COMUNICACIONES

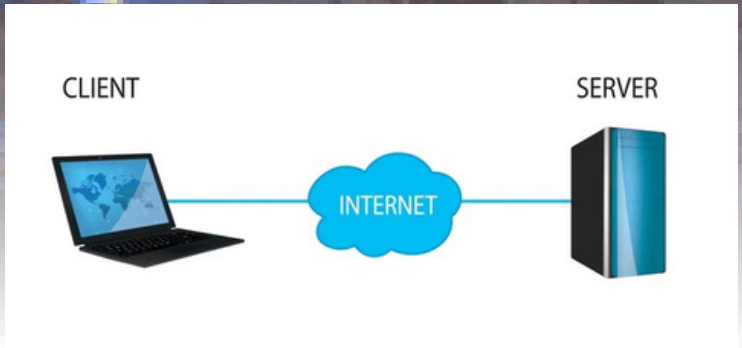
UDS
Mi Universidad

ALUMNO:ERICK DANIEL GALLEGOS LOPEZ

DOCENTE: LUIS ALBERTO ALTUZAR GARCIA

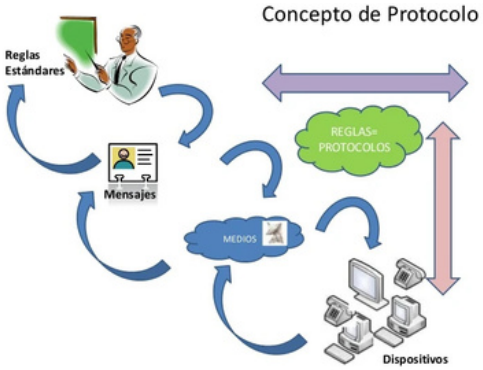
CONCEPTOS:

Protocolos de comunicación
Modelo OSI y TCP/IP
TCP vs UDP
Puertos y sockets
Comunicación cliente-servidor



PROTOCOLOS DE COMUNICACIÓN

Los protocolos de comunicación son un conjunto de reglas y convenciones que determinan cómo dos o más dispositivos se comunican entre sí para compartir información. Son esenciales para la transmisión y recepción correcta de datos en redes, Internet y sistemas de comunicación en general.



Los protocolos de red son las reglas que permiten la comunicación entre dispositivos en una red. Existen muchos tipos de protocolos, algunos importantes son: TCP/IP, HTTP, FTP, SSH, UDP, SNMP, IPsec, VPN, SSL/TLS, y otros más.

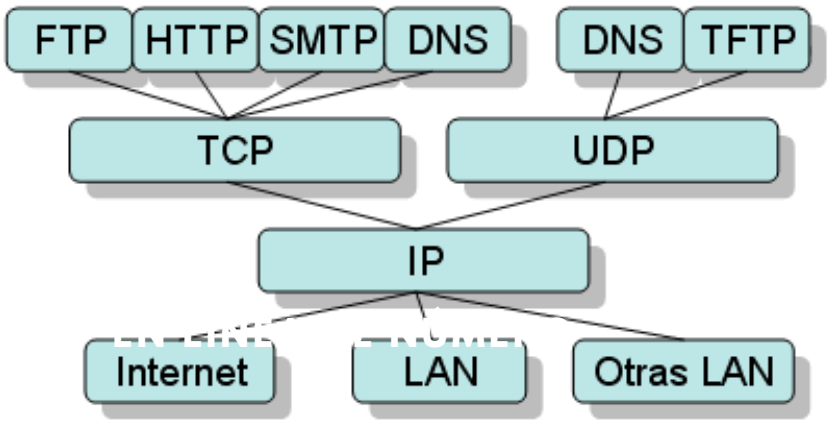
Caracteristicas

Definición de reglas: Establece como deben estructurarse los mensaje, como se codifican los datos, como se gestionan los errores y como se establece conexion

Estandarización: permite que dispositivos de distintos fabricantes se compartan informacion de manera compatible

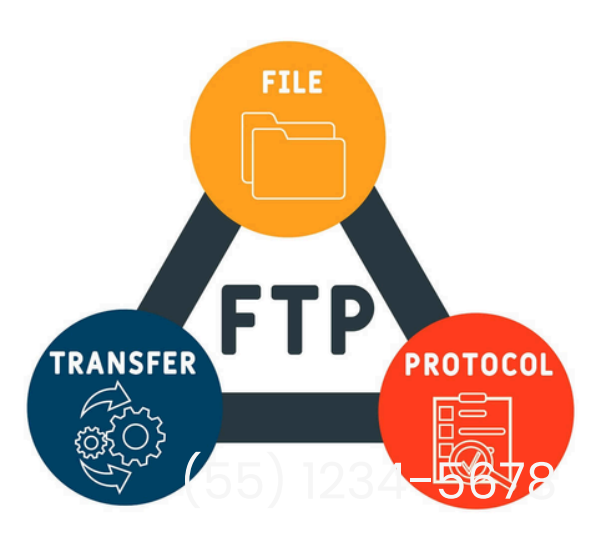
Escalabilidad: se puede adaptar a diferentes tipos de red o aplicaciones , dede redes locales hasta redes mundiales

fiabilidad: Garantizan que la información se transmite de manera correcta y completa, evitando errores y pérdidas de datos.



AQUI ALGUNOS DE LOS TIPOS DE COMUNICACION MAS CONOCIOS O USADOS

- **TCP/IP: ES EL PROTOCOLO FUNDAMENTAL DE INTERNET, UTILIZADO PARA LA COMUNICACIÓN ENTRE DISPOSITIVOS EN LA RED.**
- HTTP: EL PROTOCOLO WEB, QUE PERMITE LA COMUNICACIÓN ENTRE NAVEGADORES Y SERVIDORES WEB.
- SMTP: EL PROTOCOLO DE CORREO ELECTRÓNICO, QUE PERMITE EL ENVÍO Y RECEPCIÓN DE CORREOS ELECTRÓNICOS.
- FTP: EL PROTOCOLO DE TRANSFERENCIA DE ARCHIVOS, QUE PERMITE LA TRANSFERENCIA DE ARCHIVOS ENTRE COMPUTADORAS.
- UDP: UN PROTOCOLO DE TRANSPORTE MÁS RÁPIDO QUE TCP, PERO MENOS FIABLE.
- DHCP: EL PROTOCOLO QUE ASIGNA DIRECCIONES IP A LOS DISPOSITIVOS EN UNA RED.
- USB: UN PROTOCOLO DE COMUNICACIÓN SERIE UTILIZADO PARA CONECTAR DISPOSITIVOS A COMPUTADORAS.
- HART: UN PROTOCOLO DE COMUNICACIÓN UTILIZADO EN LA AUTOMATIZACIÓN INDUSTRIAL.
- UN PROTOCOLO DE COMUNICACIÓN LIGERO UTILIZADO EN EL INTERNET DE LAS COSAS (IOT).
- COAP: OTRO PROTOCOLO DE COMUNICACIÓN UTILIZADO EN EL IOT, SIMILAR A HTTP, PERO MÁS LIGERO Y EFICIENTE

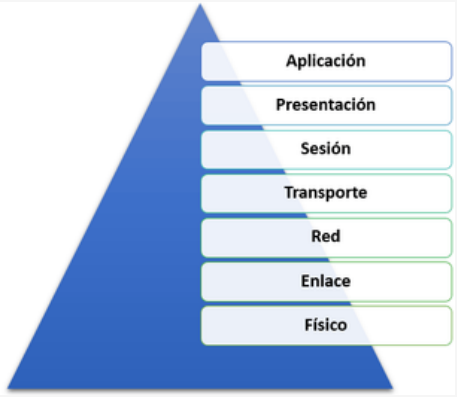


MODELO OSI

¿QUE ES ?

El modelo Open Systems Interconnection (OSI) es un modelo conceptual creado por la Organización Internacional para la Estandarización, el cual permite que diversos sistemas de comunicación se conecten usando protocolos estándar.

El modelo OSI se puede ver como un lenguaje universal para la conexión de las redes de equipos. Se basa en el concepto de dividir un sistema de comunicación en siete capas abstractas, cada una apilada sobre la anterior.



NIVELES DEL MODELO OSI

- capa 1: capa fisica:
  La capa física implica el equipo físico que transfiere datos, como conmutadores y cables. En esta capa, los datos se convierten en cadenas de 1 en 1 y 0 en 0. En la capa física, los dispositivos tienen que acordar un método para distinguir los 1 de los 0, lo que permite que los datos digitales sean interpretados adecuadamente por cada dispositivo.
- capa 2: capa de enlace de datos: La capa de enlace de datos es como la capa de red, excepto que la capa de enlace de datos facilita la transferencia de datos entre dos dispositivos que utilizan la misma red. En la capa de enlace de datos, los paquetes se dividen en piezas denominadas marcos.
  Dentro de la capa de enlace de datos, tiene dos subcapas, las capas de control de acceso a v medios (MAC) y control de enlace lógico (LLC).

- capa 3: capa de red:

a capa de red facilita la transferencia de datos cuando dos redes se comunican entre sí. Si dos dispositivos de comunicación utilizan la misma red, entonces no hay necesidad de la capa de red.
La capa de red divide los segmentos que provienen de la capa de transporte. Estos se denominan paquetes. La división de los segmentos en paquetes ocurre en el dispositivo del remitente y se vuelven a ensamblar en el dispositivo receptor.
La capa de red también funciona como una herramienta de eficiencia. Descubre la ruta física óptima necesaria para llevar los datos a su destino. Esta función se denomina “enrutamiento”.

- capa 4: capa de transporte :

La capa de transporte maneja la comunicación de extremo a extremo entre los dispositivos que interactúan entre sí. La gestión de la comunicación implica tomar los datos en la capa de sesión y dividirlos en partes denominadas segmentos. La capa de transporte en el dispositivo que recibe la comunicación maneja el reensamblaje de los segmentos en datos que es consumible por la capa de sesión.
La capa 4 es donde funcionan los números de puerto del **Protocolo de control de transmisión (TCP)** y del **Protocolo de datagrama de usuario (UDP)**. Las direcciones de protocolo de Internet (IP) operan en la capa 3, la capa de red. TCP, UDP e IP son protocolos que facilitan la forma en que se envían y reciben los datos.

NIVELES DEL MODELO OSI

- capa 5: capa de sesión :

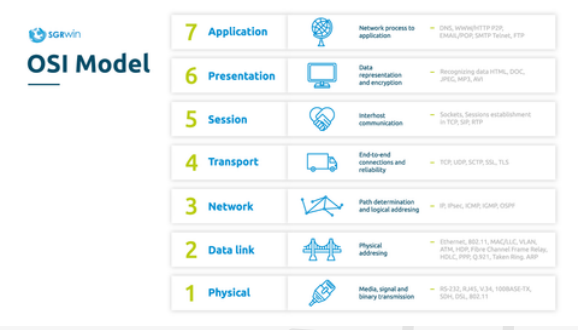
La capa de sesión maneja la apertura y el cierre de las comunicaciones de red entre dos dispositivos que interactúan. La “sesión” se refiere al tiempo entre la apertura y el cierre de la interacción. La capa de sesión se asegura de que la sesión esté abierta durante un período suficiente para que se envíen todos los datos necesarios. Luego, la capa de sesión cierra la sesión para evitar gastar recursos innecesarios.

- capa 6: capa de presentacion : La capa de presentación se encarga de preparar los datos para la capa de aplicación. Los dos dispositivos que se comunican pueden utilizar diferentes métodos de codificación de sus datos. Por lo tanto, la capa 6 convierte los datos entrantes en algo que se puede leer en la capa de la aplicación. Esto incluye cifrar y descifrar datos.

La capa de presentación también comprime los datos que provienen de la capa de aplicación antes de enviarlos a la capa 5, la capa de sesión.

- capa 7: capa de aplicación:

capa de aplicación es la más cercana al usuario final. Inicia la comunicación entre el usuario y las aplicaciones con las que interactúa personalmente. En esta capa, los datos se traducen de la sintaxis a la que se convirtió en algo que el usuario puede leer.
Algunos ejemplos de aplicaciones de capa 7 incluyen un navegador web como Chrome, Safari o Firefox, o una aplicación de correo electrónico. La capa 7 también puede identificar socios de comunicación, verificar qué recursos están disponibles y asegurarse de que la comunicación esté sincronizada correctamente.

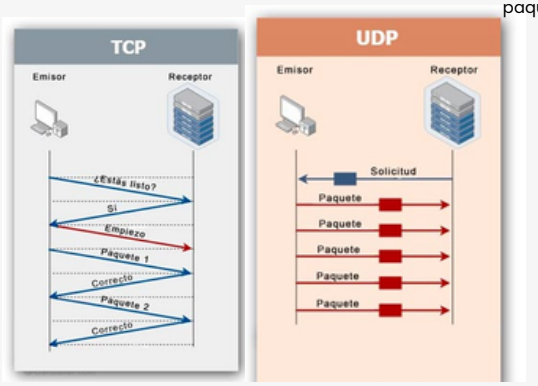


TCP vs UDP

TCP

El UDP es más rápido pero menos fiable que el TCP, otro protocolo de transporte habitual. En una comunicación TCP, los dos ordenadores comienzan estableciendo una conexión mediante un proceso automatizado llamado "protocolo de enlace".

- tipo de conexion : requiere una conexion establecida antes de transmitir datos
- secuencia de datos: puede secuenciar datos (enviarlos en un orden especifico)
- retransmisión de datos: puede retransmitir datos si los paquetes no llegan
- entrega: la entrega es garantizada
- comprobar errores: una verificacio exhaustiva de errores garantiza que los datos lleguen en el estado previsto
- radiodifucion: no soportado
- velociadad: entrega de datos lenta pero segura



UDP

el UDP es un método estandarizado para transferir datos entre dos ordenadores en una red. Comparado con otros protocolos, el UDP realiza este proceso de forma sencilla: envía paquetes (unidades de transmisión de datos) directamente a un ordenador de destino, sin establecer primero una conexión, ni indicar el orden de dichos paquetes, ni comprobar si han llegado como estaba previsto. (Los paquetes UDP se llaman "datagramas").

- tipo de conexion : no nesesita conexion para iniciar y finalizar una transferencia de datos
- secuencia de datos: no se puede secuenciar ni organizar los datos
- retransmisión de datos: no se transmiten datos- no se puede recuperar datos perdidos
- entrega: la entrega no esta garantizada
- comprobar errores: la verificacion minima de errores cubre los aspectos basicos, pero puede que no evite todos los errores.
- radiodifucion: apoyado
- velociadad: datos, pero con riesgos de datos incompletos

Puertos y sockets

En las redes, los puertos y sockets son componentes clave para la comunicación entre dispositivos. Los puertos son números que identifican un proceso o aplicación específica en un equipo, mientras que los sockets son los puntos finales de comunicación que incluyen la dirección IP y el número de puerto, permitiendo la transmisión de datos entre dispositivos.

puerto

La funcione del puerto es funguir como identificadores logicos para las aplicaciones que utilizan una red estospuertos igual cuentan con un alcance que va
de los puertos van del 0 al 65535.
ya que venimos hablando de comunicaciones de red y ya tenemos el concepto de http deberías de saber lo siguiente, algunos servicios que usamos ya tienen un puerto asignado, lo cuales nos frindan accesibilidad y seguridad que ahí estará el sitio ejemplo: como HTTP (80), HTTPS (443) y FTP (21). estos puertos solo abarcan del 0 - 1023

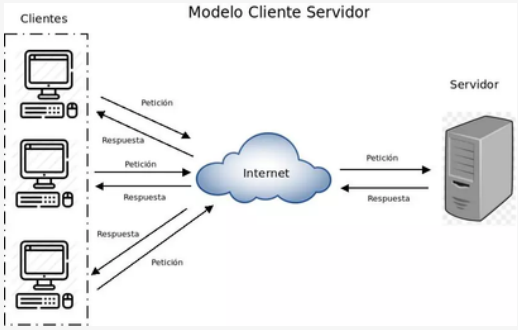
stock

ojo: los puertos encima del 1023 puedes ser usados temporalmente por aplicaciones ya que aun no han sido ocupados

Un socket es una combinación de la dirección IP de un dispositivo y el número de puerto utilizado por una aplicación.
Los sockets actúan como puntos finales de comunicación, permitiendo a las aplicaciones intercambiar datos. existen dos tipo de stock TCP y UDP.
que se utilizan con protocolos de transporte específicos. los cuales tienen sus propias ventajas ya sea por seguridad o velocidad
Una dirección de socket suele incluir el protocolo de transporte, la dirección IP de origen y destino, y los puertos de origen y destino.

comunicación cliente-servidor

La comunicación cliente-servidor es un modelo fundamental en redes y sistemas distribuidos donde un cliente solicita servicios a un servidor, que a su vez los proporciona. Este modelo permite la interacción entre dispositivos, facilitando tareas como la navegación web, el envío de correo electrónico y el acceso a bases de datos.



tipos de requisitos o de reglas para lograr la comunicación cliente-servidor o mejor conocidos como tipos de clave de cliente- servidor

Comunicación sincrónica

La comunicación síncrona se produce en tiempo real, lo que requiere que tanto el cliente como el servidor estén disponibles simultáneamente. Se caracteriza por respuestas inmediatas y es crucial para aplicaciones que exigen un intercambio de datos oportuno.

uso:

- Interacción en tiempo real
- Retroalimentación inmediata
- Ideal para aplicaciones sensibles al tiempo

ventajas

- Interacción en tiempo real
- Retroalimentación inmediata
- Ideal para aplicaciones sensibles al tiempo

Claves Asimétricas

- Utilizan un par de claves: una clave pública para cifrar y una clave privada para descifrar.
-
- Son más seguras para la transmisión de datos, porque la clave pública puede ser compartida libremente, mientras que la clave privada debe ser guardada por el usuario.
-
- Se utilizan para la autenticación, el cifrado y la firma digital de datos.