



Argentina \$ 22.- // México \$ 49.-

3

Técnico en

REDES & SEGURIDAD

DISPOSITIVOS DE RED

En este fascículo conoceremos el hardware utilizado en redes, así como también sus funciones y características. Además, todos los aspectos fundamentales sobre seguridad en redes cableadas.



Incluye libro:
Aspectos legales

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

Curso visual y práctico Técnico en redes y seguridad es una publicación de Fox Andina en coedición con Dálaga S.A. Esta publicación no puede ser reproducida ni en todo ni en parte, por ningún medio actual o futuro sin el permiso previo y por escrito de Fox Andina 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.

Copyright © Fox Andina S.A. I, MMXIII.



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...

Dispositivos y cables utilizados en redes.
Además, realizaremos procedimientos
prácticos, como la colocación de fichas
RJ-45 y la instalación de placas de red PCI.



En la clase anterior, vimos los conceptos relacionados con los tipos de redes y sus topologías, clasificamos las redes dependiendo de su alcance y extensión, y también vimos en detalle las topologías de red que existen y los estándares Ethernet. Por otra parte, analizamos las características del modelo OSI, describimos las principales particularidades de cada una de sus capas, vimos el funcionamiento del protocolo TCP/IP y, finalmente, dimos un vistazo a ciertos conceptos importantes sobre seguridad.

En la presente entrega, nos dedicaremos a revisar los principales dispositivos y cables que utilizaremos en una red de datos. Conoceremos cada uno de ellos, y mencionaremos sus características y ventajas. Aprenderemos a colocar las fichas RJ-45 en los cables de par trenzado e instalaremos una placa de red PCI. Para continuar, veremos qué son las subredes y revisaremos algunos conceptos sobre seguridad.

3

2

Dispositivos utilizados en redes

6

Tipos de cable de par trenzado

16

Paso a paso: Instalar una placa de red PCI

18

¿Qué son las subredes?





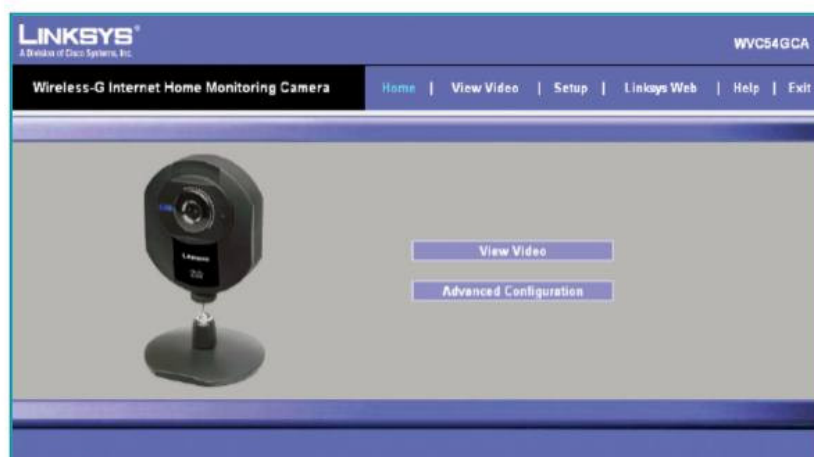
Dispositivos utilizados en redes

En estas páginas conoceremos los detalles y características de los dispositivos imprescindibles para implementar una red, como aquellos que cumplen funciones específicas o generales.

Aquellos dispositivos que nos permiten comunicarnos con otros equipos, desde una PC hacia otra PC o a la impresora que se encuentra conectada en la red, son considerados dispositivos utilizados en redes. Según nuestra necesidad, podemos adquirir dispositivos de menor o mayor complejidad, que se diferencian en primarios y secundarios. Los primeros son necesarios para la conexión de red, en tanto que los segundos son los que se usan para una función en particular, pero cuya ausencia no afecta el desempeño de la red en su conjunto. A continuación, veremos en detalle cada uno de ellos.

Placa de red Ethernet

También llamado **NIC** (*Network Interface Card*), es el dispositivo principal de una red, ya que por medio de él se conectan los demás dispositivos a través del cable de par trenzado. Existen placas de red Ethernet para PC o notebooks, y algunas



Esta imagen nos muestra una captura de la sección de administración de una cámara de seguridad IP.

ya vienen incorporadas al motherboard. Si esta placa llega a fallar, es posible conseguir otras con formato PCI o, incluso, USB. Su velocidad puede llegar hasta 1000 Mbps (*Gigabit Ethernet*).

El funcionamiento de esta placa es sencillo: recibe las señales de la PC y las transmite por la boca de conexión hacia otra placa Ethernet conectada en otra PC, que procesa las señales recibidas.



Configuración de dispositivos

Los routers y switches de capa 3 pueden configurarse por medio del navegador, asignando previamente una dirección IP fija a la PC que está conectada. Luego, si activamos la configuración del router para que entregue direcciones lógicas de manera automática (DHCP), podemos optar por cambiar la IP de la PC, para que tome automáticamente la asignada por el router. Los routers de mayor complejidad utilizan un tipo de cable especial llamado cable consola para realizar su configuración.

Antes existían las placas con conexión por BNC, que utilizaban cable coaxial, pero actualmente están en desuso.

Interfaz inalámbrica

Tiene un funcionamiento similar al de la **placa de red Ethernet**, pero no utiliza cables sino ondas de radio. En la actualidad, esta interfaz forma parte de todos los equipos portátiles, como notebooks, **tablets**, **smarthphones** y consolas de videojuegos. La velocidad depende de la tecnología, y los distintos tipos se diferencian por letras, tal como se aprecia en la tabla de la página 5.

Hub o concentrador

Fue el primer dispositivo que permitió conectar varios equipos. Su funcionamiento consistía en repetir la señal que recibía. Por ejemplo, imaginemos un **hub** con 8 puertos, en cada uno de los cuales se conectaba una PC. Cuando la PC1 enviaba datos a la PC2, el hub recibía la señal por el puerto de conexión de la PC1 y la reenviaba por los demás puertos (PC2 a PC8). La PC2 recibía la señal y la decodificaba, mientras que los demás equipos descartaban el mensaje, porque no estaba dirigido a ellos. Esto traía como consecuencia la generación de tráfico en vano, que ralentizaba el funcionamiento de la red. Actualmente, el hub se encuentra en desuso.

LAS FUNCIONES DEL ROUTER O DE UN FIREWALL PUEDEN IMPLEMENTARSE CON UN SERVIDOR DEDICADO.

Puente o bridge

Un **puente** puede considerarse como la versión mejorada de un hub; físicamente, son muy parecidos, pero su funcionamiento es distinto. El puente trabaja en la capa 2 del modelo OSI (enlace de datos) y está diseñado para segmentar la red en dominios de colisiones. Posee una pequeña memoria donde se almacenan las direcciones MAC



Las placas de red con varios puertos suelen ser utilizadas en servidores.

de los equipos conectados a él (tabla de puente), de manera que, al recibir una trama de datos para enviar, compara la dirección MAC de destino con su tabla. Si dicha MAC se encuentra en el mismo segmento de la red que el origen, no envía los datos a otros segmentos, lo que reduce el tráfico y permite que más de un dispositivo mande datos simultáneamente. Cuando el puente recibe una trama para una MAC que no está almacenada en su tabla, transmite los datos a todos los dispositivos conectados, menos a aquel desde el cual los recibió. Hace un tiempo, el puente se utilizaba en conjunto con el hub; por ejemplo, había hubs en cada oficina (ventas, marketing, call center), y estos, a su vez, se conectaban a un puente central para compartir información.

Switch

El **switch** reemplazó la combinación de hubs y puentes. Puede tener varios puertos, lo que permite ampliar la red fácilmente, y su funcionamiento es similar al de un puente. Podría definirse al switch como un puente multipuerto. Para su funcionamiento, se basa en las direcciones MAC, generando una tabla con aquellas que están conectadas a cada puerto. Es posible conectar dos o más switches entre sí, y cada uno aprenderá del otro sus respectivas tablas de MAC (tablas de conmutación). Al igual que sucede con el

puente, para su funcionamiento el switch compara, de las tramas recibidas, la dirección MAC de destino con su tabla de conmutación, y reenvía las tramas al puerto correspondiente. Existen switches de **capa 3** (red) que operan con direcciones IP y tienen algunas de las funciones de un router, como la posibilidad de crear redes virtuales (**VLAN**) y establecer el límite de ancho de banda a puertos específicos.

Router

Este dispositivo nos permite conectarnos a una **WAN** (*Wide Area Network*), es decir, a Internet.



El periscopio evita tener cables colgando cuando no hay ningún equipo conectado a la patchera.

Trabaja en la capa 3 del **modelo OSI** (red) y envía paquetes de datos basándose en direcciones IP. El **router** puede tomar decisiones sobre cuál es la mejor ruta para el envío de paquetes, y admite que se conecten a él diferentes tecnologías, como Ethernet y fibra óptica, ya que toda su conmutación se realiza por medio del protocolo IP. Al trabajar en la capa 3, tiene su propia IP (que se puede configurar) y, además, es posible configurarlo para que entregue automáticamente direcciones IP a los dispositivos que se van conectando (**DHCP**) de manera directa o indirecta (por ejemplo, a través de un switch). Su funcionamiento es sencillo: analiza los paquetes entrantes, elige la mejor ruta para reenviarlos y los conmuta por el puerto correspondiente. El modelo de router y la complejidad de configuración dependerán de lo que necesitemos. Podemos encontrar routers que admiten un solo proveedor ISP, y otros que pueden admitir simultáneamente dos o más proveedores, conexiones VPN, etc.

Router inalámbrico

Un router inalámbrico posee las mismas características que uno tradicional, pero con el agregado de que permite realizar conexiones inalámbricas. Además, para acceder a la conexión proporcionada por ellos se pueden establecer contraseñas con diferentes tipos de cifrado, destinadas a proteger la red, tal como se observa en la tabla que sigue a continuación.

Routers inalámbricos	
Norma	Nivel de seguridad
Abierta	Sin petición de contraseña
WEP	64 bits, contraseña de 5 caracteres 128 bits, contraseña de 13 caracteres 256 bits, contraseña de 29 caracteres
WPA / WPA2	Llave pública, de 8 a 63 caracteres
Filtrado MAC	Solo las MAC dadas de alta en el router podrán conectarse a la red

Repetidor

Las señales pierden integridad a medida que avanzan por la longitud del cable, y esto limita la distancia que pueden cubrir. Para evitar esta restricción, se utilizan repetidores, que trabajan en la capa 1 del modelo OSI, cuya única función es regenerar la señal de entrada y enviarla a su salida.

LOS ROUTERS INALÁMBRICOS TRABAJAN CON ONDAS DE RADIO. SI PONEMOS DOS CERCANOS, DEBEMOS ESTABLECER CANALES DE FRECUENCIA DISTINTOS.

Access point

Su función es permitir la conexión inalámbrica a la red cableada establecida o llegar a lugares donde la señal Wi-Fi sea débil, ya que tiene conexión directa por cable con el router. Se le asigna una dirección IP para su configuración. Es posible utilizar un router inalámbrico como access point, pero sus funciones serán limitadas, ya que el modo AP, o un AP, deja las funciones principales al router.

Firewall

Si bien el router posee algunas funciones de seguridad, estas son limitadas en comparación con las de un **firewall**. Este dispositivo examina cada paquete de la red, y decide si enviarlo o bloquear su acceso para permitir solo el tráfico seguro. Es utilizado principalmente en entidades bancarias como complemento para efectuar transacciones.

Patcheras

Cuando la red de una empresa crece de manera significativa, es preciso dedicar un espacio exclusivo a los dispositivos que la componen, como servidores, routers, switches, etc. La **patchera** es un elemento pasivo que sirve para mantener organizado el cableado estructurado, de modo que, ante un inconveniente, sea rápido y sencillo ubicar el cable y el puerto afectados, y se llegue a una pronta solución.



La patchera puede venir en módulos desmontables o toda armada; incluso, hay patcheras con forma de V.



La **Sling Box Tuner** permite realizar streaming de video de alta calidad en toda la red, incluso, a través de Internet.

Se conecta directamente al router o switch, mientras que los equipos lo hacen a la patchera. Por ejemplo, si disponemos de varios switches de 32 bocas, en los cuales se conectan todos los equipos de una empresa, podemos optar por poner patcheras de 16 bocas o de diferentes colores, para separar el cableado en grupos y así facilitar la identificación de los equipos.

Periscopio o roseta

Se trata de un pequeño gabinete que se ubica debajo del escritorio o en un punto central de la oficina. El periscopio es el extremo de la patchera, y en él encontramos la boca en la que se conectará el cable del equipo (impresora, PC, notebook, etc.). La ventaja de este elemento es que permite mantener el orden y la prolijidad del cableado, ya que en el mismo **periscopio**, según el modelo, podemos contar con puertos RJ-45, USB y tomacorrientes.

Gateway

Un **gateway** o puerta de enlace es un dispositivo que permite conectar redes de protocolos o arquitecturas diferentes. El router, por ejemplo, tiene funciones de gateway, ya que permite conectar la red local (LAN) con la externa (WAN). Por otra parte, un gateway USB posee una entrada de red RJ-45 y un puerto USB. Si instalamos el software del dispositivo, luego podremos acceder desde la red a cualquier equipo que se haya conectado a ese USB, como una impresora, un escáner o un disco externo. Un ejemplo es el **Encore ENNUS1**.

Módem USB 3G / 3.5G

Se trata de un dispositivo que brinda conexión a Internet utilizando tecnología celular. Físicamente, tiene la apariencia de un pen drive. Posee espacio para insertar una memoria microSD y un slot para colocar el chip de telefonía celular. Al igual que los celulares, estos módems vienen bloqueados para usarlos únicamente con chips del proveedor al que se los

Transferencia inalámbrica	
Norma	Velocidad de transferencia
802.11a	25 - 54 Mbps
802.11b	5 - 11 Mbps
802.11g	25 - 54 Mbps
802.11g+	25 - 108 Mbps
802.11n	50 - 300 Mbps

adquirimos. Incluyen el propio software para la conexión, lo cual los convierte en una herramienta muy útil para efectuar una conexión inmediata. La velocidad de conexión estará limitada por la infraestructura que posea el proveedor; generalmente, es de mayor velocidad en lugares céntricos, y disminuye a medida que nos alejamos.

Sistema de vigilancia IP

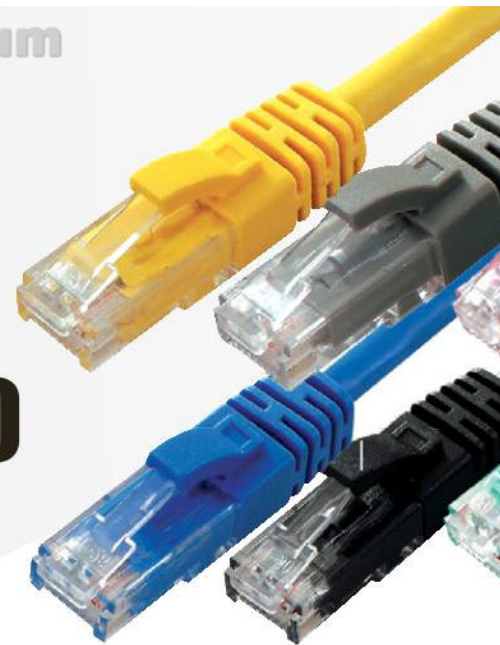
Se trata de un equipo **NVR** (*Network Video Recorder*) al que se le pueden conectar 4, 8 o 16 cámaras de vigilancia de manera cableada. El NVR se conecta al router, y se puede acceder a él desde la propia red interna o a través de Internet, usando un nombre de usuario y contraseña. El NVR suele tener un sistema operativo Linux adaptado para tal fin. Admite el agregado de discos rígidos para almacenar las filmaciones, y de forma automática, esas se pueden ir eliminando a medida que se graban las nuevas. También da la posibilidad de enviar mails con fotos adjuntas ante la detección de movimiento en lugares que hayamos configurado como críticos. ■

Skype

Es uno de los programas utilizados para realizar llamadas telefónicas. Incluso, es posible contratar un número o desviar llamadas a nuestro celular, y comprar paquetes de minutos fijos para llamadas a celulares o telefonía fija, con costos accesibles. Skype fabricó dispositivos que, físicamente, son similares a un celular y se conectan a sus servicios utilizando cualquier red inalámbrica disponible.



Tipos de cable de par trenzado



Conoceremos las principales características y usos de los diversos cables de par trenzado.

El cable de par trenzado está formado por dos conductores eléctricos aislados, los cuales son entrelazados para anular interferencias de fuentes externas. Como realiza el transporte de la señal en modo diferencial, uno es positivo, y el otro, negativo; por esta razón, la señal total transmitida está dada por la resta de ambas positivo - negativo. Se trata del medio universal para la conexión de redes cableadas.

Cables de datos

Los cables de datos están constituidos por grupos de pares trenzados, cables multipares, en los que podemos encontrar cables de 2, 4, 6, 8, 14, 25, 28, 56, 112, 224 o hasta 300 pares (los cables mayores a 25 pares son utilizados en general por empresas de servicios, y su cableado es subterráneo). El cable por fibra óptica ofrece una mayor velocidad y puede abarcar distancias mayores; pero debemos tener en cuenta que su precio es elevado para redes de pequeña distancia, en las cuales se requieren pocos metros de longitud.

Categorías

Los cables utilizados para la transmisión de señales se diferencian en categorías para su uso:

► **Categoría 1:** es el cable utilizado para la telefonía convencional. Está formado por 2 pares de cables trenzados.

Su velocidad es inferior a 1 Mbps.

► **Categoría 2:** utilizado por algunas redes como Apple Talk (protocolo de red de Apple). Está compuesto por 4 pares de cables. Su velocidad máxima puede llegar hasta 4 Mbps.

► **Categoría 3:** utilizado por redes con una velocidad de hasta 16 Mbps. Debemos tener en cuenta que esta categoría de cable se encuentra definida por la norma 10BaseT.

► **Categoría 4:** puede soportar un flujo de datos menor a 20 Mbps. Se usa principalmente en redes token ring (arquitectura de red diseñada por IBM).

► **Categoría 5:** es el más utilizado en la actualidad. Puede transmitir datos a 10 Mbps y 100 Mbps, aunque se puede usar para conexiones de 1 Gbps en full duplex.

EL CABLE POR FIBRA ÓPTICA OFRECE UNA MAYOR VELOCIDAD Y PUEDE ABARCAR DISTANCIAS MÁS GRANDES, PERO SU PRECIO ES ELEVADO PARA REDES DE PEQUEÑO TAMAÑO.

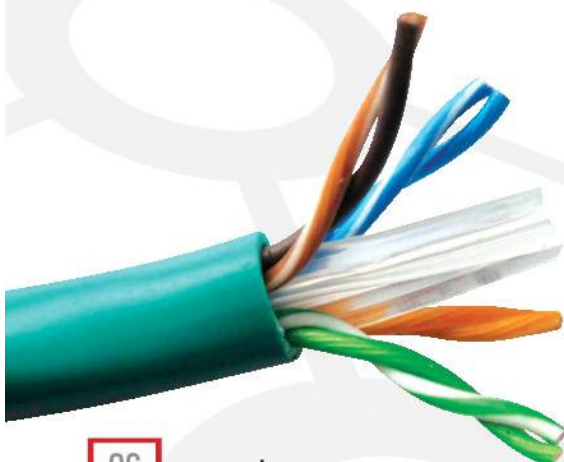
Está normalizado por el estándar 100BaseT.

► **Categoría 5e:** es la versión mejorada de la categoría 5. Se utiliza para velocidades de 100 Mbps y 1 Gbps.


► **Categoría 6:** se usa para velocidades de 1 Gbps. Este tipo de cable, en su interior, incluye un separador plástico, que aísla a cada par trenzado.

► **Categoría 6e:** se trata de un cable que puede ser utilizado en conexiones de hasta 10 Gbps.

► **Categoría 7:** está diseñado para transmitir en 10 Gbps. Es compatible con las categorías 5/5e/6/6e. Se diferencia de los anteriores porque cada par está aislado, y una malla recubre los pares, lo que reduce las interferencias que podrían afectarlo.



Cable de par trenzado de categoría 6. Podemos ver el cable de drenaje, la cubierta metálica y también el separador interno.



La malla externa de color en el cable UTP puede ser útil para diferenciar la conexión entre distintos equipos.

► **Categoría 8:** soporta frecuencias de hasta 1200 MHz. Es un cable multipropósito, es decir, se lo puede implementar para conexiones de telefonía convencional y para transmisión de señales de banda ancha. En su interior posee un alambre de drenaje, que en contacto con la pantalla de aluminio (que recubre a todos los pares), reduce la impedancia.

Recubrimiento

Además de la diferenciación por categoría, los cables de par trenzado se distinguen por su recubrimiento externo (malla del cable), característica que los hace adecuados para instalaciones internas o externas; entre ellos podemos encontrar:

► **UTP** (*Unshielded Twisted Pair*): cable de par trenzado sin apantallar. Sus pares trenzados están en contacto (separados por la malla que recubre a cada conductor) y solo recubiertos por su malla externa. Su manipulación es sencilla, ya que es el más flexible de todos los cables. Es el tipo más utilizado en cableados internos.

► **STP** (*Shielded Twisted Pair*): cable de par trenzado apantallado. Sus pares se encuentran en contacto, pero todos están recubiertos por un protector de aluminio, para reducir las interferencias externas. También llevan una malla exterior.

► **FTP** (*Foiled Twisted Pair*): similar al STP, pero en vez de estar recubierto por una pantalla de aluminio, utiliza una pantalla conductora global trenzada. Su manipulación es más compleja, ya que si se dobla demasiado el cable, los conductores internos pueden romperse.

► **SFTP** (*Screened Fullyshielded Twisted Pair*): cable de par trenzado de apantallado total. En este caso, cada par trenzado está protegido por una cubierta de aluminio o pantalla trenzada, y luego, todos están resguardados por otra capa de cubierta metalizada, para ofrecer una mayor protección a interferencias de origen externo. Su manipulación es muy complicada, y se lo usa, en especial, para cableados troncales.

Distancias

Existen distancias máximas que se pueden cubrir sin necesidad de tener repetidores de señal. La nomenclatura se puede dividir en tres partes, que son las siguientes:


- La primera parte hace referencia a la velocidad máxima de transmisión que corresponde, expresada en Mbits.
- La segunda parte de la nomenclatura se usa para el tipo de transmisión, banda base o banda ancha.
- La tercera parte es un número o letra, que puede indicar la distancia máxima o el medio físico para el cual se establecen los puntos que mencionamos anteriormente.

A partir de esto, para el cable de par trenzado, tenemos:

- **10BaseT:** establece una conexión para 10 Mbps, en banda base, para cable de par trenzado (categoría 3 o superior), con una distancia máxima de 100 metros.
- **1Base5:** para conexiones de 1 Mbps, en banda base, con una distancia máxima de 100 metros.
- **100BaseTX:** para cables de categoría 5 a una velocidad de 100 Mbps, en banda base; tengamos en cuenta que ofrece una distancia máxima de 100 metros.
- **1000BaseT:** es adecuada para cable de categoría 5 o superiores; establece una velocidad de 1000 Mbps (1 Gbps) para distancia máximas de 100 metros.

Extremos

Para los extremos del cable de red de par trenzado, se utilizan unas fichas especiales, similares a las de cableado telefónico, pero más grandes, llamadas RJ-45. Con ayuda de una pinza crimpadora, podremos armar el cable de red. Si tenemos que dejar una boca o varias para futuras conexiones, conectamos el extremo del cable (un cable por boca) a la roseta. Para probar el cable de red, podemos utilizar un tester, que nos permite identificar rápidamente si algún par no está bien armado. ■

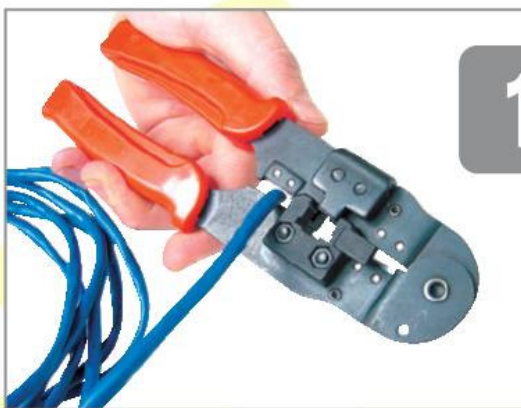


Cable de par trenzado de 25 pares, utilizado en telefonía. Además de la separación de colores de pares, puede presentar cintas separadoras.

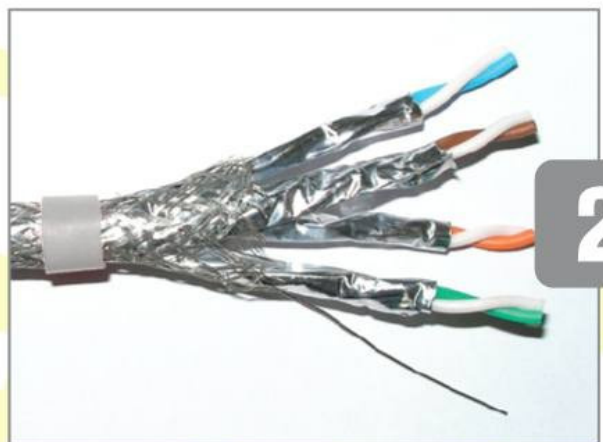


Colocar fichas en cables de par trenzado

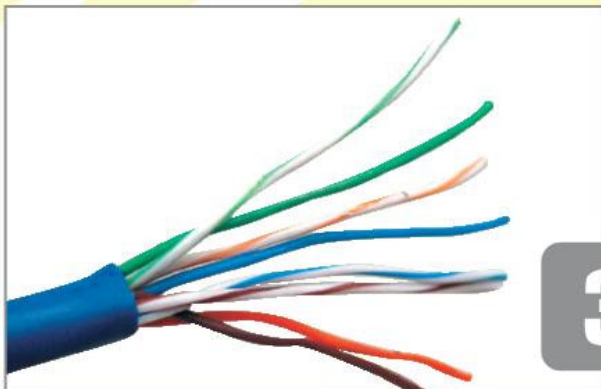
Un cable UTP bien armado nos ahorra una serie de futuros problemas de conexión. Colocar las fichas es sencillo, aunque requiere de precisión.



1



2



3



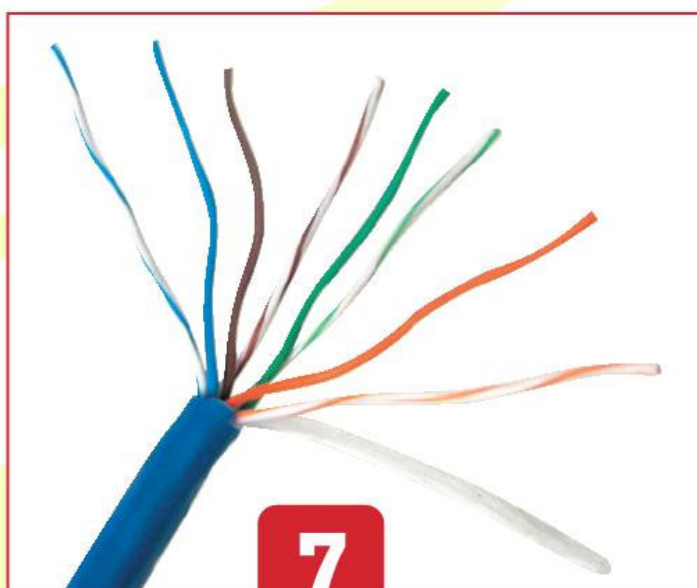
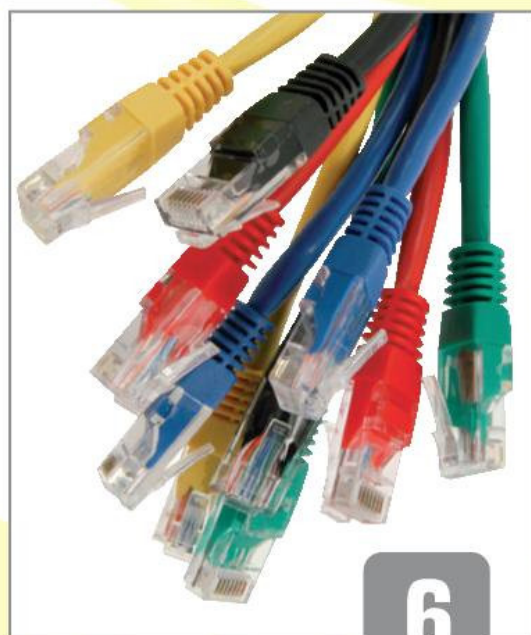
4

1 Usando la pinza crimpadora, tomamos el cable UTP y cortamos con mucho cuidado la cobertura que protege los ocho filamentos trenzados. Debemos asegurarnos de que el corte no afecte ni siquiera mínimamente los filamentos, ya que es indispensable conservar la integridad de estos para lograr una conexión efectiva.

2 La colocación de un capuchón protector alarga la vida útil del cable, y disminuye el ingreso de humedad y polvo al interior de la ficha RJ-45. Antes de los siguientes pasos, colocamos el protector y lo dejamos libre mientras trabajamos con los filamentos.

3 Debemos liberar al menos 4 cm de filamentos con el fin de trabajar en el alisado y el ordenamiento por colores, según la norma que hayamos establecido. Una vez ordenados, tomamos los filamentos desde la base y los cortamos en forma recta con una extensión aproximada de 1,5 cm.

4 Antes de poner los cables en la ficha RJ-45, debemos cortar cuidadosamente los extremos. La colocación en la ficha debe hacerse con precisión, cuidando que el orden de colores no se altere y que los cables hagan tope en el extremo de la ficha, ubicada con los pines a nuestra vista.



5 Regresamos a la pinza crimpadora y colocamos la ficha RJ-45 en el compartimento correspondiente. Presionamos firmemente; si consideramos necesario, lo hacemos dos veces. Una vez crimpada, sujetamos la ficha y tiramos con suavidad del cable para asegurarnos de que los filamentos estén ajustados.

6 Es importante recordar o establecer una norma para ordenar los filamentos cruzados de los cables. Consideremos que existen dos normas estandarizadas: la TIA-568 y la TIA-568B. Los cables que por lo general nos conectan a Internet guardan la misma norma en sus dos extremos. Si deseamos conectar dos dispositivos, como, por ejemplo, dos switches, será necesario que el cable utilizado posea una norma distinta en cada uno de sus extremos. También es posible adquirir cables ya preparados y listos para usar.

7 Aunque es sencilla, es importante prestar atención a esta tarea. Un cable mal crimpado, ya sea por falta de presión en los pines de la ficha o por no seguir algunas de las normas estandarizadas, nos implicará mayor tiempo de trabajo en el diagnóstico de un problema de conexión.

Componentes de redes

LAS REDES ACTUALES UTILIZAN TODO TIPO DE COMPONENTES. CADA UNO CUMPLE SU FUNCIÓN ESPECÍFICA, DESDE DARNOS ACCESO A INTERNET, HASTA INTERCONECTAR DOS REDES DE DISTINTO TIPO, PASANDO POR DISPOSITIVOS PARA IMPULSAR LA SEÑAL INALÁMBRICA.



Tarjeta PCI

Una tarjeta de red PCI le permite a cualquier equipo de escritorio formar parte de una red cableada. Existen, además, interfaces de red externas USB, o en formato CardBus, y también, tarjetas para redes de fibra óptica.



Repetidor Wi-Fi

Los repetidores Wi-Fi reciben la señal inalámbrica emitida por un access point y vuelven a emitirla, para así alcanzar mayores distancias. Son ideales para viviendas de más de una planta o departamentos de varios ambientes.

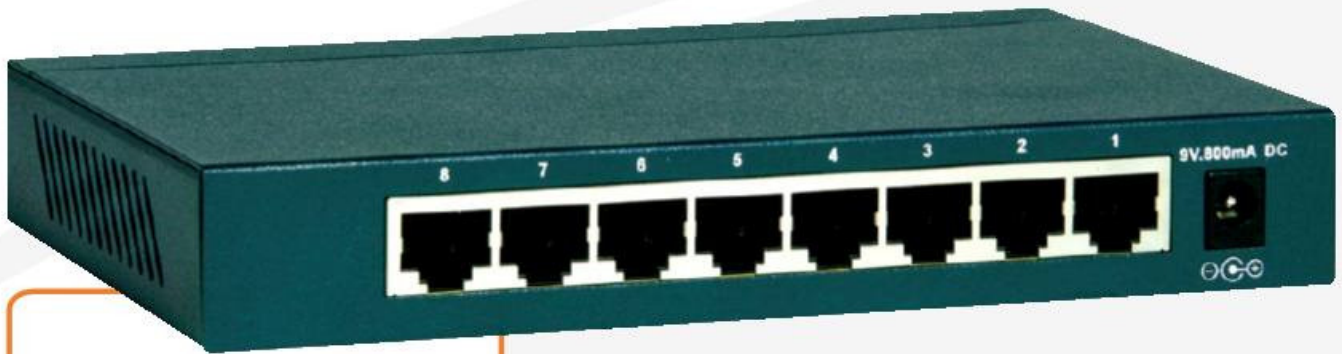
Uplink

Los dispositivos como el switch fueron diseñados para poder conectarse entre sí. Cuando se interconectan varios switches, hablamos de un stacking o apilamiento. Debemos tener en cuenta que es posible apilar hasta cuatro switches, aunque necesitamos contar con los dispositivos que tienen un conector señalado como uplink para cumplir esta función. De esta forma, si seguimos agregando computadoras a una red y se acaban los puertos disponibles, podremos conectar otro hub al ya existente y, entonces, seguir conectando más equipos, haciendo que nuestra red pueda crecer sin inconvenientes. Sin duda, se trata de una forma muy sencilla para conectar más equipos a una red de datos.



Módem

Los módems de banda ancha cumplen la función de convertir la señal que llega por el cable coaxial a un cable de red de par trenzado. Son un buen ejemplo de gateway, ya que permiten establecer la conexión de dos redes totalmente distintas.



HUB

Los hubs ya están en desuso debido a su escasa eficiencia al entregar paquetes de red de una PC a otra. Como no poseían la electrónica suficiente, cada paquete enviado debía recorrer toda la red hasta dar con el destinatario.



Router

Los routers se emplean generalmente en grandes corporaciones, data centers y proveedores de Internet. Funcionan de manera similar a los switches, pero con mayor eficiencia: pueden analizar las diferentes rutas e interconexiones para elegir la menos congestionada, la más veloz, y saltar enlaces caídos.



Gateway

Un gateway es un dispositivo que cumple la función de unificar dos o más redes de diferente tipo o medio de conexión. Por ejemplo: una Ethernet 100BaseTX con una red basada en ArcNet. De esta forma, se presenta como un dispositivo esencial para empalmar redes ya creadas, sin que sea necesario realizar la tarea de volver a implementar una de ellas.



Access point

Los access points nos permiten dar conexión de red e Internet a varios equipos vía cable de par trenzado (TP) y a decenas de equipos mediante la conexión inalámbrica incorporada. Dependiendo de la marca y del modelo de access point que tengamos, nos encontraremos con una interfaz de configuración distinta, a través de la cual accederemos a todas las opciones de configuración necesarias para utilizar las opciones del dispositivo.

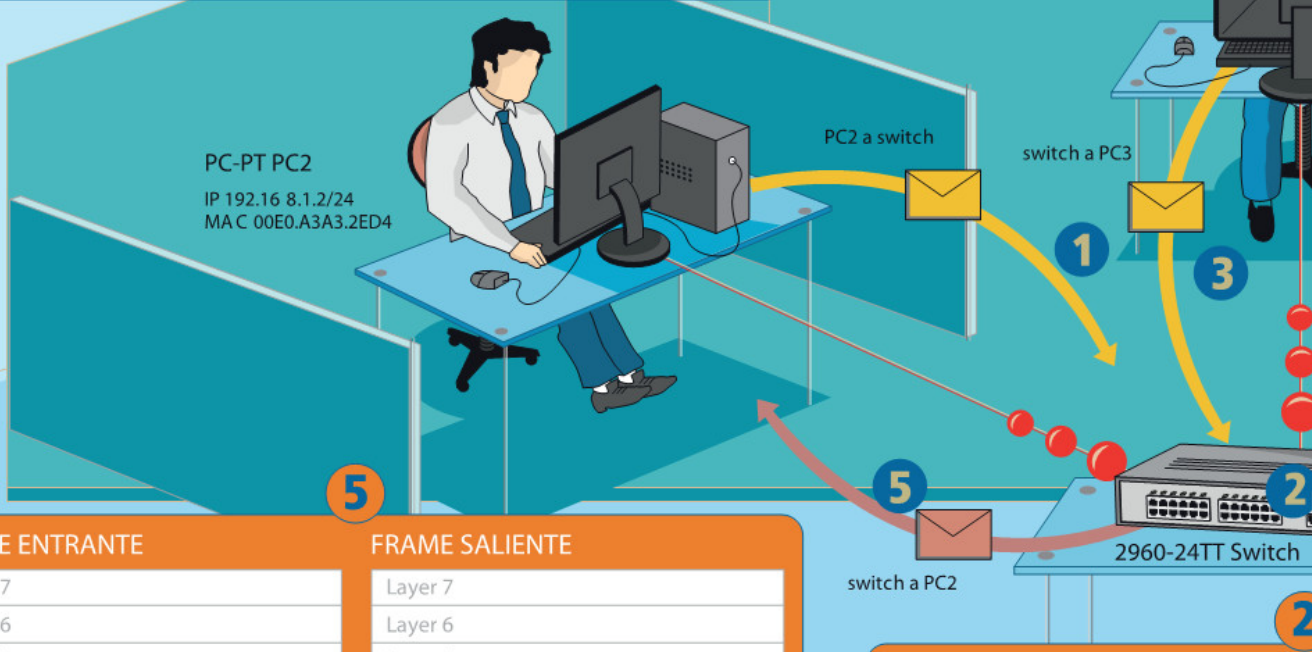
→ El switch

1

FRAME ENTRANTE	FRAME SALIENTE
Layer 7	Layer 7
Layer 6	Layer 6
Layer 5	Layer 5
Layer 4	Layer 4
Layer 3	Layer 3: IP Header Src. IP: 192.16 8.1.2, Dest. IP: 192.16 8.1.4 ICMP Message Type: 8
Layer 2	Layer 2: Ethernet II Header 00E0.A3A3.2ED4 >> FF:FF:FF:FF:FF:FF:
Layer 1	Layer 1: Port(s): Fast Ethernet

2

FRAME ENTRANTE
Layer 7
Layer 6
Layer 5
Layer 4
Layer 3
Layer 2: Ethernet II Header 00E0.A3A3.2ED4 >> FF:FF:FF:FF:FF:FF:
Layer 1: Port(s): Fast Ethernet



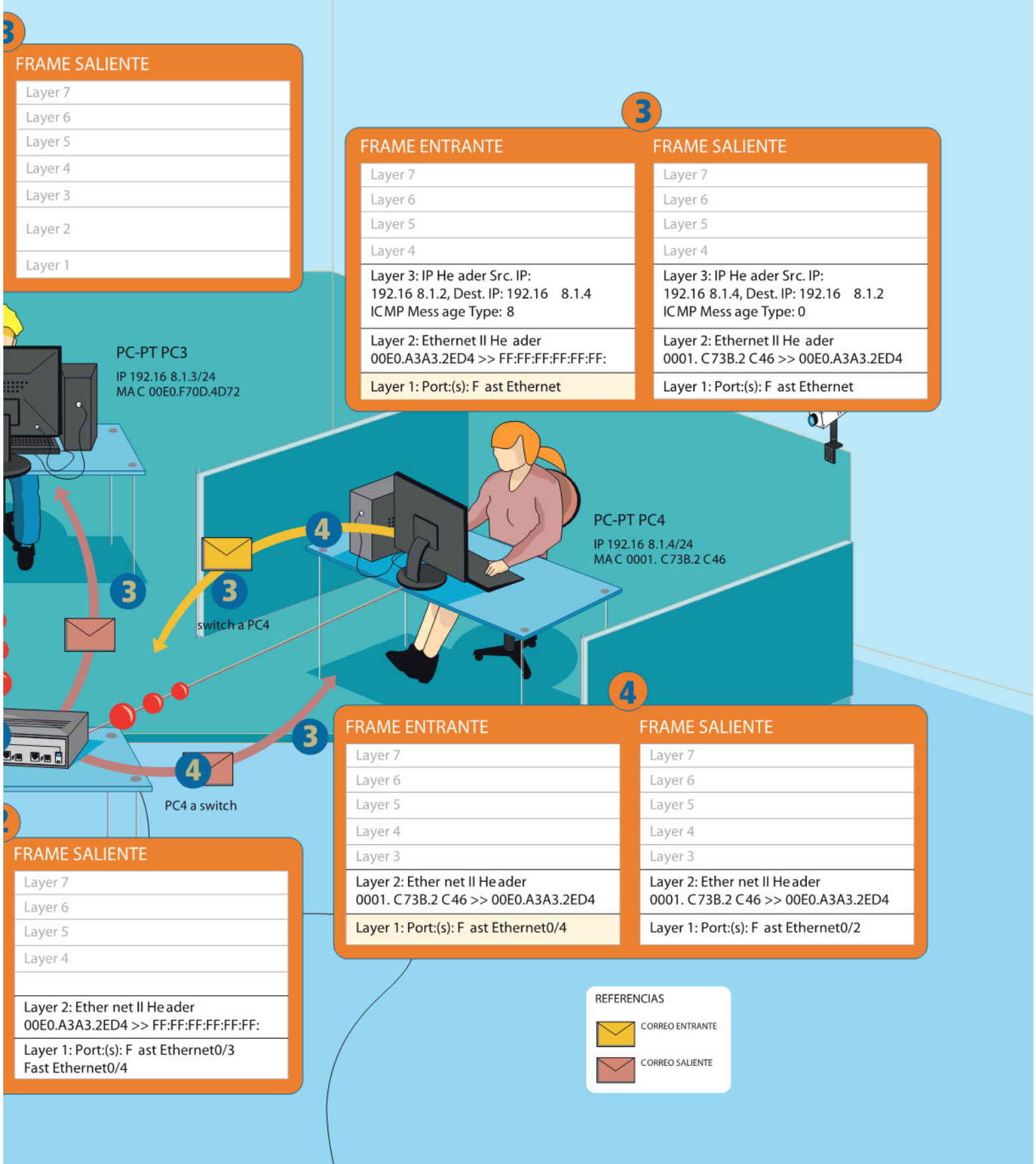
5

FRAME ENTRANTE	FRAME SALIENTE
Layer 7	Layer 7
Layer 6	Layer 6
Layer 5	Layer 5
Layer 4	Layer 4
Layer 3: IP Header Src. IP: 192.16 8.1.4, Dest. IP: 192.16 8.1.2 ICMP Message Type: 0	Layer 3
Layer 2: Ethernet II Header 0001. C73B.2 C46 >> 00E0.A3A3.2ED4	
Layer 1: Port(s): Fast Ethernet	Layer 1

2

FRAME ENTRANTE
Layer 7
Layer 6
Layer 5
Layer 4
Layer 3
Layer 2: Ethernet II Header 00E0.A3A3.2ED4 >> FF:FF:FF:FF:FF:FF:
Layer 1: Port Fast Ethernet0/2

UN SWITCH ES UN DISPOSITIVO DISEÑADO PARA AYUDAR A RESOLVER PROBLEMAS DE RENDIMIENTO EN LA RED, COMO ANCHOS DE BANDA PEQUEÑOS Y EMBOTELLAMIENTOS. AQUÍ LO CONOCEREMOS.



FRAME SALIENTE

Layer 7
Layer 6
Layer 5
Layer 4
Layer 3
Layer 2
Layer 1

FRAME ENTRANTE

Layer 7
Layer 6
Layer 5
Layer 4
Layer 3: IP Header Src. IP: 192.16 8.1.2, Dest. IP: 192.16 8.1.4 ICMP Message Type: 8
Layer 2: Ethernet II Header 00E0.A3A3.2ED4 >> FF:FF:FF:FF:FF:FF:
Layer 1: Port(s): Fast Ethernet

FRAME SALIENTE

Layer 7
Layer 6
Layer 5
Layer 4
Layer 3: IP Header Src. IP: 192.16 8.1.4, Dest. IP: 192.16 8.1.2 ICMP Message Type: 0
Layer 2: Ethernet II Header 0001.C73B.2C46 >> 00E0.A3A3.2ED4
Layer 1: Port(s): Fast Ethernet

FRAME SALIENTE

Layer 7
Layer 6
Layer 5
Layer 4
Layer 3
Layer 2: Ethernet II Header 00E0.A3A3.2ED4 >> FF:FF:FF:FF:FF:FF:
Layer 1: Port(s): Fast Ethernet0/3

FRAME ENTRANTE

Layer 7
Layer 6
Layer 5
Layer 4
Layer 3
Layer 2: Ethernet II Header 0001.C73B.2C46 >> 00E0.A3A3.2ED4
Layer 1: Port(s): Fast Ethernet0/4

FRAME SALIENTE

Layer 7
Layer 6
Layer 5
Layer 4
Layer 3
Layer 2: Ethernet II Header 0001.C73B.2C46 >> 00E0.A3A3.2ED4
Layer 1: Port(s): Fast Ethernet0/2

REFERENCIAS

 CORREO ENTRANTE

 CORREO SALIENTE

Interfases de red

EN ESTAS PÁGINAS CONOCEREMOS LOS DISTINTOS TIPOS DE CONEXIÓN UTILIZADOS EN LOS ADAPTADORES DE RED. SE TRATA DE INTERFACES ADECUADAS PARA EQUIPOS TANTO DE ESCRITORIO COMO PORTÁTILES: PCI, EXPRESSCARD Y USB, ENTRE OTROS.



USB a Ethernet

Pequeño dispositivo adaptador de USB a Ethernet. Es ideal para equipos portátiles, como notebooks y netbooks, y gracias a la popularidad de la interfaz USB, se lo puede conectar también en equipos de escritorio que no posean una tarjeta de red instalada.



USB

Interfaz USB que permite conectarse a redes inalámbricas, tanto en netbooks y notebooks, como en computadoras de escritorio. El uso de este tipo de dispositivos es ideal cuando el adaptador Wi-Fi incorporado en equipos portátiles se daña o deja de funcionar.



Cardbus

Tarjeta de formato Cardbus (también conocida como PCMCIA). Las placas de este formato se utilizan para dotar a una notebook de una interfaz de red Ethernet. Pueden emplearse, además, si la interfaz incorporada en forma original en el equipo portátil ha dejado de funcionar o se encuentra dañada por algún motivo.

LEDs indicadores

Las placas de red Ethernet tienen LEDs indicadores de Link (conexión) y de Collision, que señalan cuando se producen colisiones al tratar de emitir paquetes. Este último LED indicador sirve para conocer a grandes rasgos, pero a simple vista, si hay mucho tráfico basura en la red, lo que indica que debemos mejorar su infraestructura y velocidad. Demasiadas alarmas continuas de colisión dan a entender que la red está congestionada y debe mejorarse.



PCI

La clásica placa de red de formato PCI es utilizada en equipos de escritorio. Algunos modelos, como el que podemos ver en la imagen, poseen un zócalo interno (para realizar la instalación de una Boot ROM), y también un conector usado para acceder y utilizar la función Wake On LAN.



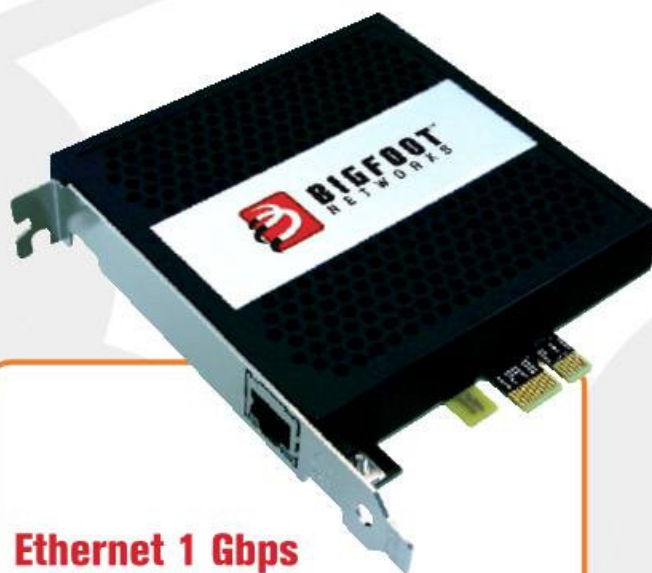
Adaptadora

Placa adaptadora que permite conectar, por ejemplo, una interfaz de red inalámbrica diseñada para equipos portátiles, en una computadora de escritorio, precisamente, en uno de los zócalos PCI del motherboard.



Inalámbrica

Placa PCI utilizada para obtener acceso a redes inalámbricas. Este modelo, en particular, es de banda dual A y G, es decir que nos permite conectarnos a redes 802.11a y 802.11g. Podemos encontrar diversos modelos de placas inalámbricas, las cuales nos ofrecen diferentes radios de alcance, dados por el poder de las antenas incorporadas.



Ethernet 1 Gbps

Interfaz de red Ethernet de 1 Gbps, con conexión PCI-Express x1, que se puede instalar en equipos de escritorio. Este modelo en particular está orientado al mercado del gaming, ya que ofrece una latencia mínima, aspecto muy bien recibido en quienes utilizan videojuegos multijugador.

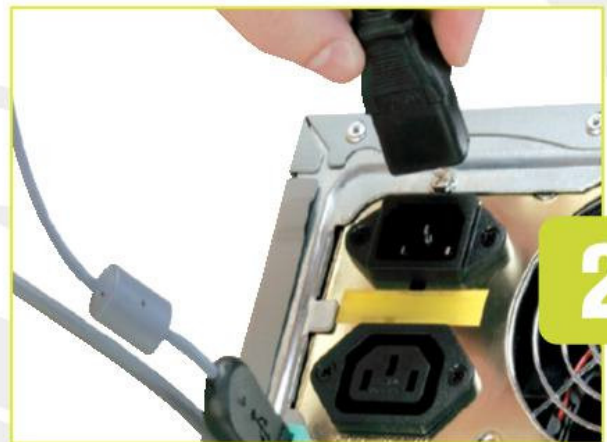


Instalar una placa de red PCI

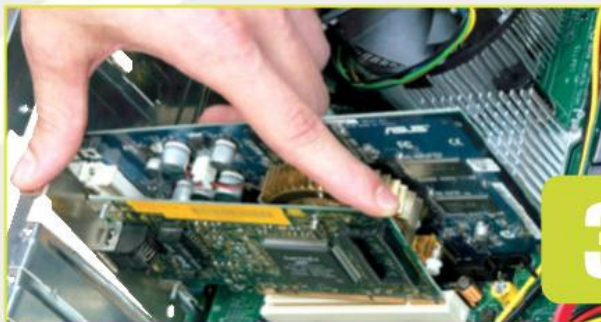
Veremos cómo colocar una placa de red y revisaremos la instalación de controladores para placas Ethernet o Wi-Fi.



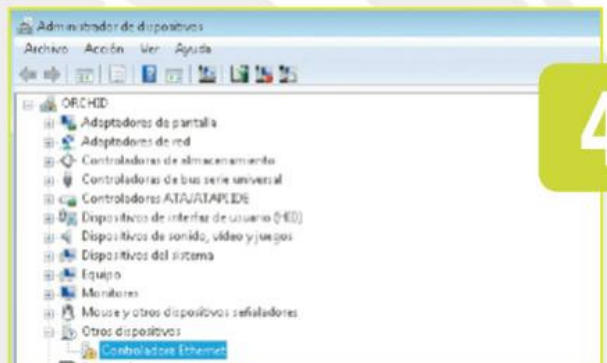
1



2



3



4

1

La placa o tarjeta de red requiere de cuidados en su manipulación, particularmente, de la descarga electrostática que emitimos en forma natural. Tomadas las precauciones del caso, quitamos la placa de su envoltorio para instalarla en el slot PCI la placa madre y retiramos la tapa lateral de la computadora.

2

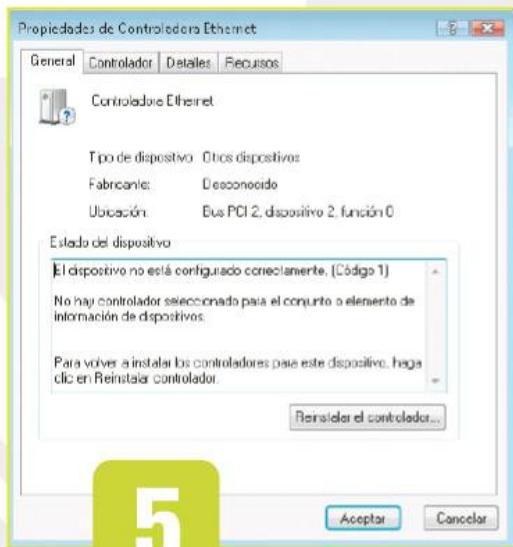
Es muy importante que la PC esté desenchufada de la corriente eléctrica. Una vez quitada la tapa del gabinete, observaremos, generalmente en la parte de abajo del microprocesador (con el gabinete parado), uno o más slots de color blanco que corresponden al bus PCI.

3

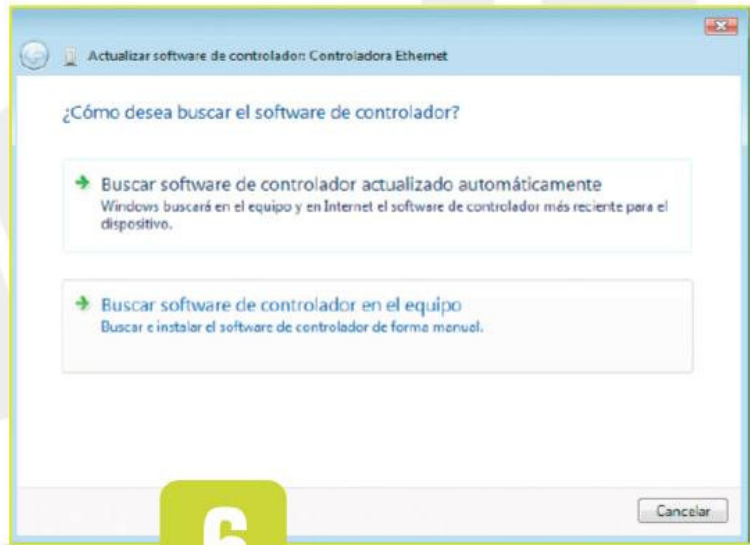
Si no encontramos los slots blancos (pueden ser de otro color), reconoceremos el bus PCI por la ranura de expansión, que debe coincidir con las conexiones o pines de la placa de red. Presionamos la placa y la atornillamos al gabinete.

4

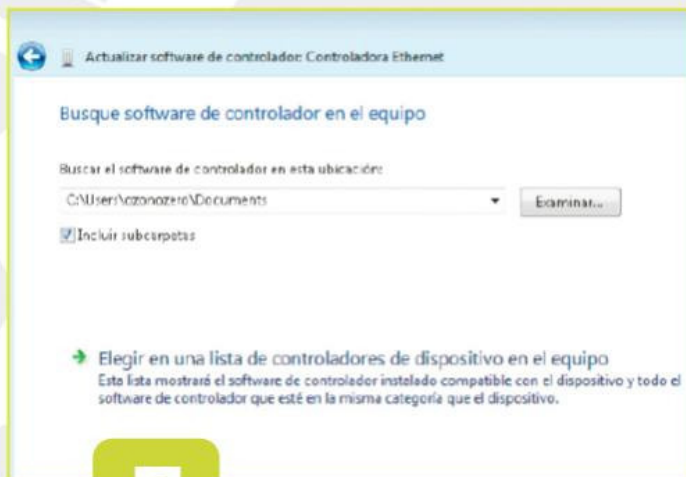
Después de verificar que la placa quedó encastrada en la ranura de expansión correspondiente, encendemos la computadora para instalar el controlador desde el CD, la unidad flash o la misma PC. Vamos a Panel de control/Sistema/Administrador de dispositivos.



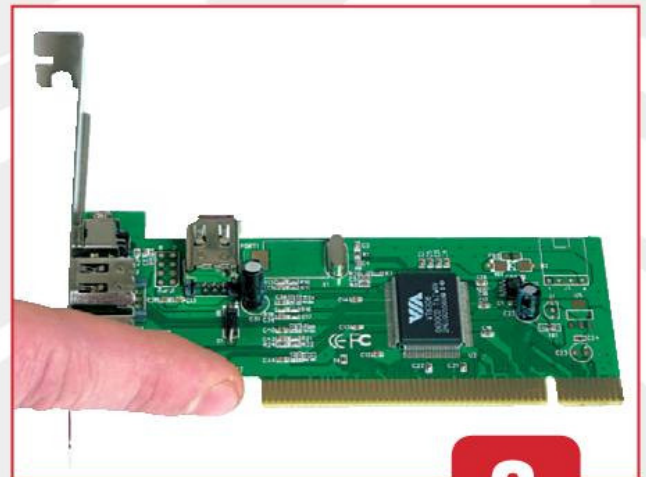
5



6



7



8

5 El dispositivo sin controlador (en este caso, la placa de red Ethernet o Wi-Fi) figura con una advertencia en amarillo sobre el icono. Hacemos doble clic sobre él y se abre la ventana de propiedades. En la pestaña General presionamos el botón Reinstalar controlador.

6 Cuando aparece esta ventana, debemos tener el CD de instalación del controlador en la lectora (o, en otro caso, conectada la unidad flash o de disco en la cual se encuentra). Para continuar, hacemos clic en la opción Buscar software de controlador en el equipo.

7 Presionamos el botón Examinar y definimos la ruta en donde está el instalador; una vez que lo hayamos encontrado, aceptamos y hacemos clic en el botón Siguiente. A partir de allí comienza la instalación. Realizamos todos los pasos hasta que el sistema nos da la opción llamada Finalizar.

8 Aunque la placa encastre perfectamente en la ranura PCI, siempre es conveniente sujetarla con un tornillo al gabinete, de modo que no registre el más mínimo movimiento. Un deficiente contacto de los pines acorta la vida útil del hardware y produce conflictos en la conexión.

→ ¿Qué son las subredes?

En esta sección analizaremos la forma en que podemos dividir una gran red en pequeñas redes interconectadas.

Las redes informáticas tienden a crecer; cada vez se conectan más y más equipos, y si no llevamos un orden en su ampliación, la tarea de administración puede volverse muy tediosa y difícil de realizar.

Ampliación de la red

Para facilitar la ampliación de la red, es posible crear subredes, es decir, ir dividiendo la red principal en pequeños segmentos siguiendo un orden lógico, para que luego su administración sea sencilla. Si la red se encuentra separada según las oficinas físicas, tenemos una división espacial y visual de los hosts (equipos conectados), y vemos qué y cuántos equipos hay por oficina, pero no se trata de subredes. Cuando las dimensiones de la red son muy amplias, y para su conexión necesitamos distintos routers ubicados estratégicamente para aprovechar el rendimiento, podríamos estar ante una división de la red a nivel físico, ya que el router se encarga de intercomunicar las distintas partes.



Los routers son dispositivos que nos permiten separar las grandes redes en otras más pequeñas, o subredes.

Subredes

Las subredes son divisiones de la red a nivel lógico, es decir, en la configuración de su dirección IP y máscara de red. Al configurar la IP de una PC, también configuramos su máscara de red y puerta de enlace. En IPv4, hay una división de clases de IP, en A, B, C, D y E, de las cuales las más utilizadas son las tres primeras. A ellas, a su vez, se las volvió a dividir en IP públicas y privadas: las públicas son para servidores

de Internet, de acceso público; en tanto que las privadas son para la configuración interna de las redes.

Cómo crear subredes

Para dividir las redes en subredes, hay que modificar su máscara de red. Esta, por medio de una operación lógica booleana con la IP, cumple la función de identificar a qué red pertenece cada PC o equipo (impresora, tablet, etc.). Por ejemplo, una PC con la IP 192.168.1.4 tiene por defecto la máscara de red 255.255.255.0, y otra PC con IP 172.16.132.178 tiene la máscara de red 255.255.0.0 (también se puede expresar como 192.168.1.4/24 y 172.16.132.178/16, donde los números después de la barra indican la cantidad de bits que se encuentran en 1). Estas PCs no pueden comunicarse entre sí, porque pertenecen a redes diferentes.



DHCP

Si nuestro router está configurado para asignar direcciones IP de forma automática (DHCP), estas serán de la red principal, y no estará dividida en subredes. Es decir, el router no puede entregar DHCP y dividir automáticamente en subredes. El proceso de subredes se lleva a cabo de forma manual.

Para poder hacerlo, necesitan de un router que permita establecer la conexión entre redes de distintos grupos. Aquí ya nos encontramos con el concepto de subredes, que consiste en ir modificando la máscara de red según nuestras necesidades. El procedimiento de modificar la máscara de red recibe el nombre de **subnetting**.

LA IMPLEMENTACIÓN DE SUBREDES NO REQUIERE UN GASTO ADICIONAL DE HARDWARE O SOFTWARE.

A medida que se modifica la máscara de subred, se reduce la cantidad de hosts que se podrán conectar a dicha red. Por ejemplo, para la máscara de red de 255.255.0.0 se pueden conectar 65534 hosts, mientras que para la máscara 255.255.255.0 se pueden conectar 254 hosts. Sería muy raro que nos quedáramos sin lugar para conectar un host a una determinada subred. Supongamos que tenemos varias oficinas, y el departamento de ventas

decide remodelar su estructura, por lo que temporalmente se ubica a los empleados en otros sectores, por ejemplo, en compras y en comercio exterior. A pesar de que su conexión física haya cambiado, todos los hosts pertenecientes a la subred de ventas podrán seguir viéndose entre sí, como lo hacían habitualmente, y no podrán ver directamente a aquellos equipos que pertenezcan a otra subred, a menos que se configure el router para permitir una comunicación transparente entre dos o más subredes. Por lo general, al hacer una división en varias subredes, la primera es otorgada al departamento de sistemas, ya que desde ahí se tendrá que administrar toda la red; en tanto que las últimas se asignarán a los servidores o departamentos que manejen información crítica de la empresa.

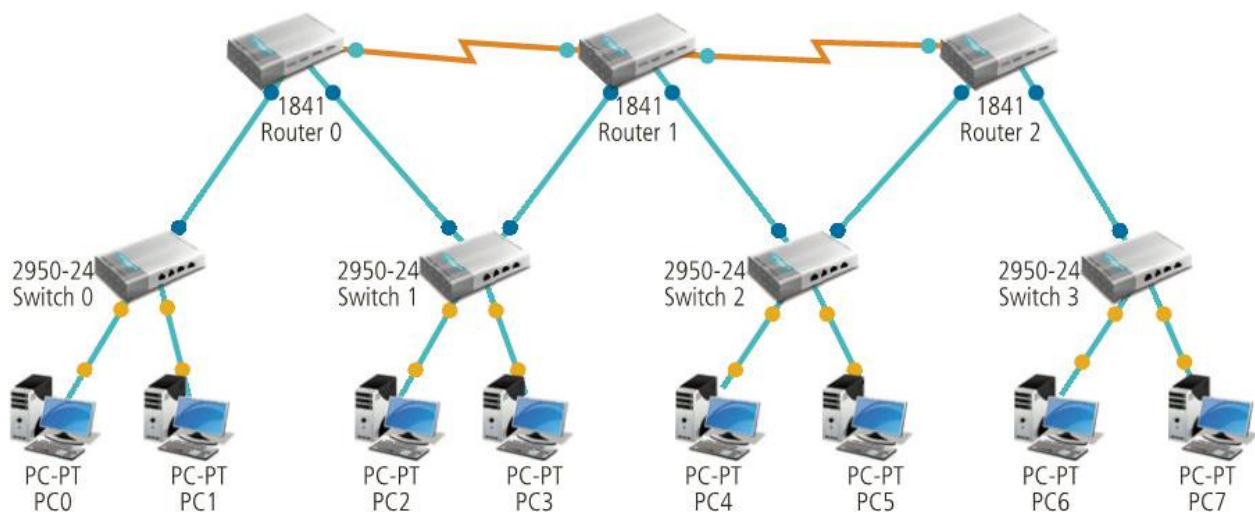
Máscara de red

La máscara de red es el factor principal en la división de redes, ya que con su configuración, podremos crear todas las subredes que necesitemos. Se trata de una dirección IP formada por dos partes: la de red y la de host. La primera identifica a la red, mientras que el resto se utiliza en la dirección IP de cada host. A nivel bit, se va

completando con 1 de izquierda a derecha contiguamente; por ejemplo, en IPv4 la máscara de red 255.255.255.0, que también podíamos expresar con /24, significa que a nivel bits, tiene 24 bits en estado 1, y luego 8 bits en estado 0. Cuando se dividen las subredes, se toman prestados bits a la parte de host, de manera que queda formada la nueva máscara de red. Podemos establecer que la máscara de red sea /27, entonces será 255.255.255.224. En IPv4, una dirección IP está formada por 32 bits, mientras que en IPv6, está formada por 128 bits. En IPv6 se utiliza la nomenclatura de "/" para indicar la máscara de red. Una IPv6 con máscara se expresa de esta forma: 4002:01AC:1E10:0200:0720:0121:0726:A512/86. Al dividir la red en subredes, se aumenta la seguridad, ya que para ciertos lugares podemos limitar estrictamente la cantidad de equipos conectados, además de que el router permite la interconexión entre subredes; este se puede configurar para permitir o denegar el acceso a determinada subred.

Implementación

La implementación de las subredes es un proceso que se lleva de la teoría a la práctica sin necesidad de agregar nuevo hardware o software: se hace directamente en la configuración IP de cada host, por lo cual cada cambio que realicemos debe hacerse de forma ordenada. Si no tenemos experiencia en subredes, es mejor dejar el trabajo en manos de quienes posean los conocimientos necesarios. ■



En este diagrama vemos una típica implementación de red con un total de cuatro subredes creadas.



La seguridad aplicada a las redes cableadas

En estas páginas revisaremos las principales opciones que debemos tener en cuenta para proteger la red a nivel hardware y lógico.

Cuando la red empieza a crecer, es preciso tener en cuenta su seguridad, ya que la conexión a Internet es compartida, y seguramente también compartiremos archivos, impresoras y unidades removibles. Al compartir la conexión a Internet, debemos pensar en la seguridad lógica de esta; es decir, cualquier equipo que se puede infectar por un software dañino descargado accidentalmente de Internet es capaz de infectar al resto de los equipos y, también, afectar al resto de la red.

Seguridad

En una red empresarial, además de la seguridad lógica, también debemos tener en cuenta la seguridad física, y restringir el acceso a ciertos sectores de la infraestructura. La seguridad de la red implica proteger la confidencialidad de la empresa, y proveer un mantenimiento continuo que asegure su comunicación y disponibilidad. La seguridad en conjunto de la red, así como los procedimientos que se deben seguir para su resolución, se encuentran detallados en el plan de contingencia, que es determinado por cada empresa según sus necesidades y clasificación de prioridades.

Para tener en cuenta

Para llevar a cabo un plan de seguridad, debemos considerar:

- ▶ **Análisis de riesgos:** evaluación de los recursos que sean críticos para el funcionamiento de la red de la empresa y, en caso de un incidente, tiempo mínimo requerido para su rápida resolución.
- ▶ **Medidas preventivas:** determinar qué personas pueden tener acceso físico o remoto a los servidores, y quiénes pueden realizar tareas de mantenimiento. Establecer filtros para definir qué usuarios pueden instalar software y tener puertos USB disponibles. Realizar actualizaciones periódicas del antivirus y service packs del sistema operativo y, también, de las aplicaciones de seguridad.
- ▶ **Prevención ante accidentes de índole natural:** establecer qué métodos se llevarán a cabo ante la ocurrencia de una catástrofe, como fuertes lluvias o incendio.

Hardware para jamming, cuya función es bloquear las señales de celulares o Wi-Fi.

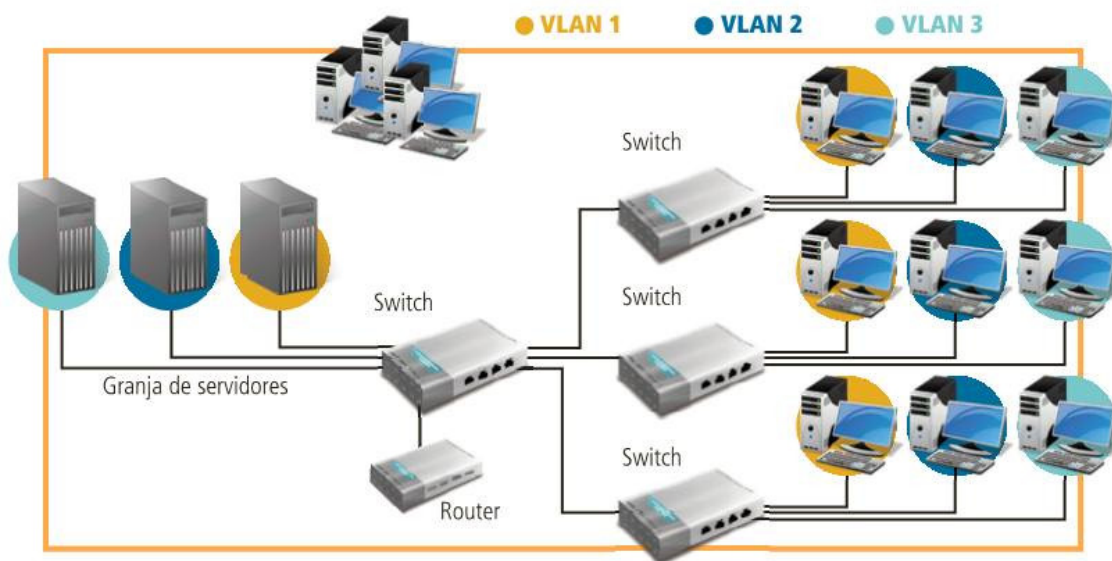


▶ **Plan de respaldo:** evaluar cómo seguir ante la pérdida de un servicio. Si se ve afectado uno o varios equipos de la red, es posible reemplazarlo en un tiempo corto, mientras que si lo que está comprometido es el servidor, donde están los datos de clientes, habrá que reducir el tiempo en determinar qué quedó sin utilidad y comenzar a realizar las tareas para poner en funcionamiento un servidor alternativo, utilizando el backup más reciente que se haya hecho.

Lo importante en el tema de seguridad es prevenir al máximo los daños que puedan suceder, y ante la inevitable ocurrencia de alguno de ellos, reducir lo más posible los tiempos para dejar otra vez operativa la red y sus servicios.

Seguridad física

Consiste en proteger los activos, evitar el hurto de partes y su deterioro, así como también evaluar qué equipos se adquirirán y por qué, las ventajas y desventajas de cada uno, y quién o quiénes



- Un switch crea un dominio de broadcast.
- Las VLANs ayudan a gestionar los dominios de broadcast.
- Las VLANs se pueden definir como grupos de puertos, usuarios o protocolos.
- Los switches LAN y el software de administración de red suministran un mecanismo para crear las VLANs.

Al utilizar switches en vez de hubs, lograremos un mayor rendimiento en el tráfico de la red y mayor seguridad.

tendrán acceso físico a ellos. También hay que tener en cuenta la seguridad física y lógica de los dispositivos de red. Dijimos que el hub distribuye los datos recibidos por todos sus puertos (menos por el que recibe la señal). Esto, además de implicar un tráfico innecesario en la red, es un riesgo de seguridad, ya que algún usuario avanzado podría interceptar esos paquetes dirigidos a otro equipo. Debido a que esta es una falla de seguridad en el hardware, solo quedará reemplazar el hub por un switch; si los costos lo permiten, lo ideal es optar por un switch de capa 3. Puede ocurrir que tengamos un router dedicado, y que exista una falla de seguridad en su sistema operativo que comprometa la seguridad de la red. En ese caso, habrá que implementar lo antes posible la actualización del SO, o si no está disponible y la falla de seguridad es considerada crítica, plantear su reemplazo temporal. Otra opción puede ser la implementación de un firewall, con lo cual podremos brindar un mayor nivel de seguridad a toda la red o solo a un determinado sector cuya información sea confidencial.

ES IMPORTANTE GENERAR CONCIENCIA EN LOS USUARIOS DE LA RED CON RESPECTO AL USO DE CONTRASEÑAS PARA ACCEDER AL SISTEMA Y A QUE ESTA NO DEBE TRANSFERIRSE A TERCEROS.

Otro sistema de seguridad en redes es el IDS (*Intrusion Detection System*), que puede ser un hardware (físicamente similar a un router) o un software que se instala en un equipo dedicado a analizar la seguridad de la red. El IDS cumple la función de detectar intrusiones dentro de la red, realizando escaneos constantes en tiempo real. Se diferencia del firewall porque este último permite bloquear el ingreso de ciertos datos, mientras que el IDS analiza los datos que ingresan y genera un reporte sobre ellos.



VeriSign

Es una empresa de seguridad informática reconocida mundialmente por proveer certificados de firmas digitales, utilizando el sistema de criptografía RSA en las conexiones SSL. Esto sirve, por ejemplo, para la visualización de mails vía web. La mayoría de las entidades bancarias emplean certificados provistos por VeriSign para efectuar sus transacciones.

IDS

Sobre la base de la información recolectada en los reportes, o ante la detección de una intrusión, hay que notificar de inmediato al Administrador de red. El IDS puede cumplir muchas funciones de forma automática, como cambiar la configuración del firewall o bloquear algún acceso.

LO IMPORTANTE ES PREVENIR LOS DAÑOS QUE PUEDAN PRESENTARSE, Y SI OCURRE ALGUNO DE ELLOS, REDUCIR EL TIEMPO PARA RESTABLECER LOS SERVICIOS AFECTADOS.

Al implementar un IDS, debemos prestar mucha atención a los reportes generados, para su correcta configuración, ya que en ocasiones, el IDS detecta una conexión segura como intrusiva y entonces bloquea la comunicación (falso positivo), o por el contrario, detecta como segura una actividad intrusiva (falso negativo). El IDS generalmente trabaja en conjunto con el IPS (*Intrusion Prevention System*), que se encarga de bloquear a nivel red (**capa 3**) las conexiones que considera intrusas. Las características principales de un IDS son las siguientes:

- ▶ Tiene que ser un sistema autónomo, que no requiera nuestra intervención ni revisión en forma diaria.
- ▶ Debe generar reportes lo más detallados posible.
- ▶ Para software IDS, tiene que permitir su ejecución en segundo plano y la administración remota.

Aunque las ventajas de la fibra óptica son evidentes, su reparación ante un corte requiere equipo y personal especializados.



- ▶ Debe ser difícil de detectar; si el IDS es detectado por otro software, su nivel de seguridad ya no es fiable.

Cableado

El cableado de la red tiene que ir por un lugar seguro, un techo falso, un sitio que no sea de muy fácil acceso, y lejos de las fuentes que pueden provocar interferencias. También debemos tener en cuenta el lugar de trabajo; por ejemplo, si nos encontramos en una planta química, para las zonas más peligrosas es mejor utilizar cable de fibra óptica, ya que no transmite pulsos eléctricos sino un haz de luz, y su material es ignífugo.

Las ventajas en cuanto a seguridad que brinda la fibra óptica son:



- ▶ Baja atenuación, lo que permite cubrir grandes distancias sin tener que colocar un **repeater** para abarcar un área mayor. Es posible tender la fibra óptica por unos cuantos kilómetros sin pérdida de señal.
- ▶ Al no manejar pulsos eléctricos, es ideal para zonas de alto riesgo (plantas químicas, centrales nucleares).
- ▶ No se ve afectada por interferencias de fuentes externas. La desventaja que posee es que, ante un corte de la fibra, si bien es posible realizar un empalme, la manipulación debe realizarla personal especializado.

Existen medios que pueden extraer físicamente la señal de la fibra óptica, pero para hacerlo, es preciso tener acceso directo al cableado, ya que este se hace a través de un splitter, un cable con forma de Y. Además, para lograr tal fin, se requiere personal altamente calificado. Es recomendable realizar un chequeo físico de la fibra óptica en las zonas que consideremos más vulnerables. En cuanto al cable de par trenzado, que es más común en las redes, también debemos establecer medidas de seguridad, y elegir qué tipo o categoría es mejor para determinados tramos de la red. Por ejemplo, para las zonas exteriores conviene elegir cable SFTP o

STP, ya que tiene mallas que lo protegen de fuentes externas que pueden provocar interferencias. Dentro de la red interna, podemos establecer ciertos colores de cables o categorías para el cableado que irá a los servidores y para el que llegará a los puestos de trabajo. Esto brinda mayor rapidez en la resolución ante una falla en el cableado.

Seguridad lógica

Para aumentar la seguridad lógica, es posible implementar la división en subredes e instalar equipos de seguridad (firewall, IDS). Además, algunos sectores pueden contar con un nivel mayor de seguridad, por ejemplo, tener una conexión a Internet



Siempre que sea posible, y cuando los costos lo permitan, reemplacemos el hub por un switch.

dedicada, exclusiva para efectuar transacciones bancarias. También hay que determinar qué hardware se puede compartir y cuál adquirir para uso exclusivo de un sector. Si el sector de finanzas necesita imprimir información confidencial, no será apropiado que comparta la impresora con otros sectores o que se encuentre fuera de sus límites.

Cable coaxial

El cable coaxial utilizado en las primeras redes cableadas era más susceptible a interferencias provenientes de diversas fuentes. Además, era de muy fácil acceso y existían mecanismos que permitían observar la señal que pasaba sin romper el cable, como los conectores vampiro. Este conector perforaba el cable hasta quedar en contacto con su núcleo, y así era posible acceder a la información transmitida sin que se notara inmediatamente ninguna anomalía en el funcionamiento de la red.

Factor humano

El punto más importante de la seguridad lógica es el factor humano, es decir, todo el personal que introducirá información. Es fundamental realizar charlas o reuniones en las que se explique la importancia de la seguridad en una red, ya que de nada nos servirá contar con los mejores dispositivos de seguridad en redes y realizar las tareas administrativas pertinentes si los usuarios tienen a la vista su nombre y contraseña para acceder al sistema. Una de las técnicas utilizadas para brindar seguridad en los datos transmitidos a través de la red es el uso de la firma digital. Esta utiliza medios criptográficos para asegurar la autenticidad de su autor y garantizar que no sufrió alteraciones durante la transmisión.

Técnicas de jamming

El **jamming** es un conjunto de señales externas que provocan interferencias en los sistemas. Estas pueden ser intencionales u ocasionales. Las primeras puede deberse a la presencia de dispositivos que están operando en la misma frecuencia de trabajo, con una corta distancia de separación. En el mercado hay disponible hardware para jamming, como los bloqueadores de señal de celular. ■

¿TE RESULTA ÚTIL?

Lo que estás leyendo es el fruto del **trabajo de cientos de personas** que ponen todo de sí para lograr un **mejor producto**. Utilizar versiones "pirata" desalienta la inversión y da lugar a publicaciones de **menor calidad**.

NO ATENTES CONTRA LA LECTURA. NO ATENTES CONTRA TI. COMPRA SOLO PRODUCTOS ORIGINALES.

Nuestras publicaciones se comercializan en kioscos o puestos de voceadoras; librerías; locales cerrados; supermercados e internet (usershop.redusers.com). Si tienes alguna duda, comentario o quieres saber más, puedes contactarnos por medio de usershop@redusers.com



La tecnología PowerOver Ethernet

En esta sección conoceremos cómo combinar la red eléctrica con la de datos sin correr riesgos de seguridad.

La tecnología **PowerOver Ethernet (PoE)**, traducida como **energía sobre Ethernet**, establece cómo transferir energía eléctrica y datos a través del cable de red UTP. De este modo, en aquellos dispositivos que sean compatibles con PoE, no necesitaremos la conexión a un toma de energía, y tendremos la ventaja de poder conectar dispositivos en lugares donde el acceso eléctrico no sea sencillo o no esté disponible. Las normas 802.3af y 802.3at del IEEE establecen la cantidad de potencia máxima, la corriente máxima y las tensiones máximas que pueden transmitirse a través de la red. En la actualidad, la potencia máxima es de 30 Watts y 600 miliamperes por par. Hay dos tipos de dispositivos para la tecnología PoE, los cuales analizaremos a continuación.

Power Sourcing Equipment (PSE)

Es el dispositivo principal de esta tecnología. Se conecta a la red eléctrica

y provee de energía a través del cable de red. Por lo general, entrega 48 V y 500 mA (20 W aproximadamente). Hay dos modelos de PSE:

► **Endpoint:** se trata de un dispositivo de red que incluye la tecnología PoE en su modo de trabajo. Podemos encontrarlo como router PoE, switch PoE o access point PoE.

► **Midspan:** es un dispositivo que solo brinda energía eléctrica al cable de red. Si nuestra red ya está armada y tenemos un router que no es compatible con PoE, pero a él conectamos un access point PoE, el PSE Midspan irá en el medio de esos dispositivos.

Powered Devices (PD)

Son los dispositivos que serán alimentados eléctricamente a través del cable de red; también se diferencian en dos categorías:

► **PD no compatibles con PoE:** son todos aquellos dispositivos



Fuente de alimentación PoE. En la conexión de datos, va el cable de red, y en la otra, se conecta el dispositivo PoE.

que requieren un cargador externo. Incluso, estos dispositivos pueden ser alimentados por el PSE, pero antes de la conexión, necesitaremos la ayuda de otro dispositivo llamado PoE splitter, que se encarga de realizar la tarea inversa al Midspan. Por un lado, el cable de red se conecta con PoE, y sus salidas proveen un conector de alimentación tradicional y el cable de red para datos.

► **PD compatibles con PoE:** son todos aquellos dispositivos que aceptan la tecnología PoE. Pueden traer o no conexión de alimentación tradicional. Un ejemplo de ellos son los teléfonos IP, cuya única conexión es un puerto Ethernet. ■



Corriente y datos

La norma PoE establece los estándares para transportar la potencia necesaria que encienda un dispositivo remoto y, a su vez, permita el envío de datos, todo a través del mismo cable de red UTP. Esto puede realizarse porque la tecnología PoE utiliza los dos pares que no emplea Ethernet. En caso de que el cable de red tenga solo los dos pares para la transmisión de datos, es posible utilizar PoE, pero lo recomendable sería emplear un cable de red de cuatro pares.

PRÓXIMA ENTREGA



4

INSTALACIÓN DE REDES CABLEADAS

En el próximo fascículo aprenderemos a planificar y presupuestar la instalación de una red cableada. Conoceremos también algunos consejos sobre seguridad física a la hora de diseñar una red.





- ▶ 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.



9 789871 857784



00003

CONTENIDO DE LA OBRA

- 1 Introducción a las redes informáticas
- 2 Tipos de redes y topologías
- 3 DISPOSITIVOS DE RED**
- 4 Instalación de redes cableadas
- 5 Puesta en marcha de una red cableada
- 6 Configuración de redes cableadas
- 7 Instalación de redes inalámbricas
- 8 Configuración de redes inalámbricas
- 9 Seguridad en redes cableadas e inalámbricas
- 10 Configuración avanzada de routers
- 11 Recursos compartidos y dispositivos multimedia
- 12 Seguridad física de la red
- 13 Impresoras de red
- 14 Hardware de servidores
- 15 Administración de Windows Server
- 16 Administración de sistemas Linux
- 17 Administración y asistencia remota
- 18 Servidores web y FTP
- 19 Servidores de mail
- 20 Servidores de archivos e impresión
- 21 Servidores adicionales
- 22 VLAN, VPN y trabajo remoto
- 23 Telefonía IP
- 24 Cámaras IP