REDES DE ORDENADORES

ÌNDICE

REDES DE ORDENADORES

El término red hace referencia a un conjunto de sistemas informáticos independientes conectados entre sí, de tal forma que posibilitan un intercambio de datos, para lo que es necesario tanto la conexión física como la conexión lógica de los sistemas. Esta última se establece por medio de unos protocolos de red especiales, como es el caso de TCP (Transmission Control Protocol). Dos ordenadores conectados entre sí ya pueden considerarse una red.

VENTAJAS DE LAS REDES INFORMÁTICAS

Rapidez

La primera de las ventajas de las redes informáticas es que proporcionan mucha rapidez a la hora del intercambio y transferencia de archivos. Sin una red informática, los archivos son guardados en memorias o discos, y más tarde hay que enviar los mismos a otra división, lo cual se traduce en un proceso muy largo.

Coste

En cuanto a equipamiento físico de la red sí que tenemos un coste del mismo, en función de la tecnología usada.

Por otra parte, la instalación de software de red en su dispositivo no es costosa y tenemos la seguridad de que durará mucho tiempo y no es necesario cambiar el software cada cierto tiempo la mayoría de las ocasiones no será necesario hacerlo.

Seguridad de la información

Nos referimos al conjunto de ***medidas preventivas y reactivas*** que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de dato. Ejemplos de ello pueden ser: evitar que se realicen copias ilegales de programas, crear contraseñas para los directorios que elijamos para restringir el acceso solo a aquellos usuarios que autoricemos, etc.

Software de administración centralizada

Desde un único equipo podemos llevar y mantener la administración de la red; ésta es una de las mayores ventajas que nos encontramos en una red. Por ejemplo, en las actualizaciones de aplicaciones, el software se puede descargar a un ordenador (servidor de archivos) y distribuirlo, eliminando la necesidad de tiempo y energía ir equipo por equipo a equipo y rastrear donde hemos aplicado la misma y donde no.

Compartir recursos

Muchas empresas no pueden pagar suficientes impresoras, plotters, etc, para cada ordenador. Sin embargo, si los ordenadores se añaden a una red, varios usuarios pueden compartirlos.

Trabajo en equipo

El ***software*** colaborativo permite que varios usuarios trabajen en un documento o proyecto al mismo tiempo. La instalación de redes informáticas permite conectar equipos de modo que puedan compartir documentos, trabajar en diseños o enviarse correos electrónicos entre ellos para finalizar proyectos.

Productividad

Las redes informáticas permiten que los trabajadores sean más productivos con su tiempo debido a que tienen acceso instantáneo a casi cualquier forma de información.

Correo electrónico

Una red informática proporciona el hardware necesario para instalar un sistema de correo electrónico, el cual ayuda todo el personal ya que es un medio que facilita la difusión de información general.

Transferencia de grandes cantidades de información en poco tiempo

Compartición de una única conexión a Internet

Esta es una de las grandes ventajas de las redes informáticas que hace que merezca la pena la inversión en hardware (cables y otros equipos), que nos permite operar con una sola conexión. Es una configuración que le da a sus defensas digitales otra capa de seguridad porque canaliza todo el tráfico en un único punto.

TIPOS DE REDES DE ORDENADORES

Las redes se configuran con el objetivo de transmitir datos de un sistema a otro o de disponer recursos en común, como servidores, bases de datos o impresoras. En función del tamaño y del alcance de la red de ordenadores, se puede establecer una diferenciación entre diversas dimensiones de red. Entre los tipos de redes más importantes se encuentran:

- *Personal Area Networks (PAN) o red de área personal*
- *Local Area Networks (LAN) o red de área local*
- *Metropolitan Area Networks (MAN) o red de área metropolitana*
- *Wide Area Networks (WAN) o red de área amplia*
- *Global Area Networks (GAN) o red de área global*

Cada uno de los diferentes tipos de redes está diseñado para ámbitos de aplicación particulares, se basan en técnicas y estándares propios y plantean ventajas y restricciones variadas

Personal Area Network (PAN)

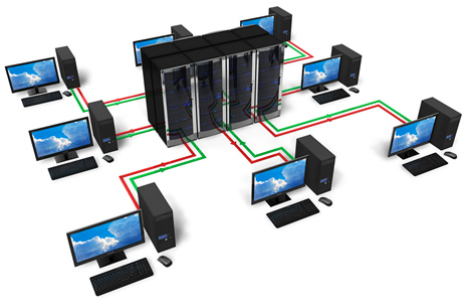
Para llevar a cabo un intercambio de datos, los terminales modernos como smartphones, tablets, ordenadores portátiles o equipos de escritorio permiten asociarse ad hoc a una red. Esto puede realizarse por cable y adoptar la forma de una Personal Area Network (PAN) o red de área personal, aunque las técnicas de transmisión más habituales son la memoria USB o el conector FireWire. La variante inalámbrica Wireless Personal Area Network (WPAN) se basa en técnicas como Bluetooth, Wireless USB, Insteon, IrDA, ZigBee o Z-Wave. Una Personal Area Network inalámbrica que se lleva a cabo vía Bluetooth recibe el nombre de Piconet. El ámbito de acción de las redes PAN y WPAN se limita normalmente a unos pocos metros y, por lo tanto, no son aptas para establecer la conexión con dispositivos que se encuentran en habitaciones o edificios diferentes.

Además de establecer la comunicación entre cada uno de los dispositivos entre sí, las redes de área personal (Personal Area Networks) permiten, asimismo, la conexión con otras redes de mayor tamaño. En este caso se puede hablar de un uplink o de un enlace o conexión de subida. Debido al alcance limitado y a una tasa de transmisión de datos relativamente baja, las PAN se utilizan principalmente para conectar periféricos en el ámbito del ocio y de los hobbies. Algunos ejemplos típicos son los auriculares inalámbricos, las videoconsolas y las cámaras digitales. En

el marco del Internet of Things (IoT), las redes WPAN se utilizan para la comunicación de las aplicaciones de control y monitorización con una frecuencia de transferencia baja. A este respecto, los protocolos como Insteon, Z-Wave y ZigBee han sido diseñados especialmente para la domótica y para la automatización del hogar.

Local Area Network (LAN)

Si una red está formada por más de un ordenador, esta recibe el nombre de Local Area Network (LAN). Una red local de tales características puede incluir a dos ordenadores en una vivienda privada o a varios miles de dispositivos en una empresa. Asimismo, las redes en instituciones públicas como administraciones, colegios o universidades también son redes LAN. Un estándar muy frecuente para redes de área local por cable es Ethernet. Otras opciones menos comunes y algo obsoletas son las tecnologías de red ARCNET, FDDI y Token Ring. La transmisión de datos tiene lugar o bien de manera electrónica a través de cables de cobre o mediante fibra óptica de vidrio.



Si se conectan más de dos ordenadores en una red LAN, se necesitan otros componentes de red como ***hubs*** (dispositivo que se emplea para concentrar el cableado de una red y ampliarla), ***bridges*** (dispositivo que interconecta segmentos de red haciendo la transferencia de datos de una red hacia otra con base en la dirección física de destino de cada paquete) y ***switches*** (dispositivo que conecta varias computadoras, impresoras y servidores para crear una red de servicios compartidos dentro de una oficina o edificio; actúa como un controlador que permite que diferentes dispositivos compartan información entre sí), es decir, ***concentradores, puentes de red y conmutadores***, los cuales funcionan como elementos de acoplamiento y nodos de distribución.

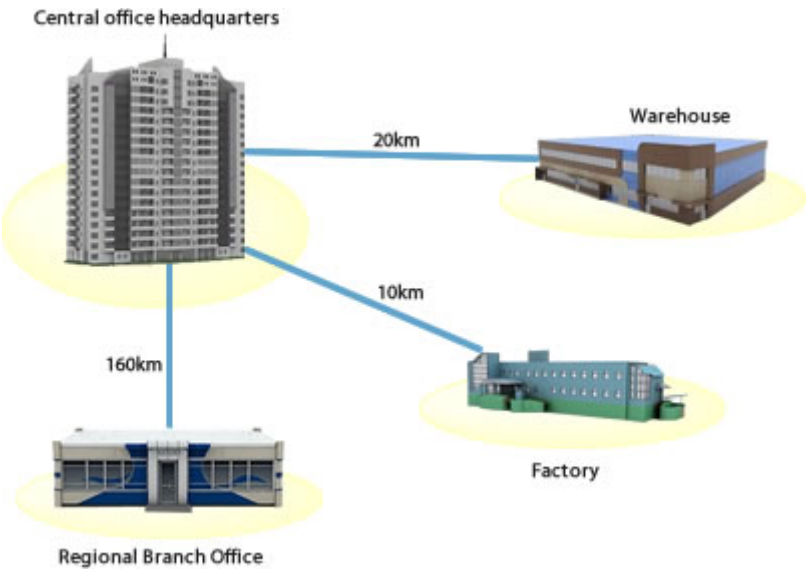
El tipo de red conocido como LAN o red de área local fue desarrollado para posibilitar la rápida transmisión de cantidades de datos más grandes. En función de la estructura de la red y del medio de transmisión utilizado se puede hablar de un rendimiento de 10 a 1.000 Mbit/s. Asimismo, las redes LAN permiten un intercambio de información cómodo entre los diversos dispositivos conectados a la red. Por ello, en el entorno empresarial es habitual que varios equipos de trabajo puedan acceder a servidores de archivos comunes, a impresoras de red o a aplicaciones por medio de la red LAN.

Si la red local tiene lugar de manera inalámbrica, se puede hablar en este caso de una Wireless Local Area Network (WLAN) o red de área local inalámbrica y los fundamentos básicos de los estándares de la red WLAN quedan definidos por la familia de normas IEEE 802.11. Las redes locales inalámbricas ofrecen la posibilidad de integrar terminales cómodamente en una red doméstica o empresarial y son compatibles con redes LAN Ethernet, aunque el rendimiento es, en este caso, algo menor que el de una conexión Ethernet.

El alcance de una Local Area Network depende tanto del estándar usado como del medio de transmisión y aumenta a través de un amplificador de señal que recibe el nombre de repetidor (repeater). En el caso de la ampliación Gigabit Ethernet por medio de fibra de vidrio, se puede llegar a un alcance de señal de varios kilómetros. No resulta muy habitual, sin embargo, que las Local Area Networks estén formadas por más de una estructura. El grupo de redes LAN geográficamente cercanas puede asociarse a una Metropolitan Area Network (MAN) o Wide Area Network (WAN) superiores.

Metropolitan Area Network (MAN)

La Metropolitan Area Network (MAN) o red de área metropolitana es una red de telecomunicaciones de banda ancha que comunica varias redes LAN en una zona geográficamente cercana. Por lo general, se trata de cada una de las sedes de una empresa que se agrupan en una MAN por medio de líneas arrendadas. Para ello, entran en acción routers de alto rendimiento basados en fibra de vidrio, los cuales permiten un rendimiento mayor al de Internet y la velocidad de transmisión entre dos puntos de unión distantes es comparable a la comunicación que tiene lugar en una red LAN.



El estándar para redes inalámbricas regionales de mayor envergadura, es decir, las denominadas Wireless Metropolitan Area Networks (WMAN), fue desarrollado con IEEE 802.16. Esta tecnología de WiMAX (Worldwide Interoperability for Microwave Access) permite crear las llamadas redes WLAN hotzones, que consisten en varios puntos de acceso WLAN interconectados en diferentes localizaciones. Las redes WMAN se utilizan para ofrecer a los

usuarios una potente conexión a Internet en aquellas regiones que carecen de infraestructura para ello, y es que el DSL, el estándar habitual de transmisión, solo está disponible técnicamente donde hay hilos de cobre.

Wide Area Network (WAN)

Mientras que las redes Metropolitan Area Networks comunican puntos que se encuentran cerca unos de los otros en regiones rurales o en zonas de aglomeraciones urbanas, las Wide Area Networks (WAN) o redes de área amplia se extienden por zonas geográficas como países o continentes. El número de redes locales o terminales individuales que forman parte de una WAN es, en principio, ilimitado.

Mientras que las redes LAN y las MAN pueden establecerse a causa de la cercanía geográfica del ordenador o red que se tiene que conectar en base a Ethernet, en el caso de las Wide Area Networks entran en juego técnicas como IP/MPLS (Multiprotocol Label Switching), PDH (Plesiochronous Digital Hierarchy), SDH (Synchronous Digital Hierarchy), SONET (Synchronous Optical Network), ATM (Asynchronous Transfer Mode) y, rara vez, el estándar obsoleto X.25.

En la mayoría de los casos, las Wide Area Networks suelen pertenecer a una organización determinada o a una empresa y se gestionan o alquilan de manera privada. Los proveedores de servicios de Internet también hacen uso de este tipo de redes para conectar las redes corporativas locales y a los consumidores a Internet.

Global Area Network (GAN)

Una red global como Internet recibe el nombre de Global Area Network (GAN), sin embargo, no es la única red de ordenadores de esta índole. Las empresas que también son activas a nivel internacional mantienen redes aisladas que comprenden varias redes WAN y que logran, así, la comunicación entre los ordenadores de las empresas a nivel mundial. Las redes GAN utilizan la infraestructura de fibra de vidrio de las redes de área amplia (Wide Area Networks) y las agrupan mediante cables submarinos internacionales o transmisión por satélite.

Virtual Private Network (VPN)

Una red privada virtual (VPN) es una red de comunicación virtual que utiliza la infraestructura de una red física para asociar sistemas informáticos de manera lógica. En este sentido, se puede tratar de todos los tipos de redes expuestos anteriormente. Lo más común es utilizar Internet como medio de transporte, ya que este permite establecer la conexión entre todos los ordenadores a nivel mundial y, al contrario de lo que ocurre con las redes MAN o WAN privadas, está disponible de forma gratuita. La transferencia de datos tiene lugar dentro de un túnel virtual erigido entre un cliente VPN y un servidor VPN.

Si se utiliza la red pública como medio de transporte, las Virtual Private Networks o redes privadas virtuales suelen cifrarse para garantizar la confidencialidad de los datos. Las VPN se emplean para conectar redes LAN en Internet o para hacer posible el acceso remoto a una red o a un único ordenador a través de la conexión pública.

FUNCIONES DE REDES DE ORDENADORES

Según la función de la red, podemos clasificarlas en:

Peer to Peer

Es un tipo de conexión con una arquitectura destinada a la comunicación entre aplicaciones. Esto permite a las personas o a los ordenadores compartir información y archivos de uno a otro sin necesidad de intermediarios.

Entre las ventajas tenemos:

- Sistema operativo; se puede utilizar cualquier sistema operativo, ya sea Windows, Linux o Mac
- Asequible de usar: configurar una red de igual a igual es más asequible para las empresas ya que no tienen que pagar los cargos ni el pago mensual de la licencia, tampoco requieren un servidor dedicado para las necesidades de su hogar.
- No se requiere un servidor dedicado.
- No hay nada más técnico que configurar. Sólo manejo del trabajo general del mismo.
- Escalable según la necesidad.

- Seguridad para los datos de la empresa: muchos otros sistemas de redes brindan seguridad al almacenamiento de datos en ellos. Pero cuando se trata de la red peer-to-peer, es más segura entre ellos. Por eso, si un nodo o dispositivo está fuera de línea o no funciona, otros dispositivos seguirán funcionando. Por lo tanto, es una de las fantásticas ventajas de las redes peer-to-peer que gusta a la mayoría de los usuarios.

Entre las desventajas tenemos:

- Sin almacenamiento centralizado: no hay ningún lugar central o dedicado para almacenar todos los datos o información esenciales. Y los archivos se almacenan en diferentes máquinas. Por tanto, una sola persona no puede tener el control adecuado sobre la accesibilidad de la información. Por lo tanto, puede presentar varios desafíos para navegar por el archivo de manera eficiente. El usuario puede tener que perder mucho tiempo.
- Un ataque de virus puede provocarlo: como cada computadora es independiente cuando se trata de almacenar datos, estos dispositivos son más propensos a verse afectados por virus o ataques de malware.
- Rendimiento lento: la cantidad de dispositivos conectados puede ralentizar el proceso. En términos simples, si aumenta la cantidad de dispositivos conectados, disminuye el rendimiento de los datos de navegación.
- Problemas en el acceso remoto: si la red contiene un tipo de código no seguro u otro código, puede ocurrir un acceso remoto no autorizado. Y en ese caso, el usuario no autorizado puede acceder a datos sensibles o información de la empresa. Por lo tanto, el usuario de la red P2P puede tener que comprometerse con esta limitación. Por lo tanto, el usuario debe asegurarse de hacer frente a este tipo de situaciones antes de implementar la red peer-to-peer.

Cliente Servidor

La arquitectura cliente servidor tiene dos partes claramente diferenciadas, por un lado la parte del servidor y por otro la parte de cliente o grupo de clientes donde lo habitual es que un servidor sea una máquina bastante potente con un hardware y software específico que actúa de depósito de datos y funcione como un sistema gestor de base de datos o aplicaciones.

En esta arquitectura el cliente suele ser estaciones de trabajo que solicitan varios servicios al servidor, mientras que un servidor es una máquina que actúa como depósito de datos y funciona como un sistema gestor de base de datos, este se encarga de dar la respuesta demandada por el cliente.

El más claro ejemplo de uso de una arquitectura cliente servidor es la red de Internet donde existen ordenadores de diferentes personas conectadas alrededor del mundo, las cuales se conectan a través de los servidores de su proveedor de Internet por ISP donde son redirigidos a los servidores de las páginas que desean visualizar y de esta manera la información de los servicios requeridos viajan a través de Internet dando respuesta a la solicitud demandada.

Las principales ventajas que ofrece son:

- Administración centrada en el servidor. Los clientes tienen poca trascendencia en el esquema y sus necesidades de administración son menores.
- Centralización de los recursos. Los recursos comunes a todos los usuarios se administran en el servidor. Así se evitan situaciones como la redundancia o inconsistencia de información en las bases de datos.
- Mejora de la seguridad. Al disponer de un mecanismo central de autenticación, las posibilidades de acceso indebido se reducen considerablemente.
- Escalabilidad de la instalación. Se pueden añadir o suprimir clientes sin que el funcionamiento de la red se vea afectado.

Las desventajas que tenemos en este modelo son:

- Coste elevado. Tanto la instalación como el mantenimiento son más elevados debido al perfil muy técnico del lado servidor.
- Dependencia del servidor. Toda la red está construida al rededor del servidor y si éste deja de funcionar o lo hace con un rendimiento inadecuado, afectará a toda la infraestructura.

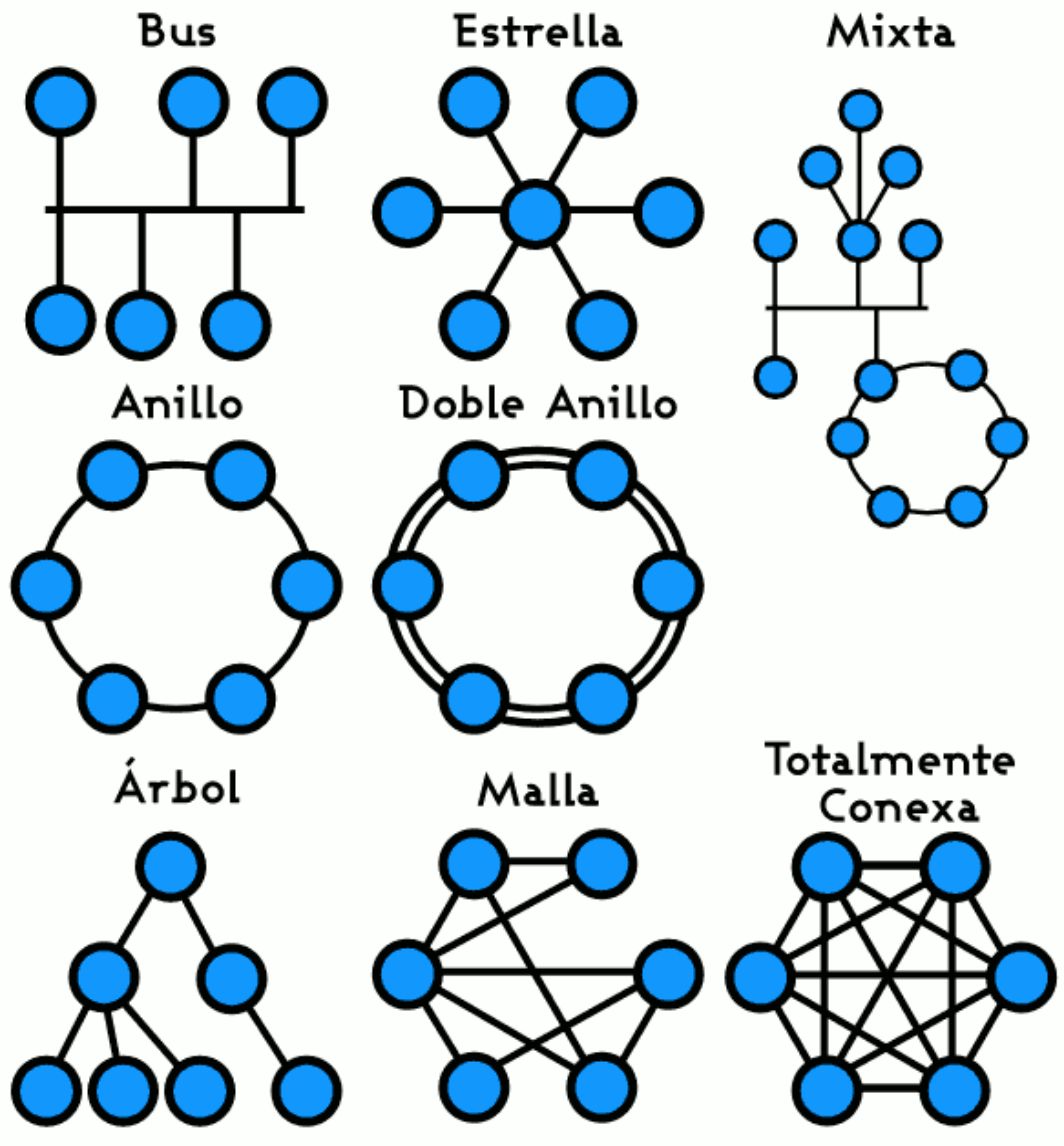
Este último inconveniente lo podemos superar gracias a sistemas como los servidores redundantes, la tolerancia a fallos y los sistemas de almacenamiento en modo RAID.

FORMA DE CONEXIÓN DE REDES DE ORDENADORES

En este caso estamos hablando de la topología de la red, que se define como un mapa físico o lógico de una red para intercambiar datos. En otras palabras, es la forma en que está diseñada la red, sea en el plano físico o lógico.

Entre ellas tenemos:

- Bus.
- Estrella.
- Malla.
- Anillo
- Doble Anillo.
- Árbol.
- Malla.
- Totalmente conexa.



CONEXIÓN REDES ORDENADORES

La conexión física en la que se basan estos tipos de redes puede presentarse por medio de ***cables*** o llevarse a cabo con ***tecnología inalámbrica***.

A menudo, las redes físicas conforman la base para varias redes de comunicación lógicas, las llamadas Virtual Private Networks (VPN). Para la transmisión de datos, estas emplean un medio de transmisión físico común como puede ser la fibra óptica y se vinculan de forma lógica a diferentes tipos de redes virtuales por medio de un software de tunelización

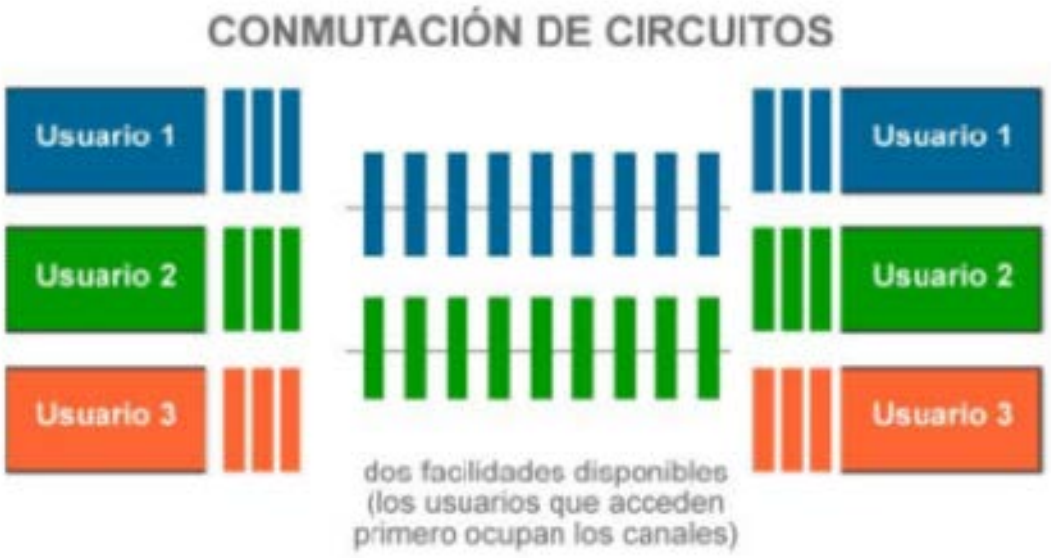
GRADO DE DIFUSIÓN DE LAS REDES DE ORDENADORES

Intranet: Una Intranet es una plataforma digital cuyo objetivo es asistir a los trabajadores en la generación de valor para la empresa, poniendo a su disposición activos como contenidos, archivos, procesos de negocio y herramientas; facilitando la colaboración y comunicación entre las personas y los equipos.

Internet: es un neologismo del inglés que significa red informática descentralizada de alcance global. Se trata de un sistema de redes interconectadas mediante distintos protocolos que ofrece una gran diversidad de servicios y recursos, como, por ejemplo, el acceso a archivos de hipertexto a través de la web

TÉCNICAS DE FUNCIONAMIENTO DE REDES WAN

Conmutación de circuitos: La conmutación de circuitos es un tipo de conexión que realizan los diferentes nodos de una red para lograr un camino apropiado para conectar dos usuarios de una red de telecomunicaciones.



La conmutación de circuitos ocupa una facilidad de manera constante durante todo el tiempo en el que se produce una llamada. Esto quiere decir que el subscriptor con una llamada en curso es el " dueño " de la línea y no puede ser interrumpido, o sea que el ancho de banda empleado está completamente dedicado al usuario. Si el servicio es solicitado por otros abonados, ellos deben usar otras facilidades o esperar a que se desocupen las que está en uso.

Conmutación de mensajes: La conmutación de mensajes es una técnica de conmutación de red en la que los datos se enrutan en su totalidad desde el nodo de origen al nodo de destino, una esperanza a la vez. Durante el enrutamiento de mensajes, cada conmutador intermedio de la red almacena el mensaje completo. Si los recursos de toda la red están ocupados o la red se bloquea, la red de conmutación de mensajes almacena y retrasa el mensaje hasta que haya suficientes recursos disponibles para la transmisión efectiva del mensaje.

En la conmutación de mensajes, los nodos de origen y destino no están conectados directamente. En cambio, los nodos intermediarios (principalmente conmutadores) son responsables de transferir el mensaje de un nodo al siguiente. Por lo tanto, cada nodo intermediario dentro de la red necesita almacenar cada mensaje antes de retransferir los mensajes uno por uno a medida que los recursos adecuados estén disponibles. Si los recursos no están disponibles, los mensajes se almacenan indefinidamente. Esta característica se conoce como almacenar y reenviar.

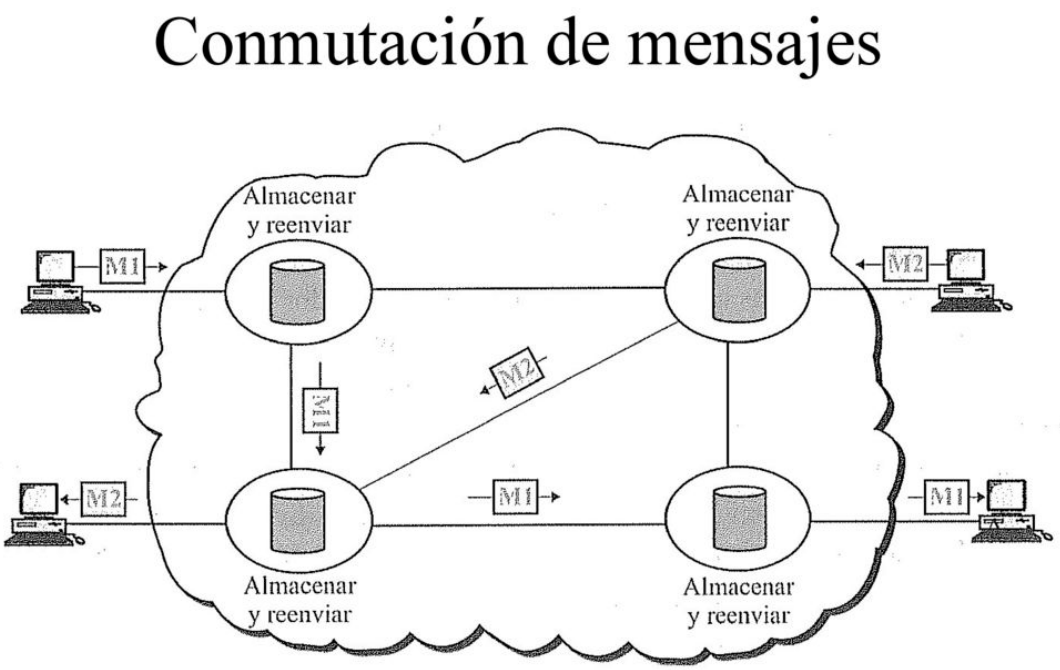
Cada mensaje debe incluir un encabezado, que generalmente consiste en información de enrutamiento, como el origen y el destino, la hora de vencimiento, el nivel de prioridad, etc.

Debido a que la conmutación de mensajes implementa la técnica de almacenamiento y reenvío, utiliza la red de manera eficiente. Además, no hay límite de tamaño para los mensajes. Sin embargo, esta técnica también tiene varias desventajas:

Debido a que los mensajes están completamente empaquetados y guardados indefinidamente en cada nodo intermedio, los nodos exigen una capacidad de almacenamiento sustancial.

Las redes de conmutación de mensajes son muy lentas ya que el procesamiento tiene lugar en todos y cada uno de los nodos, lo que puede resultar en un rendimiento deficiente.

Esta técnica no es adecuada para procesos interactivos y en tiempo real, como juegos multimedia y comunicación por voz.



Conmutación de paquetes: La conmutación de paquetes es un método de agrupar los datos transmitidos a través de una red digital en paquetes. Los datos en el encabezado son utilizados por el hardware de red para dirigir el paquete a su destino donde la carga útil es extraída y utilizada por el software de la aplicación.

La conmutación de paquetes es una tecnología que divide los datos en las comunicaciones de red en pequeñas partes manejables, llamadas paquetes. Al enviar un archivo grande en varios fragmentos pequeños a través de una red, la conmutación de paquetes minimiza el impacto de los errores de transmisión de datos. También se evitan los cuellos de botella de tráfico, lo que permite que los datos fluyan de la manera más eficiente posible a través de la red.

La idea de las comunicaciones de red implica seguir un conjunto exacto de reglas para mover los datos de una ubicación, o nodo, en la red a otra. Internet es simplemente una gran red y la conmutación de paquetes se produce cuando se mueven todos los datos a través de Internet. El Protocolo de control de transporte / Protocolo de Internet (TCP / IP) y Frame Relay son ejemplos de protocolos de conmutación de paquetes. Algunas tecnologías de telefonía móvil también utilizan este tipo de tecnología.

Cuando se emplea la conmutación de paquetes, el software de enrutamiento de red divide el archivo en varios paquetes pequeños de datos de entre 1,000 y 1,500 bytes cada uno, etiquetando cada paquete con información de encabezado. En el encabezado, el software de enrutamiento incluye instrucciones para volver a ensamblar el archivo de los paquetes en el orden correcto. También incluye la información de destino, antes de enviar los paquetes a través de la red.

A medida que los paquetes viajan a través de la red, es posible que se separen, tomando diferentes rutas de enrutamiento, según el tráfico de Internet. Los enrutadores y conmutadores de la red utilizan la información del encabezado para determinar la ruta más eficiente para mover cada paquete a su destino. La conmutación de paquetes permite un uso eficiente del ancho de banda de la red, ya que el envío de numerosos paquetes pequeños se adapta mejor a la capacidad de la red que el envío de archivos grandes intactos.

Una vez que los paquetes llegan al destino, independientemente del orden en el que llegan, el software de enrutamiento vuelve a ensamblar el archivo correctamente, utilizando la información del encabezado. Si todos los paquetes llegaron intactos y sin errores, el archivo está listo para usarse. Sin embargo, si un paquete llegó con un error, el software de enrutamiento puede solicitar que se vuelva a enviar el paquete. Al utilizar esta tecnología, solo se debe reenviar una parte de todo el archivo, lo que reduce el tráfico general de la red.

La Arquitectura de Red

La arquitectura de red es el diseño de una red de comunicaciones. Es un marco para la especificación de los componentes físicos de una red y de su organización funcional y configuración, sus procedimientos y principios operacionales, así como los protocolos de comunicación utilizados en su funcionamiento.

¿Qué es el modelo OSI?

El Open Systems Interconnection Model, conocido como modelo OSI por su abreviatura, fue creado por la Organización Internacional para la Normalización (ISO) como modelo de referencia para el establecimiento de una comunicación abierta en diferentes sistemas técnicos. Para entenderlo mejor, es necesario transportarse a los comienzos de la era de Internet: a finales de los años 70, los fabricantes más destacados en el ámbito de la tecnología de redes tuvieron que hacer frente al problema de que sus dispositivos solo podían conectarse a través de una arquitectura de red privada. Por aquel entonces, ningún fabricante pensó en crear componentes de software y hardware siguiendo las especificaciones de otros fabricantes y un proyecto como Internet presupone, en cambio, ciertos estándares que posibiliten la comunicación.

El protocolo OSI es el resultado de un intento de normalización y, como marco conceptual, ofrece los fundamentos de diseño para normas de comunicación no privativas. Para ello, el modelo de ISO OSI divide el complicado proceso de la comunicación en red en siete estadios denominados capas OSI. En la comunicación entre dos sistemas, cada capa requiere que se lleven a cabo ciertas tareas específicas. Entre ellas se encuentran, por ejemplo, el control de la comunicación, la direccionalidad del sistema de destino o la traducción de paquetes de datos a señales físicas. Sin embargo, el método solo funciona cuando todos los sistemas participantes en la comunicación cumplen las reglas. Estas se establecen en los llamados protocolos, que se aplican a cada una de las capas o que se utilizan en la totalidad de las mismas.

El modelo de referencia ISO no es propiamente un estándar de red concreto, sino que, en términos abstractos, describe cuáles son los procesos que se han de llevar a cabo para que la comunicación funcione a través de una red.

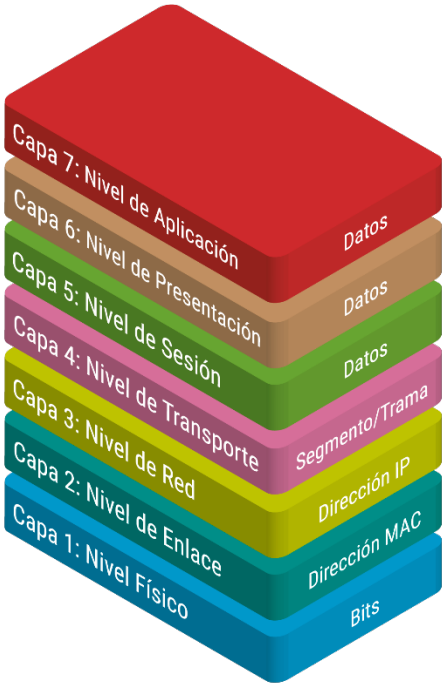
Las capas OSI

A los usuarios puede parecerles que la comunicación entre dos ordenadores es algo trivial. Y, sin embargo, en lo que concierne a la transmisión de datos en una red, tienen que llevarse a cabo numerosas tareas y cumplirse determinados requisitos en cuanto a fiabilidad, seguridad e integridad, lo que ha puesto de manifiesto la necesidad de dividir la comunicación en red por capas. Cada una de ellas está orientada a una tarea diferente, por lo que los estándares solo cubren una parte del modelo de capas. Este tiene una estructura jerárquica, es decir, que cada capa tiene acceso a una inferior por medio de una interfaz y la pone a disposición para las capas que están por encima de ella. Este principio tiene dos ventajas esenciales:

a) Las tareas y requisitos que han de realizarse y cumplirse están claramente definidos.
b) Los estándares para cada capa pueden desarrollarse de manera independiente.

Debido a que cada una de las capas está delimitada con independencia de las otras, los cambios realizados en las normas de una de ellas no influyen en los procesos que se están desarrollando en las otras capas, lo que facilita la introducción de nuevas normas.

En función de sus tareas, las siete capas del modelo ISO pueden subdividirse en dos grupos: capas orientadas a aplicaciones y capas orientadas al transporte. Los procesos que tienen lugar en cada una de las capas pueden visualizarse en el ejemplo de la transmisión por correo electrónico desde un terminal a un servidor de correo:



Capas orientadas a aplicaciones

Las capas superiores del protocolo OSI se denominan capas orientadas a aplicaciones. En este sentido, se establece una diferenciación entre capa de aplicación, capa de presentación y capa de sesión.

> ***Capa 7*** - ***Capa de aplicación*** (application layer): este es el nivel del modelo OSI que está en contacto directo con aplicaciones como programas de correo electrónico o navegadores web y en ella se produce la entrada y salida de datos. Esta capa establece la conexión para los otros niveles y prepara las funciones para las aplicaciones. Este proceso se puede explicar mediante el ejemplo de la transmisión por correo electrónico: un usuario escribe un mensaje en el programa de correo electrónico en su terminal y la capa de aplicación lo acepta en forma de paquete de datos. A los datos del correo electrónico se le adjuntan datos adicionales en forma de encabezado de la aplicación: a esto se le llama también “encapsulamiento”. Este encabezado indica, entre otras cosas, que los datos proceden de un programa de correo electrónico. Aquí también se define el protocolo que se usa en la transmisión del correo electrónico en la capa de aplicación (normalmente el protocolo SMTP).
>
> ***Capa 6*** - ***Capa de presentación*** (presentation layer): una de las tareas esenciales de la comunicación en red es garantizar el envío de datos en formatos estándar. En la capa

de presentación, los datos se transportan localmente en formato estandarizados. En el caso de la transmisión de un correo electrónico, en esta capa se define el modo en que se tiene que presentar el mensaje. Para ello, el paquete de datos se completa para que se cree un encabezado de presentación que contiene los datos acerca de cómo se ha codificado el correo (en España se utiliza normalmente ISO 8859-1 (Latin1) o ISO 8859-15), en qué formato se presentan los archivos adjuntos (p. ej., JPEG o MPEG4) o cómo se han comprimido o cifrado los datos (p. ej., SSL/TLS). De esta manera se puede asegurar que el sistema de destino también ha entendido el formato del correo electrónico y que el mensaje se va a enviar.

Capa 5 – Capa de sesión (session layer): esta capa tiene la misión de organizar la conexión entre ambos sistemas finales, por lo que también recibe el nombre de capa de comunicación. En ella se incluyen los mecanismos especiales de gestión y control que regulan el establecimiento de la conexión, su mantenimiento y su interrupción. Para controlar la comunicación se necesitan unos datos adicionales que se deben añadir a los datos del correo electrónico transmitidos a través del encabezado de la sesión. La mayoría de los protocolos de aplicación actuales como SMTP o FTP se ocupan ellos mismos de las sesiones o, como HTTP, son protocolos sin estado. El modelo TCP/IP, en calidad de competidor del modelo OSI, agrupa las capas OSI 5, 6 o 7 en una capa de aplicación. NetBIOS, Socks y RPC son otras de las especificaciones que recoge la capa 5.

Capas de transporte

A las tres capas del protocolo OSI para las aplicaciones se suman cuatro capas de transporte y en ellas se puede distinguir entre la capa de transporte, la capa de red, la capa de vínculo de datos y la capa física.

Capa 4 – Capa de transporte (transport layer): la capa de transporte opera como vínculo entre las capas de aplicaciones y las orientadas al transporte. En este nivel del modelo OSI se lleva a cabo la conexión lógica de extremo a extremo (el canal de transmisión) entre los sistemas en la comunicación. Para ello, también se tiene que añadir cierta información en los datos del correo electrónico. El paquete de datos que ya se amplió para el encabezado de las capas orientadas a las aplicaciones se complementa en la capa 4 con un encabezado de transporte. En ello entran en juego protocolos de red estandarizados como TCP o UDP (User Datagram Protocol). Además, en la capa de transporte también se definen los puertos a través de los cuales las aplicaciones pueden dirigirse al sistema de destino. Asimismo, en la capa 4 también tiene lugar la asignación de un determinado paquete de datos a una aplicación.

Capa 3 – Capa de red (network layer): con la capa de mediación la transferencia de datos llega a Internet. Aquí se realiza el direccionamiento lógico del equipo terminal, al que se le asigna una dirección IP. Al paquete de datos, como los datos del correo

electrónico del ejemplo, se le añadirá un encabezado de red en el estadio 3 del modelo OSI, que contiene información sobre la asignación de rutas y el control del flujo de datos. Aquí, los sistemas informáticos recurren a normas de Internet como IP, ICMP, X.25, RIP u OSPF. En lo relativo al tráfico de correo electrónico, se suele utilizar más TCP que IP.

Capa 2 – Capa de vínculo de datos (data link layer): en la capa de seguridad, las funciones como reconocimiento de errores, eliminación de errores y control del flujo de datos se encargan de evitar que se produzcan errores de comunicación. El paquete de datos se sitúa, junto a los encabezados de aplicación, presentación, sesión, transporte y red, en el marco del encabezado de enlace de datos y de la trama de enlace de datos. Además, en la capa 2 tiene lugar el direccionamiento de hardware y, asimismo, entran en acción las direcciones MAC. El acceso al medio está regulado por protocolos como Ethernet o PPP.

Capa 1 – Capa física (physical layer): en la capa física se efectúa la transformación de los bits de un paquete de datos en una señal física adecuada para un medio de transmisión. Solo esta puede transferirse a través de un medio como hilo de cobre, fibra de vidrio o aire. La interfaz para el medio de transmisión se define por medio de protocolos o normas como DSL, ISDN, Bluetooth, USB (capa física) o Ethernet (capa física).

Encapsulado y desencapsulado

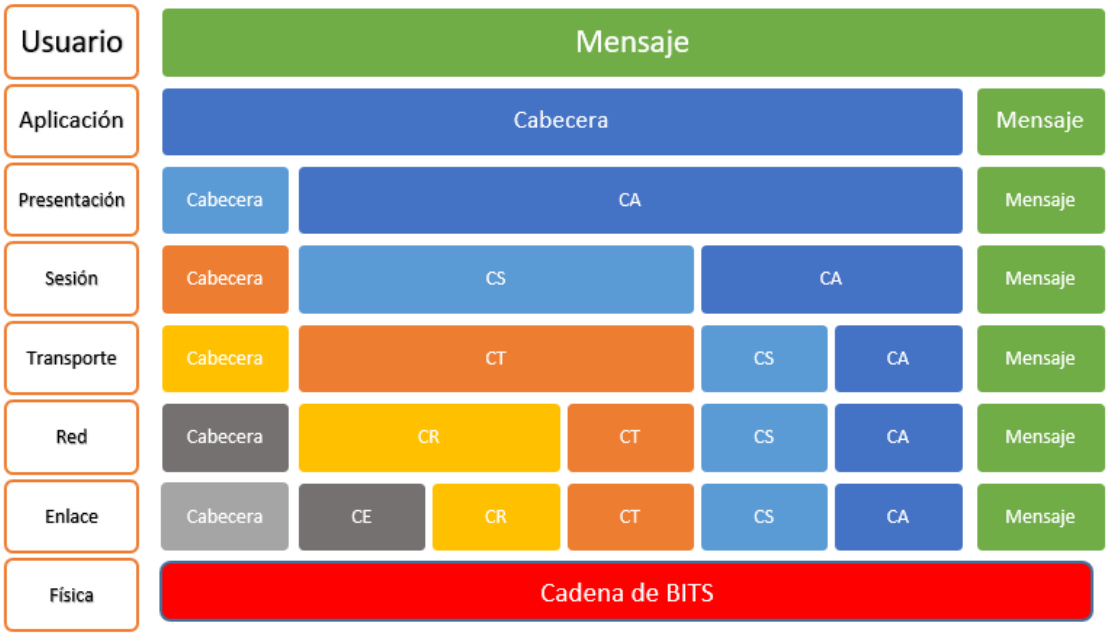
Los paquetes de datos no solo recorren cada capa del modelo OSI, sino también el sistema del remitente y el sistema de destino. Cualquier otro dispositivo por el que deba pasar un paquete de datos forma parte de las capas 1 y 3. El correo electrónico del ejemplo pasa por el router como señal física antes de avanzar por Internet. Esta se establece en la capa 3 del protocolo OSI y solo procesa información de las tres primeras capas, sin tener en cuenta las capas que van desde la 4 a la 7. Para poder acceder a datos importantes, el router tiene que descomprimir (“desencapsular”) el paquete de datos encapsulado y, en este proceso, se recorren las diferentes capas OSI en orden inverso.

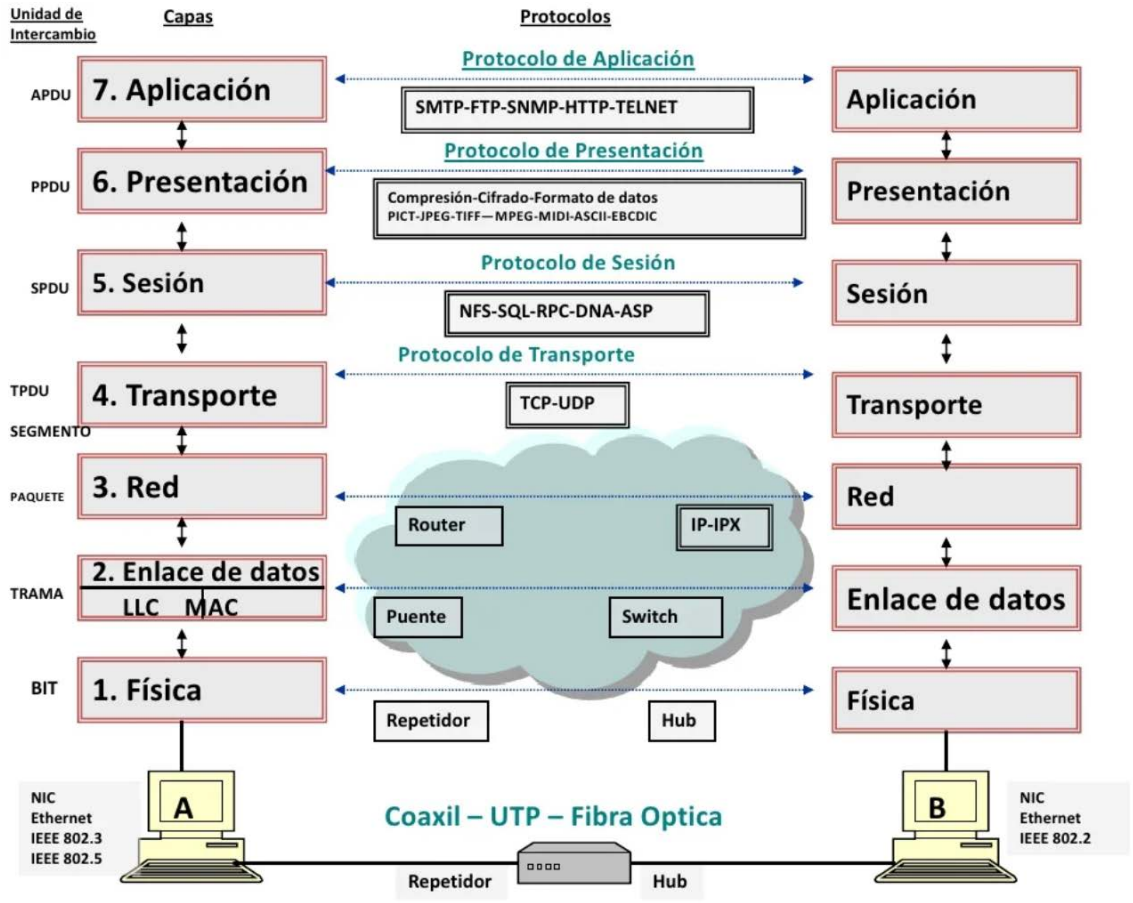
En primer lugar, se produce la decodificación de señales en la capa de transferencia de bits y, a continuación, se leen las direcciones MAC de la capa 2 y las direcciones IP y los protocolos de enrutamiento de la capa 3. Con estos datos, el router ya se encuentra en condiciones de tomar una decisión en cuanto a su reenvío. El paquete de datos, encapsulado de nuevo y basándose en la información obtenida, puede ser reenviado entonces a la próxima estación, en su camino hacia el sistema de destino.

Por regla general, en la transmisión de datos participa más de un router y en ellos tiene lugar el proceso de encapsulado y desencapsulado hasta que el paquete de datos llega a su destino (en este ejemplo, un servidor de correo electrónico) en forma de una señal física. El paquete de datos también pasa, aquí, por el proceso de desencapsulado, para lo que se recorrerán desde la primera hasta la séptima capa del modelo OSI. El mensaje enviado a través del cliente de correo

electrónico llegará, por lo tanto, al servidor de correo electrónico, donde estará disponible para que otro cliente de correo electrónico pueda acceder a él.

Modelo OSI gráficamente

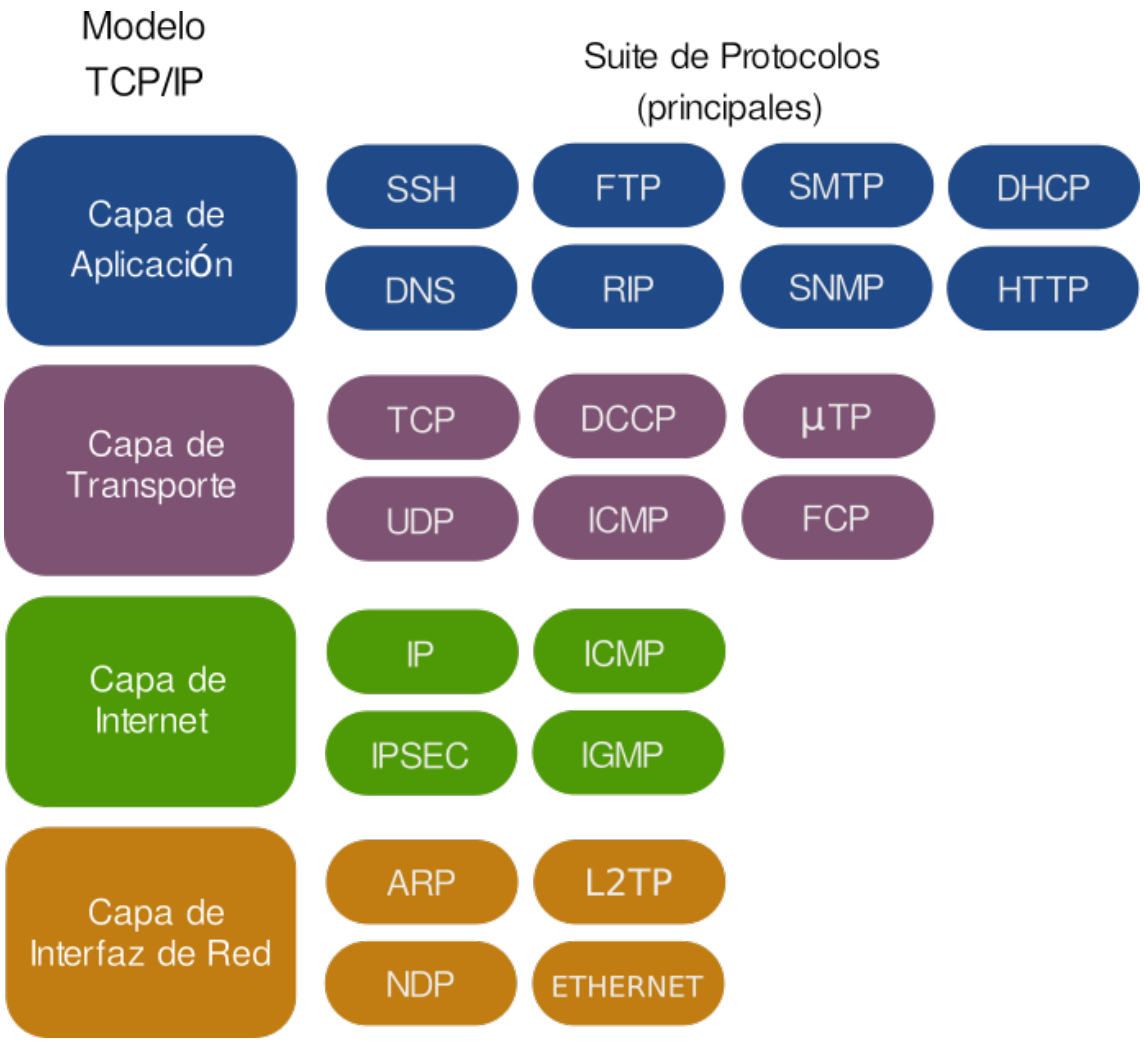



Unidad de Intercambio
Capas
Protocolos
Protocolo de Aplicación
APDU
7. Aplicación
SMTP-FTP-SNMP-HTTP-TELNET
Aplicación
Protocolo de Presentación
PPDU
6. Presentación
Compresión-Cifrado-Formato de datos
PICT-JPEG-TIFF—MPEG-MIDI-ASCII-EBCDIC
Presentación
Protocolo de Sesión
SPDU
5. Sesión
NFS-SQL-RPC-DNA-ASP
Sesión
Protocolo de Transporte
TPDU
SEGMENTO
4. Transporte
TCP-UDP
Transporte
PAQUETE
3. Red
Router
IP-IPX
Red
TRAMA
2. Enlace de datos
LLC MAC
Puente
Switch
Enlace de datos
BIT
1. Física
Repetidor
Hub
Física
NIC
Ethernet
IEEE 802.3
IEEE 802.5
A
Coaxil – UTP – Fibra Optica
B
NIC
Ethernet
IEEE 802.2
Repetidor
Hub


Unidad de Intercambio
Capas
Envío de un correo electrónico utilizando el protocolo de la capa de aplicación SMTP
APDU
7. Aplicación
SMTP
Aplicación
PPDU
6. Presentación
Compresión-Cifrado-Formato de datos
PICT-JPEG-TIFF—MPEG-MIDI-ASCII-EBCDIC
Presentación
SPDU
5. Sesión
DATOS
Sesión
PDU
4. Transporte
TCP-UDP
Transporte
Enc de red+DATOS
PAQUETE
3. Red
Router
IP-IPX
Red
TRAMA
2. Enlace de datos
LLC MAC
Enc de trama+Enc de red+DATOS+Fin de trama
Puente
Switch
Enlace de datos
BIT
1. Física
Repetidor
Hub
Física
01111011110111000011101O
NIC
Ethernet
IEEE 802.3
IEEE 802.5
A
Coaxil – UTP – Fibra Optica
B
NIC
Ethernet
IEEE 802.2
Repetidor
Hub

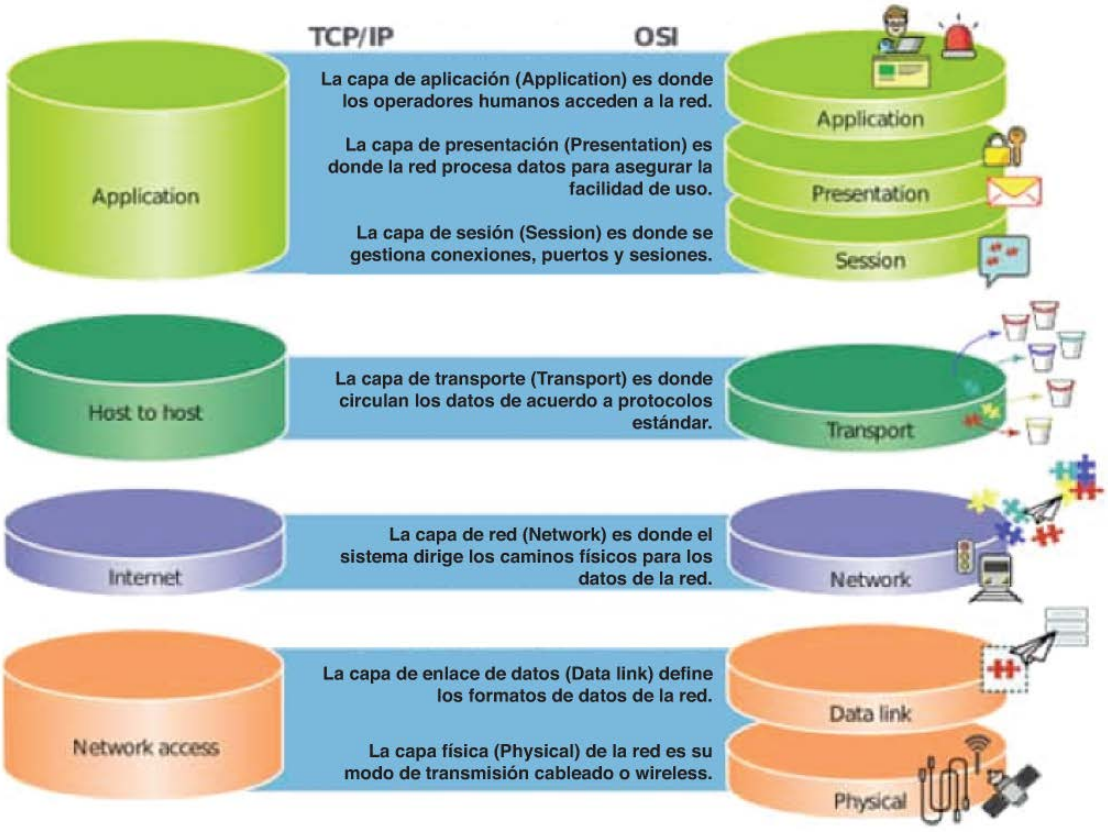
¿Qué es el modelo TCP/IP?

Es una arquitectura de red, que a veces se confunde con el protocolo de su propio nombre. Es la arquitectura más utilizada.



El modelo de capas TCP/IP prescinde de las capas de Presentación y Sesión debido a que la mayoría de las aplicaciones no las utiliza. En la capa de aplicación encontramos todos los protocolos de alto nivel como http, ssh, smtp, etc. Además unifica las capas de enlace y física, formando la capa llamada red subred, host a red, interfaz de red.

Comparativa de las capas del modelo OSI con el modelo TCP/IP



ELEMENTOS DEL NIVEL FÍSICO

Como hemos visto en el modelo OSI, en esta capa es donde se establecen los tipos de medios a utilizar para la transmisión de datos, las características físicas del medio, niveles de voltaje para representar los ceros y unos que simbolizan la información.

El medio físico elegido para la transmisión de la señal de información es de vital importancia ya que las características del mismo pueden perjudicar o no a la señal, permitiendo por ejemplo un exceso de ruido en la misma (interferencias), mayor o menor velocidad de la misma, etc.

Los tipos de señales que pueden transportar la información son de tipo:

- Eléctrico.
- Electromagnética.
- Lumínica.

Clasificamos a los medios físicos en dos tipos: ***guiados*** *(la señal se transmite de forma que el medio guía a ésta)* ***y no guiados*** *(señales electromagnéticas que se propagan en el medio libre, con o sin atmósfera).*

En ambos casos, debemos de tener en cuenta las siguientes características para todos ellos:

a) ***Velocidad de transmisión de datos:*** número de bits que es capaz de transmitir en un segundo. Se mide en Mbps.
b) ***Ancho de banda que soportan:*** es la diferencia entre la mínima y la máxima frecuencia de señal que pueden transmitir el medio físico. Un canal puede ser utilizado por señales de diferentes frecuencias. Si se puede transmitir muchas señales, la información que atravesará el canal será mayor.
c) ***Espacio máximo entre dos repetidores:*** el medio físico que se utilice dictará la distancia que deben tener como máximo dos nodos de la red para que puedan comunicarse. Si debemos configurar una red con muchos ordenadores y bastante extensa, probablemente tenemos que hacer uso de repetidores que deben contemplar esta distancia.
d) ***Fiabilidad:*** depende en gran medida del medio que se use. Una red cableada será más fiable que una red inalámbrica.