-

UD 09. ARQUITECTURA Y COMPONENTES DE LA RED

Sistemas informáticos
CFGS DAW

Borja Salom
b.salomsantamaria@edu.gva.es
2022/2023

Versión:230126.1040

Licencia

Nomenclatura

A lo largo de esta unidad se utilizarán diferentes símbolos para distinguir elementos importantes dentro del contenido. Estos símbolos son:

Importante

Atención

Interesante

ÍNDICE

1. Características de las redes informáticas **4**
1.1 Sistema de comunicación 5
1.2 Redes informáticas 6
1.3 Clasificación de las redes 8
1.4 Redes WAN 10
2. Arquitectura de la red **11**
2.1 Modelo OSI y protocolos TCP/IP 12
2.2 Protocolo de comunicación 13
2.3 Funcionamiento de una arquitectura basada en niveles 14
2.4 TCP/IP 16
2.5 El nivel de acceso a la red 17
2.6 La capa de Internet o red 18
2.7 El nivel de transporte 19
2.8 El nivel de aplicación 20
3. Topologías de red y modos de conexión **21**
3.1 Autobús y anillo 22
3.2 Estrella 23
3.3 Modo infraestructura y modo ad-hoc 24
4. Componentes de una red informática **25**
4.1 Clasificación de los medios de transmisión 26
4.2 Cableado estructurado 27
4.3 Elementos de interconexión 29
4.4 Tarjetas de red y direccionamiento MAC 30
4.5 Interruptores 31
4.6 Enrutadores 31
4.7 IDS 33

UD09. ARQUITECTURA Y COMPONENTES DE LA RED

1. CARACTERÍSTICAS DE LAS REDES INFORMÁTICAS .

Las redes están en todas partes, y las redes informáticas forman parte del sistema de conexión global cada vez más extendido conocido como Internet. Como futuro profesional del sector informático, una de las cosas que debes saber es: cómo funcionan los ordenadores y cómo se conectan entre sí para formar sistemas más amplios que, en la mayoría de los casos, utilizan redes de diferentes características.

En esta unidad de trabajo verás los principios de las redes informáticas, para posteriormente poder aplicarlos.

Definimos una red informática como dos o más dispositivos conectados para compartir los componentes de su red y la información que puede estar almacenada en todos ellos.

Si tomamos como referencia la definición dada por Andrew S. Tanenbaum, una red informática es un conjunto de equipos informáticos conectados entre sí mediante dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con el fin de compartir información y recursos.

Esta última definición es la que servirá de punto de partida para el desarrollo de la unidad de trabajo, ya que, como verás, para trabajar con redes de ordenadores necesitamos conocer los sistemas de comunicación más utilizados, la arquitectura que los hace posibles, los protocolos asociados, la forma de conectarlos y sus componentes.

Aunque en el desarrollo de la unidad veremos diferentes características de las redes de ordenadores, y daremos una explicación más amplia, es conveniente comenzar citando algunas de las más importantes, y que han contribuido a su generalización:

- **Conectividad**: posibilidad de conectar diferentes dispositivos entre sí para compartir recursos propios o externos, tanto en entornos locales como remotos.
- **Escalabilidad:** una red informática puede ampliar fácilmente sus posibilidades, además esta red puede conectarse con otras redes, y así proporcionar mayores beneficios.
- **Seguridad:** esta característica es deseable y necesaria, aunque no siempre se cuida lo suficiente. En algunos casos, las redes aumentan la seguridad frente a la pérdida de datos, ya que duplican la información, y en otros casos,
  disminuyen la seguridad de esos datos, ya que están más disponibles. Conviene considerar esta característica como una de las más importantes.

- **Optimización de costes:** si podemos compartir recursos, y estos recursos nos dan mayor productividad, además de facilitarnos el trabajo, estamos optimizando costes y rentabilizando mejor nuestra inversión.

1.1 Sistema de comunicación .

Según el Diccionario, sistema, en una de sus acepciones, es el conjunto de reglas o principios sobre una materia racionalmente vinculados entre sí. En este mismo diccionario podemos buscar la palabra comunicación, y encontramos que se puede definir como la transmisión de señales mediante un código común entre el emisor y el receptor.

Por tanto, podemos definir un sistema de comunicación como un conjunto de elementos que, siguiendo determinadas reglas, intervienen en la transmisión de señales, permitiendo el intercambio de información entre un emisor y un receptor.

De esta definición podemos deducir los componentes de un sistema de comunicación, que serán:

- **Emisor:** elemento que transmite la información.
- **Receptor:** elemento que recibe la información.
- **Canal:** medio por el que se transmite la información, utilizando señales debidamente codificadas.

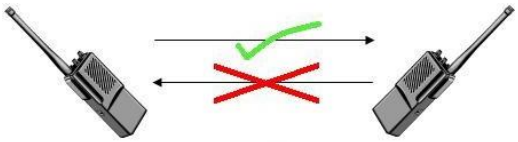
Como podemos deducir, es necesario que el emisor y el receptor codifiquen la información de forma que ambos se entiendan, por lo que necesitan crear un conjunto de reglas que regulen la comunicación entre ellos, este conjunto de reglas es lo que conocemos como protocolo de comunicación.

Teniendo en cuenta que la transferencia de información entre emisor y receptor se realiza a través del canal de comunicación, podemos definir este último como el medio físico por el que se transporta la información convenientemente cifrada, siguiendo protocolos establecidos.

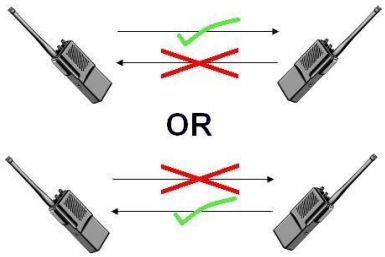
Así, podemos clasificar los sistemas de comunicación según distintos puntos de vista. Si tenemos en cuenta el medio de transmisión, podemos tener sistemas en línea o cableados y sistemas inalámbricos.

Por otra parte, si el criterio que utilizamos es la direccionalidad de la transmisión, los sistemas de comunicación pueden clasificarse en:

- **Simplex:** Cuando la comunicación se realiza en un solo sentido. El emisor emite y el receptor recibe. Ejemplo: Cuando escuchamos música en la radio, sólo recibimos.



- **Semidúplex (half duplex):** Cuando la comunicación se realiza en ambos sentidos, pero no simultáneamente. El emisor emite, el receptor recibe, el receptor se convierte en emisor y el emisor en receptor. Ejemplo: Hablar por el walkie-talkie.



- **Dúplex (full duplex):** Cuando la comunicación se realiza en ambos sentidos simultáneamente. Ambos son emisores y receptores al mismo tiempo. Ejemplo: Las redes informáticas suelen funcionar así.

Otros criterios utilizados para clasificar las comunicaciones son:

- Según la forma de sincronizar las señales: así tenemos comunicaciones síncronas y asíncronas.
- Según la naturaleza de la señal: este criterio nos lleva a utilizar los términos de comunicaciones analógicas y digitales. Esta última clasificación es más utilizada en el campo de las comunicaciones, por lo que para nosotros será más apropiado hablar de transmisiones analógicas o digitales. Esto es así
  porque los ordenadores son sistemas que se basan en el uso de señales digitales.

Además de estos criterios, también existen dos conceptos relacionados con las comunicaciones que debemos conocer, uno de ellos es el término de Equipo Terminal de Datos (ETD), que serán todos los equipos, ya sean emisores o receptores de información. El otro término es el de Equipo de Comunicación de Datos (ECD) que es cualquier dispositivo que participa en la comunicación pero que no es ni el emisor original ni el receptor final.

1.2 Redes informáticas .

Red de ordenadores o red informática: es un conjunto de equipos informáticos conectados entre sí mediante dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos con el fin de compartir información y recursos.

El principal objetivo de la creación de una red informática es compartir recursos e información, garantizar la fiabilidad y disponibilidad de la información, aumentar la velocidad de transmisión de datos y reducir el coste global de estas

acciones.

Si conectamos dos ordenadores entre sí ya tenemos una red, si conectamos más ordenadores, añadimos impresoras, y conectamos dispositivos que permitan el acceso a Internet, estamos consiguiendo que nuestra red crezca y tenga más recursos, ya que los recursos individuales se pueden compartir. Esta es la idea principal de las redes, ya que a medida que conectemos más dispositivos y éstos compartan sus recursos, la red será más potente.

Por tanto, las principales ventajas de las redes informáticas serán:

- ✓ La posibilidad de compartir recursos.
- ✓ La posibilidad de compartir información.
- ✓ Aumentar las posibilidades de colaboración.
- ✓ Facilitar la gestión centralizada.
- ✓ Reducir costes.

Si analizamos algunas de estas ventajas, está claro que utilizar redes informáticas para trabajar es mejor que hacerlo de forma aislada.

Cuando se trata de compartir recursos, la mayoría de nosotros tenemos en mente la conexión a Internet. Es obvio que una única conexión compartida a Internet es más barata que tener una conexión para cada ordenador. Ésta ha sido una de las principales razones del éxito de las redes informáticas. Pero no debemos olvidar otros recursos no menos importantes, como el uso de periféricos compartidos como: impresoras, discos duros en red, escáneres, etc. En este apartado de recursos compartidos, también debemos mencionar la posibilidad de compartir software. El software compartido está creciendo, y en algunos entornos de trabajo es imprescindible.

Relacionada con la posibilidad de compartir recursos, tenemos la posibilidad de compartir información. De esta forma podremos utilizar bases de datos compartidas, documentos que podrán ser leídos, e incluso elaborados, por varios usuarios diferentes.

Esto último enlaza con otra de las ventajas, que es la posibilidad de colaboración. Cuando compartimos recursos e información, aumentan las posibilidades de colaboración. Además, esta colaboración puede darse entre personas que están en la misma oficina o instituto, pero también puede darse entre personas que están tan alejadas que ni siquiera llegan a conocerse. Esto último está muy de moda; seguro que ha oído hablar del concepto de computación en nube para referirse a la posibilidad de ofrecer servicios informáticos a través de Internet. Este concepto está estrechamente ligado al uso de redes informáticas e Internet.

Respecto a la gestión centralizada de recursos, comentar que mejora la seguridad de los sistemas, suele optimizar el rendimiento de la red y es más barata.

Por último, podemos decir que el principal objetivo de cualquier asociación, corporación o persona es que a la hora de realizar una inversión, ésta no sea excesiva. Si se realiza una buena planificación de la red, y un buen diseño de la misma, seguramente se reducirán los costes de implantación y mantenimiento.

1.3 Red clasificación

Las redes pueden clasificarse según distintos conceptos, nosotros nos centraremos en los más utilizados.

Por alcance o extensión tenemos:

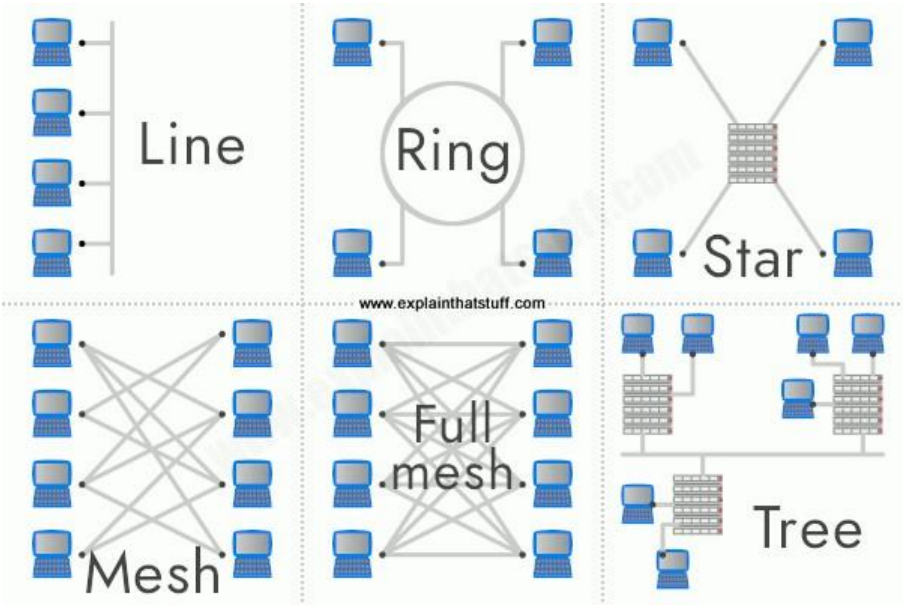
- **La red de área personal o PAN (personal area network)** es una red informática utilizada para la comunicación entre dispositivos informáticos cercanos a una persona.
- **Red de área local o LAN (local area network)** es una red que se limita a un área especial y relativamente pequeña, como una habitación, un aula, un solo edificio, un barco o un avión. Las redes de área local -6-Desarrollo de Aplicaciones Web Tema 3 tienden a tener las velocidades más altas, y son considerado el elemento esencial para la creación de redes más amplias.
- **Una red de área de campus o CAN** es una red informática que conecta redes de área local a través de un área geográfica limitada, como un campus universitario o una base militar. Este término suele utilizarse como extensión de LAN, ya que lo que realmente hay son redes locales conectadas entre sí.
  otra para cubrir un área mayor.
- **La red de área metropolitana o MAN (metropolitan area network)** es una red de alta velocidad (banda ancha) que proporciona cobertura en una amplia zona geográfica. Este concepto se utiliza para definir redes que cubren extensiones relativamente grandes, y que necesitan recursos adicionales a aquellos
  que necesitaría una red local.
- **Las redes de área extensa o WAN (wide area network)** son redes informáticas que se extienden por una amplia zona geográfica. Dentro de esta clasificación podemos encontrar las redes de telecomunicaciones que permiten el uso de Internet, y la propia Internet, que puede considerarse como una
  gigantesca red WAN.

Según las funciones de sus componentes:

- **Las redes entre iguales o peer-to-peer**, también conocidas como redes entre pares, son redes en las que ningún ordenador se encarga de su funcionamiento. Cada ordenador controla su propia información y puede funcionar como
  un cliente o servidor según sea necesario. Los sistemas operativos más utilizados incluyen la posibilidad de trabajar de esta forma, y una de sus características más destacadas es que cada usuario controla su propia seguridad.
- **Las redes cliente-servidor**, se basan en la existencia de uno o varios servidores, que darán servicio al resto de ordenadores que se consideran clientes. Este tipo de redes facilita la gestión centralizada. Para crear redes de este tipo necesitamos sistemas operativos de tipo servidor, como por ejemplo
  Windows 2008 server o GNU-Linux. Hay que tener en cuenta que, en principio, cualquier distribución de Linux puede actuar como servidor,

aunque existen distribuciones especialmente recomendadas para este fin, como Debian, Ubuntu server, Red Hat enterprise, etc.

La forma de conectar los ordenadores nos da otra clasificación muy utilizada, que es lo que se conoce como topología. En este apartado sólo citaremos algunas topologías ya que en esta unidad dedicaremos un apartado a explicarlas con más detalle. Entre las topologías de conexión podemos citar: bus, anillo, estrella, árbol, malla, doble anillo, mixta y totalmente conectada.



Según el tipo de conexión que podamos tener:

- **Redes cableadas:** En este tipo de redes se utilizan diferentes tipos de cables para conectar los ordenadores, más adelante estudiaremos lo relacionado con los tipos de cables más utilizados.
- **Redes inalámbricas:** Son redes que no necesitan cables para comunicarse, existen diferentes tecnologías inalámbricas que estudiaremos más adelante.

Otra clasificación interesante es la que tiene en cuenta el grado de difusión, en esta clasificación distinguimos dos tipos de redes:

- **Intranet** es una red informática que utiliza alguna tecnología de red para uso comercial, educativo u otro uso privado, es decir, no comparte sus recursos o información con otras redes, a menos que éstas se autentiquen, o cumplan ciertas medidas de seguridad.
- **Internet** es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, lo que garantiza que las heterogéneas redes físicas que la componen funcionen como una única red lógica mundial. Es precisamente esta característica la que ha hecho que
  la generalización del uso de Internet y que todas las redes funcionen con protocolos TCP/IP.

1.4 WAN redes

Hemos visto que las redes WAN (redes de área extensa) son redes informáticas que se extienden sobre una amplia zona geográfica. Dentro de esta clasificación podemos encontrar las redes de telecomunicaciones que permiten el uso de Internet, y la propia Internet, que puede considerarse como una gigantesca red WAN.

Las redes WAN son capaces de cubrir distancias de unos 100 a unos 1000 km, dando servicio a un país o a un continente. Un ejemplo de este tipo de red sería Internet o cualquier red de características similares.

Hay redes WAN construidas por y para una organización o empresa concreta y son de uso privado, otras las construyen los proveedores de Internet (ISP) para ofrecer conexión a sus clientes.

Hoy en día, Internet proporciona WAN de alta velocidad y la necesidad de redes WAN privadas se ha reducido drásticamente, mientras que las redes privadas virtuales que utilizan el cifrado y otras técnicas para hacer que esa red sea dedicada no dejan de aumentar.

Normalmente, la WAN es una red punto a punto que utiliza la conmutación de paquetes. Las redes WAN pueden utilizar sistemas de comunicación por satélite o radio.

Las redes WAN basan su funcionamiento en técnicas de conmutación. Podemos definir las técnicas de conmutación como la forma en que un usuario y otro establecen la comunicación. Estas técnicas son:

- **Conmutación de circuitos**: consiste en el establecimiento de un enlace físico para la transmisión entre dos nodos, que se liberará cuando finalice la comunicación en el caso de utilizar una red conmutada, o permanecerá si se utiliza una red dedicada (Ejemplo: transmisión de datos a
  a través de la red telefónica conmutada).
- **Conmutación de mensajes:** es un método basado en el tratamiento de bloques de información, dotados de una dirección de origen y una dirección de destino, de esta forma la red almacena los mensajes hasta comprobar que han llegado correctamente a su destino y proceder a su retransmisión. o
  destrucción. Es una técnica utilizada con el servicio de télex y en algunas aplicaciones de correo electrónico.
- **Conmutación de paquetes:** consiste en dividir el mensaje en paquetes. La comunicación entre dos ordenadores implica la transmisión de paquetes. Cada paquete se envía de un nodo de la red al siguiente. Cuando el nodo receptor recibe completamente el paquete, lo almacena y
  lo reenvía al nodo siguiente. Este proceso se repite hasta que el paquete llega al destino final. Se han definido dos tipos de técnicas para el uso de la conmutación de paquetes: los datagramas y los circuitos virtuales. Internet es una red de conmutación de paquetes basada en datagramas.

Las redes de área extensa suelen estar soportadas por redes públicas de telecomunicaciones que son las que todos conocemos y que solemos utilizar para conectarnos a Internet. Ejemplos de estas redes serán:

- La red telefónica básica o red telefónica conmutada (RTB o RTPC)

nos permite hablar por teléfono, pero si utilizamos un módem podemos transmitir datos a baja velocidad.

- El bucle de abonado digital asimétrico, más conocido como ADSL, los operadores de telefonía ofrecen la posibilidad de utilizar una línea de datos independiente de la línea telefónica, aprovechando el ancho de banda disponible por encima del requerido por el servicio telefónico hasta el límite permitido por la propia línea.
- La telefonía móvil a través de UMTS o telefonía 3G, ofrece la posibilidad de transferir tanto voz y datos (una llamada telefónica o una videollamada) como datos no vocales (como descargas de software, intercambio de correo electrónico y mensajería instantánea).
- Internet por cable, mediante módems de cable o routers, las redes de cable ofrecen la posibilidad de utilizar cable de fibra óptica combinado con cable coaxial, para dar acceso a Internet de alta velocidad.

2. LA ARQUITECTURA DE RED .

Cuando hablamos de arquitectura de red, podemos pensar en cómo está construida la red, los cables, los equipos, etc. Pero no es así, el concepto de arquitectura de red es más amplio e incluye cuestiones relacionadas con el hardware y el software de una red.

Antes de definir el concepto de arquitectura de red, es conveniente que entiendas que uno de los problemas más importantes a la hora de diseñar una red no es que los ordenadores se conecten entre sí, sino que estos ordenadores puedan comunicarse, entenderse, compartir recursos , que, al fin y al cabo, es lo que queremos. Para ello ya hemos dicho que se necesitan protocolos de comunicación. Debido a la complejidad que supone considerar la red como un todo, se consideró oportuno organizar las redes como una serie de capas, donde cada capa se encargara de alguna función. De este modo, se reduciría la complejidad del diseño de la red y de las aplicaciones utilizadas en ella.

Por lo tanto, podemos definir la arquitectura de red como el conjunto de capas o niveles, junto con los protocolos definidos en cada una de estas capas, que hacen posible que un ordenador se comunique con otro independientemente de la red en la que se encuentre.

Esta definición implica que la especificación de una arquitectura de red debe incluir información suficiente para que, cuando se desarrolle un programa o se diseñe un dispositivo, cada capa responda adecuadamente al protocolo apropiado.

De todo esto podemos concluir que la arquitectura de la red deberá tener en cuenta al menos tres factores importantes como son:

- La forma en que están conectados los nodos de una red, que suele conocerse como topología, además de las características físicas de estas conexiones.

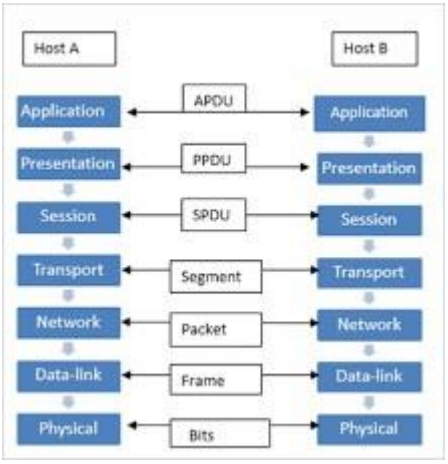
- La forma de compartir información en la red, que en algunos casos requerirá elegir un método de acceso a la red y algunas reglas para evitar la pérdida de información.
- Algunas reglas generales que no sólo promueven la comunicación, sino que también establecen, mantienen y permiten el uso de la información, estas reglas serán los protocolos de comunicación.

A continuación estudiaremos con más detalle cómo funcionan las arquitecturas basadas en niveles, los protocolos y lo más importante, veremos los dos modelos más importantes en el desarrollo de redes, el modelo de referencia OSI y la pila de protocolos TCP/IP, que podemos considerarla como la arquitectura base para las comunicaciones en Internet.

2.1 Modelo OSI y protocolos TCP/IP .

Ya hemos comentado anteriormente que la arquitectura de red se dividió por niveles o capas para reducir la complejidad de su diseño. Esta división por niveles implica que cada uno de estos niveles tiene asociados uno o varios protocolos que definirán las reglas de comunicación de la capa correspondiente. Por este motivo, también se utiliza el término pila de protocolos o jerarquía de protocolos para definir la arquitectura de red que utiliza determinados protocolos. Lo veremos más claramente cuando expliquemos el conjunto de protocolos TCP/IP.

Pero, ¿cómo funciona una arquitectura basada en niveles? Para explicarlo utilizaremos distintos gráficos que creemos que pueden ilustrar mejor la explicación.



En el gráfico anterior, podemos ver el esquema de una arquitectura de red de siete niveles. Podemos ver dos ordenadores que tendrán la arquitectura implementada, como tenemos siete niveles, cada nivel tendrá sus protocolos, por lo que podemos decir que las comunicaciones entre niveles iguales se hace a través de los protocolos correspondientes. Pero el flujo real de información, con los datos que queremos transmitir, irá de un ordenador a otro, pasando por cada uno de los niveles. Esto implica que en realidad los datos no se transfieren directamente de una capa a otra del mismo nivel, sino que cada capa pasa los datos y la información de control a la capa adyacente. De este modo, la información irá

a través de todas las capas, se transferirá al medio de transmisión adecuado y posteriormente ocurrirá lo mismo, pero en sentido inverso, en el otro ordenador. De esta forma, la información llegará a su destino y cada nivel sólo se ocupará de los datos y la información de control que necesite, según el protocolo utilizado, sin preocuparse de lo que hagan o necesiten los demás niveles.

Cabe mencionar que con esta forma de trabajar, cada capa tiene unos servicios asignados, además las capas son jerárquicas y cada una tiene unas funciones, de esta forma los niveles son independientes entre sí, aunque los datos necesarios se pasan de una a otra.

Para ello, las capas adyacentes disponen de lo que se denomina una interfaz. En este contexto, la interfaz definirá las operaciones y servicios que la capa inferior ofrece a la superior.

Cuando los diseñadores, proyectistas o fabricantes quieren hacer productos compatibles, deben seguir los estándares de arquitectura de red, para ello es importante definir interfaces claras entre niveles y que cada nivel tenga sus servicios bien definidos.

Todo ello implica que para el buen funcionamiento de la red deben respetarse ciertas reglas, como: que los servicios se definan mediante protocolos estándar, que cada nivel sólo se comunique con el nivel superior o inferior, y que cada nivel inferior preste servicios. a su nivel superior.

Cabe destacar que este tipo de arquitectura por niveles implica que cada nivel genera su propio conjunto de datos, ya que cada capa pasa los datos originales junto con la información que genera, con el fin de controlar la comunicación por niveles. Esta información para los niveles inferiores es tratada como si fueran datos, ya que sólo será utilizada por el nivel correspondiente del ordenador de destino. Más adelante veremos los diferentes nombres que tienen estos datos dependiendo de la arquitectura utilizada.

Por último, cabe destacar que las arquitecturas de red basadas en capas facilitan las compatibilidades, tanto de software como de hardware, así como futuras modificaciones, ya que no es necesario cambiar todas las capas cuando queremos mejorar el sistema. Bastaría con modificar los protocolos por niveles y podríamos conseguir mejoras en el sistema.

2.2 Comunicación protocolo.

Como hemos visto anteriormente, un protocolo de comunicaciones es un conjunto de reglas estandarizadas para la representación, señalización, autenticación y detección de errores necesarias para enviar información a través de un canal de comunicación.

Entre los protocolos necesarios para establecer la comunicación, necesitamos protocolos para:

- Identificar al remitente y al destinatario.
- Definir el medio o canal que puede utilizarse en la comunicación.
- Definir el lenguaje común que se utilizará.

- Definir la forma y la estructura de los mensajes.
- Ajusta la velocidad y el tiempo de los mensajes.
- Definir la codificación y encapsulación del mensaje.

Los protocolos utilizados en las redes se adaptan a las características del emisor, el receptor y el canal, además los protocolos deben definir los detalles de cómo transmitir y entregar un mensaje.

Si nos centramos en las redes de ordenadores, podemos definir algunas cuestiones que deben resolver los protocolos de red, estas cuestiones serán:

Enrutamiento: En las redes de ordenadores pueden existir diferentes rutas para llegar a un mismo destino, por lo que se debe elegir una de ellas, siendo deseable que siempre se elija la mejor o más rápida. Por ello, las arquitecturas de red deben disponer de protocolos que sirvan para este fin, vamos a ver cuales son y a que nivel se resuelve.

Direccionamiento: Como una red está formada por muchos nodos conectados entre sí, debe haber alguna forma de saber cuál es cuál. Para ello necesitamos definir direcciones de red que nos permitan determinar a qué ordenador quiero conectarme o dónde debo conectarme para llegar a un destino. Para ello, las arquitecturas de red definen protocolos de direccionamiento, desde un punto de vista lógico y físico, que se definen a niveles adecuados para que la comunicación sea posible y no se produzcan duplicaciones.

La necesidad de compartir un medio de comunicación: Puede darse el caso de que se comparta un mismo medio de transmisión, por lo que deben establecerse mecanismos para controlar el acceso al medio y el orden en que se accede a él.

Saturación: Los protocolos de cualquier nivel deben ser capaces de evitar que el receptor del mensaje, o los dispositivos intermedios que actúan en la transmisión del mismo, se saturen. Esto suele ser un problema, y no siempre es fácil de resolver, pero un buen diseño y la adaptación de la red a las necesidades ayudan.

Control de errores: Es deseable que los protocolos de red dispongan de mecanismos de control de errores. Como veremos cuando analicemos las arquitecturas de red, este control puede realizarse desde distintos puntos de vista y a distintos niveles.

Hemos mencionado algunas cuestiones, pero está claro que los protocolos resuelven muchas más, lo importante es tener en cuenta que gracias a unos protocolos estandarizados, y a un buen diseño de red, podemos conseguir que ordenadores de todo el mundo se comuniquen entre sí.

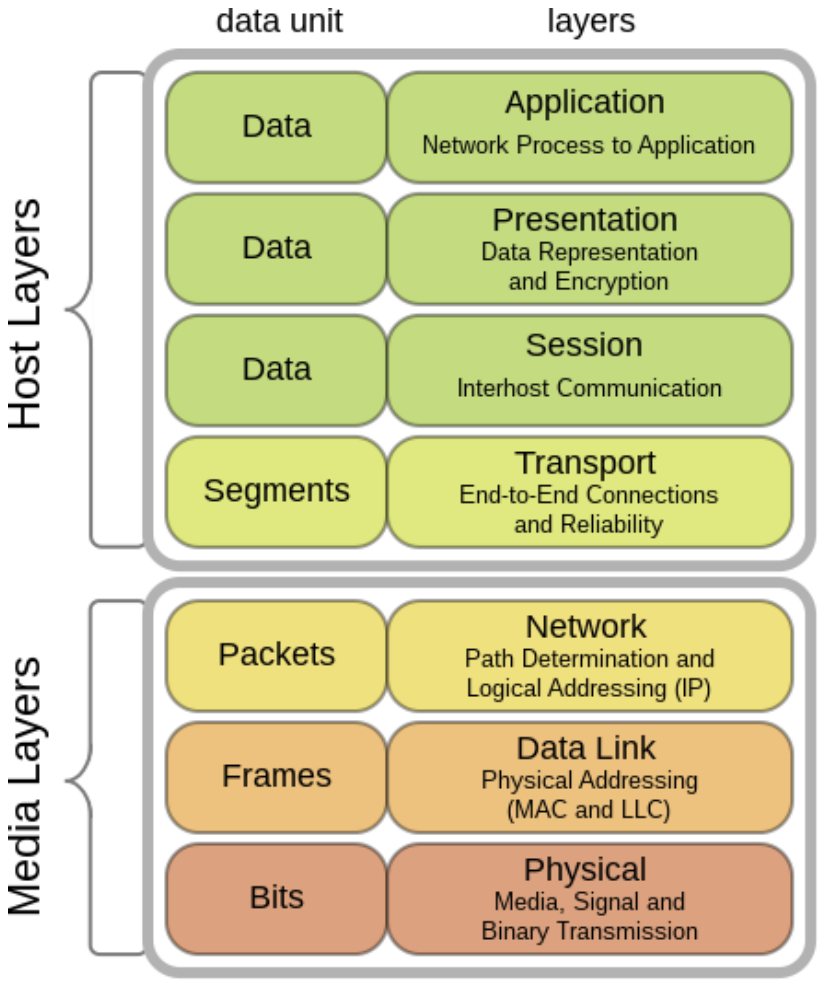
2.3 Funcionamiento de una arquitectura basada en niveles .

El modelo OSI, acrónimo en inglés de Open System Interconnection o traducido, Interconexión de Sistemas Abiertos, es el modelo de red creado por la Organización Internacional de Normalización (ISO) en 1984. Este modelo define un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicación. Cabe señalar que el modelo OSI simplifica

actividades de la red, ya que agrupa los procesos de comunicación en siete capas que realizan diferentes tareas. Es conveniente tener en cuenta que el modelo OSI no es una arquitectura desarrollada en cualquier sistema, sino una referencia para desarrollar arquitecturas de red, de forma que los protocolos que se desarrollen puedan ser conocidos por todos.

Aunque el modelo OSI no está realmente desarrollado en ningún sistema, es conveniente conocerlo y aplicarlo, ya que nos ayuda a entender los procesos de comunicación que ocurren en una red, y también puede utilizarse como referencia para realizar la detección de errores o un plan de mantenimiento.

La representación gráfica del modelo OSI suele hacerse en forma de pila, donde la capa de aplicación 7 estaría en la parte superior y la capa 1 o física en la inferior.



Es conveniente mencionar que en ocasiones se hace referencia a que las capas 1, 2 y 3 del modelo están relacionadas con el hardware y las capas 5, 6 y 7 con el software, siendo la capa 4 una capa intermedia entre el hardware y el software. . Esto suele ser así porque los dispositivos y componentes de red suelen trabajar en los niveles 1 a 3, siendo los programas los que trabajan en los niveles superiores.

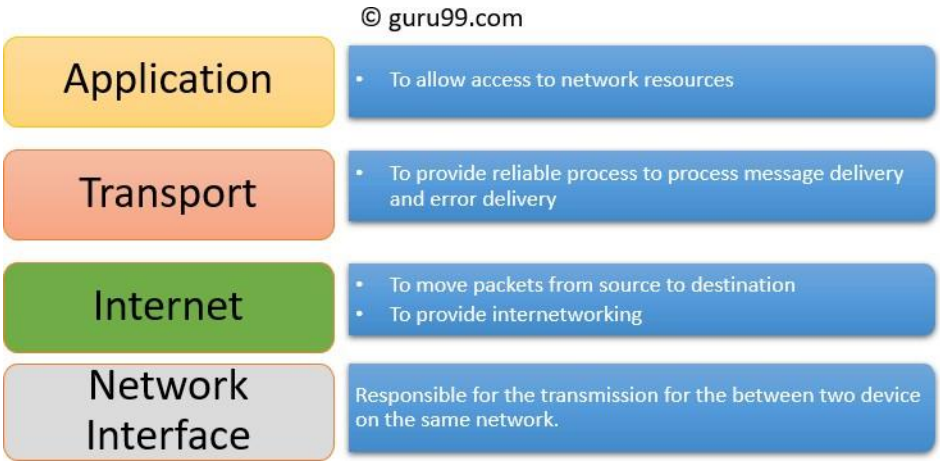
2.4 T CP/IP

Cuando se habla de protocolos TCP/IP, en realidad se hace referencia a la arquitectura de red que incluye varios protocolos de red, entre los cuales dos de los más destacados son el protocolo TCP (Transmission Control Protocol) y el protocolo IP (Internet Protocol).

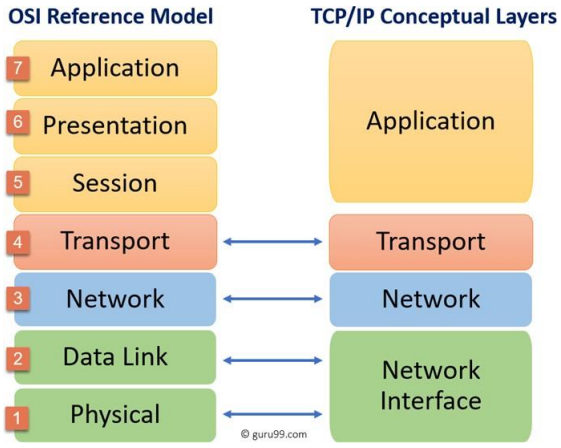
Por ello, sería conveniente considerar este modelo como una arquitectura en sí misma, por ser la más utilizada, ya que es la base de las comunicaciones por Internet y de los sistemas operativos modernos.

Cuando nos referimos a la arquitectura TCP/IP o al modelo TCP/IP, nos estamos refiriendo a un conjunto de reglas generales para el diseño y la implementación de protocolos de red que permiten la comunicación entre ordenadores. Como veremos con más detalle a lo largo de esta unidad, existen protocolos para distintos tipos de servicios de red.

La arquitectura TCP/IP se compone de cuatro capas o niveles que son:



Una comparación de esta arquitectura con el modelo OSI puede verse en el siguiente gráfico.



La arquitectura TCP/IP está estructurada en capas jerárquicas y se utiliza en Internet, por lo que en algunos casos oirá hablar de la familia de protocolos de Internet refiriéndose a esta arquitectura cuando trabaje en Internet.

Hay que recordar que, en algunos casos, la capa de acceso a la red se divide en una capa de hardware o física y una de enlace de datos, de modo que la arquitectura tendría cinco niveles en lugar de cuatro. Esto suele hacerse en referencia al modelo OSI. En realidad, esto puede hacerse y no cambiaría la estructura de la arquitectura.

2.5 El nivel de acceso a la red .

La arquitectura TCP/IP en su estandarización original no se preocupó demasiado del nivel físico en sí, de hecho, al principio sólo se preocupó de estandarizar los protocolos relacionados con el enlace de datos, de ahí el nombre de este nivel.

Posteriormente, con el auge de las redes de todo tipo, se vio que cada vez había que tener más en cuenta los estándares que ya existían desde el punto de vista físico, y por ello algunos autores, desarrolladores y diseñadores consideran que la arquitectura TCP /IP consta en realidad de cinco capas, siendo la primera la capa física o de hardware y la segunda la capa de enlace de datos, tal y como recomienda el modelo OSI.

Para nosotros es suficiente considerarlo como uno, tal y como se menciona en el RFC 1122, documento que define el modelo TCP/IP.

La función principal de este nivel es convertir la información proporcionada por el nivel de red en señales que puedan ser transmitidas por el medio físico. La función inversa es convertir las señales que llegan a través del medio físico en paquetes de información que puedan ser manejados por el nivel de red. En este nivel hay que tener en cuenta las cuestiones relacionadas con las conexiones físicas, que en las redes locales vienen definidas por la norma Ethernet. Esta norma define las características del cableado y la señalización de la capa física, así como los formatos de las tramas de datos de la capa de enlace de datos. Ethernet es la base de la norma IEEE 802.3, una norma internacional que puede utilizarse tanto en redes locales como de área extensa.

Otro aspecto importante de este nivel está relacionado con el direccionamiento físico. Este concepto proviene de lo que se considera una subcapa de la capa de enlace de datos, y se denomina control de acceso al medio, cuyas siglas en inglés, MAC, se utilizan para definir lo que se conoce como direcciones MAC.

La dirección MAC es un identificador de 48 bits, normalmente representado como números hexadecimales, en un formato de 6 bloques de dos números hexadecimales, divididos por dos puntos. El formato es el siguiente:

FF:FF:FF:FF:FF:FF

Los 24 bits más significativos (los de la izquierda) determinan el fabricante y se conocen como Identificador Único Organizativo, y los 24 bits menos significativos (los de la derecha) identifican una interfaz concreta. De este modo, ninguna tarjeta de red

tiene la misma dirección física.

En este nivel existe un protocolo relacionado con el direccionamiento físico. Este protocolo es ARP.

ARP son las siglas de Address Resolution Protocol (Protocolo de Resolución de Direcciones), este protocolo trabaja a nivel de enlace de datos y se encarga de encontrar la dirección física o MAC que está relacionada con la dirección lógica correspondiente, que, como veremos en el siguiente apartado, se corresponde con la dirección IP. Lo que hace ARP es traducir direcciones lógicas (IP) a direcciones físicas (MAC). Existe su inverso, RARP, que significa reverse address resolution protocol, hace la función inversa del protocolo ARP pero no es muy utilizado.

2.6 La capa de Internet o red .

La capa de red del modelo TCP/IP se considera la capa de arquitectura más importante, ya que permite a las estaciones enviar información a la red en forma de paquetes. Estos paquetes viajan por la red de forma independiente, pudiendo atravesar diferentes redes y sin un orden establecido. Esta es una de las principales ventajas de esta arquitectura y por eso es la base de Internet.

El objetivo principal de la capa de red será encaminar los paquetes desde el nodo de origen hasta el nodo de destino.

En la arquitectura TCP/IP, la capa de red es casi totalmente comparable a la capa de red del modelo OSI, pero en el caso de la arquitectura TCP/IP, la capa de red no se ocupa de las tareas de ordenar los paquetes cuando llegan. a su destino. Es lo que se conoce como servicio sin conexión. Cuando los paquetes se tratan de forma independiente, conteniendo cada uno la dirección de destino, se dice que se utiliza la técnica de datagramas, por lo que Internet es una red de conmutación de paquetes basada en datagramas.

Entre las funciones de la capa de red se encuentran:

- **Direccionamiento:** Permite la identificación única de cada nodo de la red. Cuando hablamos de direccionamiento a este nivel, hablamos de direccionamiento lógico, para distinguirlo del direccionamiento físico que ya hemos visto antes.
- **Conectividad**: Conseguir que los nodos de una red se conecten, independientemente de la red a la que pertenezcan.
- **Enrutamiento**: También llamado enrutamiento, los protocolos de esta capa deben ser capaces de encontrar el mejor camino entre dos nodos.
- **Control de congestión**: Es conveniente controlar el tráfico, ya que si un nodo recibe más información de la que puede procesar, se produce la saturación y este problema puede extenderse a toda la red.

Para realizar todas estas funciones, el nivel de red utiliza diferentes protocolos, entre los protocolos más destacados de este nivel tenemos:

- **IP**: Protocolo de Internet, o Protocolo de Internet proporciona enrutamiento sin conexión de paquetes y es utilizado tanto por el origen como por el destino para la comunicación de datos.
- **ARP y RARP**: También se utilizan en la capa de enlace de datos y sirven para relacionar direcciones IP con direcciones MAC y viceversa.
- **ICMP**: Internet Control Message Protocol, proporciona capacidades de envío y control de mensajes. También se considera un protocolo de capa de transporte, y herramientas como ping y tracert lo utilizan para funcionar.
- **OSPF**: Es un protocolo de enrutamiento que encuentra el camino más corto entre dos nodos de la red.
- **RIP**: Routing Information Protocol, al igual que OSPF, también busca el camino más corto, pero utilizando otras técnicas de enrutamiento.

Como se puede ver, este nivel tiene varias funciones y varios protocolos, pero podemos decir que el más importante de todos, de hecho, da nombre a la arquitectura, es el protocolo IP.

El protocolo IP, además de lo mencionado anteriormente, también proporciona direcciones IP. Una dirección IP es un número que identifica lógica y jerárquicamente una interfaz dentro de una red que utiliza el protocolo Internet. Más adelante aprenderás más sobre el direccionamiento IP, pero ahora es conveniente que sepas que existen dos versiones: IPv4 (IP versión 4) e IPv6 (IP versión 6). Se diferencian en el número de bits que utilizan, la versión 4 utiliza direcciones de 32 bits y la versión 6 utiliza direcciones de 128 bits.

Las direcciones IP de ejemplo son:

- IP versión 4: 192.168.1.11 (Utilizando valores decimales).
- Versión IP 6: 2001:0DB8:0000:0000:0000:0000:1428:57AB (Utilizando valores
  en hexadecimal y puede simplificarse como: 2001:0DB8::1428:57AB)

2.7 El nivel de transporte .

Cumple la función de establecer las reglas necesarias para establecer una conexión entre dos dispositivos remotos. Al igual que las capas anteriores, la información que maneja esta capa tiene nombre propio y se denomina segmento.

Por lo tanto, la capa de transporte debe encargarse de unir varios segmentos del mismo flujo de datos. Dado que la capa de red en la arquitectura TCP/IP no se ocupa del orden de los paquetes ni de los errores, es en esta capa donde deben cuidarse estos detalles.

El nivel de transporte de la arquitectura TCP/IP es totalmente comparable al nivel de transporte del modelo OSI, por lo tanto podemos decir que este nivel es responsable de la transferencia sin errores de datos entre el emisor y el receptor, aunque no estén conectados directamente, así como de mantener el flujo de la red. La tarea de esta capa es proporcionar un transporte de datos fiable

de la máquina de origen a la de destino, independientemente de las redes físicas.

Varios protocolos funcionan a este nivel, pero los dos más importantes son TCP y UDP.

TCP es un protocolo fiable, orientado a la conexión, diseñado específicamente para proporcionar un flujo fiable de bytes de extremo a extremo a través de redes poco fiables. Por eso es tan útil en Internet, ya que a diferencia del tráfico en una sola red donde conoceremos sus características, las redes que la componen pueden tener topologías, anchos de banda, retardos, tamaños de paquetes, etc. diferentes. Pero TCP tiene un diseño que se adapta dinámicamente a las propiedades de estas redes y permite la conexión en muchos tipos de situaciones.

UDP es un protocolo sin conexión y poco fiable, este protocolo proporciona todo lo necesario para que las aplicaciones envíen datagramas IP encapsulados sin tener una conexión establecida. Uno de sus usos es en la transmisión de audio y vídeo en tiempo real, donde no es posible realizar retransmisiones debido a los estrictos requisitos de retardo en estos casos.

Cuando un proceso de aplicación quiere establecer comunicación con otro proceso de aplicación remoto, debe especificar a cuál conectarse. El método que se utiliza normalmente es definir direcciones de transporte en las que los procesos pueden escuchar peticiones de conexión. Estos puntos finales se denominan puertos.

Por lo tanto, un puerto serán las direcciones de transporte en las que los procesos pueden escuchar las solicitudes de conexión. El término puerto se utiliza en Internet, el término genérico es Transport Service Access Point, cuyas siglas en inglés son TSAP.

Los números de puerto son utilizados por TCP y UDP para identificar las sesiones que establecen las diferentes aplicaciones. Algunos puertos son:

- **20**: Datos FTP (File Transfer Protocol).
- **21**: Control FTP.
- **53**: DNS (Servicio de Nombres de Dominio).
- **80**: http (Protocolo utilizado para servir y descargar páginas web)

2.8 La aplicación nivel.

El nivel de aplicación contiene los programas de usuario (aplicaciones) que permiten a nuestro ordenador crear textos, chatear, leer el correo, visitar páginas web, etc.

Este nivel incluye todos los programas la página utilizan alto nivel para comunicarse. protocolos que

En la arquitectura TCP/IP, este nivel incluye los niveles de sesión, presentación y aplicación del modelo OSI.

Algunos de los protocolos de la capa de aplicación son:

- **FTP**: Protocolo utilizado para transferir archivos entre un ordenador y otro.

- **DNS**: Domain Name Service, es el sistema utilizado en Internet para convertir los nombres de los nodos de red en direcciones de red.

- **SMTP**: Protocolo simple de transferencia de correo basado en texto que se utiliza para intercambiar mensajes de correo electrónico. Se basa en el concepto cliente-servidor, en el que un cliente envía un mensaje a uno o varios servidores.
- **POP**: Post Office Protocol, es utilizado por los clientes de correo para recuperar mensajes de correo almacenados en un servidor.
- **SNMP**: Protocolo de gestión de redes, permite supervisar y controlar los dispositivos de red y gestionar la configuración y la seguridad.
- **HTTP**: Hypertext Transfer Protocol, es el protocolo utilizado en las transacciones de páginas web. Define la sintaxis y la semántica utilizadas por los elementos de software de la arquitectura web (clientes, servidores, proxies) para comunicarse. Es un protocolo orientado a las transacciones y sigue el esquema petición-respuesta
  entre un cliente y un servidor. Tiene una versión segura que es HTTPS.

Una vez que conocemos los diferentes niveles de la arquitectura podemos definir el concepto de socket. Un socket es una conexión que está formada por la unión de la dirección IP más el puerto que se utiliza para la conexión. Como cada puerto está asociado a una aplicación, podemos decir que no habrá dos conexiones iguales en el mismo instante de tiempo. Ejemplo: 192.168.1.11:80, esto significa que el ordenador cuya dirección es 192.168.1.11 está utilizando el puerto 80, que está asociado a la capa de aplicación del protocolo http, por lo tanto esto puede significar que el ordenador está visitando una página web o sirviendo una página web. Este concepto seguramente te será útil más adelante cuando programes servicios web o aplicaciones que utilicen Internet.

3. TOPOLOGÍAS DE RED Y MODOS DE CONEXIÓN .

La topología de red se define como la cadena de comunicación que utilizan los nodos que componen una red para comunicarse. La topología puede referirse tanto al camino físico como al camino lógico. Normalmente utilizaremos la topología desde el punto de vista físico y, por tanto, la consideraremos como la forma en que se conectan los ordenadores de una red. Entre las topologías de conexión podemos citar: bus, anillo, estrella, árbol o jerárquica, malla, doble anillo, mixta y totalmente conectada. A la hora de realizar una instalación de red, es conveniente realizar un diagrama de red que muestre la ubicación de cada ordenador, de cada equipo de interconexión e incluso del cableado. Suele hacerse a partir de los planos del edificio o planta donde se ubica la red y es una herramienta útil a la hora de su mantenimiento y actualización.

La topología lógica o esquema lógico, nos muestra el uso de la red, el nombre de los ordenadores, las direcciones, las aplicaciones, etc. En estos esquemas se puede representar un grupo de ordenadores con un solo icono. En la próxima unidad utilizarás este tipo de esquemas.

Como ejemplo, te mostramos un gráfico que muestra una red de ordenadores que dispondrá de conexión a Internet gracias a un router. La red está representada por un óvalo con la dirección de red dentro y el nombre de la red fuera. Este tipo de esquemas lógicos pueden ser más o menos complejos pero

sirven para darnos

una idea de cómo está conectada una red. Existen programas que permiten realizar estos diagramas, pero pueden hacerse con cualquier programa de dibujo, siempre que queden claros todos los elementos que se representan en el gráfico.

Si tenemos en cuenta las topologías físicas, también pueden tener más o menos detalle en su representación, pero la idea fundamental es mostrar cómo están conectados los dispositivos desde un punto de vista físico, como analizaremos más adelante.

Otro concepto relacionado con la forma de conectar los ordenadores en una red es el de modo de conexión, este concepto está relacionado con las redes inalámbricas, representa la forma en que los ordenadores se pueden conectar a una red de forma inalámbrica. Se definen dos modos de conexión inalámbrica, que son:

- Modo infraestructura: Suele incluir un punto de acceso.
- Modo ad hoc: No requiere punto de acceso.

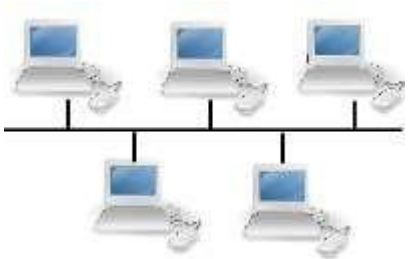
Un poco más adelante veremos más detalles sobre estos dos modos de conexión. Sólo comentar que estos modos de conexión se utilizan principalmente en el diseño de redes locales inalámbricas o redes Wi-Fi.

Es conveniente que sepas diferenciar las topologías y los modos de conexión, las primeras están más relacionadas con las conexiones físicas y el diseño, y las otras tienen relación con el diseño de redes inalámbricas.

3.1 Autobús y anillo

La topología de bus utiliza un único cable troncal con terminaciones en los extremos para que los ordenadores de la red se conecten directamente a la red troncal. Las primeras redes Ethernet utilizaban esta topología con cable coaxial.

Actualmente se utilizan variantes de la topología de bus en redes de televisión por cable, en la conexión troncal de redes de fibra óptica y en la instalación y funcionamiento de máquinas y equipos industriales utilizados en procesos de producción.



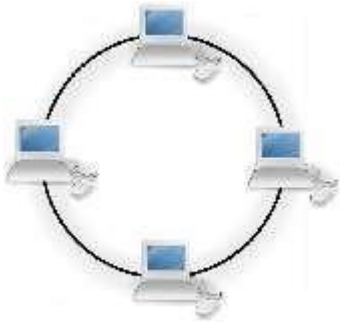
La topología en anillo conecta cada ordenador o nodo con el siguiente y el último con el primero, creando un anillo de conexión física. Cada estación tiene un receptor y un transmisor que actúa como repetidor, pasando la señal a la siguiente estación. En este tipo de red, la comunicación se da por el paso de un token, de esta forma se evitan posibles pérdidas de información por colisiones. Las redes locales Token-ring utilizan una topología en anillo aunque la conexión

física sea en estrella.

Existen topologías de doble anillo en las que dos anillos permiten el envío de datos en ambos

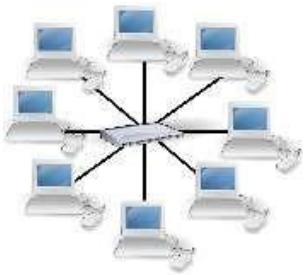
direcciones. Esta configuración crea redundancia (tolerancia a fallos).

Esta topología se utiliza en redes FDDI o Fiber Distributed Data Interface, en español Interfaz de Datos Distribuida por Fibra, que puede utilizarse como parte de una red troncal que distribuye datos por fibra óptica. En algunas configuraciones de servidores también se utiliza este tipo de topología.



3.2 S alquitrán

La topología en estrella conecta todos los ordenadores a un nodo central, que puede ser: un router, un switch o conmutador, o un hub o concentrador. Las redes de área local modernas basadas en la norma IEEE 802.3 utilizan esta topología.



El equipo central de interconexión canaliza toda la información y todos los paquetes de usuario pasan por él. Este nodo central realizará funciones de distribución, conmutación y control. Es importante que este nodo esté siempre activo, ya que si falla toda la red se quedará sin servicio.

Entre las ventajas de utilizar esta topología tenemos que esta topología es tolerante a fallos ya que si un ordenador se desconecta no perjudica a toda la red, también facilita la incorporación de nuevos ordenadores a la red siempre que el nodo central tenga conexiones, y permite evitar conflictos de uso.

Una extensión de la topología en estrella es la estrella extendida o árbol, en la que las redes en estrella se conectan entre sí.

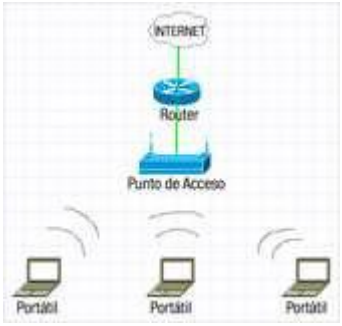
Cuando la estrella extendida tiene un elemento del que parte, hablaremos de topología en estrella jerárquica, donde a partir de redes conectadas en estrella obtenemos una red más amplia que mantiene una jerarquía de conexiones, ya que tenemos un nodo que es el inicio de la jerarquía. Este nodo suele ser un router y a partir de él se crea una red de área local que permite prestar servicios a redes de área local más pequeñas.

Este tipo de topología es muy típica en redes de área local donde el principio de la jerarquía será el router que se conecta a Internet, normalmente el proporcionado por la compañía de telecomunicaciones, y el resto son los switches que dan servicio a las diferentes aulas, salas de ordenadores, despachos, etc.

Esta topología tiene la ventaja de que desde una única conexión a Internet, por ejemplo, podemos dar servicio a varias redes locales o subredes, con el consiguiente ahorro de costes. Su principal inconveniente está precisamente en la jerarquía, si falla el equipo de interconexión de mayor jerarquía, la red deja de prestar los servicios para los que fue diseñada.

3.3 Modo infraestructura y modo ad-hoc .

Como hemos visto, existen varias formas de conectar ordenadores en una red que denominamos topologías. Estas topologías, en principio, servirían de base para cualquier tipo de red de área local, ya sea cableada o inalámbrica. Pero en las redes inalámbricas que siguen el estándar IEEE 802.11, se introduce un concepto diferente, que es el modo de conexión.



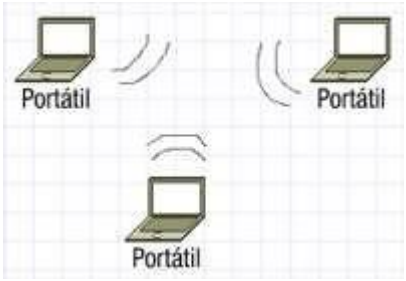
En las redes inalámbricas con el estándar IEEE 802.11, también llamadas redes Wi-Fi, se especifican dos modos de conexión, que son el modo infraestructura y el modo ad-hoc. Cabe mencionar que a veces se oye hablar de modo de conexión o topología de conexión para referirse a la forma de conectar los dispositivos inalámbricos, y de modo de funcionamiento para referirse al funcionamiento del equipo. En nuestro caso preferimos utilizar el término modo de conexión.

El modo infraestructura suele utilizarse para conectar equipos inalámbricos a un

red cableada existente, sus características principales es que utiliza un equipo de interconexión como puente entre la red inalámbrica y la red cableada. Este equipo de interconexión se denomina Punto de Acceso y puede ser un equipo especialmente diseñado para este fin que sólo realiza esta función, o puede ser un router con características de punto de acceso. Suele utilizarse como punto de acceso a la infraestructura de cable que permite la conexión a Internet, el router inalámbrico instalado por la compañía de telecomunicaciones.

En modo infraestructura, todo el tráfico de la red inalámbrica se canaliza a través del punto de acceso, y todos los dispositivos inalámbricos deben estar dentro del área de cobertura del punto de acceso para poder establecer comunicación entre ellos.

El modo ad-hoc permite conectar dispositivos inalámbricos entre sí, sin necesidad de utilizar ningún equipo como punto de acceso. De este modo, cada dispositivo de la red forma parte de una red entre iguales (Peer to Peer).



Este tipo de conexión permite compartir información entre ordenadores que se encuentran en un lugar determinado de forma puntual, por ejemplo una reunión, también se puede utilizar para conectar dispositivos de juego para jugar entre ellos.

Una tercera posibilidad es combinar ambos modos de conexión, para aprovechar las ventajas de ambos.

4. COMPONENTES DE UNA RED INFORMÁTICA .

En este punto repasaremos algunos de los componentes más importantes que conforman una red informática. Como ya hemos visto, una red informática, o red de ordenadores, es un conjunto de equipos informáticos conectados entre sí mediante dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio de transporte de datos, con el fin de compartir información y recursos y ofrecer servicios. Este término también engloba aquellos medios técnicos que permiten compartir información.

Por lo tanto, podemos considerar que los componentes de la red son los propios ordenadores con sus sistemas operativos que permiten utilizarlos, y todo el hardware y software que ayudan al funcionamiento de la red. En este punto nos centraremos en el hardware, ya que el software lo estudiarás en las siguientes unidades.

Algunos de estos componentes serán:

- **El cableado de red y sus conectores**, que permiten la transmisión de la

señal.

- **El rack o armario de conexiones** es un bastidor diseñado para alojar equipos electrónicos, informáticos y de comunicaciones.
- **El patch panel,** paneles de conexión que sirven como terminadores de cable y ayudan a organizarlo.
- **Las tarjetas de red**, que permitirán la conexión del ordenador, ya sea por cable o de forma inalámbrica.
- **Los conmutadores o switches,** que permiten la conexión de distintos ordenadores entre sí y de segmentos de red entre sí.
- **Routers o encaminadores,** también conocidos como encaminadores, que permiten conectar diferentes redes, como una red de área local con Internet.
- **Puntos de acceso,** que permiten la interconexión de dispositivos inalámbricos entre sí, y/o la conexión de dispositivos cableados con inalámbricos.
- **Cortafuegos,** que pueden ser dispositivos de hardware con software específico para bloquear el acceso no autorizado a la red, o software específico que se instala en ordenadores y/o servidores para impedir el acceso no autorizado.
- **Servidores,** que no son más que ordenadores con un sistema operativo específico para actuar como servidor, o con sistemas operativos no servidores pero con software de servidor.

Además de estos componentes, también consideramos parte de la red a los ordenadores que van a trabajar en ella, que en muchos casos se denominan estaciones de trabajo. Cualquier dispositivo que pueda conectarse a la red para prestar un servicio, como impresoras, discos duros de red o cualquier periférico que se conecte a un ordenador de la red, también es un componente de la red y suele denominarse nodos. grid.

Antes de desarrollar cualquiera de los conceptos explicados, cabe mencionar que entre los servidores de red que darán servicio a la red, podemos encontrar: servidores de ficheros, servidores de correo, servidores de páginas web, servidores de impresión, etc.

4.1 Clasificación de los medios de transmisión .

El medio de transmisión constituye el canal que permite la transmisión de información entre dos terminales de un sistema de transmisión. Por lo tanto, en las redes informáticas serán los canales que transmiten información entre los nodos de la red, ya sean ordenadores, servidores, etc. Las transmisiones suelen realizarse mediante ondas electromagnéticas que se propagan a través del canal.

Unas veces el canal es un medio físico y otras no, ya que las ondas electromagnéticas son susceptibles de ser transmitidas a través del vacío. Por ello podemos clasificar los medios de transmisión en:

- **Medios guiados:** conducen las ondas electromagnéticas a través de una trayectoria física.
- **Medios no guiados:** proporcionan un soporte para las ondas que se

transmiten, pero no las directas.

Por lo tanto, cuando hablamos de medios guiados, nos referimos a los diferentes

tipos de cables que se pueden utilizar. Entre los tipos de cables más utilizados se encuentran los de par trenzado, los coaxiales y los de fibra óptica. Más adelante daremos más detalles sobre ellos.

Cuando hablamos de medios no guiados, nos referimos a la posibilidad de transmitir ondas electromagnéticas, a través del aire o del vacío. Esta particularidad permite crear redes inalámbricas y disponer de sistemas de telecomunicaciones sin cables, como teléfonos móviles o conexiones a Internet a través de teléfonos móviles.

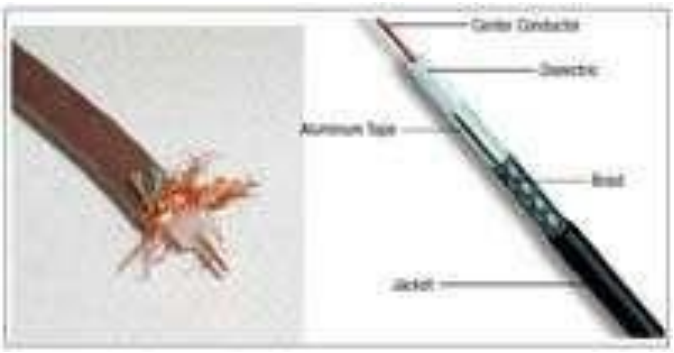
Cableado y conectores.

En este punto vamos a hacer un resumen de los tipos de cables más utilizados en la conexión de redes informáticas y los conectores más utilizados.

El cable más utilizado en redes de área local es el par trenzado de ocho hilos. Consta de ocho hilos de distintos colores y se utiliza en redes informáticas según la norma IEEE 802.3 (Ethernet).

Los colores son: blanco-naranja, naranja, blanco-verde, verde, blanco-azul, azul, blanco-marrón y marrón. La distribución de estos colores cuando se conecta al conector está estandarizada, para que las conexiones de red sean fácilmente reconocibles.

El conector utilizado con este cableado es el RJ-45, que tiene un macho y una hembra.



El cable coaxial también se utiliza en redes informáticas. Este cable está compuesto por un hilo conductor, llamado núcleo, y una malla externa separados por un dieléctrico o aislante.

Los conectores que se suelen utilizar son el BNC y el tipo N. Dentro del cable coaxial existen diferentes estándares, dependiendo de su uso. Actualmente el cable coaxial no se utiliza para montar redes informáticas, sino para la distribución de señales de televisión, Internet por cable, etc.

En la distribución de la señal de Internet por cable, el cable coaxial se utiliza para conectar el centro de distribución de Internet que llega hasta la calle o el barrio con la casa del abonado. En este caso, se suele utilizar cable de tipo RG6, que permite distintas configuraciones para incluir conexiones telefónicas y transmisión de datos.

4.2 Cableado estructurado .

La infraestructura de telecomunicaciones necesaria para conectar un edificio o un grupo de edificios se denomina cableado estructurado. Esta infraestructura incluye

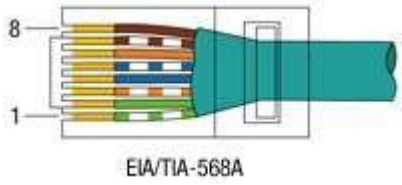
cables y tubos, regletas, armarios, dispositivos, espacios específicos, etc. El cableado estructurado define algunos subsistemas para organizar la instalación del cableado. Los subsistemas de cableado estructurado son:

- Cableado del campus o interconexión de edificios.
- Entrada del edificio, punto donde se conectan los cables exteriores con los interiores.
- Sala de equipos, sala donde se distribuyen todas las conexiones del edificio.
- Cableado troncal o backbone, cableado de distribución vertical entre plantas.
- Armarios de distribución, donde confluyen los cables y se montan los equipos de control.
- interconexión, utilizando bastidores y paneles de conexión.
- Cableado horizontal, cableado de planta.
- Área de trabajo.

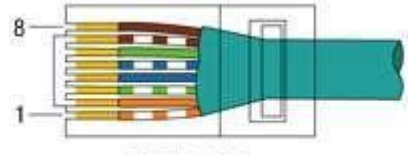
Existen normas de cableado estructurado que especifican cómo organizar la instalación de cableado. Estas normas especifican el tipo de cable, los conectores, las longitudes máximas de los tramos, la organización de los elementos de interconexión, la ubicación de los dispositivos, etc. Por ejemplo, en el cableado horizontal se recomienda un máximo de 100 metros desde el armario de distribución o rack hasta la zona de trabajo.

Otra norma a tener en cuenta es la ANSI/EIA/TIA 568 A y B, que entre otras cosas define la distribución de colores en la conexión del cable de par trenzado con los conectores RJ-45. Las distribuciones 568 A y B son:

Conexiones 568A y 568B		
Pin	568-A	568-B
1	blanco-verde	blanco-naranja
2	verde	naranja
3	blanco-naranja	blanco-verde
4	azul	azul
5	blanco-azul	blanco-azul
6	naranja	verde
7	blanco-marrón	blanco-marrón
8	marrón	marrón



EIA/TIA-568A



EIA/TIA-568B

En las conexiones de red utilizaremos cables directos, lo que significa que los dos extremos tendrán el mismo estándar. Se recomienda utilizar el 568B. En caso de querer hacer un cable cruzado utilizaremos el estándar 568A en un extremo y

el estándar 568B en el otro. Los cables cruzados se utilizan para conectar dos

equipos del mismo tipo, por ejemplo, de ordenador a ordenador.

4.3 Interconexión elementos.

Cuando hablamos de elementos de interconexión, nos referimos a todos los elementos que permiten conectar equipos en una red. Normalmente nos referiremos a los elementos de interconexión de una red de área local, aunque los elementos de interconexión pueden pertenecer a cualquier tipo de red.

Una forma de clasificar los equipos de interconexión es teniendo en cuenta el nivel al que trabajan tomando como referencia el modelo OSI. Por ello vamos a realizar una clasificación tomando este modelo como referencia.

A nivel físico tenemos:

- Tarjetas de red: pueden ser cableadas o inalámbricas. Las tarjetas de red permiten a los ordenadores conectarse a la red.
- Concentradores también conocidos como hubs: permiten distribuir la señal a distintos ordenadores sin discriminar entre ellos.
- Repetidores: pueden ser locales o remotos, y su función es repetir la señal para regenerarla y/o amplificarla.

A nivel de enlace de datos tenemos:

- Conmutadores o switch: se encargan de conectar segmentos de red, y ordenadores entre sí, pero de forma más eficiente que un hub, ya que sólo envía la información al ordenador que la necesita.
- Puentes o bridges: conectan subredes, transmitiendo tráfico no local generado de una a otra.
- Puntos de acceso: pueden considerarse elementos de nivel de enlace de datos, se encargan de conectar los elementos inalámbricos entre sí y permiten el acceso de dispositivos inalámbricos a redes cableadas.

A nivel de red:

- Router o encaminador: se encarga de conectar diferentes redes. Su principal uso es en la conexión a Internet, ya que permite que las redes de área local se conecten a Internet. Se basa en el uso del protocolo IP, por lo que necesita que se le asignen al menos dos direcciones IP, una para Internet y otra para la red local.
  uno para la red local. También se encarga de los protocolos de enrutamiento y control de red. Puede ofrecer servicio inalámbrico y, por tanto, proporcionar servicio de punto de acceso.

En niveles superiores:

- Pasarelas: Los equipos de interconexión que trabajan en niveles superiores del modelo OSI suelen denominarse pasarelas. Existen diferentes tipos de pasarelas, podemos tener las que se encargan de conectar redes con diferentes tecnologías, las que facilitan el control de acceso a una
  red, los que controlan el acceso no autorizado. En función de su

función, también pueden ser servidores, cortafuegos, etc.

Hay que tener en cuenta que un equipo que trabaja a un nivel suele ser capaz de dar servicio a los niveles inferiores, un ejemplo muy conocido es el caso del router. Unrouter trabaja a nivel de red, pero puede actuar como switch ya que lleva incorporadas varias conexiones RJ-45 y da servicio a varios ordenadores, y en el caso de ser inalámbrico, puede actuar como punto de acceso para que los ordenadores inalámbricos tengan conexión a Internet a través suyo.

4.4 Tarjetas de red y direccionamiento MAC .

Ya hemos explicado algo sobre las tarjetas de red, ahora explicaremos algunas de sus características más importantes.

Una tarjeta de red o adaptador de red permite la comunicación con dispositivos conectados entre sí y también permite compartir recursos entre dos o más ordenadores. Las tarjetas de red también se denominan NIC del inglés network interface card o en español tarjeta de interfaz de red.

Su función principal es permitir la conexión del ordenador a la red, para ello se graban en la tarjeta los protocolos necesarios. Todas las tarjetas de red tienen grabada la dirección MAC correspondiente. Como ya hemos visto, la dirección MAC está formada por 48 bits y permite identificar la tarjeta a nivel de enlace de datos. Esta dirección se conoce como dirección física y es única.

Las tarjetas de red pueden conectarse al ordenador mediante uno de los buses internos, como el PCI, utilizando el bus USB externo, o estar integradas en la placa.

La tarjeta debe determinar la velocidad de transmisión, la cantidad de información a transmitir, qué protocolos utilizar y todos los parámetros físicos de la transmisión. Una vez hecho esto, debe transformar la información que llega a través de la conexión con el ordenador, para poder ser transmitida, lo hace convirtiendo la información en una secuencia serie de bits, convenientemente codificados, para formar una señal eléctrica adecuada. al medio de transmisión.

La mayoría de las tarjetas tienen los mismos componentes, destacamos:

- El procesador principal.
- Transceptor que es el dispositivo encargado de acceder al medio.
- Un conector wake on LAN que permite al ordenador arrancar desde otro ordenador de la red.
- Indicadores de estado para saber si estás conectado y si estás enviando o recibiendo datos.
- Dependiendo de si la tarjeta es para redes cableadas o inalámbricas, tendremos una conexión RJ-45 hembra o una conexión de antena, ya sea interna o externa.

La instalación y configuración de la tarjeta dependerá del sistema operativo, pero en general, necesitaremos que tenga una dirección IP configurada, una máscara de red configurada y una puerta de enlace definida. Puedes practicar esto en el

siguientes unidades del módulo.

Gracias a la relación que se establece entre la dirección IP MAC de la tarjeta y la dirección que se le asigna, se puede identificar un ordenador en la red

4.5 S brujas.

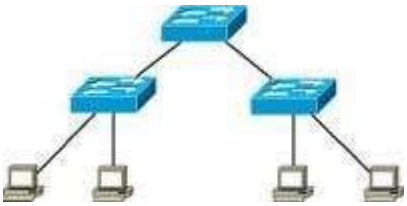
El conmutador o switch es un elemento de interconexión que funciona a nivel de capa 2 o enlace de datos, permitiendo conectar dos o más segmentos de red. El conmutador nos permite conectar diferentes ordenadores para que puedan conectarse entre sí, y que tengan acceso a otros segmentos de la red. El switch funciona almacenando las direcciones MAC de los ordenadores que están conectados a él y de los dispositivos que hay en cada segmento. Gracias a ello, es capaz de conectar un ordenador con otro de forma eficiente, sin necesidad de enviar la información a toda la red.

Esta característica es la que lo convierte en el elemento central de conexión en las redes de área local con topología en estrella.

Utilizar un conmutador tiene algunas ventajas, como conseguir altas velocidades de conexión y permitir múltiples transmisiones simultáneas, de modo que se pueden conectar más de dos ordenadores al mismo tiempo.

El inconveniente de utilizar conmutadores es que sólo pueden conectar redes con la misma topología, aunque pueden funcionar a distintas velocidades.

Un ejemplo de conexión de segmentos puede verse en la siguiente imagen.



Existen conmutadores de capa 3 o layer 3, que tienen las ventajas de los switches en cuanto a velocidad y además pueden elegir la mejor ruta entre distintos dispositivos. Una de las aplicaciones más importantes de los conmutadores de capa 3 es la posibilidad de definir redes de área local virtuales, o VLAN. Las VLAN son redes lógicamente independientes dentro de una misma red física.

4.6 R outers.

El router o encaminador es el equipo de interconexión de redes que se encarga de conectar dos redes diferentes.

Es un equipo de interconexión de capa 3 o nivel de red. Los routers dirigen el tráfico de red, buscando el mejor camino para llegar al destino. Trabajan con paquetes que contienen la información de las direcciones IP de origen y destino, así como los propios datos del mensaje.

Dada la popularidad del nombre en inglés, utilizaremos indistintamente router, encaminador o enrutador, para que le resulte más fácil familiarizarse con el término.

Hay que tener en cuenta que cada puerto o interfaz del router estará conectado a una red diferente, por lo que todos los routers deben tener al menos dos direcciones IP ya que pertenecerán al menos a dos redes diferentes. Hay que tener en cuenta que un router, además de las funciones de conexión de diferentes redes y funciones de enrutamiento, es capaz de filtrar, transferir direcciones, enlazar y actuar como switch. Para llevar a cabo sus funciones, un router necesita almacenar información sobre las redes a las que puede acceder, esto se hace a través de la tabla de enrutamiento, que no es más que una tabla donde se almacena cómo llegar de una red a otra, utilizando qué Interfaz.

Los algoritmos de enrutamiento que se utilizan permiten trabajar con rutas estáticas y con rutas dinámicas. Hablamos de rutas estáticas cuando el router mantiene la información de forma permanente y sin cambiar las rutas que pueden seguir los paquetes. Las rutas estáticas son útiles cuando sólo hay una forma de conectarse a Internet ya que el paquete seguirá siempre el mismo camino. Las rutas dinámicas serán útiles cuando tengamos varias posibilidades de conectarnos a otra red, en este caso es conveniente que el router pueda recoger información de la red para elegir el mejor camino posible.

Los routers necesitan ser configurados para funcionar correctamente, en la configuración se suelen definir las direcciones IP de cada una de las interfaces, se incluye información sobre las máscaras de subred, se especifica si se va a utilizar una pasarela, qué servidores DNS se van a utilizar, si se va a proporcionar el servicio de asignación de direcciones IP mediante DHCP, etc. En algunos casos es posible configurar qué puertos van a estar abiertos, y en el caso de los routers inalámbricos las características de configuración de las redes inalámbricas, que veremos un poco más adelante.

La mayoría de las veces utilizaremos un router para conectarnos a Internet, ya sea por ADSL o por cable. En estos casos, los routers suelen estar configurados por los proveedores de servicios de Internet, y no tendremos que configurar mucho, estos routers se llaman routers ADSL o routers por cable.

En algunas ocasiones oirás hablar de un router neutro, se trata de una terminología utilizada para diferenciar el router que une dos redes locales del que te permite conectarte a Internet.

Normalmente, cuando utilizas un router como parte de tu red doméstica o de trabajo, este será el que te permita conectarte a Internet, por lo tanto en la configuración del ordenador, tendrás que poner la dirección del router como puerta de enlace, ya que a esta puerta de enlace enviará el ordenador todos los paquetes que no sean propios de la red y por lo tanto será la "puerta" para salir a Internet. En estos casos, los routers utilizan el NAT o traducción de direcciones de red

mecanismo que permite intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles. Verás estos conceptos y la configuración de los parámetros necesarios en el sistema operativo en sucesivas unidades de trabajo.

4.7 IDS

En las redes informáticas hemos visto que podemos tener diferentes dispositivos para hacerlas funcionar. Además de los equipos de interconexión, podemos tener servidores que realizan diferentes funciones, como hemos comentado anteriormente. Pues bien, todos estos equipos necesitan mantener medidas de seguridad, para evitar que usuarios no autorizados puedan hacer uso de la red u obtener información no autorizada.

En mayor o menor medida, todos los equipos aplican medidas de seguridad más o menos complejas, pero existe la posibilidad de implantar un sistema de detección de intrusos que cumpla estas premisas de seguridad.

Esto es precisamente lo que hace IDS, ya que IDS son las siglas de Intrusion Detection System o Sistema de Detección de Intrusiones, que podemos definir como una aplicación utilizada para detectar accesos no autorizados a un ordenador o red.

Suele haber dos tipos de IDS:

- N-IDS: que se encargan de detectar los accesos no autorizados a la red.
- H-IDS: que se encargan de detectar el acceso no autorizado a ordenadores o hosts.

Los N-IDS necesitan un hardware exclusivo, ya que deben ser capaces de analizar todo el tráfico de la red. Una solución es integrar el N-IDS en el cortafuegos, de esta forma el IDS se encarga de detectar posibles accesos no autorizados y el cortafuegos de impedir el acceso.

H-IDS puede integrarse en el propio sistema del ordenador, y también combinarse con los cortafuegos instalados en cada equipo.

Es importante establecer las diferencias entre IDS y cortafuegos, ya que no son lo mismo. El IDS detecta intrusiones pero no las evita, y el cortafuegos limita el tráfico para evitar intrusiones pero no las detecta, de ahí que la combinación de ambos sea una buena opción para una red.

Este concepto de detección/prevención es el que inspira una tendencia más actual que es la de los llamados IPS. Un IPS es un Sistema de Prevención de Intrusiones, en este caso no sólo se detecta la intrusión sino que se impide el acceso a la misma. Existen soluciones de software y/o hardware del tipo IDS e IPS.