 -c 4  
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.  
64 bytes from 192.168.1.1: icmp_seq=1 ttl=63 time=2.10 ms  
64 bytes from 192.168.1.1: icmp_seq=2 ttl=63 time=2.97 ms  
64 bytes from 192.168.1.1: icmp_seq=3 ttl=63 time=2.51 ms  
64 bytes from 192.168.1.1: icmp_seq=4 ttl=63 time=6.03 ms  
  
--- 192.168.1.1 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3006ms  
rtt min/avg/max/mdev = 2.100/3.404/6.032/1.549 ms  
cesur@cesur-VirtualBox:~$
```



VÍDEO DE INTERÉS

Iníciate en la herramienta Winreshark en este vídeo:



5. MONITORIZACIÓN DE REDES

Además de la comprobación del funcionamiento a nivel de conexión de la red con el sistema operativo en el que se ha implementado, disponemos de la opción de monitorizar la red para auditar los registros obtenidos respecto a su rendimiento, por lo que vas a ser el encargado de monitorizar la red para la recopilación de esos registros.

El administrador de un sistema informático suele utilizar, además de los comandos citados en el apartado anterior, software especializado en monitorización de redes, que le permite detectar posibles problemas y le ayuda a solucionarlos. Algunas de las herramientas más conocidas en este campo son:

- **Nagios.** Está considerado uno de los más populares, si no el más popular, sistemas de monitorización de red. Fue diseñado originalmente para ejecutarse en Linux, pero actualmente también dispone de versiones para Windows. Nagios proporciona supervisión de los servicios de red (SMTP, POP3, HTTP, NNTP, ICMP, SNMP, FTP, SSH) y recursos de host (carga del procesador, uso de disco, los registros del sistema), entre otros.

Nagios tiene un diseño simple que ofrece a los usuarios la libertad para desarrollar sus chequeos de servicio sin esfuerzo propio basado en las necesidades y mediante el uso de cualquiera de las herramientas de apoyo que guste. Cuando los servicios o los problemas de acogida se plantean, la notificación será enviada a la persona que está a cargo de la red a través del correo electrónico, SMS, etc.



ENLACE DE INTERÉS

Para ampliar información y descargar este software visita la web oficial:



- **Zabbix.** De configuración sencilla, cuenta con una interfaz gráfica bastante intuitiva. Permite monitorizar un elevado número de nodos sin que su rendimiento se vea afectado.

Para almacenar los datos de seguimiento, puede utilizar MySQL, PostgreSQL, Oracle o SQLite como base de datos. Sin necesidad de instalar ningún software en el host de seguimiento, Zabbix permite a los usuarios comprobar la disponibilidad y capacidad de respuesta de los servicios estándar, como SMTP o HTTP. Para supervisar las estadísticas, tales como carga de la CPU, utilización de la red y espacio en disco, un agente de Zabbix debe estar instalado en la máquina host. Zabbix incluye soporte para la monitorización a través de SNMP, TCP y controles ICMP, IPMI y parámetros personalizados como una opción para instalar un agente en los hosts.



ENLACE DE INTERÉS

En la web oficial de Zabbix podrás descargar el software y conocer más información al respecto:



- **Pandora FMS.** Se puede considerar una suite de monitorización, ya que además de revisar redes, también permite monitorizar servidores y aplicaciones. Incluso dispositivos móviles, ya que incorpora un avanzado sistema de geolocalización.

Dispone de una versión Community, de código abierto, disponible para pequeñas empresas y usuarios particulares.



ENLACE DE INTERÉS

Amplia información y descarga este software en su web oficial:



6. PROTOCOLOS TCP/IP

Te han solicitado que realices un pequeño resumen de los distintos protocolos TCP/IP que existen, pues al haber instalado la red de la empresa de acuerdo a ellos, es necesario conocer las diferentes capas en la que trabajan los distintos protocolos.

Vamos a ver los diferentes tipos de protocolos TCP/IP:

- De la capa de internet.
- De la capa de transporte.
- De la capa de aplicación.

Protocolos de la capa de Internet.

- **IP (Internet Protocol):** Es uno de los protocolos más importantes del modelo, y se encarga de la preparación de los paquetes de datos (datagramas IP) para su envío. Para ello se añaden a dichos paquetes tanto la dirección IP del emisor como la del destinatario, de modo que se pueda saber exactamente a qué equipo debe entregarse la información.
- **ICMP (Internet Control Message Protocol):** Es un protocolo de control y notificación de errores. Se emplea, por ejemplo, cuando ejecutamos el comando ping.

Protocolos de la capa de transporte.

- **TCP (Transmission Control Protocol):** Es, junto a IP, el protocolo que da nombre al modelo. A diferencia de IP, es un protocolo orientado a conexión. Es decir, que se encarga de que se establezca una conexión entre la máquina emisora y la receptora de los datos enviados, pudiendo así comprobar que dichos datos se han entregado de forma correcta. Para ello añade una serie de información de control a los datagramas IP, generando un nuevo bloque de datos que se denomina segmento TCP.
- **UDP (User Datagram Protocol):** A diferencia del anterior, es un protocolo no orientado a conexión, que no proporciona detección de errores. Es por ello más rápido, y suele emplearse en comunicaciones de voz y vídeo, en las que pueden admitirse algunos errores en la transmisión.

Protocolos de la capa de aplicación.

- **HTTP (HyperText Transfer Protocol):** Es la base de la transmisión de datos en la web (WWW). Cuando, a través de un navegador, se solicita un recurso (como una página web) este protocolo realiza una petición al servidor que lo contiene,

estableciéndose un intercambio de peticiones y respuestas que nos permitirán acceder a dicho recurso.

- **FTP (File Transfer Protocol):** Es el protocolo que se utiliza para transferir ficheros entre un equipo cliente y otro servidor. Se emplea, por ejemplo, para alojar un sitio web dentro del servidor correspondiente.
- **SMTP (Simple Mail Transfer Protocol):** Junto a POP e IMAP, es el protocolo encargado de gestionar el servicio de correo electrónico (e-mail).

7. CONFIGURACIÓN DE REDES

En la configuración de una red informática en el que estás trabajando, va a ser necesario que conozcas cómo es la configuración de la red en sí misma, pero también los diferentes componentes con que cuenta y que también deberás configurar y comprobar su compatibilidad.

Los sistemas operativos suelen disponer de paquetes propios de acceso a red, que por defecto suelen ser del tipo TCP/IP, aunque, en determinadas ocasiones, puede ser necesario algún tipo de driver o controlador de los adaptadores de red, es decir, un software adicional y concreto para que un específico adaptador de red pueda ser utilizado por el sistema.

De este modo, encontramos:

Dispositivos como son:

- Modem o router.
- Tarjetas de red.
- Concentradores.
- Conexiones de los equipos.

Parámetros:

- En una red TCP/IP: IP, máscara de red, puerta de enlace y servidor DNS.

En la configuración de una red debemos de tener en cuenta otra serie de cuestiones como son, el sistema operativo donde encontramos dos tipos: 1) Propietario, es el caso de Windows, y 2) libre, como es el caso de Linux.

Además, deberá tenerse en cuenta si la red de tipo cableado (LAN) o inalámbrica (WLAN).

En los siguientes subapartados, vamos a ir viendo los distintos aspectos de configuración en los diferentes tipos de redes.

7.1. Configuración de los adaptadores de red en sistemas operativos libres y propietarios

Dependiendo del sistema operativo instalado podemos diferenciar entre sistemas propietarios y sistemas libres.

Configuración en sistemas propietarios.

Partimos de la base de que todas las configuraciones de adaptadores de red y características de la propia red, deben contar con permisos de administrador del sistema.

Un paso previo a la instalación de cualquier dispositivo de red, es la consulta de sus características y recomendaciones que realiza el fabricante del hardware.

Si nos centramos en Windows como sistema operativo propietario, y, en concreto en Windows 10, accedemos a través del botón secundario del ratón → Personaliza → Temas → Configuración de iconos de escritorio, donde debemos pinchar sobre Icono de red.

A partir de ahí, Menú contextual → Propiedades → Cambiar la configuración de adaptador, apareciendo la lista de todos los adaptadores disponibles.

Dentro de las propiedades del adaptador de red, en Opciones avanzadas, permite la configuración de aspectos físicos de la interfaz, que suelen ser suficientes con la que trae configurada por defecto. Pasando a continuación a la configuración de red.

Debemos tener en cuenta que cada adaptador de red tiene su propio icono y configuración de red propia, a la que podemos acceder desde su menú contextual.

En el caso de Windows la configuración TCP/IP, se realiza seleccionando el protocolo y pinchando sobre el botón Propiedades, pudiendo realizar una asignación manual en la que debemos especificar: IP, máscara de red, puerta de enlace y servidor DNS. O, por el contrario, dejar la configuración de modo automático.



¿SABÍAS QUE...?

El comando `ipconfig` permite ver y actualizar la configuración TCP/IP de una tarjeta de red.

Configuración en sistemas libres.

No olvidemos que, al igual que en el caso de sistemas propietarios, todas las configuraciones de adaptadores de red y características de la propia red, deben contar con permisos de administrador.

La instalación y configuración puede realizarse bien mediante entornos gráficos, bien a través de comandos, como por ejemplo “`sudo`” y “`su`”, en el caso de otorgar permisos de administrador.

Para la configuración del adaptador de red, debemos conocer el archivo que todo dispositivo lleva asociado y que se localizan en la carpeta `/dev`, con las identificaciones:

- `ens33` o `eth0` en el caso de Ethernet.
- `wlan0` para wifi.
- `ppp0` en el caso de módem.
- `tr0` para Token Ring.

Los dispositivos conectados los encontramos en el directorio `/sys`, pudiendo consultar los dispositivos conectados mediante:

```
$ls /sys/class/net
```

La activación y desactivación de dispositivos puede realizarse mediante los comandos `ifup` e `ifdown`, en el primer caso permite la activación y el envío y recepción de señales. En el segundo caso desactiva la interfaz, evitando el envío y recepción de señales.

Cuando lo que pretendemos es la instalación de un adaptador Ethernet en Linux, los drivers deben añadirse al núcleo como módulos cargables, iniciándose a la hora de hacerlo el propio núcleo de Linux.

A continuación, el núcleo detecta automáticamente el adaptador de red, seleccionando el módulo correspondiente y llevando a cabo la carga.

Podemos consultar la configuración de los interfaces mediante el comando `ifconfig`, con opciones como:

- `ifconfig`. Muestra todos los interfaces configurados.
- `ifconfig -a`. Muestra todos los interfaces configurados y sin configurar.
- `ifconfig eth0`. Devuelve la información del parámetro especificado, en este caso `eth0`.

7.2. Interconexión de redes: Adaptadores de red y dispositivos de interconexión. Enrutamiento

Cuando el objetivo es la conexión de equipos a través de una red, existen una serie de cuestiones a tener en cuenta, entre los equipos que componen la red:

- Medios físicos que soportan la red.
- Velocidades de transmisión.
- Tamaño de transmisión.
- Configuración de subredes.
- Características del servicio ofrecido a nivel de fiabilidad.



Dispositivos de interconexión de red.

Fuente: http://cidecame.uaeh.edu.mx/lcc/mapa/proyecto/libro27/48_dispositivos_de_interconexin.html

A la hora de realizar la interconexión de redes, se emplean una serie de dispositivos de interconexión, entre los que destacamos:

- Repetidores. Realizan la conexión a nivel físico, amplificando y generando la señal, con compensación en el caso de atenuación o distorsión debida a la propagación por el medio físico. Destacan por características como:
 - Utilizados para incrementar la longitud de la red.
 - Sólo trabajan con señales físicas, operando con cualquier protocolo.

- Mínimo retardo, al no procesar tramas.
 - Gran simplicidad y bajo coste.
 - Su número total está relacionado con la longitud de red.
 - No limita el ancho de banda a los equipos.
 - Posibilidad de instalación en distintos tipos de redes (local o extensa).
- Puentes. Elementos que operan a nivel de enlace, se caracterizan por:
 - Aislar el tráfico de red.
 - Más complejos y costosos que los repetidores.
 - Operan en modo transparente.
 - No existe limitación conceptual en el número en una red.
 - Generan tráfico adicional en la red, utilizan algoritmos de enrutamiento.
 - Filtrado de tramas por dirección física y protocolo.
 - Su utilización es en redes locales.
- Enrutadores. También conocidos como encaminadores, encargados de la transformación a nivel de red, todos los nodos deben contar con un nivel de red determinado. Características:
 - Transparentes a nivel superior de red.
 - Creación de redes independientes o subredes mediante el aislamiento de segmentos de red.
 - Interconexión de distintos tipos de red.
 - No existe limitación conceptual del número en una red.
 - Mayor retardo que puentes.
 - Complejos y costosos.
 - Utilizados en redes locales y extensas.
- Gateway (pasarelas). Realizan transformaciones a niveles superiores al nivel de la red, interconectan aplicaciones, sistemas, redes o equipos de arquitecturas diferentes.
- Hubs. Permiten la conexión de un determinado número de dispositivos de red.

Enrutamiento.

Consiste en encontrar un camino que vaya desde el origen al destino, mediante nodos de conmutación o enrutadores intermedios (routers), debiendo definir qué camina a utilizar será el más corto, con el fin de minimizar la métrica del enrutamiento.

En esas métricas que debemos tener en cuenta, que puede ser sólo una o varias combinadas, entre las que encontramos:

- Número de saltos, donde cuentan el número de routers y/o redes intermedias que el paquete deberá atravesar de inicio a fin.
- Distancia geográfica, referida a los kilómetros que recorrerá el paquete.
- Retardo promedio, relativo al retardo de las líneas, y que, será proporcional a la distancia recorrida por el paquete.
- Ancho de banda, es la velocidad de transmisión que disponen las líneas por las que circula el paquete.
- Nivel de tráfico, hace referencia al uso de las líneas, permite seleccionar la que tenga menos tráfico.

La transmisión del paquete (forward), se realizará por el enlace adecuado hasta su destino, interviniendo en el proceso:

- Tablas de enrutamiento, en las que se utiliza el campo dirección destino del paquete (IP), y que se irá basando en el siguiente salto, teniendo las entradas en la tabla (camino) que podrán ser por host, red o por defecto, y con clase o sin clase.
- Etiquetas, utilizadas para etiquetar cada datagrama IP, conmutándose en función de la etiqueta (orientado a conexión), cuenta con un campo identificador de flujo en la cabecera IPv6, reduciendo la complejidad de la tabla de encaminamiento, utilizando como técnica para la aceleración de conexiones, la conmutación de etiquetas de protocolos múltiples MPLS (Multiprotocol Label Switching).

Dentro de las técnicas de encaminamiento tenemos las siguientes:

1. Encaminamiento local.

Son técnicas en las que no se tiene en cuenta la topología global de la red, utilizando sólo la información local, entre ellas distinguimos entre:

- a Encaminamiento aleatorio. La selección del camino de salida por el encaminador es de modo aleatorio, como ventajas, su sencillez de implantación y la ausencia de necesidad de informaciones globales.

Como inconvenientes, la no utilización del camino más corto y posibilidad de uso de rutas incorrectas provoquen la no llegada del paquete a destino.

b Encaminamiento aislado.

La decisión del camino a seguir es sólo con información local, como puede ser por tener en cuenta el ancho de banda o la línea de salida menos congestionada, por ejemplo. Cuenta con las mismas ventajas y desventajas que en el caso de encaminamiento local.

c Encaminamiento por inundación. El proceso es el envío del paquete a todos los vecinos excepto el origen del paquete. Ante la posibilidad de copias duplicadas de paquetes, deben utilizarse optimizaciones como el uso de identificadores de paquetes o el campo de cuenta de saltos de cada paquete. Entre sus ventajas encontramos que es una técnica muy robusta, al probar todos los caminos posibles, y la llegada de una de las copias por el camino más corto, por el contrario, el envío de un gran número de paquetes puede saturar la red.

2. Encaminamiento estático.

Se tiene en cuenta topología de red, constituyendo las tablas de encaminamiento de forma manual, sin adaptación a los cambios de red.

3. Encaminamiento dinámico.

La construcción de las tablas de encaminamiento se realiza de manera automática, a través del intercambio periódico de información entre los encaminadores, permitiendo una adaptación continua y automática a los cambios que se produzcan en la red. Tenemos los siguientes tipos:

a Encaminamiento por vectores de distancia o algoritmo de Bellman-Ford.

La técnica mantiene en cada encaminador una tabla de encaminamiento con una entrada por cada posible destino de red, que contendrá como información, el destino, el siguiente nodo y la distancia. En ese punto, los nodos intercambian información periódicamente con sus vecinos (vectores de distancia), resultando la distancia total a cada destino, la suma de la anunciada más la distancia al router, estableciendo el coste de utilización en función del número de saltos de red. Un ejemplo de este tipo de encaminamiento es el Routing Information Protocol (RIP).

b Encaminamiento por estado de los enlaces. En este caso, cada encaminador mantiene una base de datos con la información sobre la

topología exacta de la red. El contenido de la base de datos está compuesto por la identificación de los nodos vecinos y distancia que queda recogida en un árbol o mapa de rutas basado en el algoritmo de Dijkstra. Un ejemplo es el Open Shortest Path First (OSPF).

En el caso de internet, y su organización en sistemas autónomos (AS), estos están compuestos por una serie de redes y encaminadores que suelen ser gestionados y administrados de forma conjunta, existiendo dos tipos de encaminadores:

- Internos, en los que se interconectan sólo redes del propio sistema autónomo, cuyo detalle conoce la organización del sistema a nivel local y que utilizan protocolos de encaminamiento del tipo IGP (Interior Gateway Protocol).
- Externos, también conocidos como de frontera o border router, donde se interconectan varios AS, no se limitan a la información local, sino que se amplía al conocimiento del resto de sistemas autónomos de la red, sin profundizar en detalles internos. Los protocolos utilizados son del tipo EGP (External Gateway Protocol).

7.3. Redes cableadas. Tipos y características. Adaptadores de red. Conmutadores, enrutadores, entre otros. Seguridad

En las redes cableadas debe tenerse en cuenta el tipo de cable empleado, de modo que disponemos de cables de par trenzado en el caso de conectores RJ45 o fibra óptica para el caso de FTTP, por ejemplo.

En una red LAN, se utiliza el grupo de tecnologías Ethernet, con una serie de opciones de estándares como Fast o Gigabit, en función de las velocidades, llegando incluso al estándar Terabit Ethernet.

En este tipo de redes con estándares Ethernet, la velocidad es determinante a la hora de conocer el tipo de cable utilizado, recogido mediante la denominación correspondiente precedida de la palabra “Base”, que nos indicará, tanto el tipo de cable como la longitud máxima de los segmentos, o incluso, la necesidad de tener que disponer de un repetidor de señal para su amplificación y regeneración, en el caso de que las distancias sean mayores, al quedar clasificados en 100, 1000 y 10G, según las velocidades en bits por segundo a las que viaja la señal a través del cableado de la red.

De este modo, encontramos en el caso de par trenzado, los siguientes tipos:

- 100Base-T

Distancia máxima del segmento 100 m, velocidad máxima 100Mbps.

- 1000Base-T
Distancia máxima del segmento 100 m, velocidad máxima 1Gbps.
- 10GBase-T
Distancia máxima del segmento 100 m, velocidad máxima 10Gbps.

En el caso de fibra óptica:

- 100Base-FX
Distancia máxima del segmento 2 Km, velocidad máxima 100Mbps.
- 1000Base-LX
Distancia máxima del segmento 5 Km, velocidad máxima 1Gbps.
- 10GBase-LX
Distancia máxima del segmento 10 Km, velocidad máxima 10Gbps.

Encontramos otra serie de elementos físicos de red como son:

- Dispositivos de conexión de cables.

Los conectores empleados con el cableado en intervienen en la transmisión de señal, debiendo adecuarse a las características del tipo de cable utilizado, van a ser los encargados de conectar los cables con la tarjeta de red.

Algunos conectores en el caso de cable, serían:

- RJ45, utilizados con cables UTP, STP, etc, es decir, con cables de pares, debiendo ser coincidente con la categoría del cable a utilizar.
- DB15, también en cableado de pares, para topologías en estrella y utilizados en conexión de transceptores o estaciones.
- BNC, para cable coaxial fino, característico de Ethernet.
- T coaxial, modo más común de conexión de una estación en un bus.
- DB25 y DB9, tipo de conectores utilizados para transmisiones en serie.

Dentro de los dispositivos para conexión de cables, tenemos además de los conectores, el resto de elementos necesarios para la conexión a las tarjetas de red, como son los transceptores (adaptadores de señal), rack (armario de conexiones), latiguillos, canaletas y placas de conexión o rosetas.

En lo que respecta a fibra óptica, tendríamos para el caso de redes locales, conectores ST y SC. Para redes tipo FDDI el conector utilizado es del tipo MIC.

Otros tipos de conectores utilizados son SC Duplex, MT Array o FC.

- Adaptadores de red.

Los adaptadores de red, tarjeta de red o Network Interface Card (NIC), son elementos físicos que componen la parte física de una red de área local, que contará con su propio software para instalación y configuración en la red.

Su incorporación a la red suele ser a través de un bus de comunicaciones del equipo, pudiendo disponer de más de una tarjeta de red con sus correspondientes configuraciones.

Su conexión al sistema es mediante el host de comunicaciones, transmitiendo el propio equipo la información de este componente mediante la interfaz a través del bus interno, en lo que se conoce como slot.

Las interfaces más utilizadas son del tipo PCI, PCMCIA y USB.

En la configuración de los adaptadores de red, hay que tener en cuenta que no todos los adaptadores sirven para todas las redes, deberán corresponderse con el tipo de red.

El modo de configuración se realiza de modo gráfico mediante el Panel de control en el caso de Windows o el Administrador de red en el caso de Linux, pudiendo hacerlo también a través de comandos directamente en el intérprete de comandos de Windows o el Shell de Linux.

- Conmutador o switch.

Almacena las direcciones MAC de todos los equipos de la red, que estén conectados a sus puertos. A la hora de recibir algún paquete a través del puerto, realiza una revisión de la MAC a la que va dirigido y lo reenvía por el puerto que tenga asignado esa dirección, liberando el resto de puertos para su utilización, optimizando el tránsito de información por la red.

- Enrutador.

El router es el dispositivo encargado de la interconexión de las diferentes redes entre sí. Tiene la capacidad de guiar el tráfico de red por el camino más adecuado, gestionando a su vez las direcciones IP y conectando los dispositivos a internet.

- HUB.

También llamado concentrador, permite la transmisión del paquete de datos recibido por un puerto al resto, diversificando su destino. Presenta el problema de que si se transmite un gran número de paquetes, es posible una saturación de la red.

- Seguridad.

A la hora de utilizar una red para compartir recursos, información o datos, es muy importante la gestión de la seguridad de la red, con el objetivo de evitar posibles ataques de intrusos que pongan en riesgo la integridad o privacidad de esos recursos o información.

Los tres aspectos claves en el tema de seguridad de redes son:

- Integridad, evitar la pérdida de información.
- Disponibilidad, acceso cuando sea necesario.
- Privacidad, controlar accesos no autorizados.

Las medidas a adoptar irán encaminadas a la detección de amenazas y generación de acciones contra ellas, entre las que destacamos:

-Control de acceso.

Limitar el acceso a determinados equipos de la red, la ejecución de comandos, etc. Además de, a nivel físico, con acceso restringidos al Centro de Proceso de Datos (CPD).

- Firewall.

También conocidos como cortafuegos, encargados de proteger los sistemas o redes de las amenazas que pudieran llegar a través de la red, o internet. Con acciones que eviten el tráfico tanto entrante como saliente, evitando así el ataque o ejecución de software no autorizado o malware.

Pueden establecerse a nivel de hardware conectado al router, o integrados en él, con la creación de zonas desmilitarizadas (DMZ) dentro de la red, que es realmente una zona aislada del resto de la red, donde pueden establecerse los servidores y recursos de red,

mediante un servidor dedicado y al que se accederá desde internet, que no permitirá la conexión desde fuera al resto de la red.

Pero, también existe la posibilidad de cortafuego mediante software que disponen los propios sistemas operativos como Windows Defender o, en el caso de Linux, ufw, iptables o nftables. Incluso recurrir a software externo de terceros a nivel aplicación como Netdefender o ZoneAlarm, o el ofrecido dentro de un paquete antivirus como AVS Firewall o Norton Firewall.

7.4. Redes inalámbricas. Tipos y características.

Adaptadores. Dispositivos de interconexión. Seguridad

En las redes inalámbricas el tipo de comunicación Wireless (sin cables) no utiliza un medio físico de propagación, se utilizan para ello la modulación de ondas electromagnéticas, propagadas por el espacio. Ello hace que los dispositivos físicos sólo existan a nivel emisor y receptor de la señal, como pueden ser antenas, ordenadores, etc.

Este tipo de redes conocidas como WLAN (Wireless LAN), realiza la conexión de dos modos operativos, uno Ad hoc, conectando dispositivos mediante Wifi de modo sencillo, sin necesidad de grandes configuraciones. Y, de otro modo, mediante infraestructura, lo cual amplía las posibilidades de red inalámbrica, utilizando un punto de acceso que le dota de mayor alcance en las comunicaciones, seguridad y opciones de configuración.

La red inalámbrica cuenta con una serie de ventajas como la movilidad y libertad de movimiento de los equipos que conforman la red, no requiere el mismo despliegue físico que la red cableada, arquitectura más sencilla y mayor flexibilidad y facilidad de instalación.

Los medios más utilizados, siguiendo los estándares IEEE, son:

- Wifi, ondas electromagnéticas invisibles que viajan a la velocidad de la luz, con cobertura de varios metros cuadrados.
- Microondas, tipo de radiofrecuencia que no supera la cobertura de la tierra y necesita disponer de antenas repetidoras para mantener su conexión, pudiendo con ello alcanzar varios kilómetros cuadrados.
- Satélite digital, orbitan en el espacio dando mayor cobertura.
- Bluetooth, para redes personales con poca cobertura y metros.

- Láser, utiliza un diodo emisor de luz como fuente de transmisión.

Entre los tipos de redes Wifi, destacamos:

Estándar	Banda (GHz)	Velocidad máxima
Wifi 4 (IEEE 802.11n)	2.4 y 5	450 Mps
Wifi 5 (IEEE 802.11ac)	5	3,5 Gbps
Wifi 6 (IEEE 802.11ax)	2.4 y 5	9,6 Gbps
Wifi 6E (IEEE 802.11n)	2.4, 5 y 6	9,6 Gbps

Dispositivos de interconexión.

- Router.

Que sustituye y engloba el encaminador de acceso a internet y el punto de acceso en un solo dispositivo. Contará con una interfaz inalámbrica, con posibilidad de contar con antena exterior o no. Y, el punto de acceso que conecta los nodos de la red para la transmisión y recepción, sirviendo de puente entre las redes cableada e inalámbrica.

La conexión a ese punto de acceso inalámbrico se realizará mediante su nombre con el mecanismo de identificación SSID (Service Set Identifier), que será el mismo para todos los miembros de la red inalámbrica y donde todos los puntos de acceso y clientes pertenecen a un mismo ESS (Extended Service Set), que llevarán el mismo ID.

- Adaptador de red inalámbrica

En el caso de redes inalámbricas, el procedimiento de instalación de una tarjeta de red es similar a la red cableada, donde los cables son sustituidos por antenas de radiación que llevan incorporadas las propias interfaces y que transmite y recibe señales RF (Radio Frecuencia).

Requieren disponer del correspondiente controlador para funcionamiento en el sistema operativo, que configurará los paquetes o tramas que circularán por la red de forma correcta.

Seguridad.

Además de ser aplicable todas las medidas de seguridad comentadas para las redes cableadas, en el caso de las redes inalámbricas, la no presencia de soporte físico para la comunicación, pueden permitir la captación de las mismas de modo externo, interviniendo la señal radioeléctrica.

Ello hace necesario contar con un método de cifrado que inicialmente se especificaba en el estándar 802.11, tipo WEP (Wired Equivalent Privacy), pero debido a su falta de robustez se desarrolló el estándar WPA (WiFi Protected Access), que utiliza el método de encriptación llamado TKIP (Temporal Key Integrity Protocol) como mecanismo de protección dentro del estándar IEEE 802.11i.

Pueden adoptarse además otro tipo de estrategias como puede ser el filtrado de direcciones MAC, almacenando las direcciones MAC para poder restringir el acceso a la red a los equipos cuya MAC no figure dentro de la lista guardada.



VÍDEO DE INTERÉS

Este video nos muestra una clasificación de redes inalámbricas



8. SEGURIDAD DE COMUNICACIONES

También existe una gran preocupación por la seguridad de red, por lo que te han encargado que diseñes una política de seguridad de comunicaciones que sea lo más eficaz posible a nivel preventivo y, en su caso, a nivel de solucionar de forma rápida cualquier ataque que se pudiera producir.

En el tema de seguridad de comunicaciones, relativa a redes informáticas, ya hemos comentado anteriormente que debemos partir de la integridad, disponibilidad y privacidad, como aspectos clave.

De este modo la forma de actuación debe centrarse en puntos relacionados con:

- Control de acceso, para usuarios que deban o no acceder a la información.
- Prueba de origen, asegurar que el emisor del dato, información o paquete es quien realmente dice ser.
- Prueba de recepción, asegurando que es el receptor correcto quien recibe el dato, información o paquete.
- No rechazo, garantiza que un extremo niegue el envío de un dato, o que el otro extremo niegue su recepción.



Seguridad comunicaciones de red

Fuente: <https://postgrado.ucsp.edu.pe/articulos/que-es-seguridad-redes/>

Podemos distinguir tres áreas de seguridad que podemos resumir en las siguientes, y que están relacionadas con:

- El perímetro, protección ante ataques del exterior que se basa en el uso de lo que se denominan firewalls o cortafuegos.
- El canal, protección de datos o información ante posibles escuchas mediante técnicas criptográficas.
- El acceso, protección y comprobación de la identificación de los usuarios, autorización de accesos y la auditoría de las acciones realizadas dentro de la red.

En el caso de los ataques que pueden producirse, podemos distinguir entre:

- a Pasivos.
 - Snooping, escucha o divulgación de la información.
 - Packet sniffing, análisis de tráfico, implica el conocimiento del contenido de la información transmitida en la comunicación.
- b Activos.
 - Spoofing o enmascaramiento, en el sentido de la suplantación de un ente autorizado para acceder a los recursos o información, pudiendo realizar acciones de creación, modificación o destrucción de información no autorizada.
 - Jamming o flooding, impide a entes autorizados el acceso a la información o recursos, a los que tienen derecho, esta acción es conocida como DoS (Denegación de Servicio).

Como contramedidas a estos tipos de ataques, debemos puntualizar que su aplicación, una vez detectado el ataque, no es la política correcta de seguridad. Deberemos detectar los ataques pasivos antes de que ocurran, mediante las contramedidas necesarias, y, en el caso de los ataques activos sí se detectan con facilidad, pero su prevención es más difícil.

A la hora de establecer las contramedidas, hay que tener en cuenta una serie de aspectos como son:

- Implantación de elementos de protección para minimizar la probabilidad de intromisión.

- Prontitud en la detección de cualquier intrusión que se produzca.
- Identificación de los datos, recursos o información afectada en el ataque, al objeto de poder ser recuperada.

En el supuesto de que el ataque se produzca desde el interior de la propia red, existen técnicas concretas que deberemos utilizar como son:

- Utilizar conmutadores (switches) y repetidores (hubs) con el fin de compartimentar la red.
- Sistemas de monitorización.
- Seguridad en servidores de red.

Cuando se implanta una política de seguridad, debe partirse de la base de que no existe una red o sistema con seguridad al 100%. Será necesario realizar una evaluación de los recursos o información a proteger, así como las áreas que deberán contar con una mayor protección, por contener datos sensibles, por ejemplo.

Es muy útil realizar una auditoría de seguridad propia o contratar una empresa externa, en la que se valoren aspectos como:

- Evaluación de información y recursos a proteger.
- Qué sistemas de seguridad se han implementado, y cuáles se podrían añadir.
- Testear los sistemas de seguridad actuales para encontrar los posibles agujeros de seguridad de la red.
- Elaboración de los correspondientes planes de contingencia y seguridad.

Tipos de ataques.

Existen multitud de tipos de ataques de uno solo o combinando varios de ellos, a continuación, veremos algunos de ellos, divididos en categorías de carácter general.

- Sniffing
El sniffer es un programa que puede instalarse en un equipo de la red, o a otro elemento como un router o Gateway de internet, y permiten la monitorización de los paquetes que circulan por la red.

Suelen utilizarse para la captura de nombres de usuario y contraseñas, números de tarjetas de crédito, direcciones de email, etc.

- Snooping

Su objetivo es idéntico al sniffing, la obtención de información sin modificarla, pero en este caso, además de interceptar el tráfico, se realiza la captura de documentos, mensajes u otro tipo de información, descargándose para su almacenamiento.

Suele utilizarse en el robo de información o software, incluso a nivel espionaje, como algunos ejemplos de gran repercusión, en el robo de archivos de números de tarjetas de crédito de prestigiosas empresas.

- Tampering

Acceso a datos, archivos o información con la finalidad de su modificación e incluso borrado. Adquieren especial importancia cuando el acceso se produce desde la cuenta de administrador del sistema o red. El objetivo suele ser dejar fuera de servicio un servicio de otra empresa competidora.

- Spoofing

Técnica que se utiliza para actuar en nombre de otros usuarios, generalmente para la realización de tareas de sniffing o tampering. Es habitual para conseguir el nombre y contraseña de usuarios legítimos con el fin de poder realizar acciones en nombre de ellos.

Existe una variante conocida como Looping, en la que el intruso utiliza la información obtenida de un sistema para conectarse a otros, utilizando multitud de estaciones intermedias, de incluso diferentes países, lo que convierte esta técnica en una forma de difícil investigación y seguimiento.

- Jamming o flooding.

Técnicas que desactivan o saturan los recursos de un sistema, como pueden ser la memoria o espacio de almacenamiento, bloqueando su uso para el resto de usuarios. Un ejemplo, lo tenemos en los proveedores de internet (IPS) que sufren bajas temporales de servicio por el ataque que explota el protocolo TCP.

- Virus.

Infecciones de sistemas que se caracterizan por su autoreproducción, no es necesario ningún tipo de ayuda para su propagación en una LAN o WAN, cuando se carece de protección antivirus.

De modo preventivo, es recomendable contar con herramientas antivirus actualizadas que puedan responder de manera inmediata a las nuevas amenazas.

- **Bombas lógicas.**
Sabotaje utilizado por empleados descontentos que introducen programas o rutinas con fecha determinada de actuación para la destrucción o modificación de información que provocará el colapso del sistema.
- **Ingeniería social.**
Acciones encaminadas a conseguir que personas hagan lo que en realidad no deberían hacer, como, por ejemplo, haciéndose pasar por administrador de un sistema, solicitar la contraseña utilizando excusas o pretextos que suenan muy convincentes.



EJEMPLO PRÁCTICO

Luisa es la responsable dentro del departamento de informática de su empresa, de la seguridad del sistema y de la red corporativa, tanto de la información contenida en los archivos almacenados y transmitidos, como del control de acceso de todos los usuarios.

Además del establecimiento de las medidas preventivas para proteger el sistema y la red, así como de las acciones más inmediatas caso de cualquier ataque, debe presentar un informe de los posibles ataques a los que deberá ir orientada la política de seguridad de la empresa.

¿Qué tipos de ataque pueden ser incluidos por Luisa en el informe?

Solución.

Los principales tipos de ataque podrían resumirse en los siguientes:

- Sniffing, El sniffer es un programa que puede instalarse en un equipo de la red, o a otro elemento como un router o Gateway de internet, y permiten la monitorización de los paquetes que circulan por la red.
- Snooping, su objetivo es idéntico al sniffing, la obtención de información sin modificarla, pero en este caso, además de interceptar el tráfico, se realiza la captura de documentos, mensajes u otro tipo de información, descargándose para su almacenamiento.
- Tampering, es el acceso a datos, archivos o información con la finalidad de su modificación e incluso borrado.
- Spoofing, técnica que se utiliza para actuar en nombre de otros usuarios, generalmente para la realización de tareas de sniffing o tampering.
- Jamming o flooding, son técnicas que desactivan o saturan los recursos de un sistema, como pueden ser la memoria o espacio de almacenamiento, bloqueando su uso para el resto de usuarios.
- Virus, infecciones de sistemas que se caracterizan por su autoreproducción, no es necesario ningún tipo de ayuda para su propagación en una LAN o WAN, cuando se carece de protección antivirus.
- Bombas lógicas, realizan un sabotaje, generalmente por empleados descontentos que introducen programas o rutinas con fecha determinada de actuación para la destrucción o modificación de información que provocará el colapso del sistema.
- Ingeniería social, son acciones encaminadas a conseguir que personas hagan lo que en realidad no deberían hacer, como, por ejemplo, haciéndose pasar por administrador de un sistema, solicitar la contraseña utilizando excusas o pretextos que suenan muy convincentes.

9. TECNOLOGÍAS DE ACCESO A REDES DE ÁREA EXTENSA

El cambio de trabajar a nivel individual a hacerlo en red, hace que la empresa pase a la utilización de tanto una pequeña LAN, como a la utilización de internet para establecer pautas de trabajo en una red extensa. Serás el responsable de establecer qué tecnologías se utilizarán para que el funcionamiento de esta WAN sea correcto y sin errores.

Una red de área extensa o WAN (Wide Area Network) es un conjunto de ordenadores con una extensión más amplia que un determinado territorio, permitiendo la conexión entre los diferentes equipos de la red sin tener en cuenta la distancia en la que se encuentren.

Entre sus principales características, podemos destacar:

- Proporciona cobertura a un amplia área geográfica o superficie.
- Cuenta con equipos dedicados a la ejecución de programas de usuario, que reciben el nombre de hosts.
- Los enrutadores son los diferentes hosts que se conectan a una sub-red.
- Existe una división entre líneas de transmisión y elementos de conmutación.
- Intervienen diferentes redes públicas en la transmisión de información.
- Habitualmente, necesita la utilización de medios de telecomunicación proporcionados por un operador externo.

Podemos distinguir entre los siguientes tipos de red extensa:

- Red dedicada, que utiliza los circuitos dedicados (analógicos o digitales) para cada transmisión sin realizar funciones de conmutación.
- Red de conmutación de paquetes, basada en la recomendación X.25.
- Red de conmutación analógica de circuitos, es el caso de la RTC (Red Telefónica Conmutada).
- RDSI (Redes Digitales de Servicios Integrados), se basa en conmutación digital de circuitos.

- Redes de conmutación rápida de paquetes, o retransmisión de tramas, con Frame Relay como ejemplo.
- Redes de transmisión de células, mediante el ATM o Modo de Transferencia Asíncrono, donde encontramos como ejemplo los RDSI-BA (Redes Digitales de Servicios Integrados de Banda Ancha).

Los distintos servicios de red extensa tienen como objetivo proporcionar al cliente una red de transmisión de datos mejorada, para lo que se ha venido utilizando distintas tecnologías como las que veremos a continuación:

- X25

No sólo se hace referencia a lo que afecta a la interfaz entre usuario y red de conmutación de paquetes, sino que también se refiere a las propias redes de conmutación de paquetes que dan soporte a los usuarios.

Las funciones especificadas son coincidentes con el modelo OSI, en sus tres capas inferiores que son física, enlace y red. Precisamente esta última será la denominada capa de paquete, que es donde se define el intercambio de información entre el equipo terminal de datos (ETD) y el equipo terminal de circuito de datos (ETCD) de la red de conmutación más cercana al usuario.

- Frame Relay.

Esta tecnología contempla la utilización de velocidades de acceso que estén por encima de 2Mbps, eliminando gran parte del coste que suponía la utilización de X.25 para red y usuario, en la utilización de líneas de alta calidad.

Como características podemos destacar:

- a. La eliminación de la capa de procesamiento al realizar la multiplexación y conmutación de conexiones lógicas en la capa de enlace, y no en la capa de red como en el caso de X.25.
- b. El control de flujo y recuperación de errores se realiza de extremo a extremo, de máquina origen a máquina destino, siendo responsables las capas superiores.
- c. La retransmisión de tramas se ofrece preservando el orden de transferencia entre origen y destino, a pesar de existir una pequeña posibilidad de pérdida de tramas.

d. Ofrece conexiones:

- Temporales, establecidas mediante un sistema de llamada que provoca la actualización de las tablas de conexión de los nodos de la red.
- Permanentes, establecidas cuando se acepta la conexión de los usuarios a la red, fijándose mediante la configuración de los nodos de red por tiempo indeterminado.

- ATM (Asynchronous Transfer Mode).

Es el Modo de Transferencia Asíncrono, similar en muchos aspectos a X.25 y Frame Relay, pero que se centra en lo que se denomina retransmisión de celdas, mediante un número de puertos fijos entre los que conmutan las celdas a velocidades de Gbits por segundo, realizando la transmisión a través de los puertos con distintas velocidades que en la mayoría de los casos necesitará el uso de tecnologías ópticas.

Las celdas ATM pueden contener unidades de datos de diferentes protocolos de red o incluso tramas de redes locales fragmentadas o encapsuladas, que actuarán junto a los conmutadores de red local como puentes permitiendo la construcción de redes virtuales locales separadas geográficamente, pero que funcionan como una sola red mediante la interconexión (red ATM), que da la posibilidad de propagar tramas de unas redes locales a otras.

RESUMEN FINAL

En esta Unidad hemos visto como configurar una red con el protocolo TCP/IP en un cliente de red, haciendo un recorrido por sus aspectos básicos de configuración como son las direcciones IP, máscaras de subred, IPv4 y IPv6, así como los modos de configuración que podemos emplear, manual o automática.

Respecto a los ficheros que existen para la configuración de una red, hemos podido ver los existentes tanto para el sistema operativo gratuito como es Linux del tipo host u hostname. Y del sistema operativo propietario Windows, desde la opción configuración de redes.

A continuación, en siguientes apartados se han ido viendo otras opciones de configuración como son a nivel puertos, distinguiendo entre puertos bien conocidos, puertos registrados y puertos dinámicos o privados.

La resolución de conectividad de sistemas operativos de red, con la opción de realizarla a través de comandos o de herramientas de diagnóstico como Auvik o Wireshark. O de monitorización de redes con herramientas como Nagios, Zabbix o PandoraFMS.

Siguiendo con TCP/IP, se han visto sus protocolos en las distintas capas como son internet, transporte y aplicación, para continuar con la configuración de redes, haciendo un recorrido por sus dispositivos, adaptadores, interconexión de redes, tanto en redes cableadas como inalámbricas.

En el apartado de seguridad de comunicaciones en redes, resumiendo una serie de actuaciones recomendadas como el control de acceso, y pruebas de recepción o rechazo, así como las distintas áreas de seguridad que se relacionan con el perímetro, canal y acceso, pudiendo distinguir entre los distintos tipos de ataques, pasivos y activos. Citando algunos de los más frecuentes tipos de ataques como sniffing, snooping, tampering o spoofing.

Para terminar, se ha hecho referencia a las redes extensas o WAN, sus características y tecnologías de acceso que podemos utilizar como son X.25 o Frame Relay.