¿Qué es una red informática?
Una red informática es un conjunto de dispositivos interconectados entre sí a través de un medio, que intercambian información y comparten recursos. Básicamente, la comunicación dentro de una red informática es un proceso en el que existen dos roles bien definidos para los dispositivos conectados, emisor y receptor, que se van asumiendo y alternando en distintos instantes de tiempo.
http://www.redusers.com/noticias/que-es-una-red-informatica/
Tipos de redes informáticas según su alcance

1. **RED DE ÁREA PERSONAL (PAN)**
   Hablamos de una **red informática de pocos metros**, algo parecido a la distancia que necesita el Bluetooth del móvil para intercambiar datos. Son las más básicas y sirven para espacios reducidos, por ejemplo, si trabajas en un local de una sola planta con un par de ordenadores.

2. **Red de área local (LAN)**
   Es la que todos conocemos y la que suele instalarse en la mayoría de las empresas, tanto si se trata de un edificio completo como de un local. Permite conectar ordenadores, impresoras, escáneres, fotocopiadoras y otros muchos periféricos entre sí para que puedas intercambiar datos y órdenes desde los diferentes nodos de la oficina.
   Las redes LAN pueden abarcar **desde los 200 metros hasta 1 kilómetro de cobertura**.

3. **Red de área de campus (CAN)**
   Qué pasa si el área de cobertura debe ser mayor a los 1000 metros cuadrados? Y no lo digo sólo por las universidades; las instalaciones de los parques tecnológicos, recintos feriales y naves comerciales pueden superar perfectamente esa superficie.
   En tal caso, tenemos las **redes CAN**. Habría varias redes de área local instaladas en áreas específicas, pero a su vez todas ellas estarían interconectadas, para que se puedan intercambiar datos entre sí de manera rápida, o pueda haber conexión a Internet en todo el campus.

4. **Red de área metropolitana (MAN)**
   Mucho más amplias que las anteriores, abarcan espacios metropolitanos mucho más grandes. Son las que suelen utilizarse cuando las administraciones públicas deciden **crear zonas Wifi en grandes espacios**. También es toda la infraestructura de cables de un operador de telecomunicaciones para el despliegue de **redes de fibra óptica**. Una red MAN suele conectar las diversas LAN que hay en un espacio de unos 50 kilómetros.

5. **Red de área amplia (WAN)**
   Son las que suelen desplegar las empresas **proveedoras de Internet** para cubrir las tipos de casino necesidades de conexión de redes de una zona muy amplia, como una ciudad o país.

6. **Red de área de almacenamiento (SAN)**
   Es una red propia para las **empresas que trabajan con servidores y no quieren perder rendimiento** en el tráfico de usuario, ya que manejan una enorme cantidad de datos. Suelen utilizarlo mucho las empresas tecnológicas. En Cisco te cuentan las ventajas de una red SAN.

7. **Red de área local virtual (VLAN)**
   Las redes de las que hablamos normalmente se conectan de forma física. Las **redes VLAN** se encadenan de forma lógica (mediante protocolos, puertos, etc.), reduciendo el tráfico de red y mejorando la seguridad. Si una empresa tiene varios departamentos y quieres que funcionen con una red separada, la red VLAN.

Intranet
Son aquellas redes internas que en las que el acceso a la información esta estrictamente limitada a personal de la compañía. Este tipo de redes se restringen con el uso de software y se usan en situaciones en las que la información a la que pueden acceder los usuarios es confidencial.

Extranet El siguiente nivel de acceso sucede cuando las compañías requieren dar acceso seguro y bajo confidencialidad a usuarios externos incluso a organizaciones diferentes a la que posee la información.

Internet Es el conjunto de extranet interconectadas entre si.

Topología de red Una topología de red es la disposición de una red, incluyendo sus nodos y líneas de conexión. Hay dos formas de definir la geometría de la red: la topología física y la topología lógica (o de señal).

La topología física de una red es la disposición geométrica real de las estaciones de trabajo. Existen varias topologías físicas comunes, como se describe a continuación y como se muestra en la ilustración.
Tipos de topologías físicas de red

En la topología de la red de bus, cada estación de trabajo está conectada a un cable principal llamado bus. Por lo tanto, en efecto, cada estación de trabajo está conectada directamente a cada otra estación de trabajo de la red.

En la topología de red en estrella, hay un ordenador central o servidor al que todas las estaciones de trabajo están conectadas directamente. Cada estación de trabajo está indirectamente conectada entre sí a través de la computadora central.

En la topología de red en anillo, las estaciones de trabajo están conectadas en una configuración de bucle cerrado. Los pares de estaciones de trabajo adyacentes están conectados directamente.

Otros pares de estaciones de trabajo están indirectamente conectados, pasando los datos a través de uno o más nodos intermedios.

Si se utiliza un protocolo Token Ring en una topología en estrella o en anillo, la señal viaja en una sola dirección, llevada por un denominado token de nodo a nodo.

La topología de red de malla (*mesh*) emplea cualquiera de dos esquemas, llamados malla completa y malla parcial. En la topología de malla completa, cada estación de trabajo está conectada directamente a cada uno de los otros. En la topología de malla parcial, algunas estaciones de trabajo están conectadas a todas las demás, y algunas están conectadas sólo a los otros nodos con los que intercambian más datos.

La topología de red de árbol utiliza dos o más redes en estrella conectadas entre sí. Los ordenadores centrales de las redes en estrella están conectados a un bus principal. Así, una red de árboles es una red de buses de redes estrella.

La topología lógica (o de señal) se refiere a la naturaleza de los caminos que siguen las señales de nodo a nodo. En muchos casos, la topología lógica es la misma que la topología física. Pero no siempre es así. Por ejemplo, algunas redes se disponen físicamente en una configuración en estrella, pero funcionan lógicamente como redes de bus o de anillo.

La importancia del sistema de comunicación

En los clusters la eficacia del sistema de comunicación es crítica. Si las comunicaciones fallan el cluster dejará de ser un cluster y se convertirá en un conjunto de máquinas que no cooperarán, algo lejos del objetivo. Por lo tanto es usual disponer en sistemas cluster de alta disponibilidad de una red alternativa por si la red principal fallara. Cabe decir que una red es un elemento bastante fiable a nivel físico: es difícil que una vez instalada y probada, falle. Sobre las topologías y tecnologías de red que existen se hablará en las próximas secciones.

¿Qué es una suite de protocolos?

Una suite de protocolos es un grupo de protocolos que trabajan en forma conjunta para proporcionar servicios integrales de comunicación de red. Las suites de protocolos pueden estar especificadas por una organización de estandarización o pueden ser desarrolladas por un proveedor. Las suites de protocolos pueden resultar un poco abrumadoras, como las cuatro que se muestran en la figura. Sin embargo, este curso solo abarcará los protocolos que forman la suite de protocolos TCP/IP.

Capa de aplicación

Sistema de nombres:
DNS: Sistema de nombres de dominio (o Servicio)

- Traduce los nombres de dominio tales como cisco.com a direcciones IP

Configuración de host:

BOOTP: Protocolo Bootstrap

- Habilita una estación de trabajo sin disco para descubrir su propia dirección IP, la dirección IP de un servidor BOOTP en la red y un archivo que debe cargarse en la memoria para iniciar la máquina
- DHCP reemplaza a BOOTP

DHCP: Protocolo de configuración dinámica de host

- Asigna direcciones IP de manera dinámica a estaciones de clientes cuando se inicia
- Permite que las direcciones vuelvan a utilizarse cuando ya no se necesitan

Correo electrónico

SMTP: Protocolo simple de transferencia de correo

- Permite los clientes envíen un correo electrónico a un servidor de correo
- Permite los servidores envíen un correo electrónico a otros servidores

POP: Protocolo de oficina de correos, versión 3 (POP3)

- Permite que los clientes recuperen un correo electrónico de un servidor de correo
- Descarga correo electrónico desde el servidor de correo al escritorio

IMAP: Protocolo de acceso a mensajes de internet

- Permite que los clientes accedan a correos electrónicos almacenados en un servidor de correo
- Mantiene el correo electrónico en el servidor

Transferencia de archivos

FTP: Protocolo de Transferencia de archivos

- Establece las reglas que permiten a un usuario en un host acceder y transferir archivos hacia y desde otro host en una red
- Un protocolo confiable de entrega de archivos, orientado a la conexión y que requiere acuse de recibo

TFTP: Protocolo de Transferencia de archivos trivial

- Un protocolo trivial de transferencia de archivos sin conexión
- Un protocolo de entrega de archivos sin acuse de recibo de grandes esfuerzos
- Utiliza menos sobrecarga que FTP

Web

HTTP: Protocolo de Transferencia de hipertexto

- Conjunto de reglas para intercambiar texto, imágenes gráficas, sonido, vídeo y otros archivos multimedia en la World Wide Web

Capa de Transporte

UDP: Protocolo de datagramas de usuario

- Habilita un proceso que se ejecuta en un host para enviar paquetes a un proceso que se ejecuta en otro host
- No confirma la transmisión correcta de datagramas

TCP: Protocolo de control de transmisión

- Permite la comunicación confiable entre los procesos que se ejecutan en hosts independientes
- Transmisiones confiables con acuse de recibo que confirman el envío correcto

Capa de Internet

IP: Protocolo de Internet

- Recibe segmentos de mensaje de la capa de transporte
- Dispone mensajes en paquetes
- Direcciona paquetes para la entrega completa a través de una internetwork

NAT: Traducción de direcciones de red

- Traduce las direcciones IP desde una red privada a direcciones IP públicas únicas de forma global

Soporte de IP

ICMP: Protocolo de mensajes de control de internet

- Proporciona comentarios desde un host de destino a un host de origen con respecto a los errores en la entrega de paquetes

Protocolos de enrutamiento

OSPF: Open Shortest Path Firts

- Protocolo de routing de link-state
- Diseño jerárquico basado en áreas
- Protocolo de routing interior de estándar abierto

EIGRP: Protocolo de enrutamiento de gate interior mejorado

- Protocolo de enrutamiento exclusivo de Cisco
- Utiliza la métrica compuesta según el ancho de banda, el retraso, la carga y la confiabilidad

Capa de acceso a la red

ARP: Protocolo de resolución de direcciones

- Proporciona la asignación de direcciones dinámicas entre una dirección IP y una dirección de hardware

PPP: Protocolo punto a punto

- Proporciona un medio de encapsulamiento de paquetes para transmitirlos a través de un enlace serial

Ethernet

- Define las reglas para conectar y señalizar estándares de la capa de acceso a la red

Controladores de interfaz

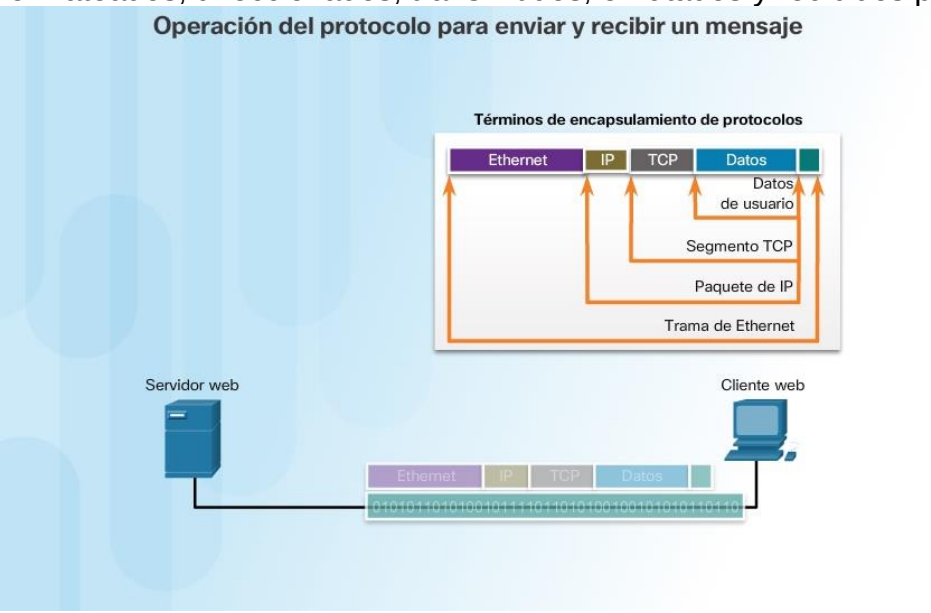
- Proporciona instrucciones a la máquina para el control de una interfaz específica en un dispositivo de red

La suite de protocolos TCP/IP se implementa como una pila de TCP/IP tanto en los hosts emisores como en los hosts receptores para proporcionar una entrega completa de las aplicaciones a través de la red. Los protocolos Ethernet se utilizan para transmitir el paquete IP a través de un medio físico que utiliza la LAN.

El **modelo TCP/IP** es una descripción de protocolos de red desarrollado por Vinton Cerf y Robert E. Kahn, en la década de 1970. Fue implantado en la red ARPANET, la primera red de área amplia (WAN), desarrollada por encargo de DARPA, una agencia del Departamento de Defensa de los Estados Unidos, y predecesora de Internet; por esta razón, a veces también se le llama **modelo DoD** o **modelo DARPA**.

El modelo TCP/IP es usado para comunicaciones en redes y, como todo protocolo, describe un conjunto de guías generales de operación para permitir que un equipo pueda comunicarse en una red. TCP/IP provee conectividad de extremo a extremo especificando cómo los datos deberían ser

formateados, direccionados, transmitidos, enrutados y recibidos por el destinatario.

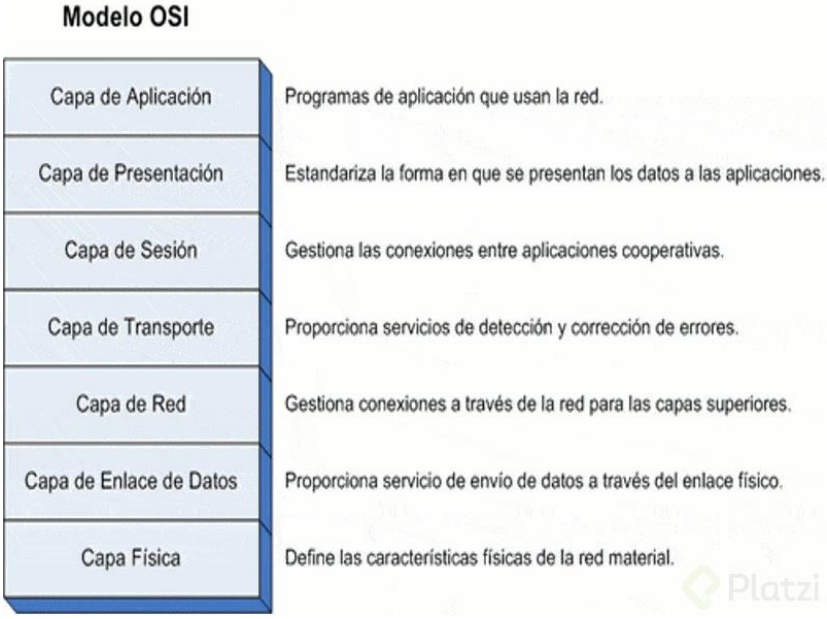


1. En la figura 1, la animación comienza con el servidor web preparando la página de lenguaje de marcado de hipertexto (HTML) como los datos que se van a enviar.
2. El encabezado HTTP del protocolo de aplicación se agrega al frente de los datos HTML. El encabezado contiene diversos tipos de información, incluida la versión de HTTP que utiliza el servidor y un código de estado que indica que tiene información para el cliente web.
3. El protocolo de capa de aplicación HTTP entrega los datos de la página web con formato HTML a la capa de transporte. El protocolo de la capa de transporte TCP se utiliza para administrar conversaciones individuales, en este ejemplo entre el servidor web y el cliente web.
4. Luego, la información IP se agrega al frente de la información TCP. IP asigna las direcciones IP de origen y de destino que corresponden. Esta información se conoce como paquete IP.
5. El protocolo Ethernet agrega información en ambos extremos del paquete IP, conocidos como la “trama de enlace de datos”. Esta trama se envía al router más cercano a lo largo de la ruta hacia el cliente web. Este router elimina la información de Ethernet, analiza el paquete IP, determina el mejor camino para el paquete, coloca el paquete en una trama nueva y lo envía al siguiente router vecino hacia el destino. Cada router elimina y agrega información de enlace de datos nueva antes de reenviar el paquete.
6. Estos datos ahora se transportan a través de la internetwork, que consta de medios y dispositivos intermediarios.
7. En la figura 2, la animación comienza con el cliente que recibe las tramas de enlace de datos que contienen los datos. Cada encabezado de protocolo se procesa y luego se elimina en el orden inverso al que se agregó. La información de Ethernet se procesa y se elimina, seguida por la información del protocolo IP, luego la información de TCP y, finalmente, la información de HTTP.
8. A continuación, la información de la página web se transfiere al software de navegador web del cliente.

Modelo OSI

El **modelo de interconexión de sistemas abiertos** (ISO/IEC 7498-1), más conocido como “modelo **OSI**”, (en inglés, ***O**pen **S**ystem **I**nterconnection*) es un modelo de referencia para los protocolos de la red (no es una arquitectura de red), creado en el año 1980 por la Organización Internacional de Normalización (ISO).[1] Se ha publicado desde 1983 por la Unión Internacional de Telecomunicaciones (UIT) y, desde 1984, la Organización Internacional de Normalización (ISO) también lo publicó con estándar.[2] Su desarrollo comenzó en 1977.[3]

Es un estándar que tiene por objetivo conseguir interconectar sistemas de procedencia distinta para que estos pudieran intercambiar información sin ningún tipo de impedimentos debido a los protocolos con los que estos operaban de forma propia según su fabricante.



¿Cuál es la diferencia entre modelo OSI y modelo TCP/IP?

Cuando hablamos de switches de capa 2 y capa 3, en realidad nos referimos a las capas de un modelo de protocolo genérico: el modelo de interconexión de sistemas abiertos (OSI), el cual es comunmente utilizado para la descripción de las comunicaciones de red. La comunicación de datos entre redes diferentes no sería posible si no existiesen reglas compartidas para su transmisión y recepción. Estas reglas se conocen como protocolos, entre los cuales se distingue el Protocolo de control de transmisión (TCP)/Protocolo de internet (IP) por ser uno de los más utilizados. Este se usa popularmente en la descripción de la red y es más antiguo que el modelo OSI, ambos con muchas capas. A continuación explicaremos cuál es la diferencia entre ellos.

Capas del modelo OSI

El modelo OSI, de siete capas, es un modelo conceptual que caracteriza y estandariza la manera en la que los diferentes componentes de software y hardware involucrados en una comunicación de red deben dividir la mano de obra e interactuar entre sí. En la siguiente figura podrá ver los nombres y funciones básicas de cada una de las capas.

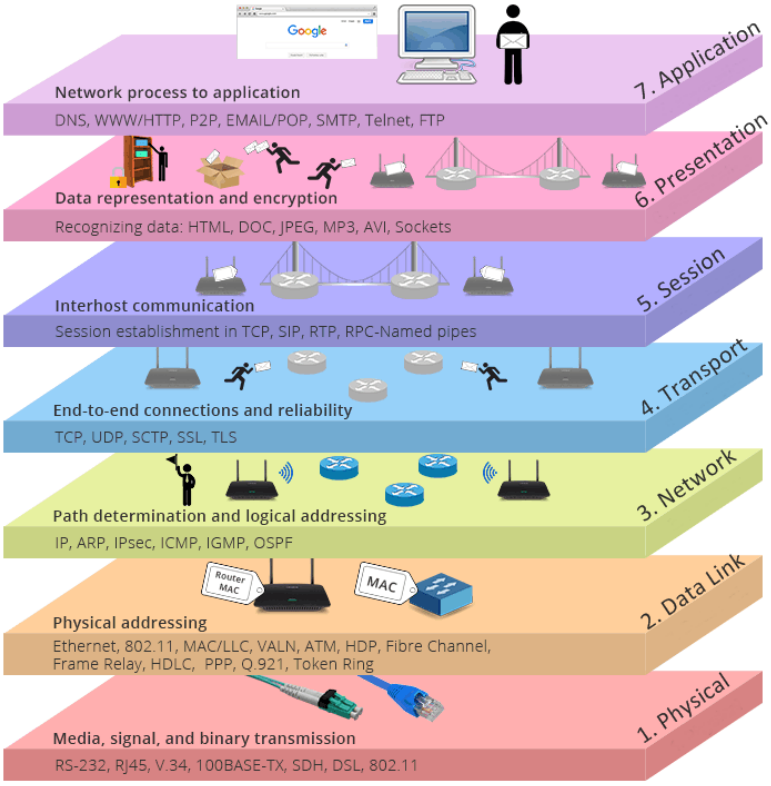


Figura 1: 7 capas del protocolo OSI

Capas del modelo TCP/IP

El modelo TCP/IP solamente tiene cuatro capas y es conocido generalmente como TCP/IP, ya que estos son sus dos protocolos más importantes.

Capa de aplicación

La capa de aplicación del modelo TCP/IP ofrece a las aplicaciones la capacidad de acceder a los servicios de las otras capas y define los protocolos que utilizan las aplicaciones para intercambiar datos. Los protocolos de la capa de aplicación más conocidos son HTTP, FTP, SMTP, Telnet, DNS, SNMP y el Protocolo de información de enrutamiento (RIP).

Capa de transporte

La capa de transporte se encarga de proporcionar comunicación de sesión y datagrama a la capa de aplicación de servicios . Los protocolos principales de esta capa son TCP y UDP. TCP proporciona un servicio de comunicaciones individual, fiable y orientado a la conexión. Es responsable de la secuenciación y detección de los paquetes enviados y de la recuperación de los paquetes perdidos en la transmisión. UDP proporciona un servicio de comunicaciones individual o grupal, sin conexión y poco fiable. Este se utiliza normalmente cuando la cantidad de datos a transferir es pequeña, como por ejemplo cuando estos caben en un solo paquete.

Capa de internet

La capa de Internet es responsable de las funciones de direccionamiento, empaquetado y enrutamiento del host. Los protocolos centrales de la capa de Internet son IP, Protocolo de resolución de direcciones (ARP), Protocolo de mensajes de control de Internet (ICMP) y Protocolo de administración de grupos de Internet (IGMP). En esta capa, el IP agrega la cabecera a los paquetes, lo que se conoce como dirección IP. En la actualidad existen tanto dirección IPv4 (32 bits) como dirección IP IPv6 (128 bits).

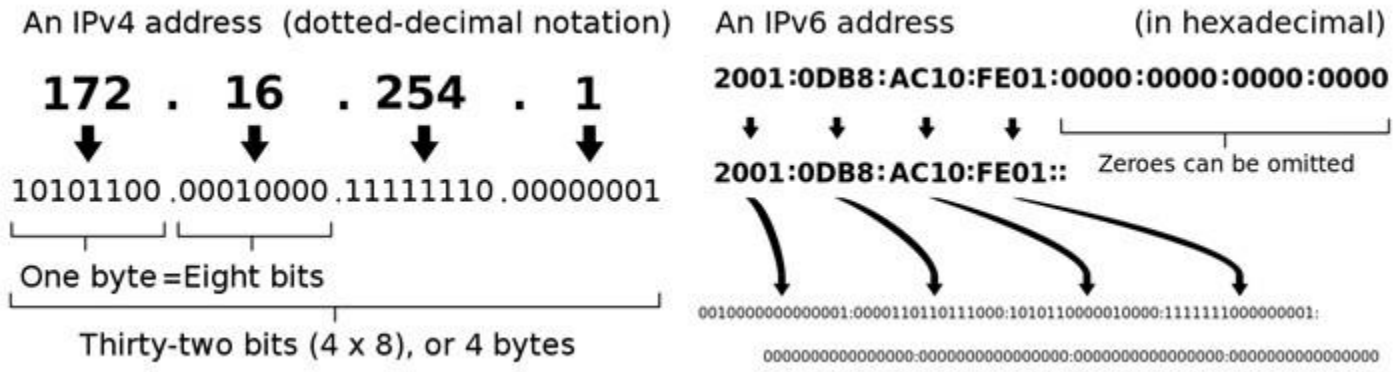


Figura 2: Dirección IPv4 y IPv6.

Capa de acceso a la red

La capa de acceso a la red (o capa de enlace) es responsable de colocar los paquetes TCP/IP en el portador de datos de la red y recibir los paquetes TCP/IP situados fuera del mismo. El protocolo TCP/IP está diseñado para ser independiente del método de acceso a la red, el formato de la trama de red y el potador. En otras palabras, este protocolo es independiente de cualquier tecnología de red específica, lo que hace que este se pueda utilizar para conectar diferentes tipos de red, como Ethernet, Token Ring y Modo de transferencia asíncrono (ATM).

¿Cómo se procesan los datos durante la transmisión?

En un sistema de capas, los dispositivos de una capa intercambian datos en un formato diferente, lo que se conoce como unidad de datos de protocolo (PDU). La siguiente tabla muestra las PDU en las diferentes capas.

Tipo de modelo	Capas del modelo OSI	Protocolo Unidad de datos (PDU)	Capas del modelo TCP/IP
Capas del host	Capa de aplicación	Datos	Capa de aplicación de datos
	Capa de presentación		
	Capa de sesión		
	Capa de transporte	Segmento de capa de transporte(TCP)/Datagrama (UDP)	Capa de transporte
Capas de medios/	Capa de red	Paquete	Capa de Internet
	Capa de enlace de datos	Trama	Capa de acceso a la red
	Capa física	Bit	

Por ejemplo, cuando un usuario solicita navegar por un sitio web en su ordenador, el software del servidor remoto primero entrega los datos solicitados a la capa de aplicación, donde se procesa de capa a capa con cada capa realizando sus funciones designadas. Los datos posteriormente se transmiten a través de la capa física de la red hasta ser recibidos por el servidor de destino u otro dispositivo. En este punto, los datos pasan nuevamente a través de las capas, cada capa realiza sus operaciones asignadas hasta que finalmente el software receptor utilice los datos.

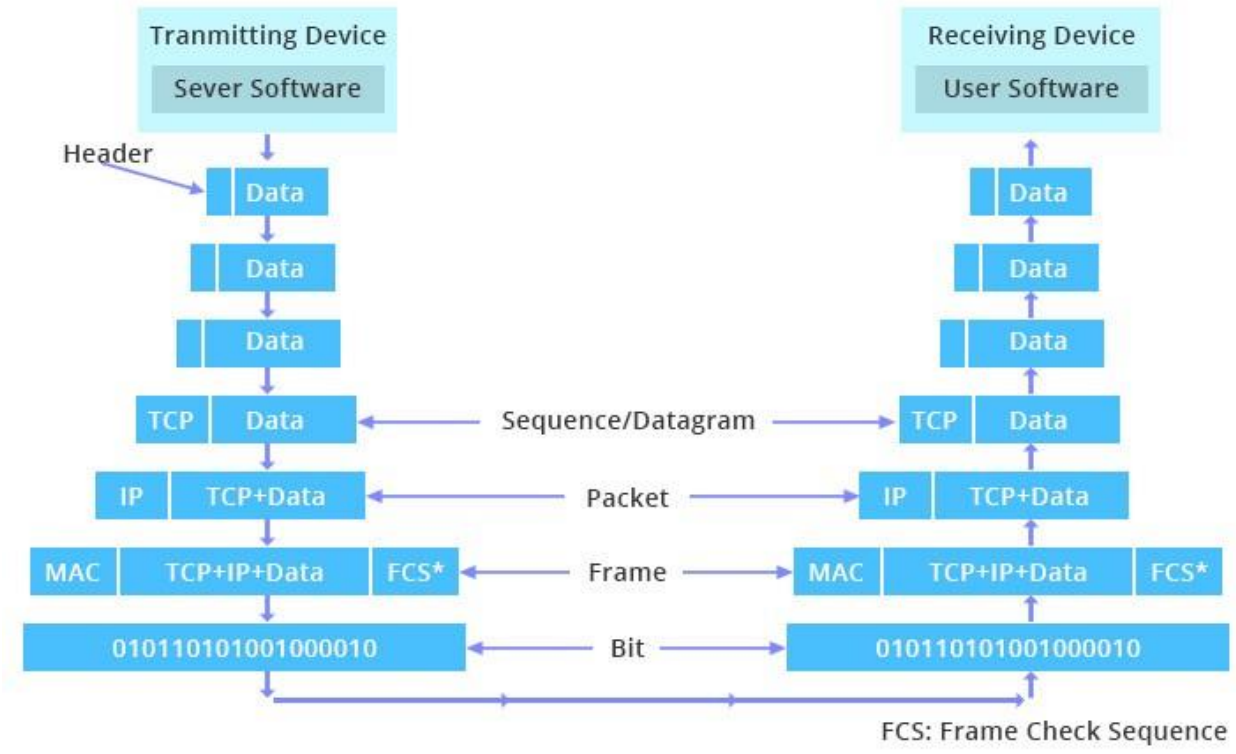


Figura 3: los datos fluyen desde las capas superiores a las capas inferiores, cada capa agrega una cabecera/pie de página a la PDU.

Durante la transmisión, cada capa agrega una cabecera, pie de página o ambos a la PDU proveniente de la capa superior, el cual dirige e identifica el paquete. Este proceso se llama encapsulación. La cabecera (y el pie de página) y el cuerpo forman la PDU para la siguiente capa. El proceso continúa hasta llegar a la capa de nivel más bajo (capa física o capa de acceso a la red), desde la cual los datos se transmiten al dispositivo receptor. El dispositivo receptor invierte el proceso,

desencapsulando los datos en cada capa con la información de la cabecera y pie de página que dirige las operaciones. Finalmente la aplicación utiliza los datos y el proceso continúa hasta que todos los datos son transmitidos y recibidos.

Gracias a que se conoce el funcionamiento de la división de capas, es posible diagnosticar el problema cuando una conexión falla . La clave es comprobar el funcionamiento desde el nivel más bajo, en lugar de desde el nivel más alto, ya que cada capa atiende a su capa immediatamente superior, por lo que será más fácil tratar los problemas de la capa inferior. Por ejemplo, si su ordenador no puede conectarse a Internet, lo primero que debe hacer es verificar si el cable de red está conectado al mismo o si el punto de acceso inalámbrico (WAP) está conectado al switch.

Modelo OSI y Modelo TCP/IP

El modelo TCP/IP es más antiguo que el modelo OSI. En la siguiente figura se muestra la correlación entre sus capas.

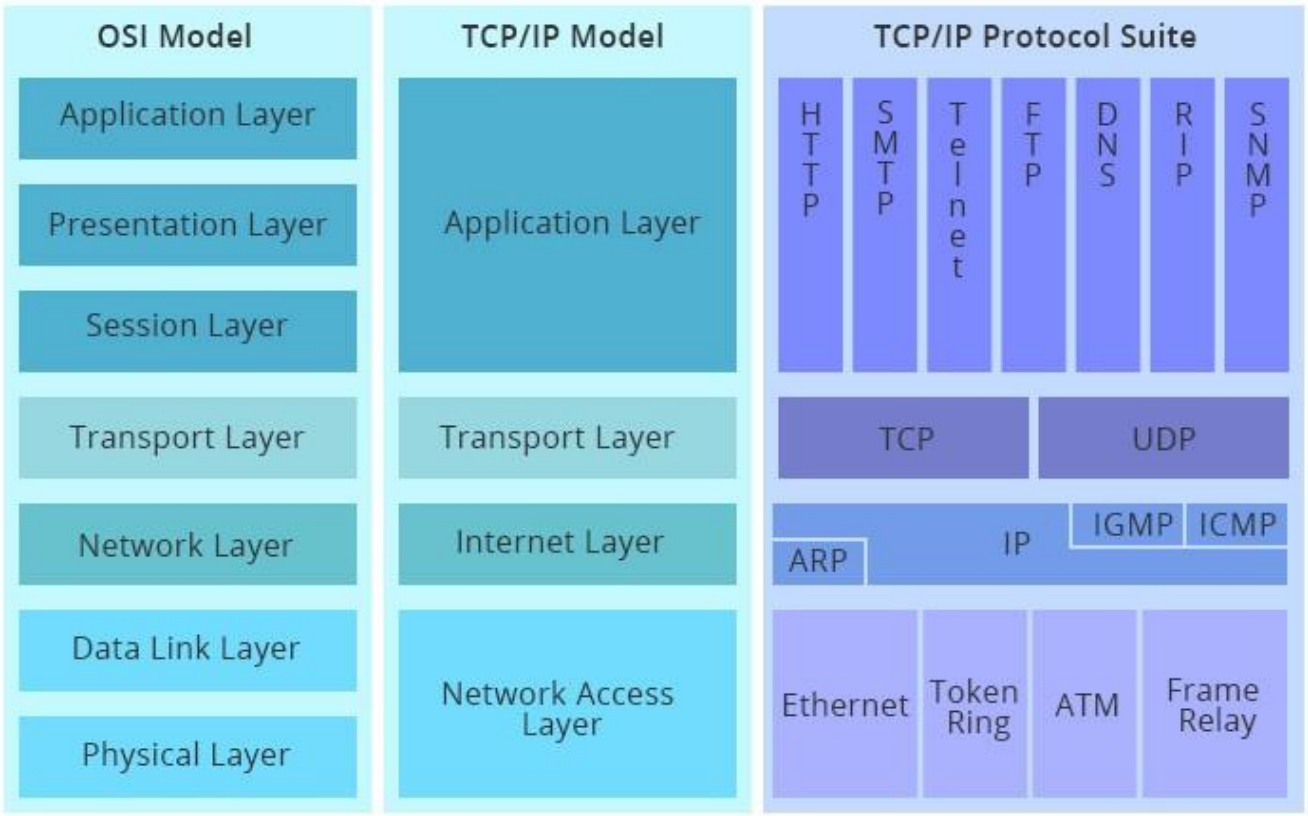


Figura 4: Modelo OSI frente a modelo TCP/IP y conjunto de protocolos TCP/IP.

Tras realizar la comparación entre las capas del modelo TCP/IP y el modelo OSI, se concluye que la capa de aplicación del modelo TCP/IP es similar a las capas OSI 5, 6, 7 combinadas, aunque el modelo TCP/IP no tiene la llamada capa de presentación o de sesión. La capa de transporte de TCP/IP abarca las responsabilidades de la capa de transporte OSI y algunas de las responsabilidades de la capa de sesión OSI. La capa de acceso a la red de TCP/IP abarca el enlace de datos y las capas físicas del modelo OSI. Tenga en cuenta que la capa de Internet de TCP/IP no aprovecha los

servicios de secuenciación y reconocimiento que pueden estar presentes en la capa de enlace de datos del modelo OSI. La responsabilidad es de la capa de transporte en el modelo TCP/IP.

Importancia de TCP/IP y OSI para la resolución de problemas

Si tenemos en cuenta los significados de los dos modelos de referencia, el modelo OSI sería solo un modelo conceptual; este se utiliza principalmente para describir, discutir y comprender funciones de red individuales. Sin embargo, TCP/IP está diseñado para resolver un conjunto específico de problemas y no para funcionar como una descripción de generación para todas las comunicaciones de red, tal y como lo hace el modelo OSI. El modelo OSI es genérico e independiente del protocolo, aunque la mayoría de los protocolos y sistemas se adaptan a él,; mientras que el modelo TCP/IP se basa en protocolos estándar desarrollados por Internet. Otro factor a tener en cuenta en el modelo OSI es que, para las aplicaciones más simples, no todas las capas son utilizadas. Si bien las capas 1, 2, 3 son obligatorias para cualquier comunicación de datos, también existen aplicaciones que pueden usar ciertas capas de interfaz expecíficas en lugar de las capas superiores habituales del modelo.

Resumen

El modelo TCP/IP y el modelo OSI son modelos conceptuales utilizados para la descripción de todas las comunicaciones de la red, a su vez, TCP/IP también es un protocolo importante que se utiliza en todas las operaciones de Internet. Generalmente, cuando hablamos de capa 2, capa 3 o capa 7 en las que funciona un dispositivo de red, nos referimos al modelo OSI. El modelo TCP/IP se usa tanto para modelar la arquitectura actual de Internet como para proporcionar un conjunto de reglas seguidas por todas las formas de transmisión a través de la red.

Una suite de protocolos es un conjunto de protocolos que nos ayudan desde las diferentes capas y servicios de la red a garantizar que la información viaja de un lugar a otro, de forma segura y confiable, algunos de estos sirven para garantizar que la información es entregada o no como lo son TCP y UDP.

En la siguiente clase estaremos hablando de los modelos de referencia para la transmisión de datos en Internet, el modelos OSI y el modelos TCP/IP. Veremos que son similares y una de las cosas por las que esto es así es porque los protocolos que ambos usan en sus capas son protocolos abiertos, de uso libre, de forma que pueden estar implementados en cualquier dispositivo de hardware o a través de software.

A continuación listo algunos de los protocolos usados en las diferentes capas de red y su funcionamiento:

De la capa de Acceso a la Red (TCP/IP) / Física + Enlace de Datos (OSI)

ARP

Es el protocolo que permite hacer la asignación de direcciones físicas y direcciones lógicas en el modelo OSI funciona en la capa de Enlace a Datos en la capa lógica.

Ethernet

Es el protocolo que nos permite definir los estándares relacionados con los medios cableados y la señalización en la capa física.

Controladores de NIC

Corresponde a la definición de los algoritmos que llevan las instrucciones a la máquina para recibir y enviar datos a través de la tarjeta de acceso a Internet del dispositivo.

Capa de Internet (TCP/IP) / Capa de Red (OSI)

IP

Protocolo de Internet, es el protocolo encargado de la asignación de direcciones lógicas a los dispositivos, recibe los segmentos de la capa de transporte y los direcciona a través de la red.

NAT

Network Address Translation, es te protocolo hace la traducción de direcciones IP privadas en direcciones IP públicas únicas globalmente.
Es un protocolo que permite a los routers enviar mensajes a través de Internet. Cada dispositivo en la red LAN sale a Internet a través de un dispositivo llamada Router que contiene un listado de direcciones IP privadas vs direcciones IP públicas.
Cuando un host quiere enviar un mensaje a un dispositivo externo el router determina a través de NAT a donde debe enviar.
Con el uso de direcciones IPv6 se espera que el uso de este protocolo no sea necesario ya que es posible asignar a cada host en en el mundo una dirección lógica única.

ICMP

Este protocolo apoya al protocolo IP proporcionando mensajes y notificaciones de error cuándo un mensaje no puede alcanzar su destino. Valida que el mensaje haya alcanzado su destino, valida también si la el tiempo de vida del mensaje ya ha sido superado entre otras cosas. Su labor es únicamente informar sobre el error sin ejecutar acción alguna para resolverlo.

Capa de Transporte (TCP/IP) / Capa de Transporte (OSI)

Los protocolos de esta capa son TCP y UDP, de ellos estaremos hablando mas adelante en el curso.

Capa de Aplicación (TCP/IP) / Capa de sesión + Capa de Presentación + Capa de Aplicación (OSI)

DNS

Domain Name System, es el protocolo encargado de hacer la traducción de direcciones IP (172.217.14.163) en textos que podamos leer y recordar fácilmente como www.google.com

DHCP

Es el protocolo encargado de asignar direcciones IP de forma dinámica a los dispositivos. Esta pendiente de liberar las direcciones cuando estás ya no están siendo usadas.

SMTP

Este es un protocolo de **envío** de correo, pongo en negrita la palabra porque este es precisamente su funcionamiento, tanto desde los hosts como desde los servidores, el protocolo SMTP es en encargado de enviar los mensajes.

POP

Junto con IMAP, POP es un protocolo encargado de la recepción de los mensajes en el dispositivo de destino. POP descarga los mensajes desde el servidor a tu pc y son eliminados del servidor. Si recibes un mensaje usando el protocolo POP ese mensaje puede ser consultado sin conexión a Internet luego de ser descargado al pc, pero si se borra de tu pc ya no hay manera de recuperarlo.

IMAP

El otro protocolo para recuperación de correo, en este caso los mails son revisados desde el servidor, de forma que se requiere conexión a Internet para leer los mensajes, puedes acceder a tus mails desde diferentes dispositivos y no tienes que preocuparte por la recuperación ya que el servidor realiza copias de seguridad para garantizar que el mail sigue disponible.

FTP/TFTP

Son protocolos para transferencia de archivos.

HTTP/HTTPS

Este es tal vez el protocolo que todos sabemos que es familiar, porque es el que usamos todo el tiempo siempre que estamos consultando información en internet. El protocolo HTTP es el conjunto de reglas que definen la forma en que son enviados los mensajes para el intercambio de texto a través de la red.

Segmentación, multiplexación, PDU (Protocol Data Unit)

Dos características que nos ayudan son el tamaño del mensaje y el formato del mensaje.

- La segmentación consiste en tomar un mensaje muy grande y dividirlo en mensajes más pequeños.
- La multiplexación es la combinación de dos o más canales de información en un solo medio de transición.

PDU Protocol Data Unit es una unidad que nos permite identificar la información a medida que es transmitida a través de las capas de red.

Recordemos que la capa Física y de medios de red es la que se encarga de hacer conexión entre dispositivos usando interfaces y direcciones físicas.

En esta capa contamos con varios dispositivos y vamos a ver cuáles son y sus diferencias.

El Switch

Es el dispositivo que nos permite realizar conexiones físicas entre hosts, el switch se encarga de filtrar y direccionar los paquetes a través de la red de área local LAN.

El switch permite la conexión entre dispositivos a través del medio cableado.

Existe otros dispositivo que nos permite hacer la conexión de manera casi igual, es el Hub, incluso pueden verse iguales, pero yo te recomiendo no usar este dispositivo.

Mientras el switch toma los paquetes que llegan y analiza las direcciones físicas de los hosts conectados para reenviar el paquete únicamente a su destinatario el hub envía el mensaje por todos los canales, sin tener en cuenta el direccionamiento.

El Access Point AP

Otro dispositivo de la capa física es el Access Point, este dispositivo es el encargado de realizar el enlace entre las redes cableadas y las redes inalámbricas. Nos permite crear redes LAN haciendo haciendo uso de las ondas de radio.

Capa de RED:
- Encargada de enrutar los datos a traves de diferentes redes
- Direccionamiento de paquetes
- Encapsular/Desencapsular paquetes

TTL Time To Live: Cantidad maxima de saltos por los que debe pasar un mensaje hasta que es rechazado (default 64)

Protocolo IP Asignación de direcciones IP, máscara de bits

El protocolo IP es el protocolo que básicamente nos permite hacer el direccionamiento y el enrutamiento de los mensajes a través de la red, a través de diferentes algoritmos, se encarga de trazar la ruta más eficiente para que los mensajes lleguen de un destino a otro.

Enrutamiento

Consiste en encontrar un camino que conecte una red con otro, ya vimos que esto se hace a través de la tabla de enrutamiento de los routers.

Direccionamiento

Se refiere a la forma en que se asignan las direcciones IP a los diferentes dispositivos, por ejemplo, la creación de subredes.

Direcciones IP

Es un identificador lógico de las interfaces de red de los dispositivos que utilizan protocolo IP para la comunicación.

IPv4 - 32 bits - 192.168.1.1
IPv6 - 128 bits - 2001:0D88:000A:0000:0000:0000:0000:1000

Se pueden clasificar en diferentes clases.

Clase A

• El primer octeto identifica la red
• Tres últimos octetos (24 bits) pueden ser asignados a los hosts
• Cantidad máxima de hosts es 224 - 2
• 167777214 hosts

Clase B

• Dos primeros octetos para identificar la red.
• Dos octetos finales (16 bits) para que sean asignados a los hosts
• Cantidad máxima de hosts por cada red es 216 – 2
• 65534 hosts

Case C

• Tres primeros octetos para identificar la red
• Octeto final (8 bits) para que sea asignado a los hosts
• Cantidad máxima de hosts por cada red es 28 – 2
• 254 hosts

Máscara de Subred

Nos permite identificar a simple vista la porción de la dirección IP que se ha asignado a la identificación de la red y la porción que se ha asignado a los hosts.

A - 255.0.0.0 o 11111111.00000000.00000000.00000000.00000000
B - 255.255.0.0 o 11111111.111111111.00000000.00000000.00000000
C - 255.255.255.0 o 11111111.11111111.111111111.00000000.00000000

Direcciones privadas: no se pueden enrutar a través de internet.
a. 10.0.0.0/8 a 10.255.255.255
b. 172.16.0.0/16 a 172.31.255.255
c. 192.168.0.0/24 a 192.168.255.255

Direcciones de loopback
127.0.0.0/8 127.255.255.254

Direcciones de Link Local
169.254.0.0/16 169.254.254.254

Test
192.0.2.0/24

En las redes de área local se asignan direcciones a los dispositivos que permiten la conexión entre ellos. Las direcciones privadas son aquellas que no se pueden enrutar a través de Internet.

Las direcciones IP públicas son aquellas que permiten la conexión a Internet.

Todos los dispositivos que están atrás de un mismo router tienen diferentes direcciones IP privadas únicas en ese segmento de red y una dirección pública que permite la conexión entre diferentes redes alrededor del mundo, esta dirección ip pública es la dirección del router.

El segmento de direcciones privadas se encuentra entre

10.0.0.0/8 a 10.255.255.255 que usualmente se asigna para redes con conexión inalámbrica ya que el rango es muy amplio y
192.168.0.0/16 a 192.168.255.255 que usualmente se asigna para redes conectadas por medio cableado, es importante resaltar que esto no implica ningún tipo de obligación o reserva de rangos, tu puedes asignar direcciones IP basándote en tus reglas de negocio.

IANA organización encargada de definir las direcciones que pertenecerán a cada región.
LANIC organiza las direcciones que le proporciono la IANA para entregarlas a los ISP de Latinoamérica.
ISP son los proveedores de Internet que reparte las direcciones IP entre sus clientes para el acceso a Internet.

Dirección de red: identifica toda la red con los bits de host todos en 0
Dirección de broadcast: dirección de difusión con todos los bits de host en 1 estas dos direcciones son las que se restan en el rango de host de red.

IP ejemplo: 183.26.103.215/30

IP en binarios: 10110111.00011010.01100111.11010111
Mascara de red: 11111111.11111111.11111111.11111100
Dirección de red: 10110111.00011010.01100111.11010100 (Se calcula haciendo una operación AND entre la IP y la máscara de red, en donde se observa que la dirección de red efectivamente en sus hosts solo tiene 0)

183.26.103.212 --> Dirección de Red
183.26.103.215–> Broadcast (Sus últimos binarios son 1)

Para el rango se hace un calculo de 2^n - 2, donde n son los bits destinados a la red (IPv4 = 32 bits, Máscara de IP ejemplo = 30 bits, 32 - 30 = 2 = n).

Subredes
Subredes nos permite dividir la red en varias mas pequeñas y así hacer la red más manejable, administrativamente.

Ejemplo de Subred
192.168.1.0/24 -> IP de clase C, hay dividir 4 subredes.
Se debe hacer el calculo de la mascara de red donde se elija un número que sea mayor a 4 en el resultado, nos da 3 y eso se suma a la mascara que teníamos actualmente, es decir queda una mascara de 27.

De los 8 bits que teníamos inicialmente (32 bits IPv4, 24 bits de la mascara, 32 -24 = 8) quedando 5 bits (por los 3 que usamos anteriormente para dividir las redes), nos quedan 30 IPs asignables.

Capa de Transporte

A esta capa llega la información de la capa de aplicación

Se encarga de definir cómo van a ser enviados los datos a través de la red, de asignar puertos y establecer esos protocolos que nos van a ayudar a que el mensaje sea enviado o que nos garantice que el mensaje llegue o no.

Tareas de la capa de Transporte

- Segmentar los datos
- Realizar el seguimiento de las conversaciones individuales
- Identificar las aplicaciones de acuerdo con el puerto

El protocolo TCP
Contrariamente a UDP, el protocolo TCP (Transmission Control Protocol) está orientado a conexión. Cuando una máquina A envía datos a una máquina B, la máquina B es informada de la llegada de estos, y confirma su buena recepción.

Aquí interviene el control CRC de datos, que se basa en una ecuación matemática que permite verificar la integridad de los datos transmitidos. De este modo, si los datos recibidos son corruptos, el protocolo TCP permite que los destinatarios soliciten al emisor que los vuelva a enviar.
El protocolo UDP
UDP (User Datagram Protocol) es un protocolo no orientado a conexión. Es decir, cuando una máquina A envía paquetes a una máquina B, el flujo es unidireccional. La transferencia de datos se realiza sin prevenir al destinatario (la máquina B), y el destinatario recibe los datos sin enviar una confirmación al emisor (la máquina A).

Capa de transporte. Es el cuarto nivel del modelo OSI encargado de la transferencia libre de errores de los datos entre el emisor y el receptor, aunque no estén directamente conectados, así como de mantener el flujo de la red.

La capa física, reciben la secuencia de 1 y 0 que llegan de la capa de enlace de datos, esa trama, la analiza, la convierte en ondas eléctricas o en ondas de radio que son enviadas físicamente a través de los medios, cable u ondas de radios.
Switch: Recibe la señal y la envia por cable, dispositivo de capa 2
Access point: Nos sirve para hacer redes lan
Para áreas más amplias WAN, necesitamos un router.
Todos los dispositivos que tengan acceso a internet, necesitan una NIC, Network Interface Card, se conecta a la Motherboard y le proporciona los puertos y todos los circuitos y algoritmos que le permite conectarse con los medios.

La capa física – Capa 1
Los datos son generados en las capas superiores de aplicación y sesión, pasan a la capa de transporte en la que son segmentados y pasan a los puertos y luego pasa a la capa de red, en la que esta información es empaquetada, se agregan unas cabeceras en las que nos va indicar las direcciones lógicas, desde donde va hacia donde llega. Esto es convertido a una trama, donde contiene informaciones físicas etc.
De la capa de enlace de datos, para la trama de bits a la capa física, esta define que tipo de señal va a ser enviada. Construye las señales y los envía a través del medio.
En el receptor, llega la señal, y es recibida por la capa física y la transforma en 1 y 0 y es desencapzulada hasta que el receptor pueda verla

Controlar componentes físicos.
Codificar/decodificar datos
Señalización

Capa de enlace de datos.
Se encarga de hacer la comunicación entre la física todo el hardware y la de red toda la parte lógica.
Para que esto pueda funcionar se usan 2 capas intermedias, tenemos una MAC que es la capa de acceso al medio físico esto es una dirección que identifica únicamente a las tarjetas de red de nuestros dispositivos.
LLC Logical Link Control
Capa de acceso lógico, nos permite transofrmar la información para que la capa de red pueda recibirla y pueda escalarla.
Funciones:
Gestión del canal
Segmentación de la trama
Control de errores
Control de flujo
Recuperación de fallos

Trama de ethernet
Conectar las capas entre