INSTALACIÓN, CONFIGURACIÓN Y ADMINISTRACIÓN

USERS

Argentina $ 22.- // México $ 49.-

5

Técnico en REDES &SEGURIDAD

PUESTA EN MARCHA DE UNA RED CABLEADA

En este fascículo revisaremos el proceso de puesta en marcha de una red cableada. Configuraremos las interfaces de red y solucionaremos los problemas más comunes.

Incluye coleccionador para toda la obra

USERS

Técnico en REDES &SEGURIDAD

Coordinador editorial
Paula Budris

Asesores técnicos
Federico Pacheco
Javier Richarte

Nuestros expertos
Valentín Almirón
José Bustos
Gustavo Cardelle
Rodrigo Chávez
Alejandro Gómez
Javier Medina
Gustavo Martín Moglie
Pablo Pagani
Gerardo Pedraza
Ezequiel Sánchez

Fe de erratas

En el fascículo 1, página 11, la definición de VLAN debería decir:

VLAN: es un tipo de red LAN lógica o virtual, montada sobre una red física, con el fin de incrementar la seguridad y el rendimiento. En casos especiales, gracias al protocolo 802.11Q (también llamado QinQ), es posible montar redes virtuales sobre redes WAN. Es importante no confundir esta implementación con la tecnología VPN.

Curso visual y práctico **Técnico en redes y seguridad** es una publicación de Fox Andina en coedición con Dálaga S.A. Distribuidores en Argentina: Capital: Vaccaro Sánchez y Cía. S.C., Moreno 794 piso 9 (1091), Ciudad de Buenos Aires, Tel. 5411-4342-4031/4032; Interior: Distribuidora Interplazas S.A. (DISA) Pte. Luis Sáenz Peña 1832 (C1135ABN), Buenos Aires, Tel. 5411-4305-0114. Bolivia: Agencia Moderna, General Acha E-0132, Casilla de correo 462, Cochabamba, Tel. 5914-422-1414. Chile: META S.A., Williams Rebolledo 1717 - Ñuñoa - Santiago, Tel. 562-620-1700. Colombia: Distribuidoras Unidas S.A., Carrera 71 Nro. 21 - 73, Bogotá D.C., Tel. 571-486-8000. Ecuador: Disandes (Distribuidora de los Andes) Calle 7° y Av. Agustín Freire, Guayaquil, Tel. 59342-271651. México: Distribuidora Intermex, S.A. de C.V., Lucio Blanco #435, Col. San Juan Tlihuaca, México D.F. (02400), Tel. 5255 52 30 95 43. Perú: Distribuidora Bolivariana S.A., Av. República de Panamá 3635 piso 2 San Isidro, Lima, Tel. 511 4412948 anexo 21. Uruguay: Espert S.R.L., Paraguay 1924, Montevideo, Tel. 5982-924-0766. Venezuela: Distribuidora Continental Bloque de Armas, Edificio Bloque de Armas Piso 9no., Av. San Martín, cruce con final Av. La Paz, Caracas, Tel. 58212-406-4250.

Impreso en Sevagraf S.A. Impreso en Argentina.

Técnico en redes y seguridad / coordinado por Paula Budris. - 1a ed. - Buenos Aires: Fox Andina, 2013
576 p. ; 28 x 20 cm. (Users; 22)

ISBN 978-987-1857-78-4

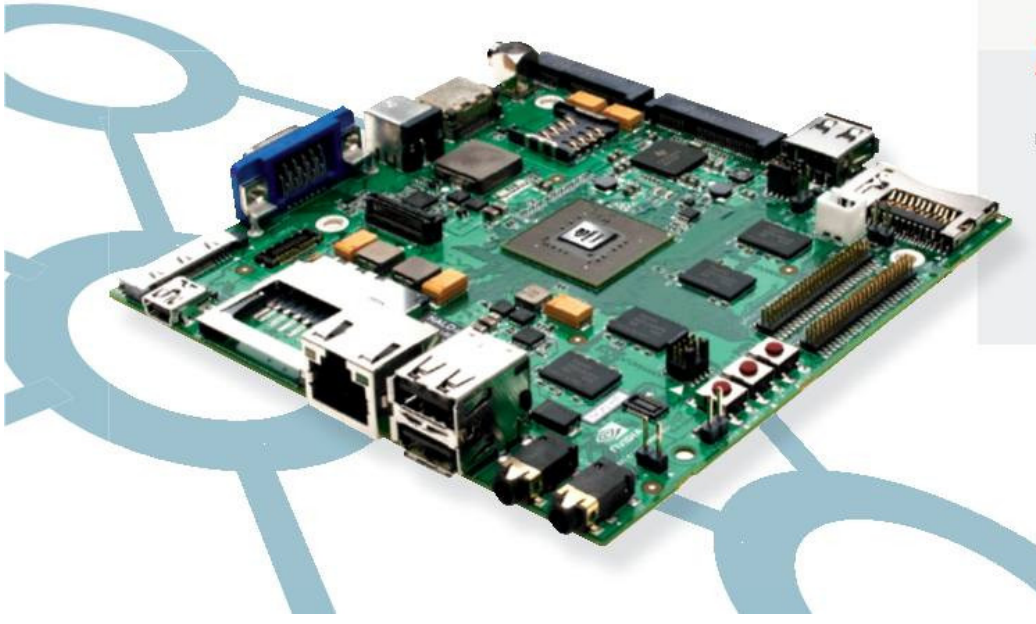
1. Informática. 2. Redes. I. Budris, Paula, coord.
CDD 004.68

En esta clase veremos...

La puesta en marcha de una red cableada, así como también todos los detalles y las consideraciones necesarias para que nuestra red funcione sin inconvenientes.

En la clase anterior vimos los consejos para enfrentar la planificación y la elaboración del presupuesto de una red cableada, analizamos el diseño de una red y todos los elementos que intervendrán en su implementación. Conocimos los detalles del cableado estructurado y algunas recomendaciones de seguridad importantes. También analizamos la instalación eléctrica y conocimos ejemplos de sistemas operativos de red; finalmente, vimos algunos detalles sobre las redes centralizadas.
En esta clase, nos dedicaremos a la implementación de una red cableada, revisaremos la configuración de una interfaz de red y veremos de qué forma podemos solucionar los problemas más comunes. Realizaremos una introducción a la seguridad relacionada con los sistemas operativos de red y conoceremos los distintos tipos de switch que existen en el mercado.
También veremos qué son los dominios y los puertos lógicos, y para terminar, aprenderemos a administrar las particiones en un disco duro y los alcances de NetBIOS.

5



Configuración de la interfaz de red

La interfaz de red instalada en la computadora nos conecta con los distintos dispositivos que integran una red. Por esta razón, debemos configurarla en forma correcta y aquí revisaremos cómo hacerlo.

En sistemas **Windows** se instalan protocolos, servicios y clientes para cada interfaz de red (Windows las define como conexiones de red). Así, por ejemplo, una **placa de red RJ-45** y una **placa de red inalámbrica** son dos conexiones distintas, en las que hay que configurar todos los elementos mencionados por separado. Por lo general, no es necesario instalar un nuevo protocolo, servicio o cliente a menos que hayamos adquirido un producto particular o interactuemos en un entorno de red que lo requiera. Cuando se instala un protocolo, servicio o cliente, se lo hace para todas las conexiones. A continuación, vamos a describir todos los componentes que se instalan en forma predeterminada con Windows (XP, 7, 8 y Server 2008).

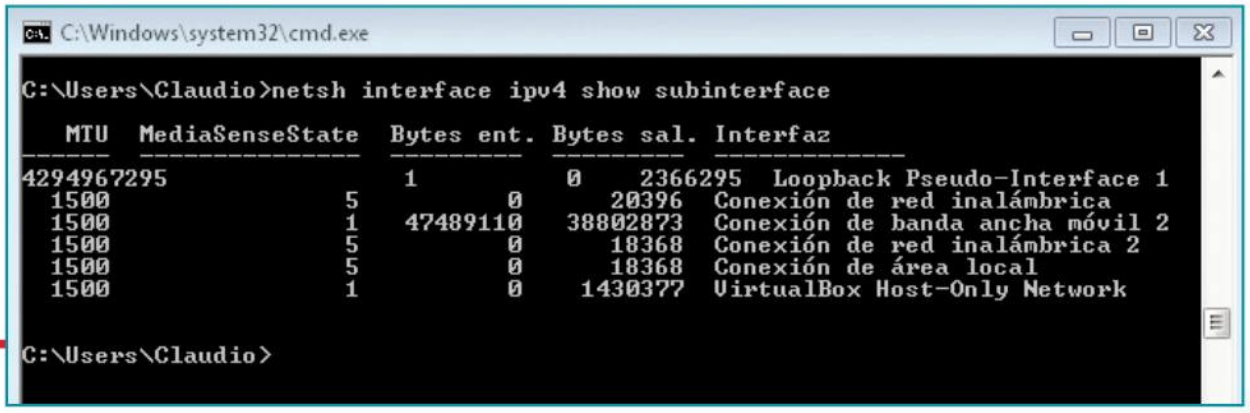
Clientes

El **Cliente para redes Microsoft** es un componente de software que viene instalado y habilitado de manera predeterminada junto con el sistema operativo, y permite que una computadora acceda a los recursos disponibles que poseen otros dispositivos para su uso dentro de una red Microsoft. Una computadora con Windows debe ejecutar el Cliente para redes si quiere acceder en forma remota a archivos, impresoras y otros recursos compartidos.

Servicios

La calidad de servicio (**QoS** o *Quality of Service*) es un conjunto de requisitos de servicio que la red debe cumplir para brindar un nivel de calidad de servicio adecuado para transmitir información. Estos requisitos se encuentran definidos por estándares QoS, y buscan optimizar velocidades de transmisión y tiempos de entrega, por ejemplo.

NO ES NECESARIO INSTALAR UN NUEVO PROTOCOLO O SERVICIO A MENOS QUE HAYAMOS ADQUIRIDO UN PRODUCTO PARTICULAR QUE LO REQUIERA.



El hecho de que una ruta presente un MTU bajo significa que los datos deben fragmentarse en paquetes pequeños para viajar por ella.

Debemos considerar que una interfaz de red se encuentra formada por la placa de red (hardware), el driver o controlador y el componente de software que debemos utilizar para gestionarla.

El **Programador de paquetes QoS** es un servicio que le proporciona al sistema operativo la capacidad de controlar el tráfico de datos que se realiza en la red.
Por otra parte, **Compartir impresoras y archivos para redes Microsoft** es un servicio que permite a otros dispositivos conectados a la misma red utilizar los recursos compartidos que posee la computadora local.

Protocolos

Un protocolo es un conjunto de reglas que definen cómo deben interactuar los roles de emisor y receptor en una comunicación, y el formato de los datos intercambiados.
El **Protocolo de Internet versión 4 (TCP/IPv4)** es una familia de protocolos de red en la que se basa Internet, y que posibilita la transmisión de datos entre equipos. Para generalizar, se denomina TCP/IP en referencia a los dos protocolos más importantes que lo componen: el protocolo de control de transmisión (TCP) y el protocolo de Internet (IP).
Existen más de cien protocolos diferentes dentro de esta familia, entre los cuales se encuentra, por ejemplo, HTTP (*HyperText Transfer Protocol* o protocolo de transferencia de hipertexto), el que se utiliza para acceder a los sitios web. La familia TCP/IPv4 emplea la versión 4 del protocolo IP, que define direcciones de 32 bits limitando direcciones únicas (es decir, 4.294.967.296) para utilizar por dispositivos en Internet. Debido al crecimiento de Internet, está cantidad de direcciones no es suficiente, y este protocolo, a pesar de encontrarse muy extendido en cuanto a uso, se está dejando de manejar, para dar paso a una nueva versión.

El **Protocolo de Internet versión 6 (TCP/IPv6)** es muy similar al que describimos con anterioridad, pero se diferencia de él por el hecho de que utiliza la versión 6 de IP. Permite diferenciar 2128 direcciones únicas para usar por dispositivos conectados a Internet. Se creó con el objetivo de resolver el problema de la cantidad de direcciones de la versión 4 y se está comenzando a implementar a nivel global.

DNS

Las computadoras manipulan y priorizan la información de manera numérica. Son altamente eficientes para buscar y ubicar direcciones IP dentro de una red. Sin embargo, los seres humanos no podemos memorizar direcciones IP y, en consecuencia, debemos utilizar otra notación más fácil de recordar, sobre todo, debido a la cantidad de dispositivos que puede haber en una red. Es por eso que las IP pueden utilizar un sinónimo o etiqueta, llamado nombre de dominio. Para convertir los nombres de dominio en direcciones IP, se usa la resolución de nombres de dominio DNS.

Para poder interactuar correctamente con dispositivos conectados en una red, debemos contar con ambos protocolos instalados, debido a que aún estamos en un período de transición, y existen dispositivos que utilizan uno u otro.

IP o Internet Protocol

IP es un **protocolo de comunicación** de datos no orientado a conexión. Se utiliza para transmitir datos entre dos dispositivos en forma bidireccional y conmutada a través de distintas redes físicas previamente enlazadas.
Se basa en el principio de que la entrega de paquetes de datos no es confiable, por lo que este protocolo tratará de realizarla de la mejor manera posible, sin garantías de arribar al destino final pero buscando la ruta más adecuada entre las que se conocen por la computadora que utiliza IP.

TCP/IP ES UNA FAMILIA DE PROTOCOLOS DE RED EN LA QUE SE BASA INTERNET Y QUE POSIBILITA LA TRANSMISIÓN DE DATOS ENTRE COMPUTADORAS.

Todos los dispositivos dentro de una red TCP/IP tienen asignada una dirección IP única. Los datos son enviados en bloques denominados **paquetes** o **datagramas** entre un dispositivo de origen y otro de destino. Cada paquete posee un **encabezado IP** en donde se encuentran las direcciones IP del dispositivo de origen y de destino de la comunicación, que serán usadas por los enrutadores (**routers**) para decidir el tramo de red por el que lo reenviarán.
El hecho de entablar una comunicación con un dispositivo por primera vez no implica una configuración previa. IP no posee ningún mecanismo de control de entrega de paquetes, de modo que un paquete se puede dañar, duplicar, llegar desordenado a destino, etc. La fiabilidad la aportan los protocolos de la capa de transporte, como TCP.

Cuando los paquetes de datos transmitidos superan el tamaño máximo del tramo (**MTU**) de red por donde van a circular, son divididos en otros más pequeños y reensamblados cuando sea necesario. Estos fragmentos pueden viajar en forma individual por caminos diferentes dependiendo de cuán congestionadas estén las rutas en cada momento.

Dirección IP

Una **dirección IP** es un número que identifica de manera lógica y jerárquica a la interfaz de un dispositivo (generalmente, una computadora) dentro de una red que utilice el protocolo IP.
Para IPv4 tiene el siguiente aspecto: `192.168.0.1`; cuatro grupos de números con un máximo de hasta tres cifras cada uno, que pueden tener valores desde `0` hasta `255` cada uno, delimitados por un punto. Existen tres clases de direcciones IP públicas que una organización puede recibir de parte de la *Internet Corporation for Assigned Names and Numbers* (**ICANN**): **clase A**, **clase B** y **clase C**.
En una red de **clase A**, el primer número es para identificar la red, y se reservan los tres últimos para asignar a los dispositivos; la cantidad máxima de dispositivos que puede tener este tipo de red asciende a 16.777.214.
En una red de **clase B**, los dos primeros números son para identificar la red, y los dos finales, para asignar a los dispositivos; la cantidad máxima de dispositivos asciende a 65.534.
En una red de **clase C**, los tres primeros números son para identificar la red, y el final, para asignar a los dispositivos, cuya cantidad máxima es de 254. Esta clase de red es la más común.
La dirección `0.0.0.0` es reservada por la **IANA** (*Internet Assigned Numbers Authority*) para identificación local.
Por su parte, la dirección `xxx.xxx.xxx.0` sirve para definir la red en la que se ubica, y se denomina dirección de red. La dirección `xxx.xxx.xxx.255` se usa para enviar paquetes a todos los dispositivos de la red en la que se ubica; se la conoce como dirección de broadcast o de multidifusión. Por último, las direcciones `127.x.x.x` se reservan para designar al dispositivo local; se denominan direcciones de bucle local o **loopback**.
A su vez, la **ICANN** reserva redes privadas (es decir que no las asigna) para que cualquier organización o institución haga uso de ellas dentro de su ámbito. Las direcciones privadas pueden ser utilizadas por los dispositivos que emplean traducción de dirección de red (**NAT**) para conectarse a una red pública, o por los que no se conectan a Internet. En una misma red no pueden existir dos direcciones iguales, pero una dirección sí se puede duplicar en dos redes privadas que no tengan conexión entre sí o que se conecten mediante el protocolo NAT.
Las **direcciones privadas** son:

- **Clase A**: 10.0.0.0 a 10.255.255.255
- **Clase B**: 172.16.0.0 a 172.31.255.255, 16 redes clase B contiguas, de uso en universidades y grandes compañías.
- **Clase C**: 192.168.0.0 a 192.168.255.255, 256 redes clase C continuas; son usadas en compañías medianas y pequeñas, además de por pequeños proveedores de Internet (ISP).

Las direcciones privadas se pueden utilizar junto con un servidor de traducción de direcciones de red (NAT) para suministrar conectividad a todos los hosts de una red que tiene relativamente pocas direcciones públicas disponibles. Según lo acordado, cualquier tráfico que tenga una dirección de destino dentro de uno de los intervalos de direcciones privadas no se enrutará a través de Internet.

Enrutamiento

El enrutamiento es un mecanismo mediante el cual los paquetes de información se encaminan desde un origen hasta un destino final, siguiendo una ruta a través de la red. En una red grande o en un conjunto de redes interconectadas, el camino que se sigue hasta llegar al destino final puede suponer transitar por muchos nodos intermedios.
La calidad de una ruta se mide a través de indicadores o métricas tales como: distancia, retardo de transmisión, cantidad de saltos (segmentos entre routers), etc.; una combinación de estos parámetros le permiten discernir a un router la mejor ruta en un instante dado para el envío de un paquete.

DHCP

Es un protocolo de red mediante el cual los dispositivos conectados a una red TCP/IP obtienen sus parámetros de configuración automáticamente. Estos parámetros son: dirección IP, máscara de subred, dirección IP de la puerta de enlace que nos comunica con otras redes, y dirección IP de un servidor de traducción de direcciones de dominio o DNS, que traduce direcciones IP en nombres de dominio. Es del tipo cliente/servidor, en donde un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme se vayan conectando y si existen direcciones disponibles. Cada dirección IP debe configurarse en forma manual para cada dispositivo y, si este se mueve a otra red, debe ser modificada.
El DHCP le permite al administrador supervisar y agilizar la distribución centralizada de las IP. De esta manera, se torna innecesario configurar las direcciones de forma manual por cada interfaz.
El protocolo DHCP incluye tres métodos de asignación de direcciones IP:

Aquí vemos los protocolos de la interfaz de red.

Cada dispositivo que se conecta a la red posee una dirección IP única.

- **Asignación manual o estática**: asigna una IP a una máquina determinada. Suele utilizarse cuando se quiere controlar la asignación de dirección IP a cada cliente y evitar que se conecten clientes no identificados.

- **Asignación automática**: asigna una IP de forma permanente la primera vez que hace la solicitud al servidor DHCP, hasta que se libera.

- **Asignación dinámica**: es el único método que permite la reutilización dinámica de las direcciones IP. El administrador de la red determina un rango de IP, y cada dispositivo conectado está configurado para solicitar su dirección al servidor cuando la tarjeta de interfaz de red se inicializa.

Direcciones estáticas y dinámicas

Las direcciones IP estáticas se utilizan, generalmente, en servidores (web, DNS, FTP, etc.) o enrutadores, para facilitar la ubicación de estos equipos dentro de una red. De otra manera, cada dispositivo de usuario final que requiera comunicarse con uno de estos dispositivos debería ubicarlo previamente dentro de la red, y esto añadiría complejidad innecesaria.
Ahora bien, puede ser que, dentro de una red, contemos con una cantidad de direcciones IP disponibles menor que la cantidad de dispositivos que desean conectarse a ella. Si se asigna una IP fija a cada dispositivo, quedarán algunos que no podrán utilizar la red. Con la asignación de IP dinámicas, solucionamos este problema, siempre y cuando todos los dispositivos nunca se conecten a la red al mismo tiempo.
Un servidor DHCP nos permite ir asignando direcciones a medida que los dispositivos se van conectando y, luego, retirarlas cuando se desconectan, para que así queden disponibles para otros. ■

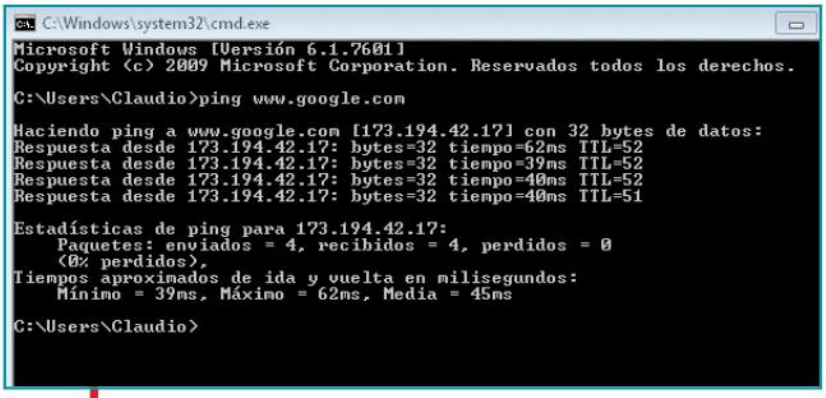
Resolución básica de problemas de red

No existe un mecanismo único para detectar fallas; solo la combinación de herramientas y el conocimiento especializado del técnico harán la diferencia para ubicar los posibles errores.

Frente a una desconexión de la red y/o de Internet, existe una serie de pasos que podemos llevar a cabo para identificar y ubicar una falla. A estos efectos, asumimos que el dispositivo formaba parte de la red antes del problema.

Una red hogareña generalmente adopta una topología estrella, en donde el dispositivo o nodo concentrador es un **router** que cumple el rol de puerta de enlace (salida hacia otras redes), **switch** (gestión de las comunicaciones entre los dispositivos de la red) y servidor DHCP (asignación de direcciones IP).

En este tipo de redes suele seleccionarse la asignación dinámica de direcciones IP, debido a que, cuando se conecta un nuevo dispositivo, evitamos tener que configurar la interfaz de forma manual (por lo general, esta configuración viene por defecto en los dispositivos). Una falla en el router implica una falla en toda la red.



El comando ping sirve para verificar el estado de una ruta de red entre dos dispositivos.

Reiniciar

Ante la presencia de una falla, como primera instancia, es conveniente **reiniciar el router**, esperar a que se ponga en línea otra vez y corroborar si el problema persiste. Los enrutadores son dispositivos que suelen estar encendidos de manera ininterrumpida, y cada cierto tiempo (en períodos largos) pueden presentar inconvenientes.

Placa de red

Acto seguido, comprobamos el funcionamiento de la placa de red presente en la computadora local. Ejecutamos el comando ping 127.0.0.1 (la **dirección IP de loopback**) desde la consola. El sistema envía cuatro paquetes de datos y espera una confirmación de recepción por cada uno desde la propia computadora. Si recibimos los cuatro acuses de recibo, significa que la placa de red funciona correctamente (tanto hardware como driver).

Ping

El término **ping** es el acrónimo de *Packet Internet Groper*, que en español se traduciría como **buscador o rastreador de paquetes en redes**. Es una utilidad que comprueba el estado de un medio de transporte a través del envío de paquetes del protocolo ICMP de solicitud y de respuesta. Sirve para diagnosticar el estado, la velocidad y la calidad de una red determinada. Ejecutando **ping** de solicitud, el dispositivo local envía un mensaje ICMP incrustado en un paquete IP.

Si no recibimos ningún acuse o nos llega un número menor que cuatro, deberemos repetir el procedimiento y, frente a una respuesta similar, reinstalar el driver de la placa o, como última instancia, reemplazar el hardware.

Cable UTP

Si la falla continúa, siguiendo con el procedimiento, deberemos cambiar el **cable UTP** por otro que funcione correctamente, en caso de encontrarnos en una red cableada.

Para redes wireless, tenemos que corroborar que la intensidad de señal sea lo suficientemente buena. Por lo menos deberíamos tener un valor en el medio de la escala. De no ser así, será necesario mover el router Wi-Fi a una posición en donde la intensidad mejore o, en su defecto, trasladar la computadora para mejorar dicha magnitud. Si la posición de uno u otro dispositivo no se puede variar, contemplemos la posibilidad de adquirir un router Wi-Fi más potente y/o con una mejor antena, cambiar la antena de la placa de red inalámbrica por otra de mayor ganancia, en caso de que sea posible, o tomar ambas medidas.

EN GENERAL, LAS REDES HOGAREÑAS SUELEN ADOPTAR UNA TOPOLOGÍA DE ESTRELLA.

Dirección IP

Supongamos que el problema persiste; entonces debemos verificar si tenemos una dirección IP asignada en caso de que la de la interfaz de red sea dinámica. Para hacerlo, en entornos Windows existe el comando `ipconfig /all`, que ejecutado en la consola, nos permite consultar los valores actuales de los parámetros de la interfaz de red.

Si no tenemos dirección IP, debemos comprobar que la interfaz tenga instalado el protocolo TCP/IP y, luego, ingresar en el firmware del router (que generalmente es el dispositivo servidor DHCP) y configurarlo correctamente. En la mayoría de los casos, la configuración de un router implica conectarse al dispositivo a través de un conector RJ-45.

Una placa de red es el componente de hardware clave de una interfaz de red.

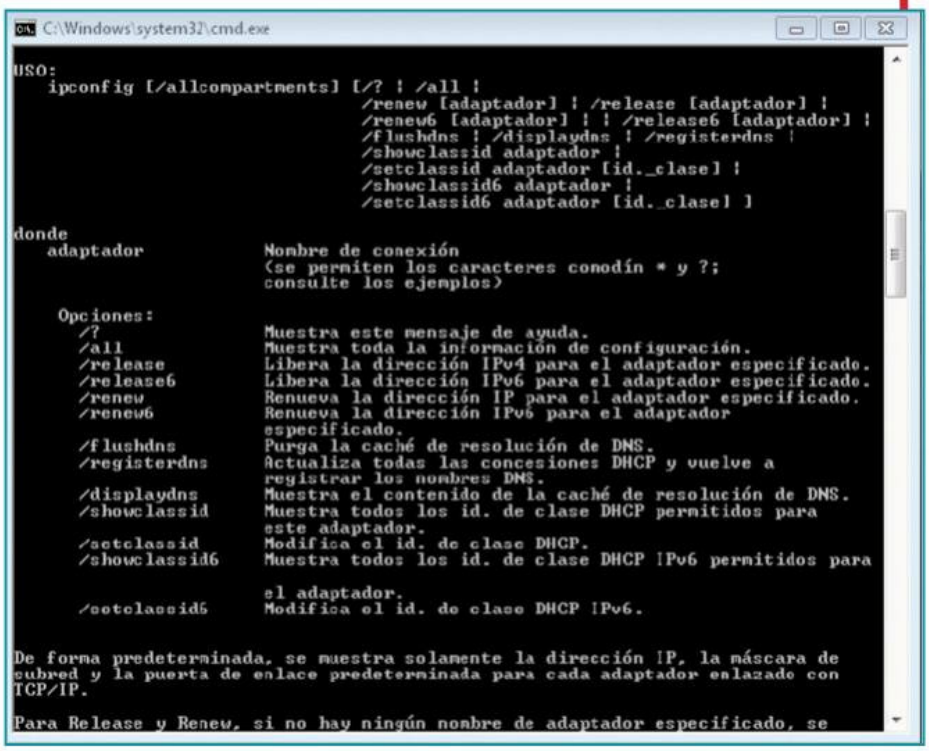
En caso de que tengamos IP asignada, ya sea manual o estática, debemos identificar la dirección del router, que suele ser siempre fija, y comprobar que exista una ruta para alcanzarlo. Para esto, ejecutamos el comando `ping` desde la consola, ingresando `ping 192.168.0.1` (ping y la dirección del router). El sistema enviará cuatro paquetes de datos y esperará una confirmación de recepción por cada uno desde el router.

Si recibimos los cuatro acuses de recibo, significa que existe una ruta entre el router y nuestra computadora. Si no recibimos ninguno, puede significar que el problema está en el medio (cable u ondas de radio).

Servidor DNS

Cuando no tenemos acceso a Internet, muchas veces se debe a que falla el servidor DNS. Para detectar este tipo de problemas, podemos, simplemente, obtener la dirección IP de algún sitio web conocido y ejecutar el comando `ping www.google.com`. Con las cuatro respuestas insatisfactorias, ejecutamos el comando: `ping 173.194.42.23`. Si las respuestas son satisfactorias, el servidor DNS no está resolviendo las direcciones IP y habrá que configurarlo correctamente o, en su defecto, apuntar a otro servidor. ■

El comando `ipconfig` permite consultar los valores de los parámetros de configuración de una interfaz de red.



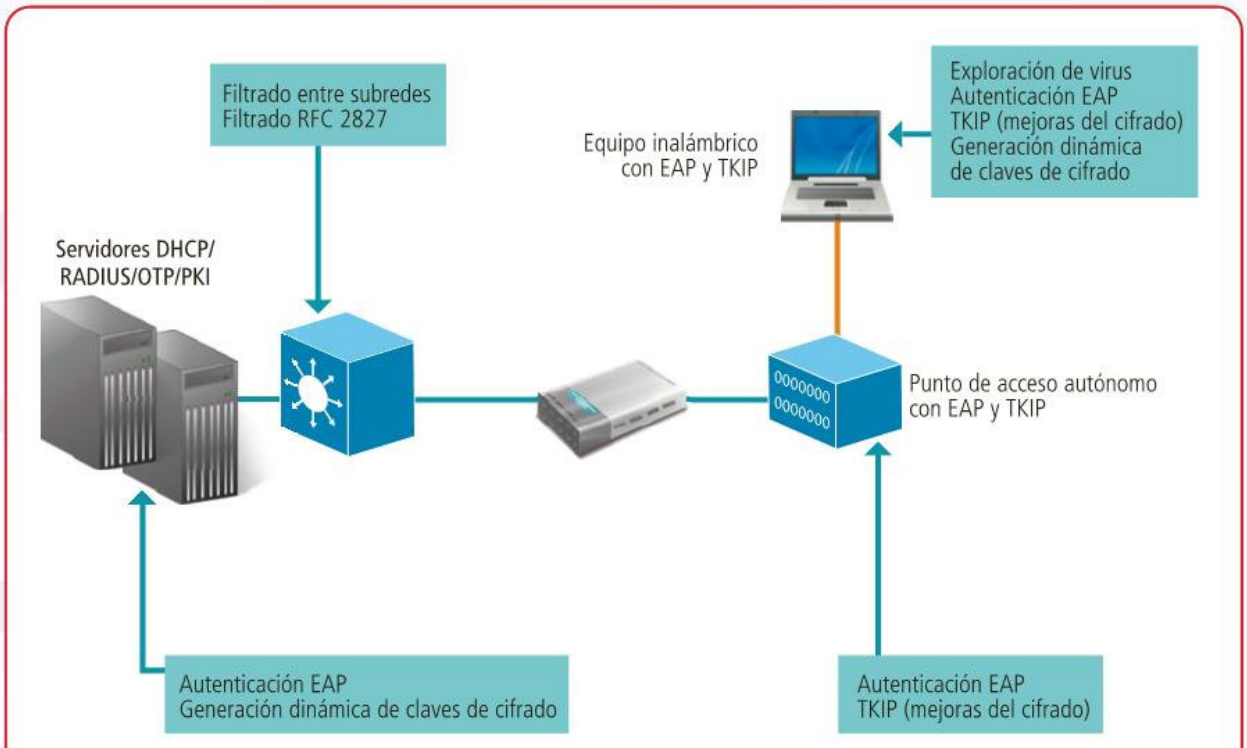
```
C:\Windows\system32\cmd.exe

USO:
   ipconfig [/allcompartments] [/? | /all |
                                /renew [adaptador] | /release [adaptador] |
                                /renew6 [adaptador] | | /release6 [adaptador] |
                                /flushdns | /displaydns | /registerdns |
                                /showclassid adaptador |
                                /setclassid adaptador [id._clase] |
                                /showclassid6 adaptador |
                                /setclassid6 adaptador [id._clase] ]

donde
   adaptador             Nombre de conexión
                         (se permiten los caracteres comodín * y ?;
                         consulte los ejemplos)

   Opciones:
      /?                 Muestra este mensaje de ayuda.
      /all               Muestra toda la información de configuración.
      /release           Libera la dirección IPv4 para el adaptador especificado.
      /release6          Libera la dirección IPv6 para el adaptador especificado.
      /renew             Renueva la dirección IP para el adaptador especificado.
      /renew6            Renueva la dirección IPv6 para el adaptador
                         especificado.
      /flushdns          Purga la caché de resolución de DNS.
      /registerdns       Actualiza todas las concesiones DHCP y vuelve a
                         registrar los nombres DNS.
      /displaydns        Muestra el contenido de la caché de resolución de DNS.
      /showclassid       Muestra todos los id. de clase DHCP permitidos para
                         este adaptador.
      /setclassid        Modifica el id. de clase DHCP.
      /showclassid6      Muestra todos los id. de clase DHCP IPv6 permitidos para
                         el adaptador.
      /setclassid6       Modifica el id. de clase DHCP IPv6.

De forma predeterminada, se muestra solamente la dirección IP, la máscara de
subred y la puerta de enlace predeterminada para cada adaptador enlazado con
TCP/IP.

Para Release y Renew, si no hay ningún nombre de adaptador especificado, se
```

Introducción a los sistemas de red

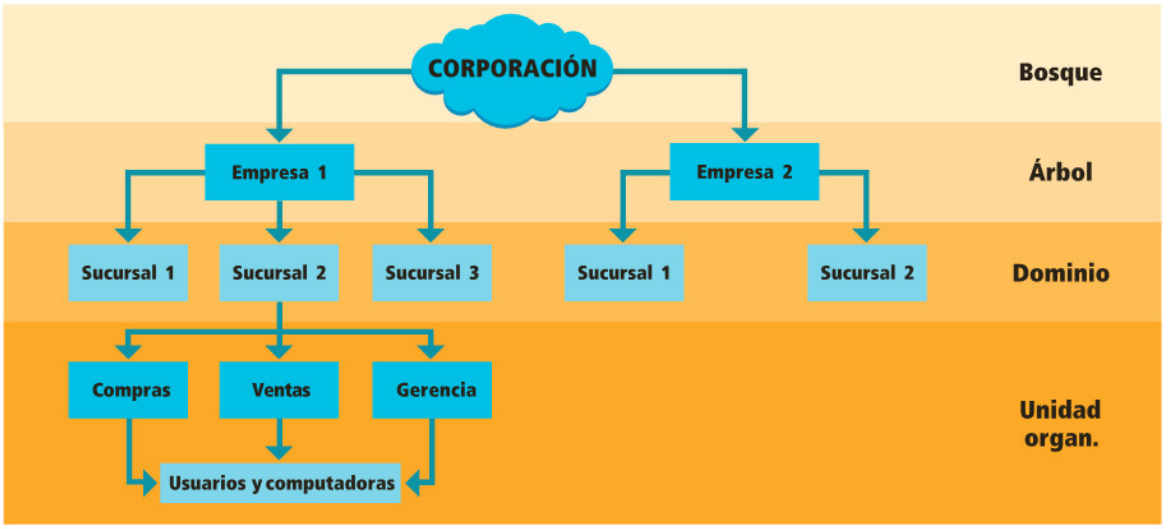
En la actualidad, la mayoría de las personas está conectada a una red informática. Las políticas de seguridad de los sistemas de red nos ayudan a minimizar los riesgos.

La palabra **seguridad**, en el ámbito informático, suele utilizarse para medir el nivel de ausencia de riesgo asociado a un elemento. Esta ausencia nunca es total (no existe nada completamente seguro) sino que varía, en mayor o menor medida, dependiendo de las acciones que tomemos para minimizar los riesgos.
Con el nacimiento de las **redes informáticas**, se tornó sencillo el hecho de compartir información entre organizaciones y/o personas físicas, con los diversos peligros de inseguridad y filtración de información que esto puede conllevar.

Toda información privada, a diferencia de la pública, se crea para un destinatario o destinatarios en particular, empresas, gobiernos, ambientes académicos, etc. Pero las redes permiten el acceso a toda persona u organización que esté conectada. Es por eso que, como creadores de información privada, debemos tener el control sobre el acceso para impedir que la red se utilice con propósitos contrarios a aquellos para los que fue concebida. No solo debemos considerar como riesgo el robo de información y su modificación o falsificación: el bloqueo de información a personas autorizadas también constituye un riesgo.



Los servidores de autenticación **RADIUS** ayudan a elevar el nivel de seguridad de una red inalámbrica.



Tal como vemos en este diagrama, un dominio de red generalmente engloba toda la red de una corporación.

La seguridad de una red no debe basarse en una medida concreta, sino en un conjunto de ellas, de manera de que si una falla, las demás se encuentren activas y eviten o reduzcan los daños. Debemos evitar ataques tanto internos como externos.

Cuentas de usuario

Ahora que ya hemos definido el concepto de seguridad, vamos a describir uno de los aspectos más importantes, que es gestionar el acceso de los usuarios. El mecanismo más extendido para validar a un usuario (saber que el usuario es quien dice ser) es a través de una cuenta, que implica que el sujeto emplee una contraseña solo conocida por él para utilizar un nodo o dispositivo de la red. Una manera de evitar negligencias es implementar la renovación de la contraseña cada cierto período de tiempo, con el fin de evitar que caiga en manos de usuarios no autorizados o, en todo caso, que los efectos de la amenaza sean temporales si no es descubierta. Cada cuenta de usuario debería de tener privilegios asociados solo a la información relevante para ella.

Control de acceso

El **control de acceso** por grupos de trabajo es un mecanismo simple y bastante eficiente para redes hogareñas, pero en redes de mayor envergadura, al ser de naturaleza descentralizada (porque el control se ejerce en cada nodo), presenta serias desventajas. Todas las computadoras de una red son potencialmente vulnerables y constituyen posibles puntos de acceso no autorizados; además, las modificaciones realizadas son difíciles de sincronizar en todos los nodos.

El uso de dominios (**Active Directory** para Microsoft) viene a resolver este problema. Básicamente, un dominio es un conjunto de computadoras conectadas en red, de las que solo una, denominada servidor de dominio, se encarga de gestionar los usuarios y los privilegios que estos poseen.

Migración de usuarios

La **migración de usuarios** es un proceso crítico, y es una buena oportunidad para corroborar y mejorar la seguridad de una red. Por lo general, sucede cuando una red crece en tamaño y, entonces, es necesario migrar usuarios y grupos locales a usuarios y grupos de dominio; o cuando se actualiza el sistema operativo de las computadoras, y se migran usuarios y grupos de dominio a una tecnología más nueva. Lo ideal es migrar, en un principio, solo las cuentas activas, y dejar para un análisis posterior y minucioso las inactivas o bloqueadas. También sería aconsejable solicitarles a los usuarios que renueven sus contraseñas. Debido a que este es un proceso que suele extenderse en el tiempo, deberíamos ir

Active Directory

Es un servicio centralizado de directorios desarrollado por Microsoft para la administración de redes de computadoras. Permite relacionar objetos con componentes de una red. Los objetos pueden ser usuarios, grupos de usuarios, permisos, y asignación de recursos y políticas de acceso. Con Active Directory, los administradores pueden establecer políticas a nivel de empresa, instalar programas y aplicar actualizaciones críticas a un conjunto de computadoras, porque este servicio almacena la información en una base de datos centralizada.

desactivando las cuentas y grupos una vez que son migrados.
Es importante controlar que la cantidad y el nivel de privilegios de los usuarios se mantengan idénticos durante el proceso de migración. Los requerimientos de aumento de cantidad de privilegios o aumento en el nivel de ellos deben satisfacerse en una etapa posterior, analizando cada caso en forma particular luego de verificar que el nivel de seguridad de la red se mantiene inmutable.

Directivas de grupo

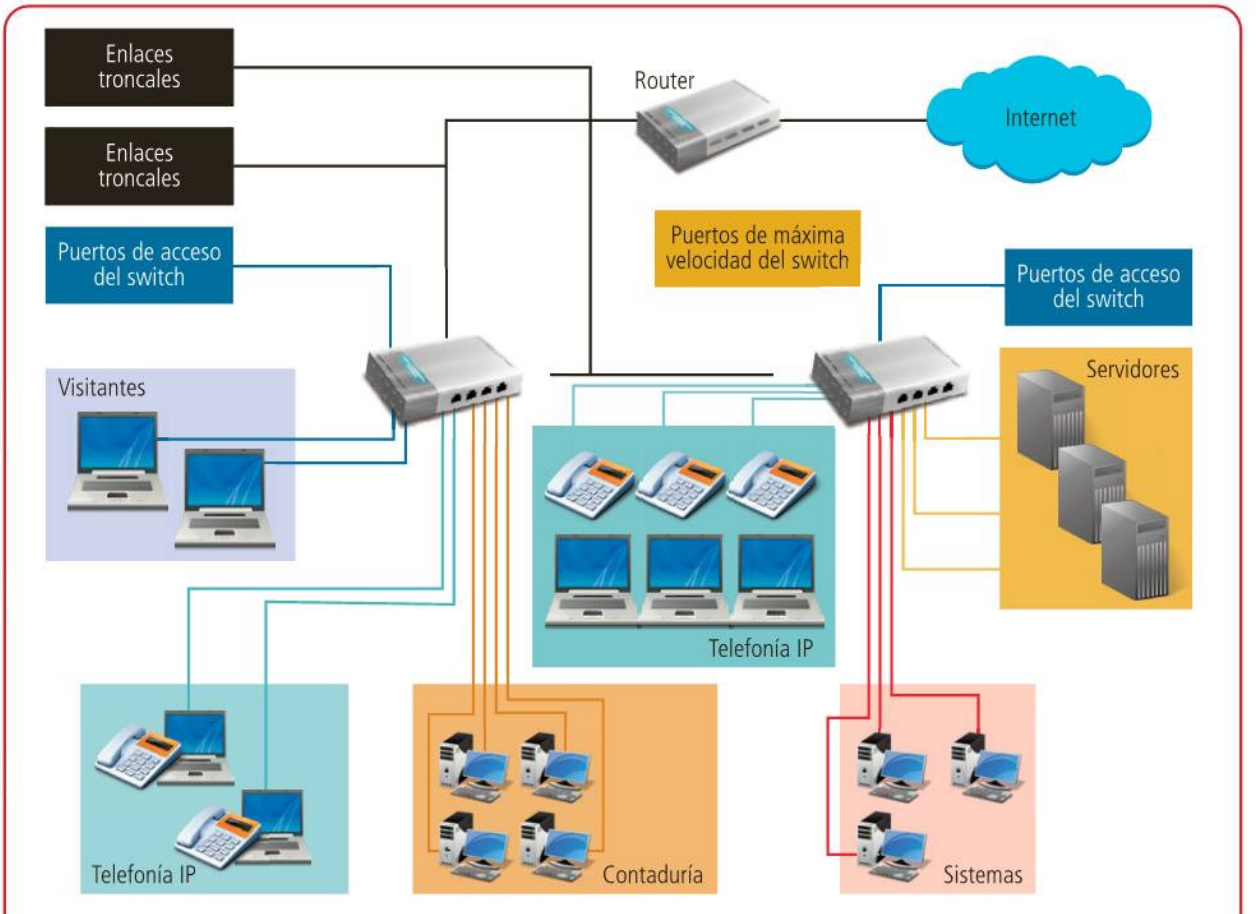
Las directivas de grupo son una característica de **Windows NT**, familia de sistemas operativos de Microsoft. Constituyen un conjunto de reglas o normas que controlan y delimitan el ámbito de actividad de las cuentas de usuario. Estas directivas proporcionan una gestión centralizada de configuración de sistemas operativos, aplicaciones y configuración de usuarios en un entorno de **Active Directory**. Las directivas de grupo controlan lo que los usuarios pueden y no pueden hacer, y su uso está más extendido en empresas y entornos académicos.
Son muy útiles para implementar medidas que tienden a impedir acciones maliciosas, como, por ejemplo, bloquear el acceso al **Administrador de tareas de Windows**, restringir el acceso a carpetas de sistema, deshabilitar la descarga de archivos ejecutables, y otras. El uso de directivas de grupo implica una reducción considerable de costos a la hora de gestionar usuarios. Existen dos tipos de directivas de grupo:

- **GPO** (*Group Policy Object* u **objeto de directiva de grupo**)
Es de naturaleza centralizada. Para este tipo de directiva, los nodos de una red actualizan o sincronizan su configuración de directivas desde un servidor cada cierto período de tiempo.

- **LGP** (*Local Group Policy* o **directiva de grupo local**)
Es de naturaleza descentralizada, y representa una versión más básica del tipo de directiva anterior. Restringe los privilegios de usuarios locales y puede implementarse en combinación con GPO.

Opciones de configuración

Las **directivas de grupo local** contienen menos opciones de configuración que los objetos de directiva de grupo, particularmente, en lo que se refiere a configuración de la seguridad. No admiten redireccionamiento de carpetas ni instalación de software de directiva de grupo.
Los sistemas **Windows** poseen un editor de directivas de grupo. Para acceder a él, debemos ir a `Inicio` y ejecutar `gpedit.msc`. ■



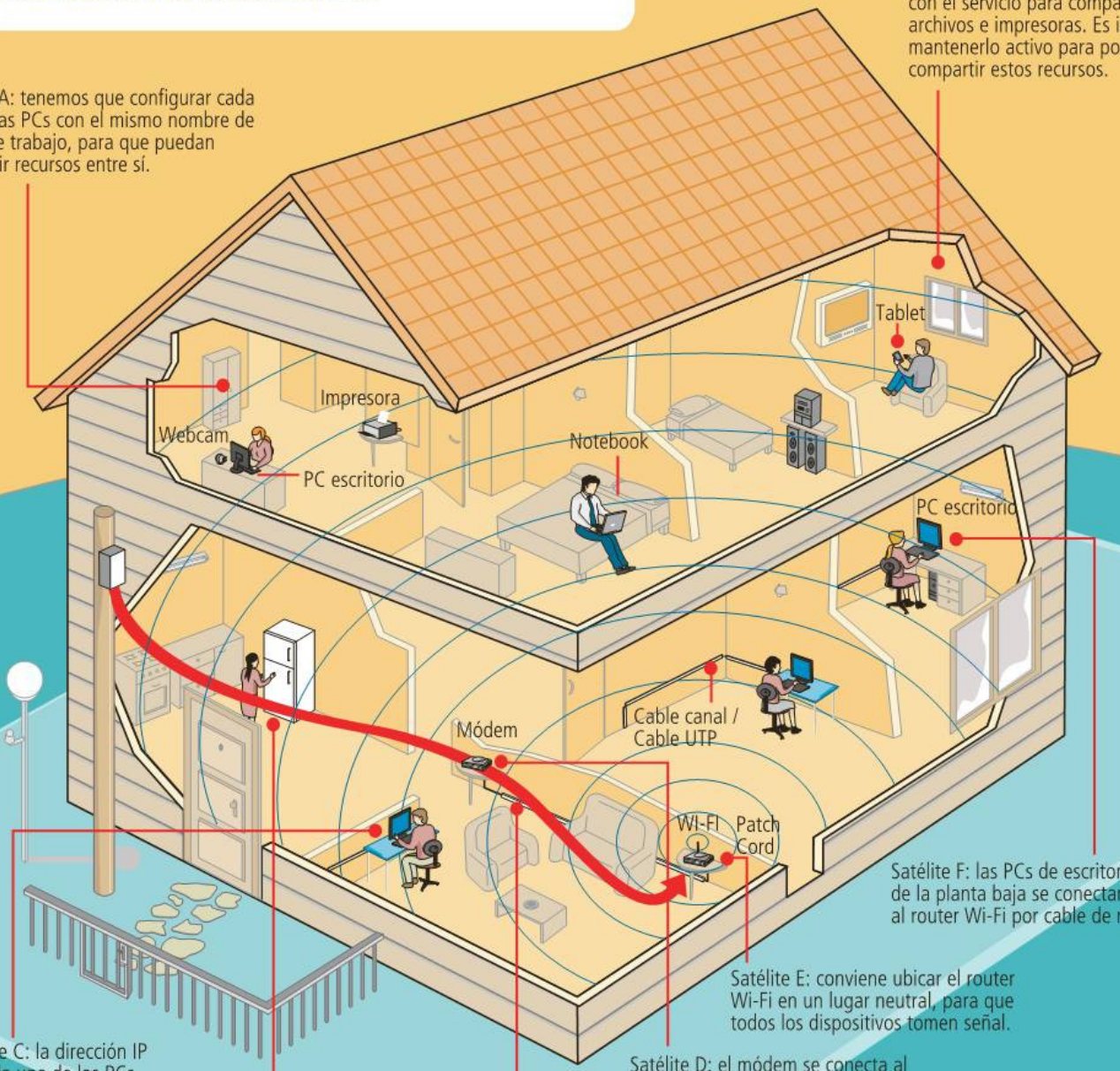
Active Directory almacena información de administración de una red en un servidor o conjunto de ellos.

La red hogareña

Los dispositivos con tecnología Wi-Fi no necesitan conexiones de cable de red. Cuando se enciende la PC, las placas de red buscarán un dispositivo Wi-Fi para asociarse. Como el nuestro cumple con la función de router, podremos acceder a Internet automáticamente.

Satélite A: tenemos que configurar cada una de las PCs con el mismo nombre de grupo de trabajo, para que puedan compartir recursos entre sí.

Satélite B: los equipos cuentan con el servicio para compartir archivos e impresoras. Es ideal mantenerlo activo para poder compartir estos recursos.



Satélite F: las PCs de escritorio de la planta baja se conectan al router Wi-Fi por cable de red.

Satélite E: conviene ubicar el router Wi-Fi en un lugar neutral, para que todos los dispositivos tomen señal.

Satélite C: la dirección IP de cada una de las PCs debe ser automática.

Satélite D: el módem se conecta al router Wi-Fi por medio de un cable corto llamado patch cord.

1 Debemos considerar las cuestiones eléctricas y la cantidad de metros entre los equipos. No podemos pasar los cables de red por donde pasan los eléctricos. Entre ellos debe haber, al menos, 30 cm de distancia.

2 Para lograr la distancia adecuada, lo ideal es implementar cable canal amurado a las paredes y pasar el cable por allí.

3 Una vez que tenemos los cables pasados por el lugar indicado, debemos instalar la ficha RJ-45 en cada uno de los extremos del cable.

4 A lo sumo, será necesario perforar las paredes con un taladro para pasar los cables hacia otras habitaciones en la misma planta.

Distintos tipos de switch

Existen diferentes tipos de switch, los cuales se diferencian por las capacidades de administración que ofrecen. La elección de uno u otro tipo depende del entorno de red que implementemos.

Un switch, también denominado conmutador, es un dispositivo digital lógico de interconexión de redes de computadoras que opera en la capa de enlace de datos del modelo OSI. Se encarga de encaminar la información que viaja por el medio de una red, en forma de paquetes, hacia su destino dentro de la misma red.
Los switches se usan como concentradores en redes en estrella y también se pueden utilizar para interconectar distintas redes conformando una topología de árbol.
Estos dispositivos verifican la dirección MAC que se encuentra en las tramas de red para dirigir los paquetes a destino.
Podemos clasificar los tipos de switch desde dos puntos de vista: de acuerdo con el método de direccionamiento de los paquetes y de acuerdo con la capa del modelo OSI en que operan.

Un switch, a diferencia de un hub, establece conexiones punto a punto entre los dispositivos que se encuentran conectados a él.

Por el método de direccionamiento

Debemos tener en cuenta que los switches pueden ser clasificados según el método de direccionamiento de los paquetes que circulan a través de él; de esta forma, encontramos los siguientes:

▶ Store-and-Forward
Guardan cada paquete en un bufer antes de direccionarlo hacia el puerto de salida. Dentro del bufer, el switch calcula un CRC (valor de verificación) y mide el tamaño del paquete. Si el CRC falla, o el tamaño del paquete es muy pequeño o muy grande, este es descartado. En caso contrario, es encaminado hacia el puerto de salida. Este método provee de un direccionamiento libre de errores, pero introduce tiempos de demora que son los empleados durante los controles.

▶ Cut-Through
Fueron diseñados para reducir las demoras. Leen los primeros 6 bytes de datos del paquete, que contiene la dirección de destino MAC, e instantáneamente lo direccionan.
El problema de este tipo de dispositivos es que no detecta errores.

▶ Adaptative Cut-Through
Este tipo de switch puede procesar paquetes en modo store-and-forward o cut-through. El modo de trabajo puede ser activado por el administrador de la red o se puede dotar de la inteligencia necesaria al dispositivo para que él mismo pueda inclinarse por uno u otro método dependiendo de las circunstancias.
Por esta razón, se presenta como el tipo de switch más versatil para toda red.

Conmutador o switch

Un conmutador, más conocido como switch, posee la capacidad de almacenar las direcciones de red que corresponden a la capa 2 (las direcciones MAC) de los dispositivos que puede alcanzar mediante sus puertos de conexión. Si encontramos un equipo que se conecta en forma directa a un puerto del switch, este se encargará de almacenar su dirección MAC. De este modo, a diferencia de los concentradores, la información va desde el origen hasta el puerto de destino en forma directa.

Por la capa en que operan

Otra forma de clasificar los switches es de acuerdo con la capa del modelo OSI en la que operan; así, encontramos los siguientes dispositivos:

La cantidad de puertos RJ-45 en un switch es variable. Por ejemplo, encontramos conmutadores de 4, 8 y 16 puertos.

▶ Conmutadores de la capa 2

Son los más comunes en entornos hogareños y funcionan como puente entre los distintos dispositivos conectados. Tienen como objetivo servir para dividir redes LAN en forma física. Analizan las direcciones MAC de destino de los paquetes. Soportan múltiples transmisiones simultáneas entre los dispositivos conectados.

UN SWITCH ES UN DISPOSITIVO DIGITAL LÓGICO QUE OPERA EN LA CAPA DE ENLACE DE DATOS DEL MODELO OSI.

▶ Conmutadores de la capa 3

Estos dispositivos son muy comunes en entornos empresariales. Nos proveen de las mismas funciones de conmutadores de capa 2 y, además, incorporan otras nuevas. Podemos citar como funciones nuevas a las de enrutamiento, verificación de la integridad del cableado y soporte a los protocolos de ruteo tradicionales (RIP, OSPF, etc.). También brindan soporte para la implementación de redes virtuales (VLAN), es decir, en forma lógica, y pueden llegar a soportar la comunicación entre ellas sin necesidad de que haya un router externo.

▶ Conmutadores de la capa 4

Constituyen la última generación de este tipo de dispositivos y no existe un acuerdo común en cuanto a su denominación. Algunos autores los definen como conmutadores de capa 3+ (layer 3 plus). Esta denominación es porque poseen las mismas capacidades que un conmutador de capa 3, pero incorporan la capacidad de establecer políticas de comportamiento y filtrado de protocolos de capas superiores (capa 4 en adelante) ,como TCP/UDP, SNMP, FTP, etc.

Consideraciones adicionales

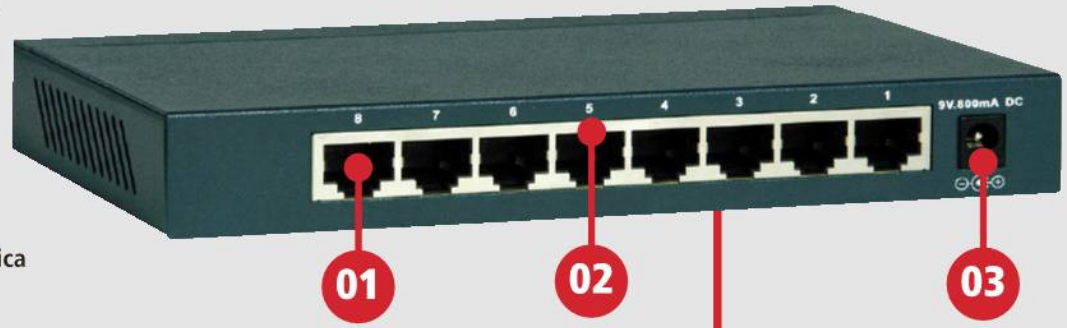
Luego de presentar ambas clasificaciones, vale la pena aclarar que en la actualidad lo más común es que nos topemos con switches que combinan clasificaciones de ambas categorías, como, por ejemplo, un dispositivo de capa 3 que direccione los paquetes en modo store-and-forward. De esta forma, la oferta comercial de dispositivos responde a todas las necesidades de un administrador de red, por lo que solo precisamos definir los requerimientos específicos y seleccionar el dispositivo que responda a lo que precisamos para implementar la red. ■

Guía Visual

01 Conector o puerto RJ-45

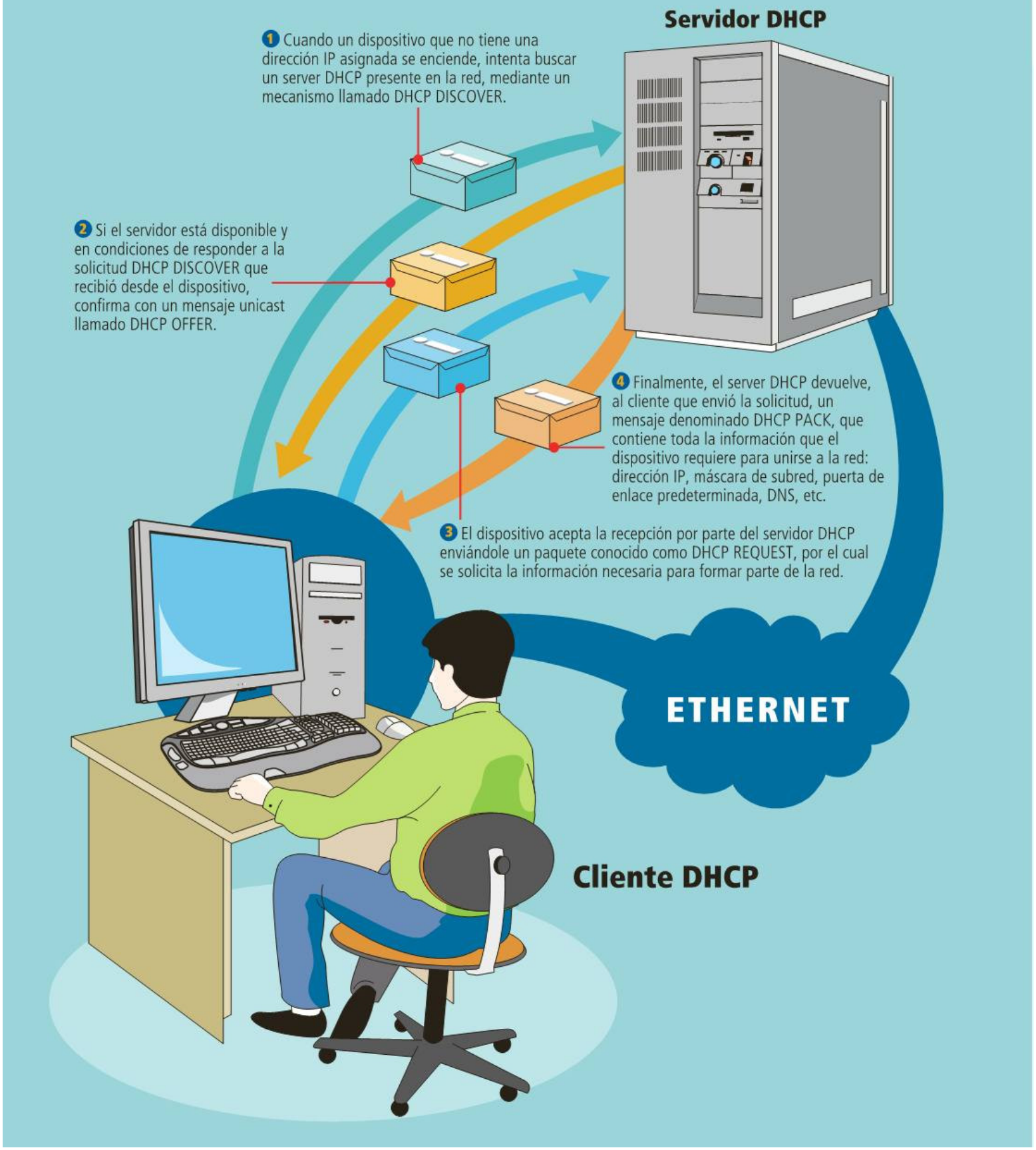
02 Número de puerto

03 Conector de alimentación eléctrica



Panel de conexión de un switch común, con ocho bocas o puertos RJ-45.

Funcionamiento de DHCP



Los dominios de red

Llamamos dominio al concentrador de la información donde se alojan los archivos de usuario, los nombres de red y otros datos importantes.

En **redes informáticas** basadas en Windows, nos encontramos generalmente con grupos del orden de 2 a 10 computadoras, conocidos como redes domésticas. Sin embargo, cuando la extensión y la dinámica de la red requiere de mayores controles, niveles de seguridad, permisos hacia los usuarios y manejo de los equipos, nos referimos a un dominio: una computadora central que, al funcionar como servidor, gestiona la información que circula en la red.

Las **redes reducidas o domésticas** se manejan, principalmente, bajo grupos de trabajo; pero cuando se trata de redes de mayor envergadura, hacen su aparición los dominios.

Grupos de trabajo

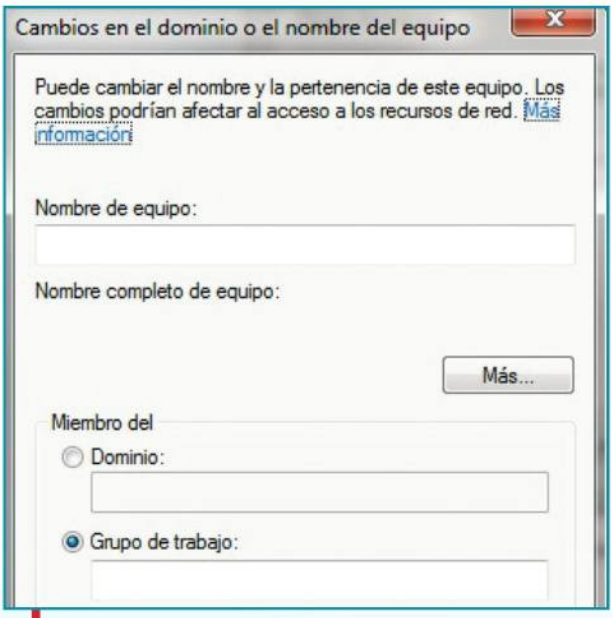
En un **grupo de trabajo**, todos los equipos se encuentran al mismo nivel; esto quiere decir que ninguno tiene prioridad sobre otro, ni sobresale a nivel de importancia; ninguno depende de otros. Otras de las características de un grupo de trabajo son las siguientes:

- Los equipos tienen sus propias cuentas de usuario. Para usar un equipo, ingresamos con la cuenta almacenada.
- Abarca redes de, aproximadamente, entre 10 y 20 equipos.
- Todos los equipos deben compartir la misma red y subred; los que están fuera del rango de la red no serán visibles.

Dominios

En un **dominio**, un equipo o más se convierten en servidores, que administran y gestionan permisos, usuarios y seguridad. Existe un **administrador** que gestiona y maneja los niveles de seguridad. Otras de las características de un dominio son:

- Para ingresar en los equipos necesitamos una cuenta de usuario en el servidor, sin importar desde qué PC se acceda.



Desde las propiedades del sistema, podemos cambiar el nombre del equipo para un dominio o grupo de trabajo.

- Pueden existir cientos de equipos conectados a la misma red.
- Los equipos pueden encontrarse en diferentes redes y se interconectan entre ellos por Internet o acceso físico.

Aun si los equipos están bajo un grupo de trabajo o un dominio, pueden llevarse a cabo las tareas básicas de intercambiar información, compartir recursos o utilizar dispositivos remotos. La diferencia reside en la implementación de seguridad, donde el usuario está más controlado y ese control se centra en menos equipos, lo que aumenta el nivel de protección. ■

Grupos de trabajo seguros

Para asegurarnos de que ningún usuario ajeno o malintencionado ingrese en nuestra red, podemos asignar una computadora como servidor principal, a la cual le indicaremos los usuarios específicos. Para hacerlo, esta PC deberá contar con una distribución de algún sistema operativo basado en servidores, que pueda gestionar los permisos de manera adecuada. De esta forma, cambiaremos automáticamente los grupos aleatorios por dominios seguros.

Qué son los puertos lógicos

Desde el momento en que un dispositivo se conecta a una red o a otros equipos, se utilizan puertos lógicos para que el intercambio de información pueda llevarse a cabo; aquí los conoceremos.

Cuando se conforma una red, los dispositivos conectados a ella intercambian información unos con otros a través de medios físicos o inalámbricos, mediante protocolos de funcionamiento y a través de instrucciones dadas. Para que esto se lleve a cabo, se utilizan diversos canales por los cuales uye la información; se los denomina puertos lógicos, y son virtuales y numerosos. A diferencia de los puertos físicos, los **puertos lógicos** alcanzan cantidades de miles, mientras que los físicos llegan a contabilizarse en decenas como máximo.

Puertos lógicos

Es posible definir al puerto lógico como la **zona de la memoria** en la computadora que se corresponde con un puerto físico o canal de comunicación, por ejemplo, una impresora asocia su canal de salida a un puerto de comunicación específico USB de la PC. Este puerto proporciona un **espacio temporal de memoria** donde se alojará

ZoneAlarm (www.zonealarm.com) es una de las alternativas más conocidas entre los firewalls gratuitos que podemos encontrar en Internet.

Firewall

Los intrusos que acceden a nuestros dispositivos se aprovechan de las debilidades de los sistemas operativos y las utilizan para ingresar a través de puertos disponibles desprotegidos. Los firewalls los controlan, gestionan y se aseguran de que tanto las entradas como las salidas sean las que el usuario gestiona. Troyanos, backdoors y malware intentan franquear los firewalls débiles, por lo cual es importante analizar periódicamente nuestros sistemas.

la información por transferir entre este espacio y el canal de comunicación. En las redes, los puertos son valores que se asignan a las múltiples aplicaciones conectadas a cada dispositivo. Las aplicaciones se conectan a Internet mediante un puerto numérico asignado y reservado para él.

Asignación de puertos

Si bien los **puertos** son asignados de manera arbitraria a las aplicaciones, algunos rangos de puertos están reservados por convenio a determinadas aplicaciones consideradas de carácter universal. Ciertos puertos son utilizados para aplicaciones clave.
La IANA (*Internet Assigned Numbers Authority*, o autoridad que asigna números de Internet) ha determinado la asignación de los puertos del 1 al 1023, detallados en la *Selected Ports Assignments*. En la tabla adjunta conoceremos algunos de ellos.

Puertos arbitrarios

Del 1025 en adelante, son puertos **arbitrarios** y no están asignados a ninguna aplicación predeterminada. Algunos **malware** y otras aplicaciones son diseñadas para realizar ingresos e intercambio de información no autorizados. A partir del puerto 1025, se los puede registrar ante la **IANA** para que sean reservados y de único uso para la entidad que los precise. Todos los puertos son necesarios para comunicarse con el exterior, tanto los lógicos como los físicos. Los puertos virtuales y físicos se diferencian porque los primeros se enlazan virtualmente con las conexiones TCP/IP mediante programas, y los segundos requieren medios físicos para interconectarse.

NetCat

Los puertos ubicados desde el 1025 en adelante, habilitados para el usuario disponga de ellos, pueden ser manipulados mediante un programa llamado **NetCat**. Se trata de una herramienta de red que, a través de comandos simples (basados en el sistema operativo MS-DOS), permite

abrir puertos TCP/UDP. Este software fue creado en 1996 por **Hobbit** y liberado bajo licencia de software libre para UNIX. Con el paso del tiempo, fue adaptado para **Windows**, **Linux** y otros sistemas. Actualmente, una de sus principales funciones es la depuración de aplicaciones de red y su uso poco ético como puerta trasera sin autorización (**backdoor**).
Algunos de los comandos básicos de **NetCat** son:

- `l`: abre el puerto para escucha (Listen). Acepta una única conexión de un cliente y se cierra.
- `k`: fuerza a que el puerto permanezca abierto tras haber recibido una conexión.

Mediante la configuración de un router, es posible asignar los puertos TCP y UTP para limitar el acceso a la red.

Se usa con el parámetro `-l` y permite infinitas conexiones.

- `u`: el puerto abierto se abre como UDP.
- `v`: muestra información de la conexión.
- `t`: respuestas compatibles para sesiones de Telnet.
- `q segundos`: tras haber recibido el EOF de la entrada de datos, espera los segundos indicados para enviarlo.
- `i segundos`: especifica un delay (retraso) de tiempo para el envío o recepción de las líneas de texto.

Recordemos que, al cerrar el programa, las conexiones permanecen en funcionamiento. ■

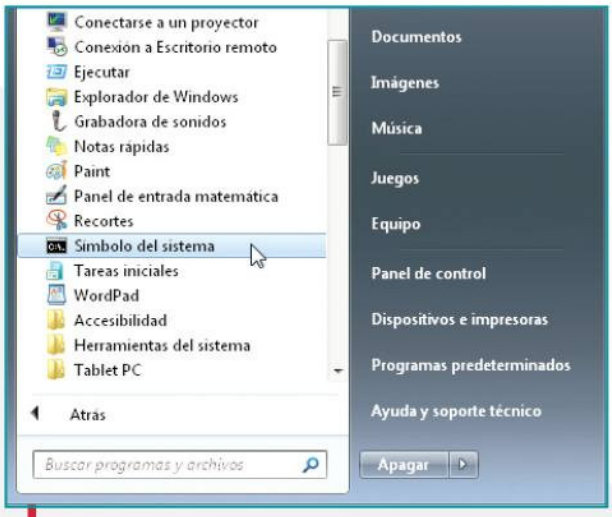
Puertos y sus usos

Puerto	Protocolo	Uso
21	TCP/UDP	FTP
22	TCP/UDP	SSH
23	TCP/UDP	Telnet
25	TCP/UDP	SMTP
66	TCP/UDP	Oracle SQLNet
79	TCP/UDP	Finger
80	TCP/UDP	HTTP – Web
107	TCP/UDP	Remote Telnet Service
110	TCP/UDP	POP3
118	TCP/UDP	SQL Services

Seguridad básica en redes informáticas

Los sistemas operativos actuales son muy seguros, pero ciertas conductas de los usuarios pueden ponerlos en situaciones de riesgo.

En forma predeterminada, **Windows** carga todos los servicios relevantes para su funcionamiento y los programas relacionados con él; incluso, levanta servicios que no son necesarios (se instalan y ejecutan gran cantidad de estos servicios, los cuales podemos necesitar o no dependiendo del perfil de usuario).
Esto quiere decir que, en la carga del sistema operativo, se activa un listado de servicios preprogramados que quedan residentes en memoria y trabajan en segundo plano, con lo cual permanecen vulnerables a ataques debido a que algunos de ellos requieren el uso de puertos disponibles y acceso a la red.
El objetivo que perseguimos es evitar que se activen los servicios que no sean necesarios, identificarlos y **aumentar la seguridad del sistema** ante el ataque de usuarios malintencionados.



La consola permite introducir los comandos para correr herramientas de sniffer; la encontramos entre las aplicaciones de Windows.

EL CONOCIMIENTO DE TÉCNICAS DE SNIFFERING NOS OTORGA HERRAMIENTAS CONCEPTUALES PARA PROTEGER NUESTRO SISTEMA DE ATAQUES EXTERNOS.

Servicios

Al identificar los **servicios útiles** y necesarios, podemos analizar el escenario de un posible ataque; esto quiere decir que limitaremos el rango de control necesario para que funcione adecuadamente (en cuanto a seguridad). Para realizar este procedimiento, aplicaremos una técnica llamada **hardening** (endurecimiento): en seguridad informática, se refiere al proceso por el cual reducimos al máximo las vulnerabilidades del sistema operativo. Para hacerlo, el **administrador del sistema** efectúa un conjunto de actividades que buscan reforzar la seguridad.
La técnica consiste, principalmente, en analizar y quitar software, usuarios, servicios, permisos, puertos, etc. Sin embargo, es importante aclarar que mediante el **hardening** no conseguiremos hacer invulnerable al sistema en cuestión, ya que solo analizaremos una de sus capas, y faltará evaluar otros factores para complementar la seguridad. Algunos de los servicios que intercambian información con la red, y que en ciertos casos pueden ser deshabilitados, son los siguientes:

- Acceso a dispositivo de interfaz humana
- Actualizaciones automáticas
- Adaptador de rendimiento de WMI
- Administración de aplicaciones
- Administración de IIS
- Internet Information Server

Modo promiscuo

En las redes informáticas, los paquetes son enviados con una dirección de destino en la que se especifica quién los envía y quién debe recibirlos. En el modo promiscuo, todos los paquetes son capturados, aunque no estén dirigidos a ese destino (normalmente, las computadoras desechan los paquetes que no están dirigidos a

su dirección), por lo que abarcan todo el tráfico de la red.
Para activar el modo promiscuo, debemos realizar las acciones que mencionamos a continuación:

▶ Si tenemos un **sistema Linux**, abrimos una consola y escribimos: ifconfig<interfaz>promisc
Usamos el comando -promisc para quitar el modo promiscuo.

▶ Si tenemos un **sistema Windows**, podemos utilizar alguno de los drivers o aplicaciones destinadas a monitorear la red, como los que conoceremos a continuación.

Sniffers

Para detectar las máquinas en modo promiscuo, existen herramientas específicas que funcionan mediante el envío de paquetes que solo recibirán aquellos equipos que estén en ese modo. Es importante para el administrador de sistemas conocer el funcionamiento básico de las herramientas y saber utilizarlas; por ejemplo, podemos mencionar las siguientes:

▶ **Tcpdump**: es uno de los sniffers más comunes. Está disponible para la mayoría de los sistemas basados en UNIX y Linux, y forma parte del sistema base de OpenBSD. Trabaja con líneas de comando, donde podemos especificar diversos patrones y protocolos.

▶ **Darkstat y traffic-vis**: funciona como demonio, recolectando estadísticas sobre el uso de la red.

▶ **Ethereal**: sniffer con interfaz gráfica, con amplio margen de uso; identifica diversos niveles y controla los puertos al grado del detalle. Prácticamente fue dejado de lado por Wireshark, la aplicación que lo reemplazó por completo.

▶ **Wireshark**: se trata del sniffer y analizador de protocolos más popular del mundo; es uno de los más completos y utilizados por usuarios avanzados en la actualidad.

Hardening

El **hardening** no solo implica el control de las aplicaciones que funcionan bajo sistemas operativos, sino que también abarca ataques físicos al hardware sobre sus debilidades. Por eso es importante realizar actualizaciones en todos los sistemas para reducir las vulnerabilidades. El estudio de los sistemas hace que surjan nuevas **vulnerabilidades**, por lo que un excelente método de control es la actualización permanente.

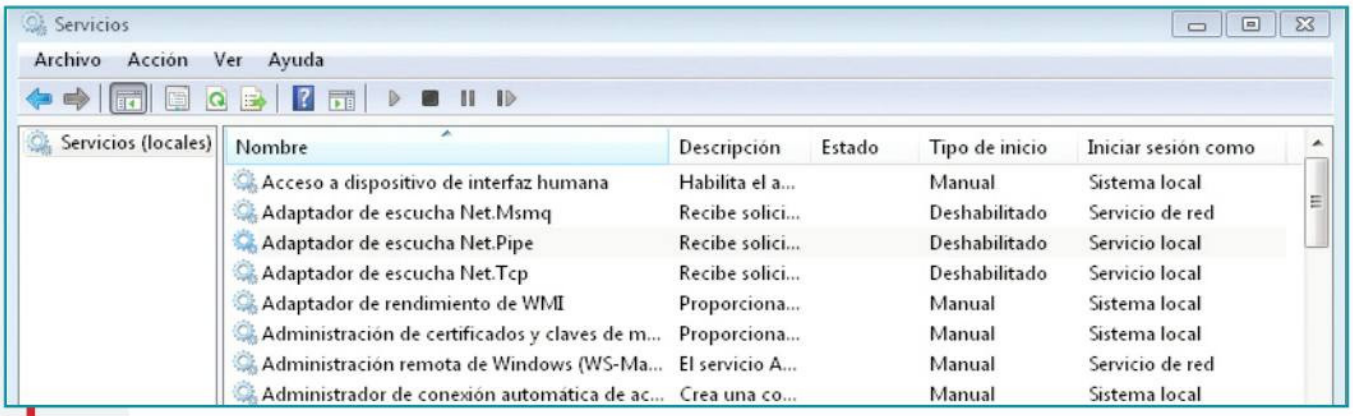
Bloqueo e identificación

Los **sniffers** pueden usarse tanto para controlar la red frente a ataques como para robar información (los usuarios pueden recolectar la información para uso propio). Si bien existen herramientas para rastrear los movimientos de paquetes intercambiados entre las computadoras, el procedimiento de bloqueo e identificación sigue siendo un procedimiento manual que se realiza mediante métodos como los siguientes:

▶ **Detección de latencia en paquetes ICMP**: este método se realiza mediante el envío simultáneo de numerosas peticiones erróneas, de modo que ningún equipo las tome en cuenta.

▶ **Detección mediante paquetes ping ICMP**: en este método se envían paquetes de información con direcciones MAC erróneas. Las máquinas en modo promiscuo responderán sin necesidad de comprobar dichas direcciones.

▶ **Detección mediante paquetes ARP**: basado en el principio de funcionamiento anterior, la solicitud es enviada a todos los rangos de IP en la red local, y solo responderá la computadora en modo promiscuo. ■



Gracias a Servicios, podemos acceder y configurar el listado de aquellos que están presentes en un sistema Windows.

Tratamiento lógico de las unidades de disco

Las unidades físicas están preparadas para ser utilizadas en toda su capacidad. Para esto, podemos dividirlas en varias unidades lógicas.

Al adquirir un **disco duro** de cualquier capacidad, este vendrá preparado para ser administrado por el usuario. Pero antes de hacerlo, habrá que darle un formato o adaptarlo a un sistema de archivos específico para alojar la información. En estas páginas aprenderemos a gestionar las particiones del disco y conoceremos algunos conceptos sobre seguridad.

Uso del disco físico

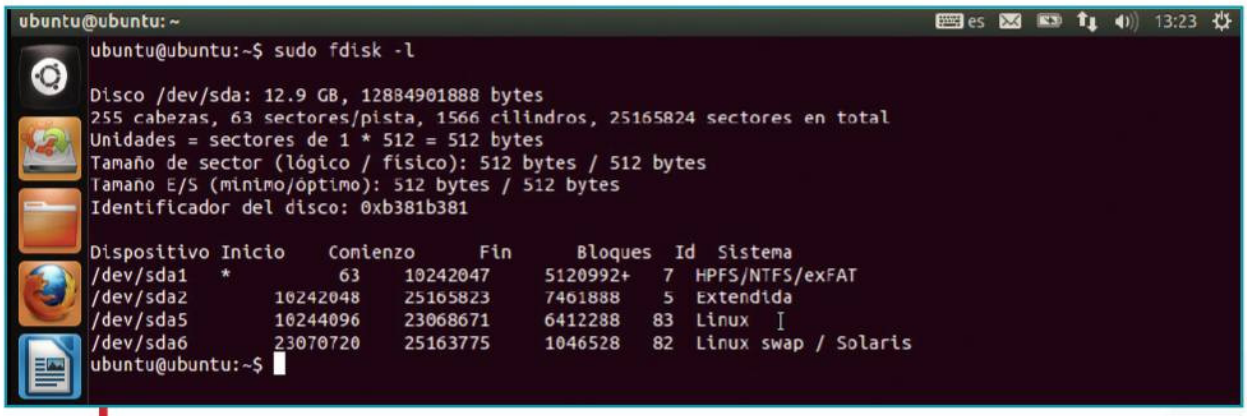
Cuando vamos a utilizar un disco duro, podemos buscar herramientas para manejar cómo funcionará, qué información podrá almacenar, en qué parte se alojarán los datos y, cómo dividirla en varias unidades lógicas. Las necesidades propias de los usuarios llevan a que las unidades físicas estén subdivididas en varias unidades, llamadas lógicas, que se comportarán como unidades virtuales cuando los sistemas operativos las lean. Su funcionalidad principal es discriminar la información y organizarla según su uso.

Sistema de archivos

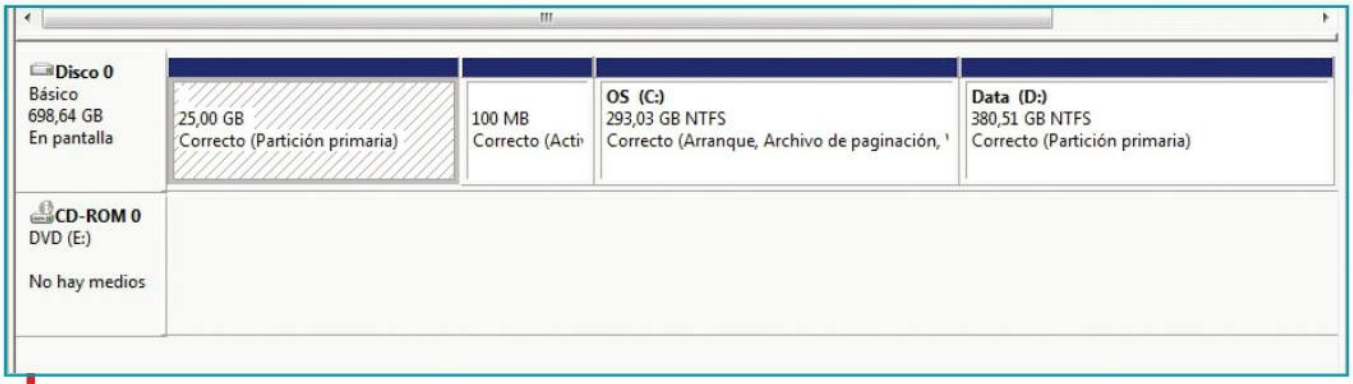
Cada **sistema de archivos** (formato) debe reconocer las particiones según su funcionamiento, ya que entre ellas serán independientes. Como todas las unidades están en el mismo disco físico, es preciso identificar cada una. Algunos sistemas de archivos están limitados en cuanto a la capacidad. Los formatos que fueron diseñados se distinguen en **FAT**, **FAT32**, **ext2**, **ext3**, **ext4**, **ext5**, **BTRS**, **FedFS**, **ReiserFS**, **NTFS**, etc. La principal diferencia entre ellos es el tamaño asignado a los clústeres, muy grandes en FAT (32 KB) y de menor tamaño para NTFS (4 KB). La disminución del tamaño de los clústeres les ha permitido a los sistemas superar barreras de almacenamiento. Los sistemas operativos viejos requieren formatos compatibles para los cuales fueron diseñados.

ES POSIBLE CREAR UNA UNIDAD PRIMARIA Y, DENTRO DE LA EXTENDIDA, VARIAS ADICIONALES.

Otros sistemas operativos precisan particiones por separado para poder instalarse. Por ejemplo, las distribuciones de Linux necesitan una partición de aproximadamente 2 GB (**swap**).



Gracias a la consola de comandos, es posible montar y desmontar unidades en distribuciones Linux.



En sistemas Windows, desde el Administrador de equipos podemos gestionar las particiones de los discos.

Seguridad

Por cuestiones de **seguridad**, una de las configuraciones más difundidas implica establecer particiones para el alojamiento de la información del usuario, separada de los archivos del sistema y las aplicaciones. Si el sistema operativo falla o las aplicaciones provocan errores irreparables que obliguen a formatear todo el sistema, la información del usuario quedará inalterada, alojada en la nueva partición. Existen diferentes esquemas de particiones para su distribución en el disco. Los más importantes son MBR (**Master Boot Record**, o registro maestro de booteo) y GPT (**GUID Partition Table**, o tabla de partición GUID). Para almacenar información, los discos deben tener un sistema de archivos (**FAT**, **NTFS**, etc., para discos duros, y **UDF** para unidades ópticas).

Gestión de unidades físicas

Cuando gestionamos las unidades físicas, es necesario crear correctamente la tabla de particiones. Esta se encuentra alojada en el MBR a partir del byte 446 y ocupa 64 bytes; contiene 4 registros de 16 bytes, los cuales definen las particiones primarias. En las tablas se aloja la información sobre la partición.

Particiones

Independiente del sistema de archivos utilizado, encontramos tres tipos de particiones distintas:

- **Partición primaria**: es la división primaria del disco. Solo pueden coexistir cuatro en el mismo disco, o tres primarias y una extendida. Un disco recién adquirido viene sin formato; al asignarle un sistema de archivos, se convertirá en su totalidad en una partición primaria completa.

- **Partición extendida**: por lo general, se la asocia con la partición secundaria. Cumple casi las mismas funciones que las primarias, con la diferencia de que puede alojar múltiples particiones lógicas. Es creada, fundamentalmente, para romper la barrera de las cuatro particiones máximas de sistemas anteriores.

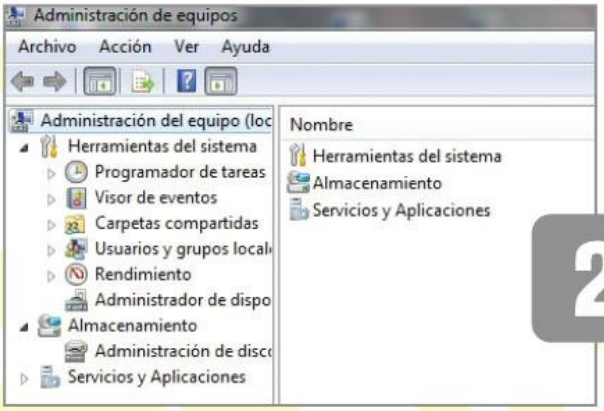
- **Partición lógica**: en general, ocupa la totalidad del espacio asignado para la partición extendida. Al ser administradas independientemente una de otra, a cada una de ellas se le puede asignar sistemas de archivos diferentes. Pueden existir hasta 23 particiones lógicas dentro de la extendida.

Al trabajar con una sola unidad física, y aun así contar con particiones, es importante tomar algunas precauciones. Ya que se trata del mismo disco, una falla general, electrónica o mecánica podría hacernos perder toda la información, sin importar la cantidad de unidades lógicas asignadas. Siempre hay que realizar backups para evitar inconvenientes. ■

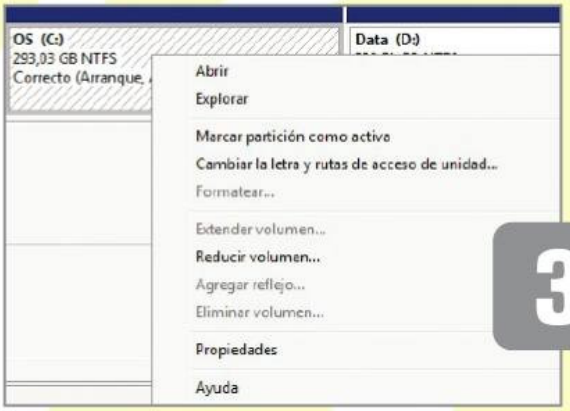
Particiones de disco en Windows y en Linux

Dentro de sistemas operativos comunes como Windows y Linux, podemos administrar los discos desde aplicaciones integradas.

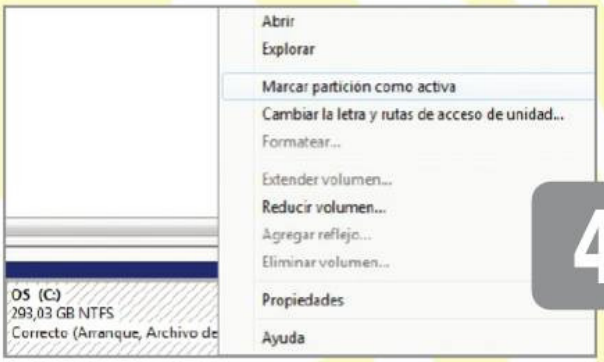
1



2



3



4

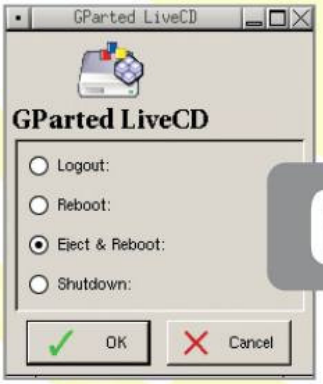
1 En primera instancia, necesitamos tener el disco duro instalado en la computadora. Una vez que esté correctamente conectado, podremos iniciar el equipo y generar las particiones que deseemos para instalar nuestros sistemas operativos.

2 Para sistemas basados en Windows, desde la misma plataforma ubicamos el icono de **Equipo**, hacemos clic derecho sobre él e ingresamos en **Administrar**. Aparecerá una interfaz que nos permitirá administrarlo. Necesitamos tener una cuenta de **Administrador**.

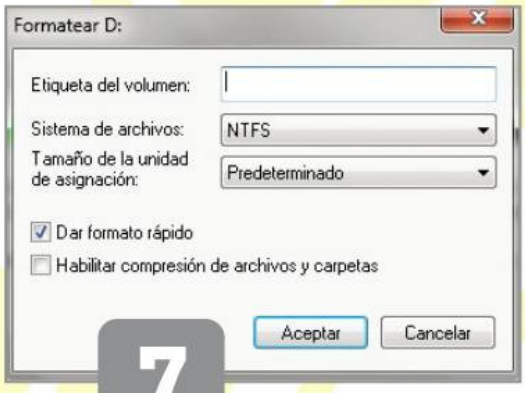
3 Ubicamos la opción **Administración de discos**, desde donde tendremos la capacidad de asignar todas las unidades, convertirlas, modificar su tamaño y establecer una como primaria, entre otras. Lo importante es tener clara la distribución que daremos a las particiones del disco.

4 Una vez distribuida la partición, debemos asignarla como primaria activa. Podemos darle el formato de archivos donde vamos a instalar el sistema operativo. Dentro de la partición extendida, asignaremos las particiones lógicas.

5



6



7

8

5 Las particiones se establecen de forma intuitiva: primaria para el sistema operativo (directorio raíz del sistema /), extendida para los datos (/home) y swap (área de intercambio que no requiere mucho espacio, con 2 GB bastará).

6 Estas separaciones podemos hacerlas según nuestras necesidades. Para distribuciones Linux, necesitamos usar una aplicación específica: **Gparted**. Se trata de un programa desarrollado para gestionar las particiones. Esta aplicación se presenta como programa instalable o como LiveCD.

7 Para los dos sistemas, los pasos que realizaremos secuencialmente serán: formatear (un clic sobre la partición desplegará las opciones), distribuir el espacio asignando particiones primarias y extendidas; y asignar un sistema de archivos compatible.

8 Siempre debemos ser cuidadosos, pues al formatear, perderemos toda la información alojada en el disco. Por lo tanto, es necesario realizar copias de seguridad y comprobar si existen errores en el disco. Solo así, no perderemos información importante.

Qué es NetBIOS

Para intercambiar archivos con otras terminales, las computadoras deben utilizar el protocolo NetBIOS. Aquí conoceremos sobre él.

IBM y **Sytec** desarrollaron en 1984 una interfaz de programación de aplicaciones (API, *Application Programming Interface*) para conectarse a la red e interactuar con ella. Se trata de **NetBIOS** (*Network Basic Input/Output System*, sistema básico de red de entrada/salida), con el cual los sistemas pueden tener acceso a los servicios de la red. Este software pudo enlazar sistemas operativos habituales al hardware específico (adaptándose al software sin enfocarse en el hardware). Con el correr de los años, el **protocolo** de aplicación NetBIOS se ha convertido en el API fundamental de la mayoría de los programas que interactúan e intercambian recursos con la red.

Protocolos

El protocolo NetBIOS debe ser transportado entre máquinas utilizando otros protocolos detallados a continuación:

- **IPC/IPX**: protocolo nativo de sistemas operativos de redes Novell (Novell Netware y Linux). El protocolo de intercambio de paquetes entre redes (IPX) es ruteable y orientado a comunicaciones sin conexión, pero en Internet solo se puede transportar si se encapsula en IP.

- **NetBEUI**: protocolo nativo de Windows, normalmente no ruteable; es una optimización realizada por Microsoft al NetBIOS para sus sistemas operativos. Los sistemas que lo implementan son varias versiones de Windows, y está programado para usar entre sistemas operativos de la misma compañía. Se puede transmitir por Internet, al igual que IPX, si se encapsula sobre IP.

El protocolo NetBEUI se utiliza para identificar a las computadoras por nombre en grupos de trabajo, en vez de utilizar las direcciones IP de cada máquina.

- **TCP/IP** o **UDP/IP**: encapsulado NetBIOS sobre protocolo Internet que permite compartir terminales remotas. Es el procedimiento más directo para encapsular la información cuando nos manejamos directamente con Internet. Sin embargo, el encapsulamiento se puede realizar sin notificación, lo que resulta en una entrada abierta a ataques por usuarios malintencionados.

Comunicación

Debemos tener en cuenta que cada dispositivo que se encuentra conectado a una red local NetBIOS puede realizar la comunicación con los otros dispositivos por medio de una conexión con otra terminal, usando datagramas NetBIOS o mediante **broadcast**. Cada una de estas sesiones permite realizar el envío de mensajes largos, y gestionar el control y la recuperación de los errores que se presenten, de modo que un dispositivo pueda comunicarse con otros al mismo tiempo, pero limitados en el tamaño del mensaje. ■

TCP vs. NetBIOS

El protocolo TCP/IP utiliza números para representar otros dispositivos (por ejemplo, 198.168.1.100), mientras que NetBIOS asigna nombres. Esto generó problemas al momento de relacionarlos. Para aplicarlos como compatibles, se emitieron los documentos RFC 1001 y 1002, donde se estandarizó la manera en que se relacionan. Este encapsulamiento es necesario para poder trabajar por Internet, y ha perdurado con el paso del tiempo.

PRÓXIMA ENTREGA

6 CONFIGURACIÓN DE REDES CABLEADAS

En el próximo fascículo conoceremos la forma en que se debe configurar una red cableada, desde los protocolos utilizados hasta la asignación adecuada de permisos.

Técnico en
REDES &SEGURIDAD

▶ PROFESORES EN LÍNEA
profesor@redusers.com
▶ SERVICIOS PARA LECTORES
usershop@redusers.com

SOBRE LA COLECCIÓN

CURSO VISUAL Y PRÁCTICO QUE APORTA LOS SABERES NECESARIOS PARA FORMAR TÉCNICOS EXPERTOS EN REDES Y SEGURIDAD. INCLUYE UNA GRAN CANTIDAD DE RECURSOS DIDÁCTICOS COMO INFOGRAFÍAS, GUÍAS VISUALES Y PROCEDIMIENTOS REALIZADOS PASO A PASO.

Con la mejor metodología para llevar adelante el montaje y mantenimiento de las redes informáticas y con los aspectos clave para brindarles la protección necesaria, esta obra es ideal para aquellos aficionados que deseen profundizar sus conocimientos y para quienes quieran profesionalizar su actividad.

REDES &SEGURIDAD 00005
9 789871 857784

CONTENIDO DE LA OBRA