Administración de la red

Jordi Serra Ruiz
Miquel Colobran Huguet
Josep Maria Arqués Soldevila
Eduard Marco Galindo

P08/81029/02268

UOC
Universitat Oberta de Catalunya
www.uoc.edu

Índice

Introducción

A la hora de diseñar e implementar una red, tenemos que tener en cuenta los seis pasos básicos siguientes:

1) Selección del diseño del cableado y del hardware.

2) Instalación del hardware y del sistema operativo de red.

3) Configuración del sistema operativo y carga de las aplicaciones.

4) Creación del entorno del usuario.

5) Inicialización de la administración de la red.

6) Mantenimiento y monitorización de la actividad de la red.

Ved también

Ved el módulo "Administración de usuarios".

En este módulo pretendemos abarcar brevemente diversos aspectos del diseño y el desarrollo posterior de una red de ordenadores. Así pues, empezaremos el módulo con la descripción de los elementos que lo integran y lo acabaremos definiendo las responsabilidades del administrador en cuanto al funcionamiento correcto de la red. No pretendemos hacer una recopilación exhaustiva de una materia tan densa y heterogénea, sino tan sólo dotar al administrador de algunos criterios generales que le puedan ayudar a la hora de empezar (y mantener) una tarea tan compleja como la que hemos descrito.

Objetivos

Los materiales didácticos de este módulo contienen las herramientas necesarias para que el estudiante alcance los objetivos siguientes:

1. Conocer básicamente los elementos físicos de una red de ordenadores y la manera en que podemos interconectar estos elementos entre sí.

2. Conocer los protocolos de comunicación que tienen que utilizar los ordenadores de la red, y también la manera en que se configuran las estaciones y algunos servicios.

3. Conocer las tareas que ha de llevar a cabo el administrador una vez la red ya se encuentre en funcionamiento (tareas de mantenimiento, supervisión y seguridad).

1. Importancia de las redes

Los ordenadores personales permiten a los usuarios individuales gestionar sus propios datos para cubrir las necesidades particulares. A pesar de todo, los ordenadores aislados no pueden ofrecer un acceso directo a los diferentes datos de una organización, ni pueden compartir de una manera fácil la información o los programas de los que disponen. En este sentido, las redes proporcionan una buena solución de compromiso entre los dos extremos: el procesamiento individual y el procesamiento centralizado.

Entre los muchos beneficios que comporta la implementación de una red, podemos encontrar los siguientes:

- Compartimentación de dispositivos periféricos: discos duros de gran capacidad, dispositivos de salida de coste elevado (como, por ejemplo, impresoras láser o trazadores –*plotters*–, etc.).

- Comunicación de los usuarios de la organización entre ellos (correo electrónico).

- Facilidad de mantenimiento del software (a menudo, buena parte del software se comparte desde la red, en lugar de instalarse individualmente en cada estación de trabajo).

- Gestión centralizada de los recursos compartidos, independientemente del grado de dispersión geográfica que pueda tener la organización.

Teniendo en cuenta esta dispersión, las redes se pueden clasificar de la manera siguiente:

- Redes de área local (LAN)[1]: de 10 a 1.000 m (por ejemplo, una sala de la organización, un campus, etc.).

- Redes de área metropolitana (MAN[2]): de 1 a 10 km (por ejemplo, una ciudad).

- Red de área extendida (WAN[3]): más de 10 km (por ejemplo, un país).

(1)LAN es la sigla de *local area network*.

(2)MAN es la sigla de *metropolitan area network*.

(3)WAN es la sigla de *wide area network*.

Teniendo en cuenta la importancia que tiene una red en la actividad diaria de cualquier organización, se hace evidente la necesidad de una figura que se encargue de diseñarla, implementarla, mantenerla y actualizarla siempre que se requiera. Esta figura, el administrador de la red, tiene que conocer los ele-

mentos físicos que la componen, los protocolos de comunicación entre los diferentes ordenadores (y sus sistemas operativos), y también los requerimientos mínimos de seguridad que tiene que satisfacer la red.

2. Elementos y diseño físico de una red

A la hora de diseñar nuestra propia red, antes de empezar, hay que tener en cuenta una serie de aspectos básicos que podemos ver reflejados en las preguntas siguientes:

- ¿Cuántos ordenadores (estaciones de trabajo) tenemos que conectar a la red?
- ¿Cuántos ordenadores habrá que añadir en futuras ampliaciones?
- ¿Dónde y cómo se disponen los ordenadores? (hay que hacer un croquis de la disposición de las máquinas).
- ¿Necesitamos un servidor?
- ¿Qué velocidad de transmisión se requiere?
- ¿Qué recursos hay que compartir?
- ¿Qué software querríamos instalar? ¿Tenemos las versiones para funcionar sobre red?

Antes de empezar a contestar estas preguntas, tendremos que hacer un breve repaso de diversos conceptos que han aparecido en otras asignaturas de redes de ordenadores.

2.1. Elementos de una red

Los elementos básicos de una red son: el cableado, los elementos de conexión y los elementos de interconexión de redes.

2.1.1. Cableado de una red

Podemos distinguir los siguientes tipos de cables:

1) Par trenzado

Este tipo de cableado está formado por diversos hilos conductores que se trenzan entre sí con la finalidad de protegerlos del ruido ambiental. Es el cableado más económico y fácil de instalar. Pueden llegar a distancias de hasta 100 m (sin sufrir amortiguamientos de la señal) y en velocidades que pueden variar entre los 10 y los 100 Mbps. Hay diversas categorías de cable par trenzado:

- Cable apantallado[4]. Formado por dos pares de hilos conductores recubiertos por una malla.

(4)En inglés, *shielded twisted pair* (STP).

- Cable sin apantallar[5]. Formado por cuatro padres de hilos conductores. En el mismo tiempo, los cables UTP se pueden subdividir en diversas categorías:
  - Categoría 3: pueden llegar a velocidades de transmisión de 30 Mbps.
  - Categoría 5: es el tipo de cable que se utiliza más a menudo. Puede llegar a velocidades de 100 Mbps (redes *faust ethernet*). La categoría 5, (también llamada 5+ o 5e), representa una mejora de la categoría 5 y puede llegar hasta 1.000 Mbps (redes *gigabit ethernet*).
  - Categoría 6: puede llegar a velocidades de 1.000 Mbps/1 Gbps.

Otras categorías de cables UTP

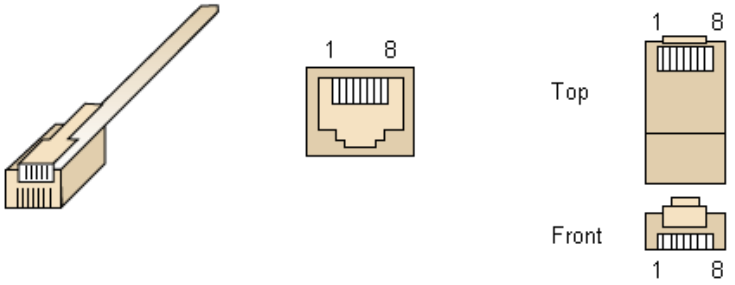
Aparte de las categorías 3, 5 y 6, existen otras categorías de cables UTP: las categorías 6e y 7, que se usarán en el futuro para redes 10, *gigabit ethernet* (10.000 Mbps).

(5)En inglés, *unshielded twisted pair* (UTP).

Podemos ver en la figura siguiente el aspecto de un par trenzado UTP[6], el conector hembra y el conector macho, respectivamente:

(6)UTP es la sigla de *unshielded twisted pair*.

Aspecto de un cable UTP



Por ejemplo, conectando todos los ordenadores en un concentrador mediante un par trenzado y sin necesidad de utilizar un servidor dedicado, podemos diseñar una red muy sencilla, perfectamente válida para compartir recursos, y que se puede ampliar fácilmente hasta ocupar todos los puertos del concentrador.

Redes punto a punto

Se llaman *punto a punto* (en inglés, *peer-to-peer*) las redes en las cuales no hay un servidor dedicado. Todas las estaciones de trabajo tienen el mismo estatus y comparten los recursos.

Crossover

Cuando se utiliza un concentrador, los dos extremos del cable (lo que se conecta en el concentrador y lo que se conecta en la tarjeta de red del ordenador) se insertan en el conector RJ45 de la misma manera, pero cuando los dos extremos se conectan directamente entre dos ordenadores, hace falta hacer lo que se llama un cable cruzado (*crossover*) e intercambiar la orden de los cables que transmiten los datos.

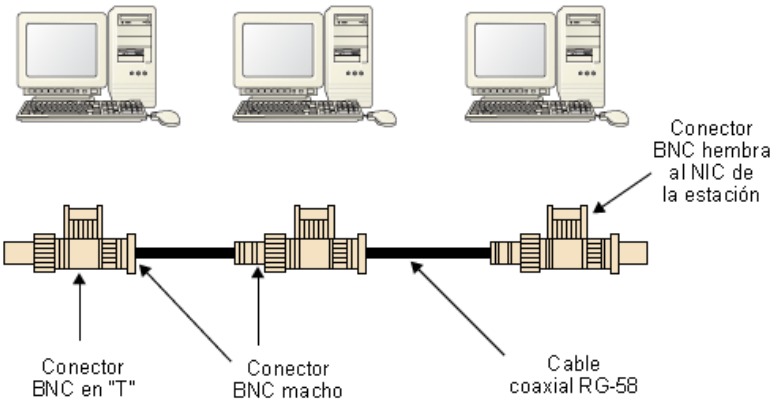
2) Cable coaxial

El cable coaxial dispone de un único conductor interno y diversas capas de protección. Hay gruesos y delgados (RG-58A/U), y en distancias no superioras a los 2 km puede permitir velocidades de transmisión de 20 Mbps, mientras que en distancias cortas (no superiores a los 100 m) puede llegar a los 100 Mbps. El cable coaxial, si se compara con el par trenzado, reduce los problemas de amortiguamiento de la señal en largas distancias y el porcentaje de potencia

que se pierde en forma de radiación. Es muy sensible a las acciones de posibles espías y susceptible al ruido producido por los aparatos eléctricos (por ejemplo, un motor).

Para conectar diferentes segmentos de cable coaxial se utilizan conectores BNC. Para conectar un ordenador a la red, se utilizan conectores BNC en forma de T.

Conexión de un ordenador a la red con cable coaxial



3) Fibra óptica

La transmisión de la información se lleva a término por un haz de luz que circula por un núcleo fotoconductor. Permite un gran ancho de banda y puede llegar a velocidades de transmisión del orden de centenares de Mbps y Gbps. La fibra óptica sufre un amortiguamiento mínimo de la señal, es inmune a las interferencias electromagnéticas y resulta difícil de interceptar y espiar, ya que no emite ninguna señal que pueda ser monitorizada. Normalmente se utiliza conjuntamente con otros tipos de cableado.

Hay dos tipos diferentes de fibra óptica, las **fibras monomodo** y las **fibras multimodo**. Las primeras se caracterizan porque sólo admiten un único modo de transporte (sólo pueden transmitir los haces de luz que siguen el eje de la fibra). Tienen un ancho de banda que puede llegar a los 100 GHz/km. Con respecto a las fibras multimodo, con un diámetro de núcleo mayor que las monomodo, transportan múltiples modos de forma simultánea. Son más fáciles de implantar y tienen un ancho de banda que puede llegar hasta los 500 MHz/km (menor que las monomodo). Pueden ser, por ejemplo, especialmente adecuadas para sistemas de videovigilancia o LAN[7].

[(7)]LAN es la abreviatura de *red de área local*.

Ved también

Ved los sistemas de videovigilancia o LAN en el módulo "Administración de la seguridad".

2.1.2. Elementos de conexión de redes

Entre los elementos de conexión de redes, podemos distinguir los siguientes:

- **Tarjetas de interfaz de red (NIC[8])**. La conexión de los ordenadores a la red se hace mediante las tarjetas de interfaz de red.

[8]NIC es la sigla de *network interface card*.

Formato de las tarjetas de red

Normalmente, las tarjetas de interfaz de red se encuentran en formato PCI o PCMCIA, en el caso de ordenadores portátiles. Cada vez hay más equipos portátiles y de sobremesa con una tarjeta integrada en la placa base. Algunos PDA disponen de tarjeta de interfaz de red incluso para conectarse a una red local sin hilo.

Tarjeta de interfaz de red

- **Cortafuegos**[9]. Es cualquier dispositivo (hardware o software) que permita evitar que los usuarios no autorizados accedan a una máquina determinada.

[9]En inglés, *firewall*.

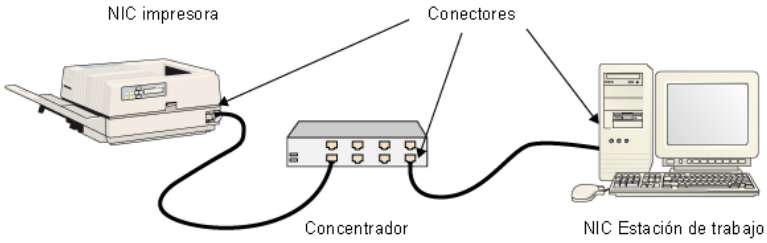
Ved también

Ved los cortafuegos en el apartado 5 de este mismo módulo.

- **Concentrador**[10]. Los concentradores son dispositivos que permiten compartir una línea de comunicación entre diversos ordenadores. Repiten toda la información que reciben de manera que la puedan recibir todos los dispositivos conectados a sus puertos.

[10]En inglés, *hub*.

Ejemplo de configuración de un concentrador



- **Conmutador**[11]. Gestiona el flujo del tráfico de red según la dirección de destino de cada paquete. En otras palabras, los conmutadores pueden averiguar qué dispositivos se encuentran conectados a sus puertos y redirigen la información únicamente al puerto de destino, en lugar de hacerlo indiscriminadamente como los concentradores.

[11]En inglés, *switch*.

Observación

Todas las estacionas conectadas al mismo concentrador o *stack* de concentradores compiten por el ancho de banda del canal.

- **Red troncal**[12]. Se llaman de esta manera los cables principales que conectan entre sí los segmentos de una red local. Habitualmente son enlaces de alta velocidad (por ejemplo, fibra óptica).

[12]En inglés, *backbone*.

- **Armarios de conexión**. Generalmente, la red se divide en diferentes armarios de conexión que abarcan todo el servicio de red en un entorno determinado como, por ejemplo, toda la planta de un edificio. Todos estos armarios tienen una conexión en un armario central en el cual, normalmente, se encuentran agrupadas todas las comunicaciones y residen los diferentes servidores. Acostumbra a ser una sala con acondicionamiento

atmosférico adecuado, tanto con respecto a la temperatura como a la humedad, y normalmente dispone de alimentación eléctrica ininterrumpida.

- **Servidor**. Es el ordenador que permite compartir sus periféricos con otras estaciones de la red. Hay de muchos tipos diferentes y se pueden agrupar en tres categorías generales: servidores de impresión, de comunicaciones y de ficheros. Dentro de una red, pueden estar dedicados exclusivamente a dar estos servicios, o bien también pueden no ser exclusivos y utilizarse como estaciones de trabajo.

- **Estación de trabajo**. Cada estación de trabajo ejecuta su sistema operativo propio (Unix, Linux, Windows 2000, etc.) y sobre este sistema operativo se ejecuta un software de red que le permite comunicarse con los servidores y los otros dispositivos de la red, de manera que sea tan sencillo gestionar los recursos locales como los del servidor.

2.1.3. Elementos de interconexión de redes

Entre los elementos de interconexión de redes, podemos distinguir los siguientes:

- **Repetidores**. Son dispositivos "no inteligentes" que amplifican la señal y evitan los problemas de amortiguamiento que se producen cuando el cable llega a una cierta distancia (recordad que, según el cableado que se utilice, estas distancias varían).

Observación

Los repetidores actúan en la capa física y los puentes actúan en la capa de enlace de datos. El encaminador actúa en la capa de red.

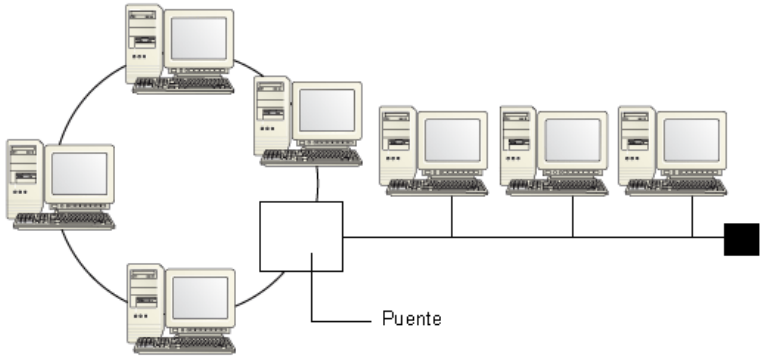
- **Puente**[13]. Conectan entre sí dos segmentos de red (que pueden ser diferentes, como se muestra en el ejemplo de la figura siguiente). A diferencia del repetidor, el puente es lo suficiente "inteligente" para filtrar el tráfico de información entre los segmentos. Con la incorporación de un puente, cada segmento tiene una dirección diferente, de manera que la información siempre se direcciona hacia su destino y se evitan los cuellos de botella que se producen cuando todas las estaciones de trabajo se conectan en el mismo segmento.

(13)En inglés, *bridge*.

Funciones de los puentes

Las funciones básicas de los puentes son: el autoaprendizaje, la filtración y el reenvío.

Interconexión de redes mediante un puente



- **Encaminador.**[14] Son dispositivos que gestionan el tráfico de paquetes que proviene del exterior de la red hacia el interior (y al revés). Pueden ser dispositivos muy sofisticados y tener capacidad de actuar como cortafuegos. Son similares a los puentes, pero en cambio ofrecen servicios de encaminamiento de los datos que se transmiten; es decir, no sólo pueden filtrar la información, sino que, además, también pueden encontrar la ruta de destino más eficiente para los paquetes de información que se transmiten.

(14)En inglés, *router*.

- **Pasarela**[15]. Actúan en los niveles superiores de la jerarquía de protocolos OSI. Permiten la interconexión de redes que utilizan protocolos incompatibles.

(15)En inglés, *gateway*.

2.2. Topología y tipos de redes

La topología de la red se refiere al camino físico que siguen los datos por la red, la manera lógica en que se conectan los diferentes dispositivos que la forman. A menudo hay que diferenciar entre la **topología lógica** y la **topografía** o **diseño físico** (la manera en que se "tiran" los cables).

Reflexión

La topología lógica puede ser, pues, diferente de la topografía, como veremos en los ejemplos que se estudiarán más adelante.

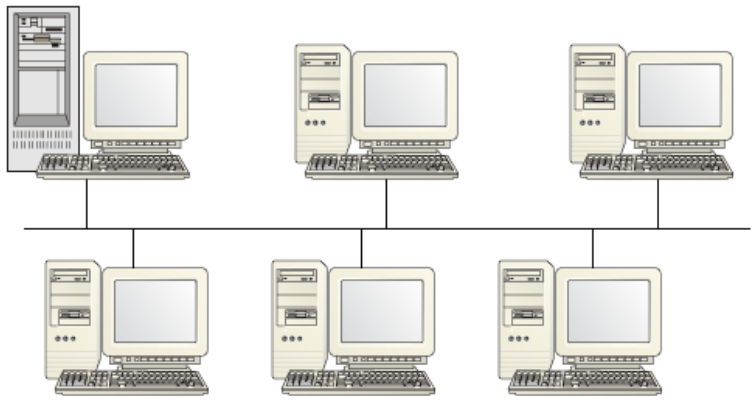
Básicamente, hay tres topologías que hay que tener en cuenta en una LAN:

- **Topología de bus**: en una red en bus, todos los nodos (los servidores y las estaciones de trabajo) se conectan a un cable común (bus). Los rasgos más característicos de esta topología son los siguientes:
  - Los nodos no retransmiten ni amplifican la información.
  - El tiempo de retención de la información en los nodos es nulo.
  - Todos los mensajes llegan a todos los nodos.
  - No es necesario ningún encaminamiento de la información.
  - La fiabilidad de la comunicación depende únicamente del bus (punto crítico).
  - La configuración es flexible y modular.
  - Es una tecnología de bajo coste que todavía se utiliza frecuentemente.

– Ofrece facilidad para interceptar la información circulante.

La existencia de un único bus hace que el exceso de tráfico pueda provocar una disminución importante del rendimiento de la red. Para controlar el tráfico de la red se pueden utilizar conmutadores que sean capaces de discriminar el tráfico circulante.

Red con topología de bus



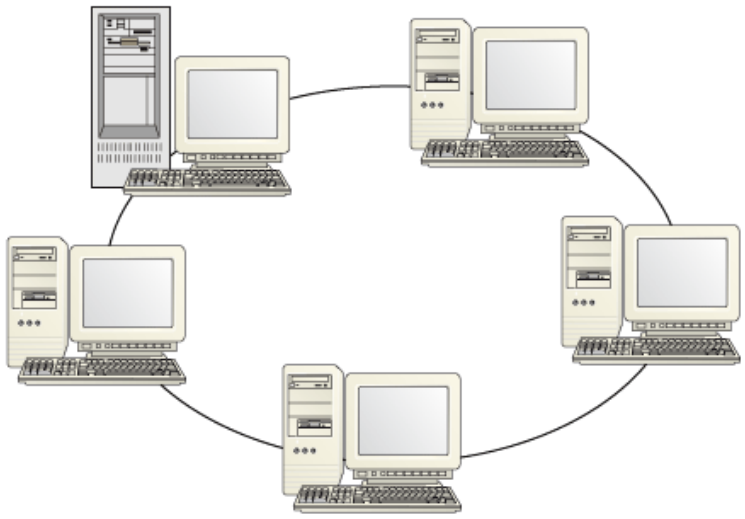
- **Topología en anillo**: en una red en anillo, el cable va de estación a estación (y al servidor) sin ningún punto final. Cada nodo tiene conexiones con dos estaciones más. Los rasgos más característicos de esta topología son los siguientes:
  – Cada nodo amplifica y repite la información que recibe.

  – Los mensajes viajan por el anillo nodo a nodo, de manera que todas las informaciones pasan por todos los módulos de comunicación de las estaciones (facilidad para interceptar la información).

  – No hay que dirigir el encaminamiento de la información.

  – La fiabilidad del anillo depende de cada uno de los nodos y de la vía de comunicación que forma el anillo. La caída de una sola estación podría provocar que la red entera dejara de funcionar.

Red con topología de anillo

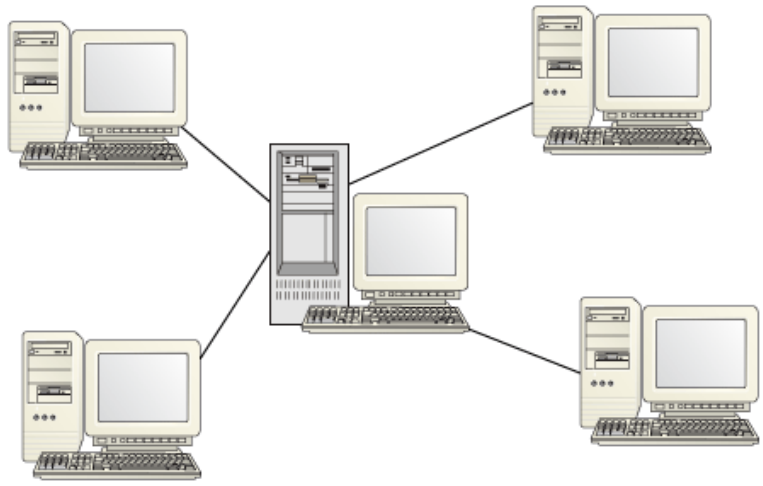


- **Topología en estrella**: en este caso, todas las estaciones de trabajo y el servidor se conectan a un solo concentrador o conmutador. Observamos que el elemento diferenciador más importante con respecto a las otras topologías es la centralización de las conexiones. Este hecho la convierte en una topología especialmente resistente a la caída de las estaciones de trabajo, aunque como principal defecto nos ofrece un punto crítico, el elemento central, el cual, si es atacado o cae por cualquier motivo, puede provocar la caída de la red entera. Los rasgos más característicos de esta topología son los siguientes:
  - Todas las estaciones se comunican entre sí mediante un nodo central.
  - El dispositivo central puede ser activo o pasivo.
  - Los fallos tienen una repercusión muy diferente según donde se producen.

Cambios en el diseño

Cuando se tienen que añadir concentradores para dar servicio a más usuarios, se tiene que plantear un posible cambio en el diseño, ya que encadenar conmutadores entre sí es muy cómodo, pero puede crear problemas de tráfico y, en ciertos casos, confusión.

Red con topología de estrella



A la hora de escoger una topología de red, se tienen que tener en cuenta los aspectos siguientes:

Documentar ayuda

"Documentar" el diseño y los componentes que forman parte de la red ayuda en las futuras tareas de mantenimiento.

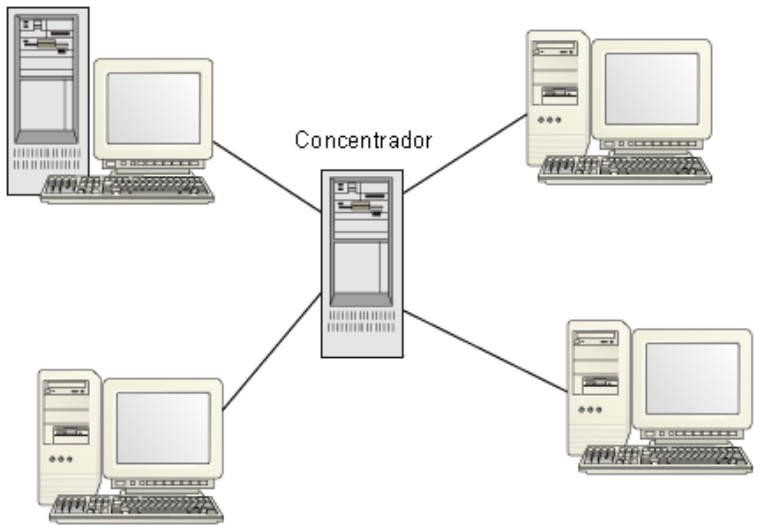
- Distancia máxima que se puede obtener.
- Número máximo de estaciones.
- Flexibilidad a la hora de añadir o eliminar estaciones de trabajo.
- Tolerancia a caídas de las estaciones.
- Retraso de los mensajes.
- Coste.
- Flujo de información que puede circular por la red.

Las topologías de bus y de anillo son las más utilizadas en redes locales, aunque por motivos de flexibilidad, fiabilidad y seguridad, el diseño físico en estrella también se ha convertido en muy popular con redes que, lógicamente, pueden funcionar en bus o anillo, pero que tienen una topología física de estrella.

Observación

Aunque físicamente no se dejen conectados, es aconsejable tener los cables tirados por los canales con un 10% más de lo que se previene utilizar.

Diseño físico basado en concentradores



Observamos que en el concentrador se mezclan todas las señales de todas las estaciones y se transmiten a todas como si se tratara de una configuración en bus.

2.3. Tipo de redes locales

El Institute of Electrical and Electronic Engineers (IEEE) es un organismo que data del año 1980 y que elaboró las normas IEEE 802.X.

Las normas IEEE 802.x definen los estándares con respecto al funcionamiento de las redes de área local:

- **IEEE 802.3**. Estándar basado en la versión 2.0 de la red ***Ethernet***. Define una red con topología de bus y método de acceso CSMA/CD (todas las es-

taciones pueden acceder simultáneamente al medio y compiten por la utilización del canal de comunicación). Su campo de aplicación se encuentra en entornos técnicos y oficinas, universidades y hospitales.

- **IEEE 802.4**. Define una red con topología de bus y paso de testigo (tan sólo puede acceder a la utilización del canal la estación en posesión del testigo). Se utiliza en entornos industriales y se conoce con el nombre de ***Token-bus***.

- **IEEE 802.5**. Estándar basado en la red ***Token-ring*** de IBM. Define una red con topología en anillo y paso de testigo. Se ha convertido en popular en entornos de oficinas, con un nivel de implantación similar a las **redes *Ethernet***.

De todos los estándares que acabamos de mencionar, posiblemente las redes *Ethernet* son las que han tenido más popularidad.

Cambios tecnológicos

Si se tiene que hacer un cambio tecnológico importante (por ejemplo, pasar de *Ethernet* de 10 Mb a 100 Mb o 1 Gb), se tendría que analizar si es mejor hacerlo de una manera gradual o bien cambiar de golpe e interrumpir todos los servicios durante el tiempo que haga falta.

La mayor parte de las implementaciones de redes *Ethernet* tienen velocidades de transmisión de 10 Mbps, y se detallan a continuación según el cableado que se utilice:

- **1Base-5**: cable de par trenzado con una velocidad de transmisión de 1 Mbps y una longitud máxima de segmento de 500 metros.

- **10Base-T**: cable de par trenzado UTP con una longitud máxima de segmento de 100 metros sobre una topología física en estrella.

- **100Base-T**: parecido al anterior, pero con velocidades de transmisión de 100 Mbps (llamadas también *fast Ethernet*).

- **10Base-5 (*thick wire*)**: cable coaxial grueso con una velocidad de transmisión de 10 Mbps. Acepta hasta 100 puestos de trabajo en segmentos de longitud de, como mucho, 500 metros.

- **10Base-2 *(thin wire*)**: cable coaxial delgado con una velocidad de transmisión de 10 Mbps. Acepta hasta 30 puestos de trabajo en segmentos de longitud de, como mucho, 185 metros.

- **10Base-F**: fibra óptica con velocidades de transmisión de 10 Mbps.

Observación

En cada implementación de red *Ethernet* (1Base-5, etc.), el primer número hace referencia a la velocidad en Mbps, y el segundo a los metros que puede tener el segmento, multiplicado por cien, sin que la señal sufra amortiguamientos.

2.3.1. Redes locales sin hilo

A la hora de escoger un tipo de red, también vale la pena considerar otras opciones diferentes de los tipos que hemos estudiado hasta ahora. Por ejemplo, en todos los tipos examinados hemos podido captar los problemas siguientes:

- Dificultad, o imposibilidad incluso, para hacer llegar el cableado cuando el sitio es físicamente de difícil acceso.
- Necesidad de hacer una estimación de crecimiento de la red y desarrollar más infraestructura de la que se necesita en un principio para poder prever este crecimiento en el futuro.
- En todos los casos, hay que agujerear las paredes o el suelo para tirar el cableado necesario.

Para poder resolver este tipo de problemas, han aparecido las llamadas redes locales sin[16] hilo, es decir, redes basadas en ondas de radio o infrarrojas. El objetivo primordial en estas redes es la comodidad del usuario final (o sea, la posibilidad de conectarse a la red desde cualquier lugar de la organización y en cualquier momento) y la facilidad de implementación y crecimiento de la red (sin olvidar que aspectos como la fiabilidad y el ancho de banda también son importantes).

(16)En inglés, *wireless local area network* (WLAN).

El IEEE[17] ha definido la norma 802.11 (y posteriores) para regular el funcionamiento de las redes sin hilo. La más extendida es la norma 802.11b, con velocidades de hasta 11 Mbps. Emite dentro de la banda de 2.4 GHz ISM (*industrial, scientific and medical*).

(17)IEEE son las siglas del Institute of Electrical and Electronic Engineers.

Normas 802.11

Hay diversas normas 802.11. Son las siguientes: 802.11a, 802.11b, 802.11g, 802.11 Super G, 802.11i y 802.16.

Las redes locales sin hilo pueden operar en modo *ad-hoc* o en modo infraestructura:

- **Modo *ad-hoc*** (cliente frente a cliente): todas las máquinas que se encuentran dentro de la misma zona de alcance se pueden comunicar entre sí directamente. No es habitual, aunque es práctico, por ejemplo, para intercambiar la información entre dos ordenadores (sería similar a la conexión de dos ordenadores mediante un cable trenzado).
- **Modo infraestructura** (cliente frente a punto de acceso): las estaciones se comunican con los llamados puntos de acceso, que actúan de repetidores y difunden la información al resto de la red.

Como la información no necesita ningún medio determinado para circular, estas redes presentan problemas de seguridad importantes. Por ejemplo, en una configuración normal de red, el cortafuegos suele ser un elemento crítico de la seguridad y reúne buena parte de las medidas de protección que evitan los ataques exteriores. En una red sin hilo, los atacantes ya no necesitan "pasar" por el cortafuegos y pueden atacar directamente otros dispositivos de la red. La norma 802.11 previene la utilización del protocolo *wired equivalent protocol* (WEP) para resolver estos problemas, pero no es un mecanismo de protección seguro porque, actualmente, puede ser descifrado sin muchos problemas.

WEP

Wired equivalent protocol (WEP) se basa en un cifrado RC4. Una clave WEP predeterminada se tiene que situar en cada punto de acceso y en cada cliente. Sólo a aquellos clientes con la misma clave se les permitirá el acceso.

A raíz de los problemas de seguridad provocados por el protocolo WEP[18], se ha desarrollado el llamado *Wi-Fi Protected Access* (WPA), el cual forma parte de la especificación 802.11i. Así pues, en la actualidad, nos encontraremos con mecanismos de seguridad como el uso de cifrado AES, un mejor protocolo de autenticación (uso del WPA) y control de la integridad del mensaje (uso de la función *hash* MIC, en lugar del CRC-32 utilizado en el protocolo WEP).

[18]Recordad que WEP es la sigla de *wired equivalent protocol*.

Elementos portables

Es importante que, para aprovechar todas las ventajas de las redes sin hilo, las estaciones de trabajo también puedan ser elementos portables, como un ordenador portátil o un PDA.

A pesar de todo, hay que tener presente que las redes locales sin hilo requieren, a causa de su naturaleza intrínseca, unas medidas de seguridad mayores que las que se adoptarían en una red "cableada" normal.

Finalmente, también hay que tener presente la tecnología *Worldwide Interoperability for Microwave Access* (WiMAX), estándar (IEEE 802.16) de transmisión sin hilo de datos, diseñada para ser utilizada en el área metropolitana, proporcionando accesos concurrentes a áreas de como mucho 48 kilómetros de radio, y con velocidades de transmisión de hasta 70 Mbps. Como es evidente, esta tecnología permite conectar nuestro dispositivo móvil (ordenador portátil, PDA, etc.) en cualquier lugar y, entre otras ventajas, podría hacer llegar Internet a zonas de difícil acceso donde no sea posible instalar ninguna infraestructura. Emite dentro de la banda de 2 a 11 Ghz y de 10 a 60 Ghz para comunicación entre antenas proveedoras de servicio. El algoritmo de cifrado utilizado es un triple DES, pero se prevé la adopción del algoritmo AES cuando empiece su comercialización.

3. Protocolos de comunicación

Una vez instalado el hardware, el cableado y los diversos dispositivos que forman la red, hay que instalar el software de red, que gestionará todos los servicios. Estos servicios se articulan sobre un conjunto de protocolos que permitirán la comunicación entre los diferentes ordenadores de la red. Los protocolos más comunes son los de la familia TCP/IP (entre otros, Apple Talk para sistemas Apple Macintosh, IPX/SPX, etc.).

Conjunto de protocolos TCP/IP

TCP e IP sólo son dos de los protocolos englobados dentro del conjunto genérico TCP/IP, pero son los más conocidos y, finalmente, los que dan el nombre a todo el conjunto. Otros protocolos TCP/IP son: *Address Resolution Protocol* (ARP), *Internet Control Message Protocol* (ICMP).

3.1. Protocolo TCP/IP

TCP/IP está formado por un conjunto de protocolos que permiten compartir recursos a los ordenadores de una red. Lo desarrolló, en 1972, el Departamento de Defensa de Estados Unidos con la finalidad de interconectar los recursos de la conocida red ARPANET (una red del Departamento de Defensa), y con el paso del tiempo se ha convertido en el estándar utilizado en Internet. También se encuentra estrechamente vinculado al sistema operativo Unix, aunque actualmente la gran mayoría de sistemas operativos soportan TCP/IP. De hecho, los protocolos TCP/IP son extremadamente flexibles, de manera que casi todas las tecnologías subyacentes (*Ethernet*, *Token-ring*, etc.) se pueden utilizar para transmitir tráfico TCP/IP.

Prototolo UDP

El protocolo *User Datagrama Protocol* (UDP) es un protocolo no fiable y no orientado a conexión, situado en la capa de transporte del modelo OSI (la misma que el protocolo TCP).

Cuando se utiliza el protocolo TCP/IP, la información se transmite como una secuencia de datagramas que contienen los datos que hay que transmitir e información de control. Cada uno de estos datagramas se envía individualmente a la red, de manera que la información original pueda ser reconstruida al llegar a la máquina destino a partir del reagrupamiento de los datagramas enviados (cabe decir que los datagramas no tienen que llegar necesariamente con el mismo orden en que fueron entregados).

El protocolo *Transmission Control Protocol* (TCP) garantiza la recepción de los datos y que los datagramas sean rehechos en el orden correcto (servicio fiable de transmisión extremo a extremo). Al mismo tiempo, este servicio descansa en el proporcionado por el protocolo *Internet Protocol* (IP), que no es fiable y que hace funciones de encaminamiento de los datagramas.

3.2. Protocolo IPv6

El protocolo IPv6, o *Next Generation Internet Protocol* (IPng), es la nueva versión del protocolo IP[19], destinada a sustituir la que todavía se está utilizando (conocida como **IPv4**). Fue diseñado por Steve Deering y Craig Mudge, y adoptado

(19)IP se la sigla de la expresión inglesa *Internet Protocol*.

por el Institute Engineering Task Force (IETF) en 1994. En la nueva versión se eliminaron aquellas funciones del protocolo IP que no se utilizaban y se añadieron nuevas. Veamos cuáles son las prestaciones más importantes del IPv6:

- **Mayor capacidad de encaminamiento**. Una de las principales deficiencias del protocolo IPv4 consistía en su poca capacidad de encaminamiento (2^{32}). Las nuevas direcciones, formadas por 16 octetos, permiten una capacidad de encaminamiento mucho más elevada y suficiente para evitar el colapso de la asignación de direcciones: 2^{128}, aproximadamente, 3,4 x 10^{38}. Además, por el mismo motivo, con IPv4 no se pueden asignar direcciones públicas a todos los usuarios o dispositivos, sin las cuales los servicios de extremo a extremo no pueden funcionar (por ejemplo, voz y vídeo sobre IP).

- **Seguridad integrada mediante *Internet Protocol Security* (IPSec)**.

- **Movilidad**: posibilidad de que un nodo mantenga su dirección IP, a pesar de su movilidad.

- **Autoconfiguración**: el nuevo protocolo también incluye de base la posibilidad de que el propio *host* sea capaz de autoconfigurar sus interfaces y conectarse a la red.

Ved también

Sobre la seguridad mediante IPSec, ved el subapartado 5.4 de este módulo, referido a las VPN.

Otras propiedades interesantes incluyen un nuevo sistema de representación de números de dominio (DNS), fácilmente ampliable a nuevas prestaciones, túneles IPv6 en IPv4 (permiten que máquinas con IPv6 instalado se puedan comunicar entre sí a través de una red IPv4), y nuevos tipos de direcciones:

- **Unicast**: un paquete entregado a una dirección de este tipo tan sólo llegará a la interfaz identificada con esta dirección (es el equivalente de las direcciones IPv4 actuales).

- **Anycast**: en este caso, la dirección llegará a "alguna" (la dirección más próxima según el protocolo de encaminamiento) de las interfaces identificadas con la dirección del conjunto.

- **Multicast**: en este caso, la dirección llegará a "todas" las direcciones de las interfaces del grupo (equivalente a las direcciones *broadcast* de IPv 4).

4. Configuración de la red en los ordenadores (cliente/servidor)

Aunque el concepto cliente/servidor abarca otros aspectos que aquí no expondremos, en el caso que nos ocupa entenderemos que el ordenador que actúa como servidor es aquel al cual llegan las solicitudes de otros ordenadores (los clientes), normalmente conectados a la misma red.

Para poder trabajar en un entorno cliente/servidor, hace falta que los clientes ejecuten el software de red sobre el sistema operativo "normal" de la estación de trabajo. Por otra parte, el servidor también ejecutará su software a la espera de recibir las solicitudes de las estaciones de trabajo que quieren acceder a sus servicios. Este flujo de información requiere que servidores y clientes compartan el mismo protocolo de comunicación.

4.1. Configuración de las estaciones de trabajo

A continuación hablaremos muy brevemente de los pasos que hay que seguir para conectar una estación de trabajo a la red. Esta operación depende mucho del sistema y protocolo que se escoja, de manera que todas las indicaciones que se darán son de carácter muy general.

1) Instalación y configuración de los controladores de la tarjeta de red. El primer paso consiste en instalar y configurar los controladores del NIC[20] de nuestra estación de trabajo. En estos casos, especialmente cuando las tarjetas son de fabricantes diferentes, la instalación y configuración de los controladores puede ser una tarea complicada en la que se tengan que resolver conflictos de entrada/salida (E/S) y de interrupciones con otros NIC u otros recursos del sistema.

[20]NIC es la sigla de tarjetas de interfaz de red, en inglés, *network interface card*.

Observación

Tened presente que una estación de trabajo puede necesitar más de una tarjeta de red.

2) Selección y configuración del protocolo de comunicación. En caso de que necesitemos conexión con Novell, habrá que instalar el protocolo SPX/IPX. Para hacerlo con Macintosh, hace falta el protocolo Apple Talk. Como ya se ha indicado, sin embargo, el protocolo más común es TCP/IP, imprescindible si queremos tener acceso a Internet.

Targeta *Plug and Play*

Si la tarjeta de red es *Plug and Play* se configurará automáticamente.

3) Instalación y configuración de clientes.

4) Otros aspectos configurables. A partir de este momento, se pueden configurar otros aspectos, como los siguientes:

- Control de accesos:
  - Por recursos: permite proporcionar una contraseña para cada recurso compartido.

  - Por usuarios: permite especificar los usuarios y grupos que tienen acceso a cada uno de los recursos compartidos.

- Compartimentación de ficheros:
  - Permiso de lectura.
  - Completo.
  - Permiso de lectura o completo según contraseña.

- Compartimentación de impresoras.

- Identificación de la máquina (será el número con el que aparecerá en la red).

- Grupo de trabajo al cual pertenece la máquina.

Instalación de impresoras

La impresora tiene que estar instalada con los controladores necesarios en el ordenador donde esté conectada. Las estaciones que la tengan que utilizar también necesitarán tener instalados los controladores.

4.2. Monitorización de la red

Una vez configurada la red, hay que supervisar su funcionamiento para garantizar la prestación de los servicios que ofrece y detectar los problemas que se puedan producir. Para poder determinar dónde se localizan los posibles problemas, hay diversas herramientas que ayudan al administrador a acotar las zonas en que se producen. Así pues, es posible tener un ordenador en el cual se vea reflejada la red y, en un momento determinado, se pueda ver qué es lo que no funciona correctamente.

Con respecto a las estaciones de trabajo, es evidente que cuando se produce algún problema los mismos usuarios se quejan y notifican que su máquina no funciona correctamente, o que el servidor da problemas. Se tiene que tener en cuenta, sin embargo, que los usuarios no tienen que ser necesariamente expertos en redes de ordenadores, y se puede dar el caso de que un usuario diga que la red no va bien (o que funciona lentamente), cuando lo que sucede en realidad es que el usuario tiene el disco duro al 99% de ocupación, y es el sistema operativo el que funciona lentamente. Sin embargo, hay herramientas de administración remota que pueden facilitar diagnósticos sin necesidad de desplazarse a la estación donde se produce el problema.

Control del estado de los puertos

Algunos dispositivos de conexión incluso disponen de un pequeño servidor web para mostrar el estado de los puertos y, simplemente escribiendo http://direccion_ip_del_dispositivo, ya se puede ver cuál es su estado.

También es importante mantener un control del funcionamiento de los conmutadores y concentradores de la red. En este sentido, hay software específico que permite la grabación de los errores de temperatura o mal funcionamiento que pueden sufrir estos equipos. Normalmente, estos dispositivos tienen dos vías de acceso, una por el puerto serie y otra por la red (cada uno de los dispositivos tendría que tener asignada una dirección IP). Una posible avería podría consistir, pues, en el hecho de que uno de los puertos de un conmutador se hubiera estropeado, de manera que utilizando la red nos podríamos conectar al conmutador y verificar el estado de los puertos.

5. Seguridad de la red

Como se ha visto en los apartados anteriores, una red es un conglomerado de muchos elementos heterogéneos. Por lo tanto, no podemos confiar la seguridad de un sistema tan complejo a la acumulación de medidas de control en el punto más evidente: el servidor. Así pues, con respecto a la seguridad de la red (entendida de la manera más genérica posible), un administrador tendría que tener en cuenta los puntos siguientes:

Ved también

Para profundizar sobre la seguridad de una red, ved el módulo "Administración de la seguridad".

- **Sistema de ficheros**. Se tiene que garantizar que sólo puedan acceder a los ficheros o modificarlos los usuarios autorizados a hacerlo.

Ved también

Ved el módulo "Administración de usuarios".

- **Código malicioso**. Se tiene que evitar el código malicioso. Se llama *código malicioso* el código que se inserta dentro de un programa "autorizado" y que hace una serie de acciones desconocidas para el usuario, las cuales actúan normalmente en detrimento suyo. Los ejemplos más conocidos de código malicioso son los virus y los troyanos.

- **Autenticación de usuarios**. Se tiene que habilitar un proceso de verificación de la identidad de una persona a la hora de acceder a un recurso. Habitualmente, los usuarios se autentican mediante un número de usuario y una contraseña (hay diferentes tipos de autenticación y diferentes políticas de asignación de contraseñas, que puede determinar un administrador).

Ved también

Ved el módulo "Administración de la seguridad" para más detallas sobre la autenticación de usuarios.

- **Criptografía**. Se tiene que utilizar herramientas criptográficas. Éstas permiten garantizar la confidencialidad de los datos que circulan por la red o se encuentran almacenadas en un sistema informático.

- **Herramientas de seguridad**. El administrador puede hacer uso de diversas herramientas con la finalidad de comprobar y mantener la seguridad de la red. En general, podemos distinguir las siguientes:
  - Herramientas para comprobar la vulnerabilidad de las mismas máquinas (por ejemplo, un escáner de puertos).
  - Herramientas que ofrecen servicios seguros (por ejemplo, el uso de *Secure Shell* en lugar del habitual *Telnet*).
  - Herramientas que garantizan la integridad del sistema (como *Tripwire*).

- **Monitorización del sistema**. Se tiene que hacer un seguimiento de la actividad del sistema. Se llama *logging* al procedimiento mediante el cual se registran, en un fichero, las actividades que tienen lugar en un sistema operativo o en una aplicación. La importancia de los ficheros log es evidente, y nos permitirá averiguar "qué" ha pasado en un sistema informático y, si hace falta, tomar las medidas adecuadas. Es muy importante plantear "qué" aplicaciones tienen que registrar log y "cuándo" lo tienen que

hacer, y también cuándo se tienen que eliminar o migrar a un dispositivo de almacenamiento para poder tener espacio en el sistema.

- **Seguridad de las topologías y los tipos de red**.

Ved también

Recordad que la seguridad de las topologías y los tipos de red son aspectos ya se han desarrollado en el apartado 2 de este mismo módulo.

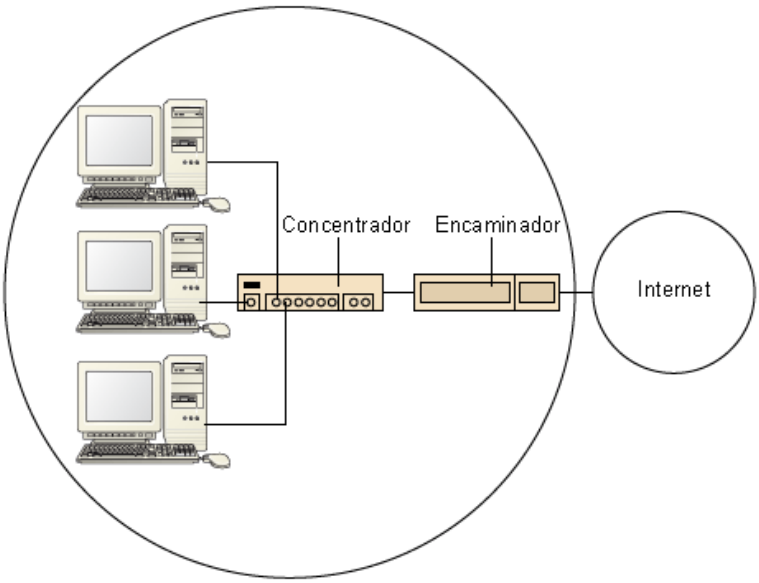
- **Seguridad del hardware de red**. Con respecto a la seguridad de los conmutadores, concentradores y encaminadores, hay que tener en cuenta los aspectos siguientes:
  - Se tiene que activar el cifrado (en caso de que los dispositivos lo admitan).
  - Cuando no sea necesario, hay que desactivar el control remoto de administración.
  - Se tienen que cambiar las contraseñas de administración predeterminadas de los dispositivos.

Contraseñas predeterminadas

Muchos intrusos (*hackers*) conocen las contraseñas predeterminadas de los dispositivos, lo cual les permite acceder a los sistemas de una manera muy sencilla y evitando todos los mecanismos de seguridad explícitos.

Hay que destacar que el encaminador se puede convertir en el punto más crítico de una red desde la perspectiva de posibles ataques externos:

El encaminador como elemento crítico en la seguridad



- **Sistema de control de acceso a LAN basado en autenticación.** Mediante este sistema, los dispositivos (en lugar de los usuarios) que quieren conectarse al medio común se tendrán que autenticar (basándose en la dirección MAC del dispositivo). Este método requiere tres componentes:
  - Cliente. Es el dispositivo (por ejemplo, un portátil) que desea conectarse a la LAN. Consiste en un software instalado o integrado en el dispositivo que se quiere autenticar.
  - Autenticador. Es el elemento que controla el acceso físico al medio, basándose en el estado de autenticación del cliente. El estado inicial de los puertos del autenticador es "no controlado"; si el proceso de autenticación finaliza afirmativamente, entonces el puerto cambia su

estado a "controlado", y el dispositivo es autorizado para acceder al medio.

– Servidor de autenticación. Es el dispositivo de "confianza" que se encargará de efectuar la validación de la identidad del cliente. Notificará el resultado al autenticador.

5.1. Cortafuegos

Los cortafuegos son dispositivos que evitan el acceso de usuarios no autorizados a un *host* determinado. El administrador tiene que instalar estos dispositivos teniendo en cuenta la estructura de la red y determinar los servicios que tienen que quedar disponibles para los usuarios.

En la práctica, las funciones del cortafuegos las pueden llevar a cabo dispositivos diversos:

- Software.
- Encaminadores.
- Ordenadores dedicados exclusivamente a las tareas de filtración de paquetes (servidores intermediarios, *proxy*).

El cortafuegos es probablemente uno de los elementos más importantes para la seguridad de nuestra red. Con su utilización es posible evitar, por ejemplo, los ataques SYN. Hay que considerar, a la hora de instalar un cortafuegos, los aspectos siguientes:

Ved también

Sobre los atacas SYN ved el módulo "Administración de la seguridad".

- No se tienen que utilizar en lugar de otras herramientas, sino conjuntamente con éstas. Tenemos que tener en cuenta que el cortafuegos será el punto que recibirá todos los ataques sobre nuestro sistema.

- Centraliza una buena parte de las medidas de seguridad de la red en un único sistema (no hace falta que sea un único dispositivo), y si se ve comprometido, la red quedará expuesta a los ataques de los intrusos.

- Puede proporcionar una falsa sensación de seguridad a los administradores. No por instalar un cortafuegos podemos asumir que la red es segura y prescindir de vigilar la seguridad de los equipos internos de la red.

En general, las decisiones básicas de configuración de un cortafuegos son:

- La configuración y el nivel de seguridad potencial del cortafuegos estará en relación al uso del dispositivo. Así, la política será diferente si conecta dos

subredes diferentes, que si tiene que filtrar los paquetes de la organización con el exterior.

- Se tiene que definir e implementar, a través de la política de seguridad, el nivel de monitorización y de control deseado en la organización. Se tiene que indicar básicamente qué se tiene que permitir y qué se tiene que denegar. Existen dos posibilidades:
  - Política restrictiva: se deniega todo aquello que explícitamente no se permite.
  - Política permisiva: se permite todo, excepto lo que se ha negado explícitamente.

- La inversión tiene que ser proporcional al valor estimado de lo que deseamos proteger. Un sistema de cortafuegos puede ser muy barato o costar miles de euros.

Existen arquitecturas de cortafuegos diferentes, pero nos centraremos en las arquitecturas DMZ. Esta arquitectura coloca una subred entre las redes externa e interna. En la mayoría de arquitecturas de cortafuegos, la seguridad se centra en el llamado *host bastion*, de manera tal que si su seguridad queda comprometida, el resto de la red queda automáticamente expuesta. Como el dispositivo *host bastion* es un objetivo interesante para muchos atacantes, la arquitectura DMZ[21] es un intento de aislarla en una red perimetral, de tal forma que el intruso que acceda a esta máquina no consiga un acceso total a la subred protegida.

[21]DMZ es la sigla de *DeMilitarized Zone*, en castellano, zonas desmilitarizadas.

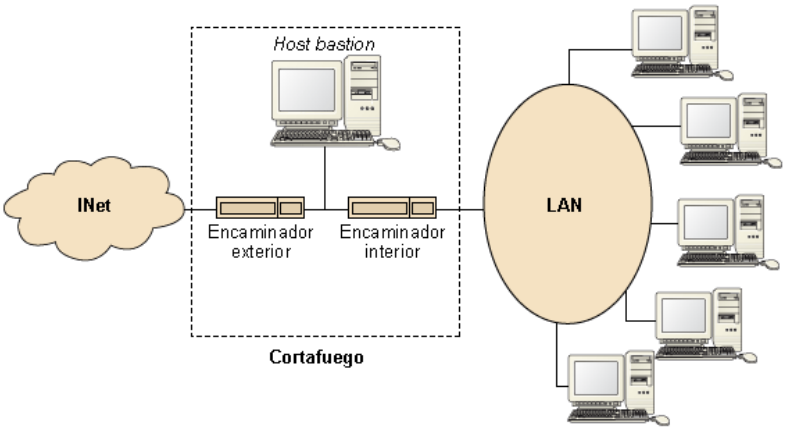
Host bastion

Host bastion es el dispositivo o sistema que se encuentra especialmente asegurado y que filtra el tráfico de entrada y salida, y oculta la configuración de la red hacia fuera.

En la actualidad, ésta es la arquitectura más compleja y segura. Se usan dos encaminadores, llamados interior y exterior, conectados ambos a la red perimetral.

En esta red perimetral, que es el sistema cortafuegos, se incluye el *host bastion*, y también se podrían incluir otros sistemas que requieran un acceso controlado, como por ejemplo el servidor de correo; el *host* y el servidor serían los únicos elementos visibles desde el exterior de nuestra red. El encaminador exterior tiene asignada la tarea de bloquear el flujo no deseado en ambos sentidos (entre la red perimetral y la red externa), mientras que el interior tiene la misma tarea, pero con el flujo de información entre la red interna y la perimetral. Un atacante tendría que romper la seguridad de ambos encaminadores para poder acceder a la red protegida.

Arquitectura DMZ



5.2. Sistemas de detección de intrusos

Los sistemas de detección de intrusos (IDS) monitorizan los contenidos del flujo de información a través de la red buscando y rechazando posibles ataques. Pueden combinar hardware y software, y normalmente se instalan en los dispositivos más externos de la red, como cortafuegos o servidores CAU[22]. Admiten dos tipos de clasificaciones:

[22]En inglés, *proxy*.

1) Según la actividad que realizan:

a) Basados en red. Monitorizan una red. Suelen ser elementos pasivos que no sobrecargan la red en exceso.

b) Basados en *host*. Monitorizan un *host* (o un conjunto de ellos) y permiten un control más detallado, registrando los procesos y usuarios implicados en las actividades registradas por el IDS[23]. Consumen recursos del *host* e incrementan el flujo de información a través de la red.

[23]Recordad que IDS es la sigla de *sistema de detección de intrusos*.

c) Basados en aplicaciones. Monitorizan los ficheros de registro o log de una aplicación específica para detectar actividades sospechosas. Consumen muchos recursos del *host*.

2) Según el tipo de análisis que realizan:

a) Basados en firmas. De forma similar a los software antivirus, estos tipos de IDS monitorizan la red en busca de patrones (firmas de ataque) que permitan identificar un ataque ya conocido. Estos tipos de IDS requieren que las bases de datos de firmas de ataque se encuentren constantemente actualizadas.

b) Basados en anomalías. En este caso, el IDS buscará comportamientos anómalos en la red (un escaneo de puertos, paquetes mal formados, etc.).

Puede producir falsos positivos a causa de la ambigüedad de lo que se podría considerar un "comportamiento anómalo de usuario", pero permiten adaptarse a nuevos ataques sin necesidad de añadir nuevas firmas.

SNORT

Un IDS muy conocido, casi una herramienta de referencia, *open source*, es el llamado SNORT.

5.3. Cebos y redes de cebos

Un cebo[24] es un sistema informático (o software) que se ofrece de forma deliberada al acceso público con la finalidad de estudiar las pautas de los posibles atacantes que pueda tener.

(24)En inglés, *honeypot*.

Por lo tanto, estos tipos de sistemas no podrán contener ninguna información importante y necesitarán herramientas pasivas de auditoría que puedan permitir conocer, con posterioridad al ataque, qué es lo que ha pasado en el sistema. Frecuentemente, estos tipos de sistemas también contienen directorios o números de ficheros con identificaciones golosas que despierten la curiosidad de los atacantes. Además de su finalidad de análisis, también pueden utilizarse para distraer la atención de los posibles atacantes del verdadero sistema, el cual no tendría que ser accesible a través del sistema utilizado como cebo. Los cebos no se encuentran, generalmente, completamente securizados y las aplicaciones y dispositivos se configuran con las opciones por defecto, las cuales suelen presentar múltiples agujeros de seguridad.

La generalización del concepto de cebo en una red se llama *honeynet*. En este caso los atacantes, además de servidores no completamente securizados, también pueden encontrar dispositivos periféricos en la red, como encaminadores o cortafuegos.

5.4. Red privada virtual

Una red privada virtual (VPN[25]) es una red privada que se extiende a diferentes puntos remotos mediante el uso de infraestructuras públicas de transporte (por ejemplo, Internet).

(25)VPN es la sigla de *Virtual Private Network*.

La transmisión de paquetes de datos se realiza mediante un proceso de encapsulamiento, y por seguridad, de cifrado, ya que no hay que olvidar que los datos circularán, durante un tiempo, por tramos de red pública. Estos paquetes de datos de la red privada viajan a través de un "túnel" definido en la red pública. Es decir, se aprovecha el bajo coste del acceso a Internet, se añaden técnicas de cifrado fuerte para conseguir seguridad y se simulan las clásicas conexiones punto a punto.

De esta forma, un usuario (una sucursal de la organización, un teletrabajador, un representante comercial, etc.) conectado a través de Internet a la red corporativa de la organización, estableciendo un túnel VPN, puede funcionar como si estuviera dentro de la propia organización a todos los efectos de conectividad.

En el caso de acceso remoto a un equipo, la VPN permite al usuario acceder a su red corporativa, asignándole a su ordenador remoto las direcciones y privilegios de la misma, aunque la conexión se haya efectuado mediante una red pública, como es Internet.

La característica que convierte la conexión "pública" en "privada" (en una VPN) es lo que se llama un túnel, término referido a que únicamente ambos extremos son capaces de ver lo que se transmite por el túnel, convenientemente cifrado y protegido del resto de Internet. La tecnología de túnel cifra y encapsula los protocolos de red que se utilizan en los extremos sobre el protocolo IP. De esta forma, podemos operar como si se tratara de un enlace dedicado convencional, de forma transparente al usuario.

El protocolo más extendido para la creación de las VPN es *Internet Protocol Security* (IPSec). Consiste en un conjunto de estándares industriales que comprueban, autentican y cifran los datos en los paquetes IP, y protegen los datos en las transmisiones de red. En definitiva, IPSec aporta la propiedad de confidencialidad mediante el cifrado de tráfico IP, integridad en el tráfico IP mediante el rechazo del tráfico modificado, así como autenticación y prevención contra los ataques de reproducción. IPSec utiliza certificados (firmados digitalmente por una entidad emisora de certificados) para comprobar la identidad de un usuario, equipo o servicio, y enlazan de forma segura una clave pública a la entidad que dispone de la clave privada correspondiente.

Otros protocolos VPN

Otros protocolos VPN son, por ejemplo, *Point-to-Point Tunneling Protocol* (PPTP) y *Layer 2 Tunneling Protocol* (L2TP).

Ved también

Ved el módulo "Administración de la seguridad".

El protocolo tiene dos formas operacionales:

- **Modo transporte**. Utilizado para proteger conexiones individuales de usuarios remotos. Las comunicaciones se cifran entre un ordenador remoto (el cliente VPN) y el servidor de VPN. Esta configuración puede ser de interés, por ejemplo, cuando la organización dispone de datos muy confidenciales que tendrían que permanecer ocultos para muchos usuarios. De esta manera, se separan los datos confidenciales gracias al servidor VPN, de forma que sólo puedan acceder a ellos los usuarios autorizados.

- **Modo túnel**. Las comunicaciones se cifran entre dos dispositivos de tipo enrutador (o un enrutador y el servidor de VPN), con el que se protegen todas las comunicaciones de todos los ordenadores situados tras cada enrutador.

Además de las VPN basadas en red pública, también hay que mencionar las VPN de confianza[26], en las cuales la extensión se realiza sobre una red privada, de confianza, y por lo tanto, permite ahorrarse el cifrado del flujo de información que circula a través del túnel. Los protocolos utilizados en estos tipos de redes son diferentes: *Asynchronous Transfer Mode* (ATM), *Multi-Protocol Label Switching* (MPLS) y *Layer 2 Forwarding* (L2F).

(26)VPN de confianza se expresa en inglés como *trusted VPN*.

6. Responsabilidades del administrador

Como podemos intuir, la administración de una red es una tarea muy compleja que abarca muchísimos aspectos, como los siguientes:

- Velar por el funcionamiento correcto de la red.
- Garantizar que el tiempo de respuesta esté dentro de los márgenes establecidos.
- Controlar la seguridad del sistema informático en la parte que utiliza la red como medio de transmisión.
- Gestionar y controlar las impresoras que forman parte de la red de ordenadores.
- Gestionar los servicios propios de la red, como el FTP, el Telnet, etc.

Aunque se puede tener la sensación de que cuando la red ya se encuentra en funcionamiento no necesita ningún mantenimiento, la configuración de la red que interconecta todos los recursos se tiene que repasar constantemente, ya que lo más habitual es que siempre haya alguna modificación en las conexiones a causa de puestos de trabajo que cambian, creación de nuevos puntos de trabajo, salas de reuniones que necesitan un punto de conexión para hacer una presentación, conexiones temporales para hacer test, etc. Por lo tanto, se tiene que tener presente que hay que tener actualizada la configuración de la red para poder responder con rapidez a cualquier petición de cambio por parte de algún usuario o departamento.

El **tiempo de respuesta** que se exija a la red también es un aspecto que el administrador tiene que poder garantizar. Muy a menudo nos podemos encontrar con usuarios que se quejan de la lentitud del sistema, pero un administrador tiene que saber demostrar que la red funciona en las condiciones que se establecieron en su día con el fin de garantizar el funcionamiento correcto de todos los servicios, y, en caso de que este tiempo no sea el esperado, tiene que acotar el problema hasta encontrar la solución o, si no se detecta ningún elemento que funcione mal en la red, proponer la solución adecuada para disminuir la carga y poder garantizar la calidad de los servicios que proporciona la red.

La importancia de la documentación

Es recomendable tener una documentación actualizada y bien detallada de la red que se administra.

Por otra parte, también es muy importante mantener un control de lo que pasa en la red y verificar si hay algún tipo de ataque al sistema informático. Hay bastantes herramientas para ayudar al administrador a registrarlos y monitorizarlos, y según las características que tenga el sistema es mejor utilizar unas que otras.

En tanto que la red es el medio a través del cual los usuarios tienen acceso a servicios proporcionados por servidores, es importante tener un control de las posibles **actualizaciones de sus sistemas operativos** y del software que tienen instalado. Paralelamente a estos servicios, hay un aspecto al que se tiene que dedicar atención: las impresoras que hay en la red tienen que tener una gestión especial, ya que los controladores tienen que estar disponibles para ser instalados en cualquiera de las máquinas que tengan que tener acceso a las impresoras, y se tiene que pensar en una estructura que permita a los usuarios tener las máquinas desligadas de las impresoras, para poder apagarlas y no tener ningún efecto sobre otros usuarios que quieran imprimir.

Ved también

En el módulo "Administración de la seguridad" encontraréis un apartado entero dedicado en el "ciberdelito".

También es especialmente importante disponer de las **licencias de software** de red (por ejemplo, las licencias de campus de la universidad). Como es evidente, instalar software con licencias monousuario en redes es una práctica que puede tener consecuencias en forma de sanción. El administrador de la red también tiene que conocer qué mecanismos tiene a su disposición para denunciar cualquier infracción de la que haya sido objeto (o que observe en la red que administra: ataques de los intrusos [*hackers*], presencia de fotografías de pornografía infantil, etc.).

Ved también

Las consideraciones sobre si las redes proporcionan (o no) un espacio de uso privado a los usuarios se verán en el módulo "Administración de la seguridad".

Resumen

Las redes de ordenadores permiten aprovechar mejor los recursos del sistema. En este módulo se han visto los elementos que forman parte de la red y algunos criterios que pueden ayudar a los administradores a la hora de escoger estos elementos y conectarlos entre sí. Una vez se dispone de la red, físicamente hablando, hay que hacer que los ordenadores hablen el mismo "idioma", es decir, tengan definido el mismo protocolo de comunicaciones (el más utilizado es el TCP/IP), cuya instalación se encuentra íntimamente ligada a la configuración de las estaciones de trabajo. A pesar de la heterogeneidad de las redes, los protocolos y los sistemas operativos de red, estas acciones siempre se tienen que hacer de una manera u otra, aunque la manera en que se hacen puede variar mucho.

Finalmente, una vez que la red ya esté en funcionamiento, el administrador no puede olvidar que las redes no se mantienen por sí solas y que requieren un gran esfuerzo de mantenimiento: creación y administración del entorno del usuario, monitorización de la red, actualización de software, detección de ataques, etc.

Actividades

1. En caso de que tengáis acceso a una red de ordenadores, responded las cuestiones siguientes:
a) Localizad e identificad físicamente todos los elementos que forman parte de la red.
b) ¿Qué topología se ha utilizado en su diseño?
c) ¿Qué protocolos de comunicación se utilizan?
d) ¿Cómo se configuran las estaciones de trabajo?
e) ¿Qué software de monitorización se utiliza?
f) Localizad e identificad los elementos de seguridad (software y hardware).

2. Si no disponéis de acceso a una red de ordenadores, enumerad y describid todos los elementos que participan en una conexión a Internet por la red telefónica:

Casa <-> Proveedor de servicios de Internet <-> Internet

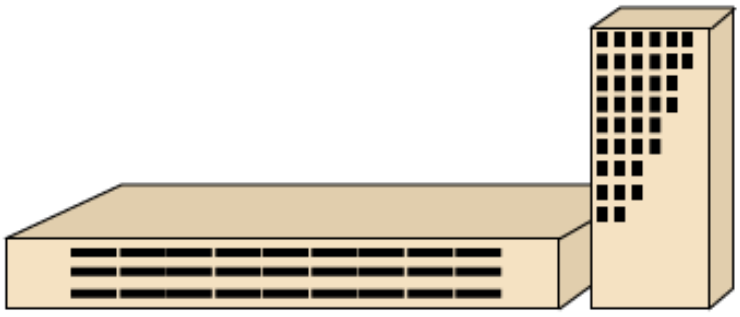
Un elemento que hará falta que tengáis en cuenta es que, con el fin de responder a posibles problemas legales (y a efectos de tarificación), un proveedor de Internet tendría que registrar las direcciones IP que va proporcionando dinámicamente a los usuarios, junto con el número de teléfono que se ha utilizado para conectarse, y también el intervalo de tiempo en que se han utilizado.

Ejercicios de autoevaluación

1. Llenad cada una de las casillas de la tabla siguiente con alguna de estas opciones: bajo/moderado/alto.

	Par trenzado	**Coaxial**	**Fibra óptica**
Coste			
Ancho de banda			
Longitud			
Interferencias			
Fiabilidad			

2. Tenéis que diseñar e implementar una red para un edificio como el siguiente, formado por un bloque de cuatro plantas y una nave industrial que trabaja con muchos motores. Diseñad un trazado para el cableado eléctrico con el fin de alimentar los motores y después poned los dispositivos de comunicación que se tendrían que instalar, tanto en la nave industrial como en el edificio, para tener una red local que comunicara las oficinas con los puntos de trabajo de la nave industrial.



3. Determinad cuál de las características siguientes no se puede atribuir a cualquier topología en estrella:

a) Todas las estaciones se conectan a un elemento central.
b) Cuando una estación emite un mensaje, siempre llega a todas las estaciones de la red.

c) Es una topología resistente a la caída de las estaciones de trabajo.
d) El dispositivo central puede ser activo o pasivo.

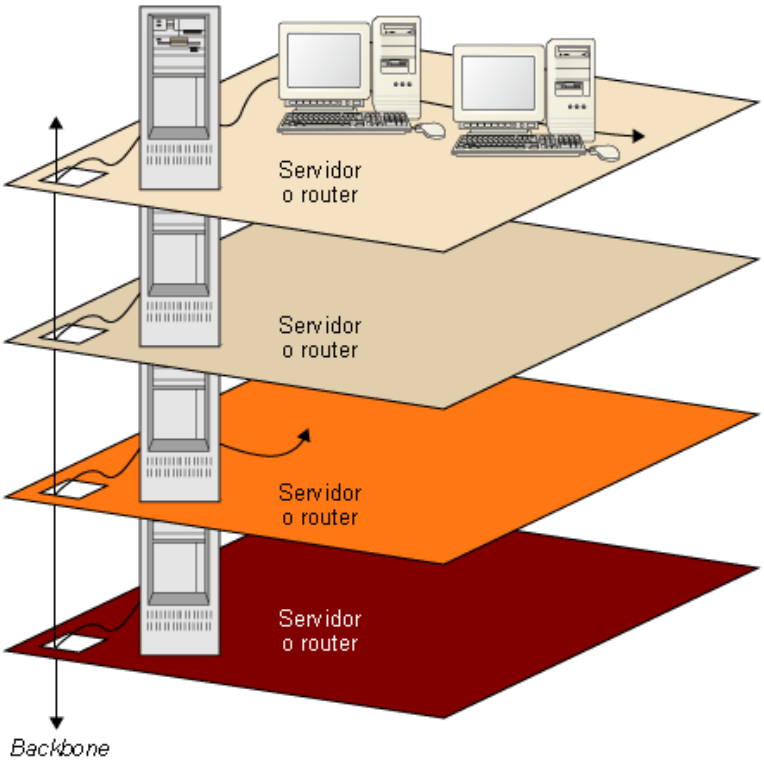
Solucionario

Ejercicios de autoevaluación

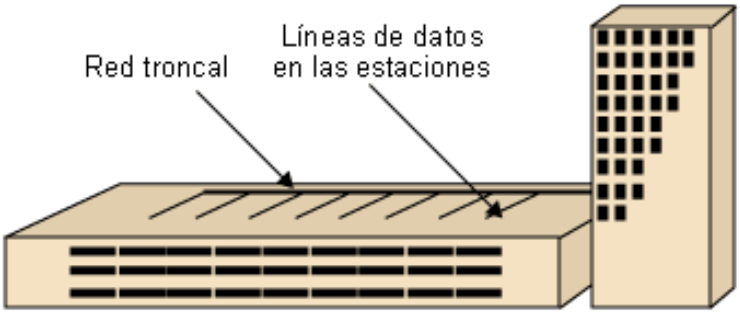
1.

	Par trenzado	Coaxial	Fibra óptica
Coste	Bajo	Moderado	Alto
Ancho de banda	Moderado	Alto	Muy alto
Longitud	100 m	1 km	Algunos km
Interferencias	Bajo	Muy bajo	Ninguna
Fiabilidad	Alto	Alto	Muy alto

2.



En la planta, el cableado también tendría que seguir un esquema de tipo red troncal (*backbone*), con ramas en los puntos necesarios. Las cuestiones básicas que hay que tener en cuenta en su diseño son las siguientes:
Las distancias del cableado no tienen que ser superiores a las permitidas. En caso contrario, hay que poner regeneradores de la señal.
Se tiene que tener muy en cuenta el problema de las interferencias eléctricas y, por lo tanto, electricidad y datos no pueden ir por los mismos sitios.
Si hay armarios de conexión, hay que tener en cuenta las cuestiones de protección de las vibraciones y de la alimentación eléctrica.



3. b.

Glosario

10Base-T *m* Cable de par trenzado UTP con una longitud máxima de segmento de 100 metros sobre una topología física en estrella.

100Base-T *m* Cable de par trenzado UTP con velocidades de transmisión de 100 Mbps.
sin. **fast Ethernet**.

10Base-2 *m* Cable coaxial delgado con una velocidad de transmisión de 10 Mbps. Acepta hasta 30 puestos de trabajo en segmentos de longitud de como mucho 185 metros.
sin. **thin wire**.

10Base-5 *m* Cable coaxial grueso con una velocidad de transmisión de 10 Mbps. Acepta hasta cien puestos de trabajo en segmentos de longitud de como mucho quinientos metros.
sin. **thick wire**.

backbone *m* Ved **red troncal**.

conmutador *m* Dispositivo que gestiona el flujo del tráfico de red teniendo en cuenta la dirección de destino de cada paquete. En otras palabras, los conmutadores pueden averiguar qué dispositivos se encuentran conectados a sus puertos y redirigen la información únicamente al puerto de destino, en lugar de hacerlo indiscriminadamente, como los concentradores.
en switch.

concentrador *m* Dispositivo que permite compartir una línea de comunicación entre diversos ordenadores. Repite toda la información que recibe para que pueda llegar a todos los dispositivos conectados.
en hub.

DHCP *m* Ved **protocolo dinámico de configuración del huésped**.

dynamic host configuration protocol *m* Ved **protocolo dinámico de configuración del huésped**.

encaminador *m* Dispositivo que gestiona el tráfico de paquetes proveniente del exterior de la red hacia el interior (y al revés). Puede tener capacidad de actuar como cortafuegos. Puede filtrar y encontrar el encaminamiento óptimo de los paquetes.
en router.

fast Ethernet *f* Ved **100Base-T**.

firewall *m* Ved **cortafuegos**.

hub *m* Ved **concentrador**.

IEEE *m* Ved **Institute of Electrical and Electronic Engineers**.

Institute of Electrical and Electronic Engineers *m* Organismo que data del año 1980 y que elaboró las normas IEEE 802.X, las cuales definen los estándares con respecto al funcionamiento de las redes de área local.
sigla: **IEEE**.

network interface card *f* Ved **tarjeta de interfaz de la red**.

NIC *f* Ved **tarjeta de interfaz de la red**.

protocolo dinámico de configuración del huésped *m* Protocolo TCP/IP que permite la asignación dinámica de direcciones IP.
en dynamic host configuration protocol.
sigla: **DHCP**.

router *m* Ved **encaminador**.

switch *m* Ved **conmutador**.

cortafuegos *m* Cualquier dispositivo (hardware o software) que permite evitar que los usuarios no autorizados accedan a una máquina determinada.
en firewall.

tarjeta de interfaz de la red *f* Tarjeta de interfaz que permite la conexión de la estación de trabajo a la red.

en network interface card.
sigla: **NIC**.

thick wire *m* Ved **10Base-5**.

thin wire *m* Ved **10Base-2**.

wireless local area network *f* Ved **red de área local sin hilo**.

WLAN *f* Ved **red de área local sin hilo**.

red de área local sin hilo *f* Red de telecomunicaciones local sin hilo basada en ondas de radio o infrarrojas.
en wireless local area network.
sigla: **WLAN**.

red troncal *f* Conjunto de cables principales que conectan entre sí los segmentos de una red local. Habitualmente son enlaces de alta velocidad (por ejemplo, fibra óptica).
en backbone.

Bibliografía

Anónimo (2000). *Linux Máxima Seguridad*. Prentice Hall.

Arnedo Moreno, J. (2002). *Redes locales sin hilos*. (Artículo UOC)

Colobran Huguet, M.; Morón Lerma, E. (2004). *Introducción a la seguridad informática*. Barcelona: Planeta UOC.

Halsall F. (1996). *Data communications, computer networks and open systems*. McGraw-Hill.

Jimeno García, M. T.; Míguez Pérez, C.; Matas García, A. M.; Pérez Agudín, J. (2008). *Guía práctica hacker*. Madrid: Anaya Multimedia.

Palet Martínez, Jordi. *Tutorial de IPv 6*.

Tanembaum, A. S. (1991). *Redes de ordenadores*. Prentice-Hall Hispanoamericana.