"The ultimate measure of a man is not where he stands in moments of comfort and convenience, but where he stands at times of challenge and controversy"

"La medida definitiva de un hombre no es dónde se encuentra en momentos de comodidad y conveniencia, sino dónde se encuentra en momentos de desafío y controversia."

"Martin Luther King, Jr" (1929 – 1968). Pastor Baptista y Líder del movimiento por los derechos civiles en E.U.A.

LUIS FELIPE GUTIÉRREZ CAMACHO

TALLER MODELOS DE COMUNICACIÓN RED

1. Modelos De Comunicación en las redes informáticas:

"Los modelos de comunicación en redes informáticas son marcos conceptuales que ayudan a entender y gestionar la comunicación entre dispositivos conectados en una red. Estos modelos proporcionan una estructura organizada para comprender cómo los datos se transmiten, reciben y procesan a través de los diferentes componentes de una red informática.

En un sentido más amplio, estos modelos describen las capas o niveles de abstracción que existen en una red y cómo interactúan entre sí para permitir la comunicación de manera efectiva. Por ejemplo, el Modelo OSI (Open Systems Interconnection) divide la comunicación en siete capas, cada una con funciones específicas, como la capa física que se ocupa de la transmisión de bits a través de medios físicos, o la capa de aplicación que maneja la interacción con las aplicaciones y servicios.

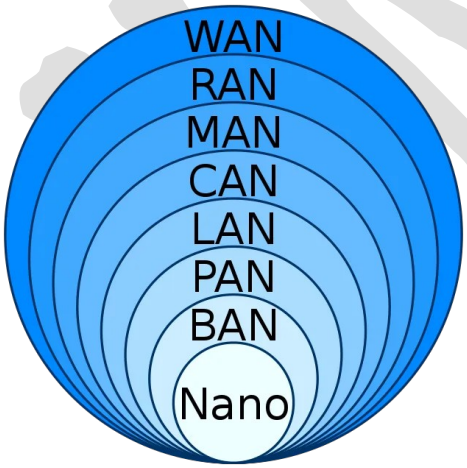
Estos modelos no solo sirven como herramientas para entender el funcionamiento interno de las redes, sino que también son fundamentales para el diseño, la implementación y el mantenimiento de sistemas de comunicación eficientes y seguros. Al seguir un modelo de comunicación específico, los ingenieros y administradores de redes pueden estructurar sus redes de manera más organizada y comprensible, facilitando así el diagnóstico y la resolución de problemas, así como la interoperabilidad entre diferentes sistemas y tecnologías de red."

2. **Tipos de modelos de comunicación, definición y funcionamiento:**

El Modelo OSI (Open Systems Interconnection) conceptualiza la comunicación en una red en siete capas: física, enlace de datos, red, transporte, sesión, presentación y aplicación. Cada capa tiene funciones específicas para garantizar una comunicación eficiente y confiable entre dispositivos.

El Modelo TCP/IP (Transmission Control Protocol/Internet Protocol) se enfoca en la conexión a redes como Internet, con cuatro capas principales: red, transporte, Internet y aplicación. Es fundamental para la comunicación en Internet y se usa ampliamente en todo el mundo.

El Modelo de referencia de interconexión de sistemas abiertos (OSIRM) también tiene siete capas: capa de usuario, capa de presentación, capa de sesión, capa de transporte, capa de red, capa de enlace de datos y capa física. Se centra en la comunicación entre sistemas abiertos.



El Modelo de red de área local (LAN) se enfoca en la comunicación dentro de una red de área local y suele incluir las capas física, de enlace de datos y de red. Se usa para describir cómo funcionan las redes locales en entornos como oficinas, hogares o campus.

El Modelo de red de área amplia (WAN) se centra en la comunicación en redes de área amplia, como las que conectan diferentes sucursales de una empresa o que abarcan grandes distancias geográficas. Incluye capas adicionales como la de transporte y aplicación.

3. **Protocolos De Comunicación:**

Protocolo de Internet (IP):

El Protocolo de Internet (IP) es uno de los pilares fundamentales de las redes informáticas. Se encarga de asignar direcciones únicas a los dispositivos (direcciones IP) y de enrutar los paquetes de datos a través de la red. Esto permite que los dispositivos se comuniquen entre sí y compartan información de manera eficiente.

IP opera en la capa de red del modelo OSI (Open Systems Interconnection) y es el protocolo más utilizado en Internet y en las redes locales. Hay dos versiones principales de IP: IPv4 (Internet Protocol version 4) e IPv6 (Internet Protocol version 6).

IPv4 es el protocolo IP original y utiliza direcciones IP de 32 bits, lo que permite un total de aproximadamente 4.3 mil millones de direcciones únicas. Sin embargo, debido al crecimiento exponencial de dispositivos conectados a Internet, el espacio de direcciones IPv4 se ha agotado en gran medida, lo que llevó al desarrollo de IPv6.

IPv6 es la versión más reciente de IP y utiliza direcciones IP de 128 bits, lo que proporciona un vasto espacio de direcciones (aproximadamente 340 sextillones de direcciones únicas). Esto resuelve el problema de escasez de direcciones IP y permite la expansión de Internet y la conectividad de una amplia gama de dispositivos, incluidos dispositivos IoT (Internet of Things) y sistemas embebidos.

El funcionamiento básico del Protocolo de Internet implica la segmentación de datos en paquetes, cada uno con una dirección IP de origen y destino. Estos paquetes son enviados a través de la red utilizando dispositivos como routers, que utilizan tablas de enrutamiento para determinar la mejor ruta hacia su destino final.

Protocolo de Control de Transmisión (TCP):

El Protocolo de Control de Transmisión (TCP) garantiza una comunicación confiable y orientada a la conexión entre dispositivos. Divide los datos en segmentos, establece conexiones y verifica la entrega correcta de los datos. También gestiona la retransmisión de datos perdidos y el control de flujo para evitar congestiones en la red.

Protocolo de Datagrama de Usuario (UDP):

A diferencia de TCP, el Protocolo de Datagrama de Usuario (UDP) ofrece una comunicación no confiable y sin conexión. Es más rápido pero menos confiable, siendo útil para aplicaciones como videojuegos, transmisiones en tiempo real y servicios de voz sobre IP (VoIP), donde la velocidad es prioritaria sobre la fiabilidad.

Protocolo de Transferencia de Hipertexto (HTTP):

El Protocolo de Transferencia de Hipertexto (HTTP) es un protocolo de aplicación utilizado para la transferencia de información en la World Wide Web. Se basa en el modelo cliente-servidor, donde un cliente (generalmente un navegador web) realiza solicitudes a un servidor web para obtener recursos, como páginas HTML, imágenes, archivos de estilo, scripts y otros elementos web.

HTTP es un protocolo sin estado, lo que significa que cada solicitud se procesa de forma independiente sin tener en cuenta las solicitudes anteriores. Esto simplifica la implementación del protocolo, pero también implica que el servidor no mantiene información sobre el estado de la comunicación entre solicitudes.

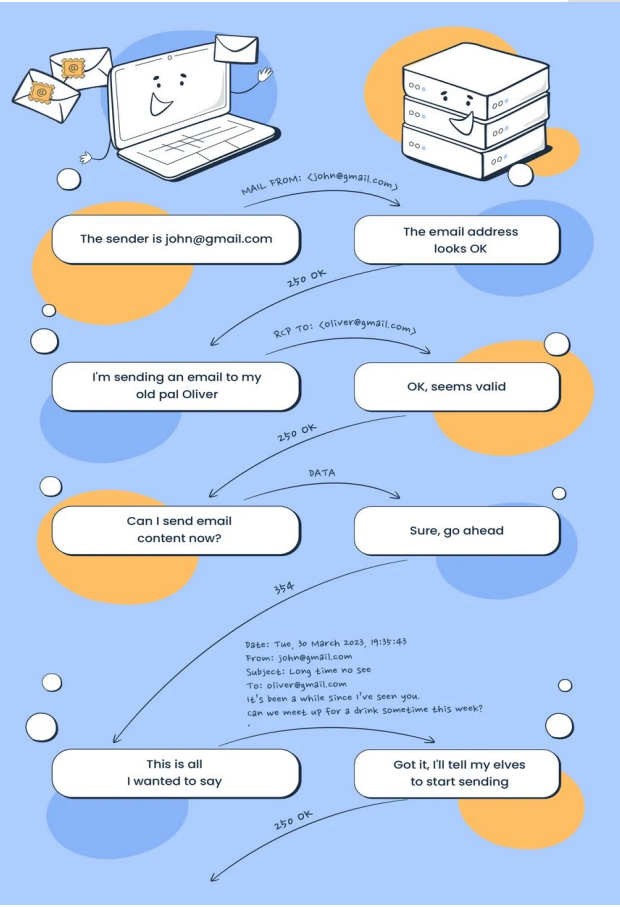
El protocolo define varios métodos de solicitud que indican la acción que el cliente desea realizar en el recurso especificado. Algunos de los métodos comunes son **GET** (solicitar la recuperación de un recurso), **POST** (enviar datos para ser procesados por el servidor), **PUT** (actualizar un recurso en el servidor), **DELETE** (eliminar un recurso en el servidor) y **HEAD** (solicitar información sobre un recurso sin obtener el contenido completo).

HTTP utiliza códigos de estado para indicar el resultado de una solicitud. Algunos códigos de estado comunes son 200 OK (la solicitud se completó correctamente), 404 Not Found (el recurso solicitado no se encuentra en el servidor), 500 Internal Server Error (error interno en el servidor al procesar la solicitud) y 302 Found (redirección temporal a otra URL).

Los mensajes en HTTP están basados en texto legible por humanos, con encabezados y contenido del mensaje. Sin embargo, la versión estándar de HTTP (HTTP/1.1) no proporciona cifrado de datos por sí misma, lo que significa que la información enviada a través de HTTP puede ser interceptada y leída por terceros. Para la seguridad de la información, se utiliza HTTPS (HTTP Secure), que es una versión cifrada y segura de HTTP que utiliza el protocolo SSL/TLS para proteger los datos transmitidos.

Protocolo de Transferencia de Archivos (FTP):

El Protocolo de Transferencia de Archivos (FTP) permite la transferencia de archivos entre un cliente y un servidor a través de una conexión de red. Proporciona funciones para subir, descargar, eliminar y administrar archivos en un servidor remoto, utilizando dos canales de comunicación separados para comandos y transferencia de datos.



Protocolo Simple de Correo (SMTP):

El Protocolo Simple de Correo (SMTP) se emplea para enviar correos electrónicos entre clientes de correo y servidores de correo. Define cómo se transmiten y entregan los mensajes de correo electrónico entre diferentes servidores y destinatarios, asegurando una entrega confiable de los correos.

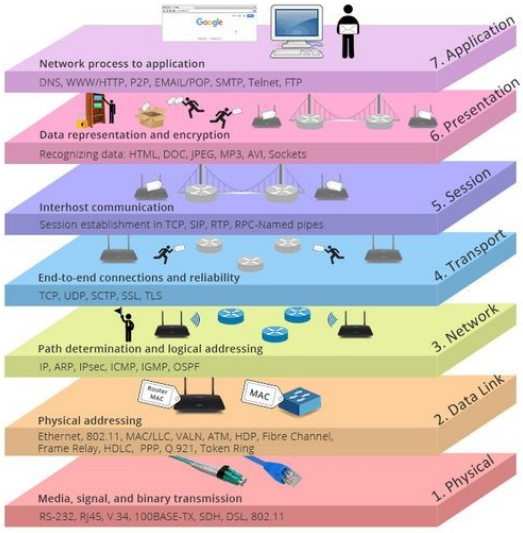
Protocolo de Acceso a Mensajes de Internet (IMAP):

El Protocolo de Acceso a Mensajes de Internet (IMAP) permite a los clientes de correo acceder y gestionar mensajes almacenados en un servidor de correo. Ofrece funcionalidades avanzadas como la capacidad de leer correos electrónicos sin descargarlos, organizar carpetas y sincronizar cambios entre dispositivos.

Protocolo de Control de Transmisión/Servicio de Mensajes en Tiempo Real (TCP/SIP):

El Protocolo de Control de Transmisión/Servicio de Mensajes en Tiempo Real (TCP/SIP) se utiliza para establecer y gestionar sesiones de comunicación en tiempo real, como llamadas de voz sobre IP (VoIP) y videoconferencias. Define cómo se inician, mantienen y finalizan las sesiones de comunicación entre dispositivos, permitiendo una comunicación eficiente y confiable en tiempo real.

4. Protocolos De Comunicación Según El Modelo OSI:



Capa de Aplicación (Capa 7):

HTTP (Protocolo de Transferencia de Hipertexto): Utilizado para la transferencia de páginas web y recursos en la World Wide Web.

FTP (Protocolo de Transferencia de Archivos): Permite la transferencia de archivos entre un cliente y un servidor.

SMTP (Protocolo Simple de Correo): Empleado para enviar correos electrónicos entre clientes y servidores de correo.

Capa de Presentación (Capa 6):

SSL/TLS (Secure Sockets Layer/Transport Layer Security): Proporciona seguridad en la comunicación, cifrando los datos para garantizar la privacidad y autenticidad.

Capa de Sesión (Capa 5):

NetBIOS (Sistema Básico de Entrada/Salida en Red): Facilita la comunicación entre dispositivos en una red, permitiendo la identificación y establecimiento de sesiones.

Capa de Transporte (Capa 4):

TCP (Protocolo de Control de Transmisión): Ofrece una comunicación confiable y orientada a la conexión, dividiendo los datos en segmentos y garantizando la entrega ordenada.

UDP (Protocolo de Datagrama de Usuario): Proporciona una comunicación no confiable y sin conexión, útil para aplicaciones que requieren velocidad sobre fiabilidad.

Capa de Red (Capa 3):

IP (Protocolo de Internet): Esencial para la comunicación en redes, asigna direcciones únicas a los dispositivos y enruta los paquetes de datos.

Capa de Enlace de Datos (Capa 2):

Ethernet: Protocolo comúnmente utilizado para la comunicación en redes locales (LAN), define cómo se transmiten los datos a través de cables o medios físicos.

PPP (Protocolo de Punto a Punto): Utilizado para establecer conexiones punto a punto, como conexiones de línea telefónica.

Capa Física (Capa 1):

RS-232 (Interfaz Serie): Define la comunicación serie entre dispositivos a través de cables.

Ethernet físico: Estándares que especifican la conexión física de los dispositivos en una red, como Ethernet 10/100/1000 Mbps.