TEMA 1.3 ARQUITECTURAS DE RED

1. ARQUITECTURA DE RED.

La organización de la red debe ser clara para que los fabricantes de software o hardware puedan diseñar sus productos con garantía de que funcionarán en comunicación con otros equipos que sigan las mismas reglas.

La arquitectura de red combina estándares, topologías y protocolos para producir una red funcional.

Existen diferentes arquitecturas de redes, entre las más conocidas, el modelo de referencia OSI, arquitectura TCP/IP.

En ocasiones cuando se habla de arquitecturas se hace referencia a las arquitecturas comerciales, entre las que se encuentran:

- Ethernet.
- Token ring.
- Modo de transferencia asíncrona (asynchronous transfer mode, ATM).
- Interfaz de datos distribuidos por fibra (Fiber Distributed Data Interface, FDDI).
- Frame Relay.

Una de las principales diferencias entre estas arquitecturas es el conjunto de reglas (protocolos) utilizadas por cada una para insertar datos en el cable de red y para extraer datos del mismo. Este conjunto de reglas se denomina método de acceso. Cuando los datos circulan por la red, los distintos métodos de acceso regulan el flujo del tráfico de red.

2. PROTOCOLO DE COMUNICACIONES.

Un protocolo es un conjunto de reglas perfectamente organizadas y convenidas de mutuo acuerdo entre los participantes en una comunicación y su misión es regular algún aspecto de la misma. Realmente un protocolo de comunicación es un programa que se instala en el origen y en el destino y que añade códigos de control a lo que se desea transmitir, y al recibir la información los elimina.

Ejemplos de protocolos son: Ethernet, Token Ring, FDDI; IP, TCP, UDP, FTP, HTTP. Cada protocolo es válido para un determinado nivel: HTTP es el protocolo (entre otros) que nos permite visualizar una página web en nuestro navegador.

La comunicación es horizontal, es decir, se darán entre niveles homónimos y hay un protocolo por cada nivel de la pila.
Los protocolos se ajustan a normativas o recomendaciones de asociaciones de estándares. Los fabricantes se ajustan a esas normas y así garantizan que son compatibles en aquellos aspectos regulados por el protocolo.

Los protocolos pueden ser **encaminables**(rutables) y **no encaminables**. Encaminables significa que un ordenador puede enviar un mensaje a otro, utilizando otros ordenadores intermedios. No encaminables exige una comunicación directa entre los dos equipos a comunicar.

3. PROBLEMAS EN EL DISEÑO DE LA ARQUITECTURA DE LA RED.

Algunos de los problemas más importantes a los que se enfrentan los diseñadores de redes de comunicaciones son:

- **Encaminamiento**: cuando existen diferentes rutas posibles entre el origen y el destino, se debe elegir una de ellas (normalmente, la más corta o la que tenga un tráfico menor).

- **Direccionamiento**: Es el mecanismo que permite que un proceso (programa) de una máquina especifique con quiere comunicarse. Suele ser normal que un equipo tenga asignadas varias direcciones diferentes, relacionadas con niveles diferentes de la arquitectura. En este caso, también habrá que establecer alguna correspondencia entre esas direcciones.

- **Acceso al medio:** en las redes donde existe un medio de comunicación de difusión, debe existir algún mecanismo que controle el orden de transmisión de los interlocutores.

- **Saturación del receptor**: esta cuestión suele plantearse en todos los niveles de la arquitectura y consiste en que un emisor rápido pueda saturar a un receptor lento. En determinadas condiciones, el proceso en el otro extremo necesita un tiempo para procesar la información que le llega. Si ese tiempo es demasiado grande con comparación con la velocidad con la que le llega la información, será posible que se pierdan datos.

- **Mantenimiento del orden**: algunas redes de transmisión de datos desordenan los mensajes que envían, de forma que, si los mensajes se envían en una secuencia determinada, no se asegura que lleguen en esa misma secuencia. Para solucionar esto, el protocolo debe incorporar un mecanismo que le permita volver a ordenar los mensajes en el destino.

- **Control de errores**: todas las redes de comunicación de datos transmiten la información con una pequeña tasa de error, que en ningún caso es nula. Tanto emisor como receptor deben ponerse de acuerdo a la hora de establecer que mecanismos se van a utilizar para detectar y corregir errores, y si se va a notificar al emisor que los mensajes llegan correctamente.

- **Multiplexación**: en determinadas condiciones la red, puede tener tramos en los que existe un único medio de transmisión que, por cuestiones económicas, debe ser compartido por diferentes comunicaciones que no tienen relación entre sí. Así, el protocolo deberá asegurar que todas las comunicaciones que comparten el mismo medio no se interfieren entre sí.

4. CAPAS O NIVELES.

Con el fin de simplificar la complejidad de cualquier red, las diferentes funciones que realizan y los servicios que proveen, se distribuyen en una serie de capas o niveles.
Las capas están jerarquizadas y cada una se construye sobre la anterior. El número de capas, funciones y servicios, depende del tipo de red.

- Toda **capa** provee de servicios a la capa inmediatamente superior, haciendo transparente el modo en que se llevan a cabo estos servicios. De este modo cada capa debe ocuparse exclusivamente de su nivel inferior a quien solicita el servicio, y de su nivel inmediatamente superior a quien devuelve el resultado.

  La capa N puede solicitar servicios a la capa N-1.
  La primera capa es una excepción, pues no tiene ninguna otra por debajo. Esta capa se encarga de operar con los medios de transmisión.
- **Servicios**: Conjunto de prestaciones ofrecidas por un nivel (proveedor) a su nivel inmediatamente superior (usuario).
- Los puntos de comunicación entre los niveles o capas se llaman puntos de acceso a los servicios (**SAP),** es decir representan el punto donde los servicios están disponibles
- El **interfaz** entre capas es el conjunto de normas de intercomunicación para que una capa pueda solicitar servicios y comunicarse con sus capas adyacentes.

  Son las fronteras entre las capas. Una capa intercambia información con sus capas superior/inferior inmediatas.
  Un cambio en algunas de las capas, siempre que se conserven las estructuras de los interfaces, no afectará a las demás. Es la gran ventaja de la arquitectura en capas: poco sensible a cambios tecnológicos que se producen por la evolución en las funciones y en los servicios de las redes.
- Las **entidades**. Cada capa tiene un conjunto de entidades que son las que realizan y ofrecen los distintos servicios. Son elementos activos en el sistema que usa protocolos para proporcionar servicios a su *Entidad par.*

El proceso de comunicación se produce entre las capas equivalentes de dos hosts distintos, es decir es una comunicación horizontal. La información y con ella la petición de servicios, va descendiendo por la estructura de capas del host emisor hasta el nivel más bajo. Desde la capa más baja se pasa al medio de transmisión por el que la información es “transportada” hasta el host destino. A partir de aquí se inicia el proceso inverso, de las capas inferiores hasta llegar a la capa equivalente en el host destino de la capa que inició el servicio en el host emisor.

5. MODELO DE REFERENCIA OSI

En 1978, la International Standards Organization, ISO (Organización Internacional de Estándares) divulgó un conjunto de especificaciones que describían la arquitectura de red para la conexión de dispositivos diferentes.

La finalidad era promover la creación de una serie de estándares que especificasen un conjunto de protocolos independientes de cualquier fabricante. Además de facilitar las comunicaciones entre los sistemas diferentes, se pretende impedir que ninguna de las arquitecturas de los fabricantes existentes adquiriese una posición hegemónica, especialmente la arquitectura SNA de IBM que era la que la ostentaba en aquel momento.

En 1984, la ISO presentó una revisión de este modelo y lo llamó modelo de referencia de Interconexión de Sistemas Abiertos (OSI). La revisión de 1984 se ha convertido en un estándar internacional y se utiliza como guía para las redes, pero es un modelo teórico no aceptado totalmente por los fabricantes, solo aceptan lo que les interesa.

El modelo OSI define siete capas en total:

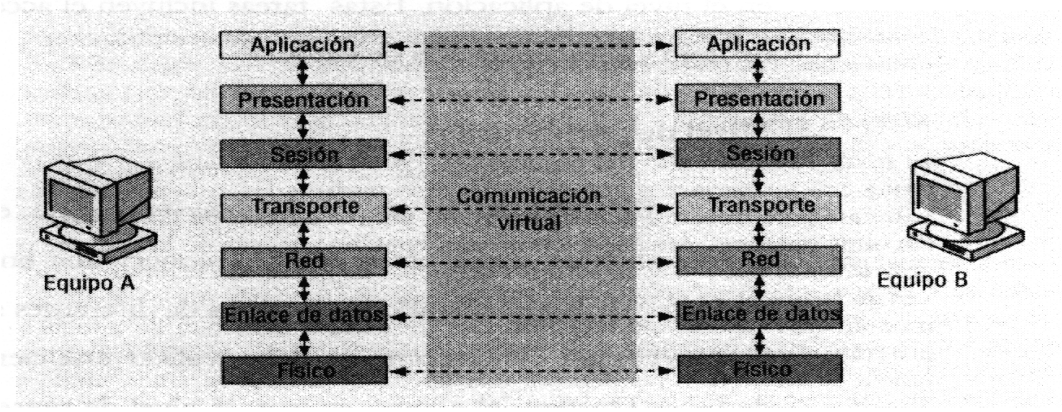
1. Física
2. Enlace
3. Red
4. Transporte
5. Sesión
6. Presentación
7. Aplicación

Además han especificado protocolos para todas las capas, aunque algunos son poco utilizados.

5.1. Relaciones entre los niveles del modelo OSI

Cada nivel proporciona servicios al nivel inmediatamente superior. Al mismo tiempo, cada nivel parece estar en comunicación directa con su nivel asociado del otro equipo. Esto proporciona una comunicación lógica, o virtual, entre niveles análogos.
Antes de pasar los datos de un nivel a otro, se dividen en paquetes, o unidades de información, que se transmiten como un todo desde un dispositivo a otro sobre una red.
La red pasa un paquete de un nivel software a otro, en el mismo orden de los niveles. En cada nivel, el software agrega información de formato o direccionamiento, al paquete, que es necesaria para la correcta transmisión del paquete a través de la red.

En el extremo receptor, el paquete pasa a través de los niveles en orden inverso. Una utilidad software en cada nivel lee la información del paquete, la elimina y pasa paquete hacia el siguiente nivel superior. Cuando el paquete alcanza el nivel de aplicación, la información de direccionamiento ha sido eliminada y se encuentra en su formato original.



Con la excepción del nivel más bajo del modelo de redes OSI, ningún nivel puede pasar información directamente a su homólogo en otro equipo. En su lugar, la información del equipo emisor debe ir descendiendo por todos los niveles hasta alcanzar el nivel físico. En ese momento, la información se desplaza a través del cable de red hacia el equipo receptor y asciende por sus niveles hasta que alcanza el nivel correspondiente.

5.1.1. Nivel de aplicación

El nivel 7, el más alto del modelo OSI, es el nivel de aplicación.
Este nivel se relaciona con los servicios que soportan directamente las aplicaciones de usuario, como software para transferencia de archivos, acceso a bases de datos, correo electrónico…
En el envío de un mensaje a través de la red entra al modelo OSI por este punto y sale por el nivel de aplicación del modelo OSI del equipo receptor
Los protocolos del nivel de aplicación pueden ser programas en sí mismos, como el FTP (File Transfer Protocol o Protocolo de Transferencia de Ficheros) o pueden ser utilizados por otros programas, como el SMTP(Simple Mail Transfer Protocol o Protocolo de transferencia de correo simple) utilizado por la mayoría de los programas de correo electrónico para redirigir datos a la red, HTTP, Telnet….

5.1.2. Nivel de presentación

El nivel 6, el nivel de presentación, define el formato utilizado para el intercambio de datos entre equipos conectados en red.
Se puede ver como el traductor de la red.
Cuando los equipos de diferentes sistemas (como IBM, Apple y Sun) necesitan comunicarse se debe realizar una cierta y reordenación de bytes.
Dentro del equipo emisor, el nivel de presentación traduce los datos del formato enviado por el nivel de aplicación en un formato intermedio. En el equipo receptor, este nivel traduce el formato intermedio en un formato que pueda ser útil para el nivel de aplicación de ese equipo.
El nivel de presentación es el responsable de

- La conversión de protocolos
- La traducción de los datos
- La modificación o conversión del conjunto de caracteres
- Compresión de datos para reducir el número de bits que se necesitan transmitir
- Cifrado (encriptación) de datos.

5.1.3. Nivel de sesión

El nivel 5, el nivel de sesión, permite que dos aplicaciones en diferentes equipos abran, utilicen y cierren una conexión llamada sesión (una sesión es un diálogo o *conversación* entre dos estaciones). El nivel de sesión es el responsable de la gestión de este diálogo.
Este realiza el reconocimiento de nombres y otras funciones, como

- Seguridad, que se necesita para permitir que dos aplicaciones se comuniquen a través de la red.
- Control del orden de intervención de los interlocutores en ciertos diálogos, pudiendo establecer prioridades a las distintas sesiones establecidas.
- Facilita a los usuarios la vuelta a un estado anterior tras un problema.
- Establece puntos de control en el flujo de datos, para que si se produce un error, sólo se transmiten de nuevo los datos posteriores al último punto de control, etc.

Esta comunicación se puede producir según los tres modos de dialogo: simplex, semiduplex y dúplex, ya vistos previamente.

5.1.4. Nivel de transporte

El nivel 4, el nivel de transporte. Asegura que la información llegue a su destino.
El nivel de transporte garantiza que los paquetes se envíen sin errores, en secuencia, y sin pérdidas o duplicados. **El control no es a nivel de bits como en la capa de enlace sino a nivel de paquetes.**
Es decir, en el equipo emisor, este nivel vuelve a empaquetar los mensajes, dividiendo los mensajes grandes (los que superan el tamaño máximo del paquete que soporta la red MTU) en varios paquetes y agrupando los paquetes pequeños en uno. En el equipo receptor, el nivel de transporte abre el paquete, reagrupa los mensajes originales y, normalmente, envía una confirmación de que se recibió el mensaje. Si llega un paquete duplicado, este nivel reconocerá el duplicado y lo descartará.
El nivel de transporte proporciona control de flujo y manejo de errores, y participa en la resolución de problemas relacionados con la trasmisión y recepción de paquetes.

5.1.5. Nivel de red

El nivel 3, el nivel de red, es el responsable de proporcionar el camino físico a través del cual irán los datos por los diferentes nodos(es el que elije el camino a seguir, el encaminamiento), lo cual implica el direccionamiento de los mensajes y la traducción de las direcciones y nombres lógicos en direcciones físicas.
Es capaz de segmentar los paquetes en trozos más pequeños.
También gestiona los problemas de tráfico en la red, como la conmutación y encaminamiento de paquetes y el control de la congestión de los datos.

5.1.6. Nivel de enlace de datos

El nivel 2, el nivel de enlace de datos, envía tramas de datos desde el nivel de red hacia el nivel físico.
En el extremo receptor, el nivel de enlace de datos empaqueta los bits puros del nivel físico en tramas de datos.

El nivel de enlace se encargará de que los mensajes entre dos puntos del camino lleguen sin errores independientemente de la tecnología de transmisión física utilizada***. El control se realiza a nivel de bits, mientras que en la capa de transporte el control de errores se realiza a nivel de paquetes.***

- Se encarga del control del enlace de datos:
  - Divide los datos en tramas y se encarga de delimitar y reconocer las tramas.
  - Resuelve pérdidas y duplicaciones.
  - Control de flujo (emisor y receptor deben ponerse de acuerdo en el ritmo de transmisión de datos) y sentidos de transmisión.

5.1.7. Nivel físico

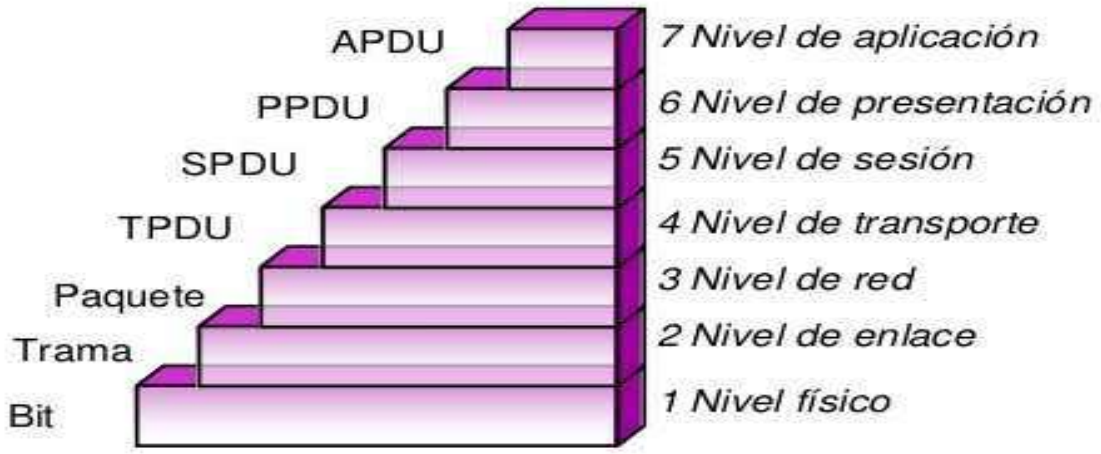
El nivel 1, el más bajo del modelo OSI, es el nivel físico. Este nivel transmite el flujo de bits sobre un medio físico (como el cable de red).
El nivel físico está completamente orientado al hardware (se indica el medio de transmisión, los conectores, especificaciones eléctricas, lumínicas y de la codificación). Los bits son transformados en pulsos eléctricos, en luz o en radio frecuencia para ser enviados según sea el medio en que se propaguen.

5.2. Encapsulacion y demultiplexacion.

Cuando una aplicación envía datos, estos son enviados desde la capa más alta hacia abajo hasta llegar a la capa física. Cada capa añade su información administrativa a los datos (cabeceras y en el caso de la capa de enlace también de cola) y se los envía a la capa inmediatamente inferior. Este proceso se denomina encapsulación y el proceso contrario demultiplexación, es decir cuando llega el paquete de información al equipo destino va de capa en capa hasta llegar a la capa de aplicación, cada capa le quita la información administrativa propia de esa capa y que fue añadida en el emisor.

5.3. Unidades de datos en el modelo OSI

Gráfico donde se puede ver como se llama a la información en cada nivel del modelo OSI



5.4. Envío de datos en una red

Se puede pensar que los datos se envían desde un equipo a otro como una serie continua de unos y ceros. De hecho, los datos se dividen en paquetes pequeños y manejables, cada uno dividido con la información esencial para ir desde el origen hasta el destino. Los paquetes constituyen los bloques básicos de comunicación de datos por la red.

Hay dos razones por las que la colocación de grandes bloques de datos en el cable ralentiza la red:

- Las grandes cantidades de datos enviados como un único bloque colapsan la red y hacen imposible la interacción y comunicación apropiada debido a que un equipo está desbordando el cable con datos.
- El impacto de la retransmisión de grandes bloques de datos multiplica el tráfico de la red.

Estos efectos se minimizan cuando estos grandes bloques de datos se dividen en paquetes más pequeños para una mejor gestión de control de errores en la transmisión. De esta forma, solo se afecta a una pequeña cantidad de datos y por lo tanto, solo se tienen que volver a transmitir pequeñas cantidades de datos, facilitando la recuperación de un error.

El equipo destino del mensaje reúne los paquetes y se estos se reorganizan en el orden de los datos originales.

6. MODELO 802

El estudio de arquitecturas en las redes LAN se centra en los niveles inferiores. Una de las propuestas más utilizadas es el modelo de referencia IEEE 802.

Los dos niveles inferiores del modelo OSI están relacionados con el hardware: la tarjeta de red y el cableado de la red. Para avanzar más en el refinamiento de los requerimientos del hardware que operan dentro de estos niveles, el IEEE (Instituto de ingenieros eléctricos y electrónicos), ha desarrollado mejoras específicas para diferentes tarjetas de red y cableado. De forma colectiva, estos refinamientos se conocen como es proyecto 802. Por tanto, el 802 se ocupa de los niveles: físico y de enlace.

Aunque los estándares IEEE 802 publicados son anteriores al modelo OSI de ISO, ambos estaban en desarrollo a la vez y compartían información de forma que son dos modelos compatibles.

Los estándares de redes de área local definidos por los comités 802 se clasifican en categorías, que se pueden identificar por el número que acompaña al 802.

Entre los estándares más relevantes tenemos los siguientes:

Especificación	Descripción
802.2	Define el estándar general para el nivel de enlace de datos. El IEEE divide este nivel en dos subniveles LLC y MAC. El nivel MAC varía en función de los diferentes tipos de red.
802.3	Define el nivel MAC para redes de bus que utilizan CSMA/CD para el acceso al medio. Este es el estándar conocido como Ethernet.
802.5	Define el nivel MAC para redes Token Ring.
802.11	Define los estándares de redes inalámbricas de área local. Es el protocolo más utilizado para el establecimiento de redes locales sin hilos. Su nombre popular es Wi-fi®
802.15	Define las redes de área personal sin cable (WPAN). Dentro de este grupo se han acogido normas de gran difusión en el mundo de las comunicaciones inalámbricas de pequeños dispositivos electrónicos, como es el caso del Bluetooth.
802.16	Define los estándares sin cable de banda ancha. Popularmente es conocido como WiMAX(Worldwide interoperability for Microwave Access), este protocolo pretende dotar de conectividad a dispositivos (ordenadores, etc.) fijos y que se encuentren a una distancia considerable. Está enfocado a zonas rurales a las cuales no se tiene acceso a través de medios guiados (cable o fibra óptica), extendiendo las redes inalámbricas a un ámbito metropolitano.

6.1. Mejoras sobre el modelo OSI

Los dos niveles inferiores del modelo OSI, el nivel físico y el nivel de enlace de datos, definen la forma en que múltiples equipos pueden utilizar la red simultáneamente sin que exista interferencia entre ellas.

Tras la decisión de que se necesitaban más detalles en el nivel de enlace de datos, el comité de estándares 802 dividió el nivel de enlace de datos en dos subniveles:

- **Control de enlace lógico (LLC, Logical Link Control**). Establece y finaliza los enlaces, controla el tráfico de tramas, secuencia tramas y confirma la recepción de las tramas.

- **Control de acceso al medio (MAC, Media Access Control**). Gestiona el acceso al medio, delimita las tramas, comprueba los errores de las tramas y reconoce las direcciones de las tramas.

7. MODELO TCP/IP

En TCP/IP se desarrollaron los protocolos y posteriormente se definió el modelo basándose en los protocolos existentes.

TCP/IP es un **conjunto de protocolos** que nacieron con la arquitectura ARPANET.

ARPANET es una red que no sigue el modelo OSI, entre otras razones, porque nació una década antes.

Los orígenes de Internet se remontan a los años sesenta. Todo el desarrollo tecnológico comenzó, como ha ocurrido en otras ocasiones, por razones militares. El Pentágono estadounidense creó la Agencia de Proyectos de Investigación Avanzada del Departamento de Defensa (ARPA) para competir con la tecnología espacial rusa, en plena guerra fría entre EE.UU. y la Unión Soviética.

El objetivo inicial fue el desarrollo de técnicas que permitieran intercambiar información de una forma sencilla y segura. Esto suponía que el sistema de comunicaciones no dependiera de un único punto estratégico y que los mensajes pudieran llegar a su destino por diversos caminos, frente a la eventualidad de un ataque militar que destruyera parte de la red de comunicaciones.

Así empezó a trabajar la red de la familia ARPA, que permite el acceso de un punto a otro de la red por caminos diversos. Posteriormente se hizo partícipe de la red al ámbito universitario y de investigación en general.

Internet comenzó propiamente en 1969, tras conectarse los ordenadores de cuatro universidades de Estados Unidos.

Aunque la familia de protocolos de ARPANET está alejada de la estructura de OSI, se han convertido en un **estándar *de facto***(estándar aceptado debido al uso, no por su publicación por una asociación de estándares.***)*** debido a que Internet se sirve de ellos
Es un protocolo abierto (no propietario). Su definición y el código para su implementación se encuentran disponibles sin cargo.
Es apropiado tanto para su uso en las comunicaciones en redes LAN como WAN.

Hay una serie de razones por las que los protocolos TCP/IP han ganado a los OSI:

- Los TCP/IP estaban ya operativos antes de que OSI se normalizara, por lo que empezaron a utilizarse y luego el coste implicado en cambiar a OSI impidió este trasvase.
- La necesidad de EEUU de utilizar un protocolo operativo hizo que adaptara el TCP/IP que ya lo era y así arrastró a los demás a su utilización (ya que es el mayor consumidor de software).
- El incremento de Internet ha lanzado el uso de TCP/IP. Toda la estructura lógica de Internet se sustenta sobre el protocolo IP (Intemet Protocol).

Históricamente, había dos desventajas principales de TCP/IP: su tamaño y velocidad.

7.1. Capas o Niveles TCP/IP.

También se habla de "la pila" de protocolos TCP/IP.

Internet no es un nuevo tipo de red física, sino un conjunto de tecnologías que permiten interconectar redes muy distintas entre sí.
El protocolo TCP/IP está formado por cuatro capas, mientras que el modelo OSI, consta de siete capas.
En la siguiente tabla vemos los modelos de referencia TCP/IP comparados con OSI :

OSI	TCP/IP
Aplicación	Aplicación
Presentación	
Sesión	
Transporte	Transporte
Red	Red/Internet
Enlace	Enlace
Físico	

CAPA ENLACE
Muchas veces esta capa recibe el nombre de DATA-LINK o Interfaz de red o Nivel de Acceso a Red. Corresponde a la capa de enlace y física del modelo OSI.
Se encarga de todo lo referente al envío de señales físicas por el medio (coaxial, hilos, fibra, etc.) así como del formato de tramas de nivel de enlace.

Utiliza **direcciones físicas** para la entrega de datos.
En la capa de enlace los datos se organizan en unidades llamadas **tramas**,

TCP/IP no define ningún protocolo específico para este nivel.

CAPA DE RED.
También llamada ***capa IP o capa de Internet***. Corresponde a la capa de red del modelo OSI.

Se encarga del movimiento de paquetes a través de la red, encaminar los paquetes hacia su destino y escoger la ruta más adecuada.
Para ello utiliza dispositivos de encaminamiento que en TCP/IP se denominan *Gateways*, aunque cada vez es más utilizado el término *encaminador o router* (que en realidad es más correcto).

Utiliza varios protocolos para encaminar y entregar los paquetes. El principal protocolo es IP.

LA CAPA DE TRANSPORTE
Corresponde a las capas de transporte y algunas de las funciones de la capa de sesión del modelo OSI. Es la **capa TCP.**

Proporciona un flujo fiable de datos entre dos equipos
Este nivel utiliza dos protocolos TCP y UDP dependiendo de que el servicio que proporcione garantice una entrega fiable de los datos (TCP) o una entrega no fiable de los datos (UDP).

CAPA DE APLICACIÓN.
Corresponde a la capa de aplicación, presentación y buena parte de las funciones de la capa de sesión del modelo OSI.

Esta capa se ocupa de lo que podemos transmitir, *proporciona los distintos servicios de Internet: correo electrónico SMTP, páginas Web HTTP, FTP*

8. RELACIÓN ENTRE EL MODELO OSI Y LA ARQUITECTURA DE UNA LAN.

Una LAN puede incorporar protocolos de múltiples capas, aunque el mayor número de protocolos pertenecerá siempre a las capas inferiores. De hecho, siempre tiene que haber una capa física, de lo contrario sería imposible la transmisión, no habría comunicación y ello inhabilitaría la red como dispositivo de comunicación.

Es normal que una LAN tenga funciones y servicios propios de capas superiores de OSI, pero lo propio de las LAN son las capas inferiores. Por ejemplo, una WAN requiere técnicas de encaminamiento, que son propias de la capa de red (nivel 3 de OSI). No todas las redes de área local pueden encaminar paquetes. Sin embargo, todas las LAN son capaces de entregar tramas de bits (nivel 2) a la capa física (nivel 1) para que sean transmitidas en forma de señales por las líneas de comunicación. Esta es la razón por la que nos centraremos más en los niveles 1 y 2 de OSI, aclarando que la LAN abarca más que estos niveles.

9. ETHERNET

A finales de los sesenta la Universidad de Hawai desarrolló una WAN denominada ALOHA. Una de las características fundamentales de la red de la universidad era que utilizaba CSMA/CD como método de acceso.

Esta red fue la base para la arquitectura de red Ethernet actual. En 1972, Robert Metcalfe y David Boggs inventaron un esquema de cableado y comunicación en el Centro de Investigación de Xerox en Palo Alto (PARC) y en 1975 introdujeron el primer producto Ethernet.

Xerox Ethernet fue tan exitosa que Xerox, Intel Corporation y Digital Equipment Corporation (**DIX**) diseñaron un estándar para Ethernet a 10 Mbps. La tecnología Ethernet fue adoptada para su estandarización por el comité de redes locales (LAN) de la IEEE como **IEEE 802.3.**

Es actualmente la arquitectura de red más popular, es un estándar que no pertenece a ninguna compañía.

9.1. Características de Ethernet

El medio Ethernet *es pasivo*, lo que significa que el emisor genera la información y esta solo se transmite, sin regenerarse en la red, por ello permite apagar un ordenador de la red y que no falle a menos que el medio sea físicamente cortado o no tenga terminador.

- **Topología tradicional:** Bus lineal
- **Topología más usada:** estrella que funciona como bus.
- **Método de acceso:** CSMA/CD.
- **Especificación:** IEEE 802.3.

9.2. Método de acceso

Un método **de acceso e**s un conjunto de reglas que definen la forma en que un equipo coloca los datos en la red y toma los datos del cable. Una vez que los datos se están moviendo en la red, los métodos de acceso ayudan a regular el flujo del tráfico de la red. Los métodos de acceso previenen que los equipos accedan simultáneamente al cable.

Ethernet utiliza el método de acceso **CSMA/CD**

CSMA/CD es un método de contienda, es un conjunto de reglas que determina el modo de respuesta de los dispositivos de red cuando dos de ellos intentan enviar datos en la red simultáneamente. La transmisión de datos por múltiples equipos simultáneamente a través de la red produce una colisión. Únicamente cuando un equipo detecta que el cable está libre comienza con su transmisión. Mientras el equipo se encuentre transmitiendo sus datos por el cable, ningún otro equipo debería poder transmitir datos hasta que los datos originales hayan llegado a su destino y el cable vuelva a estar libre. En el caso de que otro equipo se pusiese a transmitir se produciría una colisión.

Tras detectar una colisión, el dispositivo espera un tiempo aleatorio y a continuación intenta retransmitir el mensaje. Si el dispositivo detecta de nuevo una colisión, espera el doble antes de intentar retransmitir el mensaje

Una vez comenzado a emitir, no para hasta terminar de emitir la trama completa.

9.3. Trama de Ethernet

Ethernet divide los datos en bloques de bits llamados **tramas.** Una trama es un paquete de información transmitido como una unidad.

Existen dos posibles formatos de trama de Ethernet: el reflejado en RFC 894 y el publicado en RFC 1042 (IEEE 802.3).
Él más usado es el Publicado en la RFC 894, aunque la mayoría de las tarjetas de red pueden transmitir usando los dos.
La diferencia entre ambas tramas es el campo Tipo en Ethernet-Dix y el campo Longitud en IEEE 802.3.

9.4. Estándares Ethernet

Los estándares Ethernet se basan en las reglas dictadas por el IEEE en la norma 802.3, que representa la red Ethernet.

Hay estándares a 10 Mbps, 100 Mbps, 1000 Mbps.
En la actualidad ya se habla de Ethernet 10G, que sería la red con tecnología Ethernet a 10Gbps.

9.5. Porque esos nombres para los estándares Ethernet

El nombre de los estándares vistos tiene una explicación.

- En primera posición aparece un numero: 10, 100… que representa la **velocidad de transmisión** permitida.
- Después Base que indica que la señal es **banda base**(señal digital que se trasmite por único canal)
- Y a continuación una letra que representa el **tipo de cable** utilizado.
  - TX- Indica que se trata de cable de par trenzado utilizando dos pares de los utilizados en transmisión de datos.
  - FX- Indica que se trata de un enlace de fibra óptica que utiliza un cable de fibra óptica de dos hilos de fibra.

10. TOKEN RING

La versión de IBM de Token Ring fue introducida en 1984.

Esta arquitectura, desarrollada por IBM, jugó un papel muy importante en el mercado de las redes de área local, pero su popularidad descendió enormemente a favor de Ethernet.
En 1985, el Token Ring IBM llegó a ser un estándar ANSI/IEEE. **(IEEE 802.5)**

Las redes *Token Ring* están implementadas en una topología en anillo, pero IBM representó físicamente el anillo mediante un dispositivo concentrador denominado unidad de acceso multiestación (*multistation access unit*, MAU), por lo tanto la Token Ring de IBM se trata de una topología lógica en anillo, pero implementado físicamente como una estrella.

Una de las ventajas del sistema Token Ring es la redundancia: si falla un elemento del sistema, la señal retrocederá pero seguirá funcionando*, ello es debido al uso del MAU, antes de que estos aparecieran si un equipo se desconectaba el anillo se rompía y fallaba la red*. La gran desventaja es el coste tanto del cableado como de las tarjetas. Además la instalación es más compleja que en la Ethernet coaxial fino y par trenzado.

10.1. Método de acceso

El método de acceso utilizado en una red *Token Ring* es de **paso de testigo.** Un testigo es una serie especial de bits que viaja sobre una red *Token Ring*. Un equipo no puede transmitir salvo que tenga posesión del testigo; mientras que el testigo está en uso por un equipo, ningún otro puede transmitir datos.

Cada equipo recibe y regenera los bits que recibe, de forma tal que actúa como repetidor cuando está activo. Cuando la información vuelve al equipo que originó la transmisión, el mensaje es retirado de la circulación.

Cuando el primer equipo de la red *Token Ring* se activa, la red pone en circulación un testigo. Este testigo se pasa de NIC a NIC en secuencia hasta que encuentra una estación que tiene datos para enviar, enviando a continuación su trama de datos.

Esta trama de datos se propaga a través del anillo, siendo regenerada por cada estación. Cada estación intermedia examina la dirección destino, ve que la trama está dirigida a otra estación y la reenvía a su destino. El supuesto receptor reconoce su dirección, copia el mensaje, comprueba los posibles errores y cambia unos bits en la trama para indicar que ha reconocido la dirección y ha copiado la trama. A continuación todo el paquete sigue girando alrededor del anillo hasta que llega a la estación que lo envió.

El emisor recibe la trama y reconoce su propia dirección en el campo de dirección origen. Examina los datos de dirección reconocida. Si están activos, sabe que la trama fue recibida correctamente. En ese momento, el emisor descarta la trama de datos ya utilizada y vuelve a poner el testigo en el anillo.

10.2. Posibles problemas en el paso de testigo

Hay varios problemas que pueden interrumpir el servicio de una red en anillo con paso de testigo:

- Una estación puede dejar de retransmitir un testigo o se puede destruir un testigo debido al ruido, en cuyo caso no hay testigo en el anillo y ninguna estación podrá enviar datos.

- Una estación emisora puede no eliminar la trama de datos que introdujo en el anillo o puede no liberar el testigo una vez que su turno ha terminado

Para gestionar estas situaciones, una de las estaciones del anillo se designa como **estación monitora o supervisora, (**es la primera máquina que se activa en el anillo**)**. Esta estación fija un temporizador cada vez que pasa el testigo. Si el testigo no reaparece en el tiempo fijado, presume que se ha perdido, genera un nuevo testigo y lo pone en la red. La estación monitora también evita que haya tramas de datos recirculando perpetuamente en el anillo activando un bit en cada trama. Cuando pasa la trama, la monitora comprueba el valor de este bit, y, en el caso de que esté activo, sabe que el paquete ya ha pasado por todo el anillo una vez y que debería ser descartado.

Si por alguna razón, la estación supervisora deja de funcionar correctamente o se desconecta, se establece un protocolo de contienda para determinar una nueva estación supervisora.

11. FDDI (Interfaz de datos distribuidos por fibra)

FDDI (Fiber Distributed Data Interface) fue diseñada por el comité X3T9-5 del Instituto Nacional de Estándares Americanos (ANSI) y distribuida en 1986. FDDI se diseñó para su utilización con equipos que requerían anchos de banda superiores a los 10 Ethernet o 4 Mbps de las arquitecturas Token Ring existentes.

Es un estándar que corresponde a una **red local con paso de testigo** sobre topología en anillo y que utiliza como línea de transmisión la **fibra óptica.** El anillo tendrá una longitud máxima de 100 km(por lo tanto no está diseñada para utilizarse como WAN). Se puede usar como una LAN, pero es **frecuente usarla como una red dorsal *(backbone)*** que interconecte redes locales entre sí. Se suele utilizar en MAN. Es adecuada para la transmisión de voz y vídeo.

Físicamente las redes FDDI se configuran como **dos anillos** de fibra que **transmiten en sentido contrario.** Si algún trozo de anillo se desactiva, el otro puede actuar como línea de retorno que garantiza que siempre habrá un anillo en funcionamiento. Normalmente los datos viajan por el anillo primario.

11.1. Método de acceso

El método de acceso utilizado en una red FDDI es el **paso de testigo**, parecido al Token Ring (IEEE 802.5), pero hay una diferencia significativa respecto al Token Ring: en una red de longitud tan grande sería una pérdida de eficacia esperar a que el testigo recorra todo el anillo. Para paliar este problema **se generan varios testigos**, lo que produce que en el interior del anillo puedan convivir varias tramas simultáneamente.

Un equipo en una red FDDI puede transmitir tantos paquetes como pueda dentro de un tiempo predeterminado antes de liberar el testigo. Tan pronto como un equipo haya finalizado la transmisión o después de un tiempo de transmisión predeterminado, el equipo libera el testigo.

Como un equipo libera el testigo cuando finaliza la transmisión, varios paquetes pueden circular por el anillo al mismo tiempo. Este método de paso de testigo es más eficiente que él de una red *Token Ring*, que permite únicamente la circulación de una trama a la vez. Este método de paso de testigo también proporciona un mayor rendimiento de datos a la misma velocidad de transmisión.

12. DISPOSITIVOS DE COMUNICACIÓN

Las redes utilizan unos dispositivos de comunicaciones que funcionan en los diferentes niveles OSI.

- **Repetidores y concentradores (hub)**:
  Trabajan en el nivel Físico del modelo OSI.
- **Puentes (bridge) y Conmutadores (switch)**
  Trabajan en el nivel de Enlace del modelo OSI.
- **Enrutadores (router)**
  Trabajan en el nivel de Red del modelo OSI.