ST0255
Telemática

Escuela de Ciencias Aplicadas e Ingeniería

2024-2

Fundamentos de protocolos

Organizaciones comunes de estandarización de protocolos

UNIVERSIDAD EAFIT

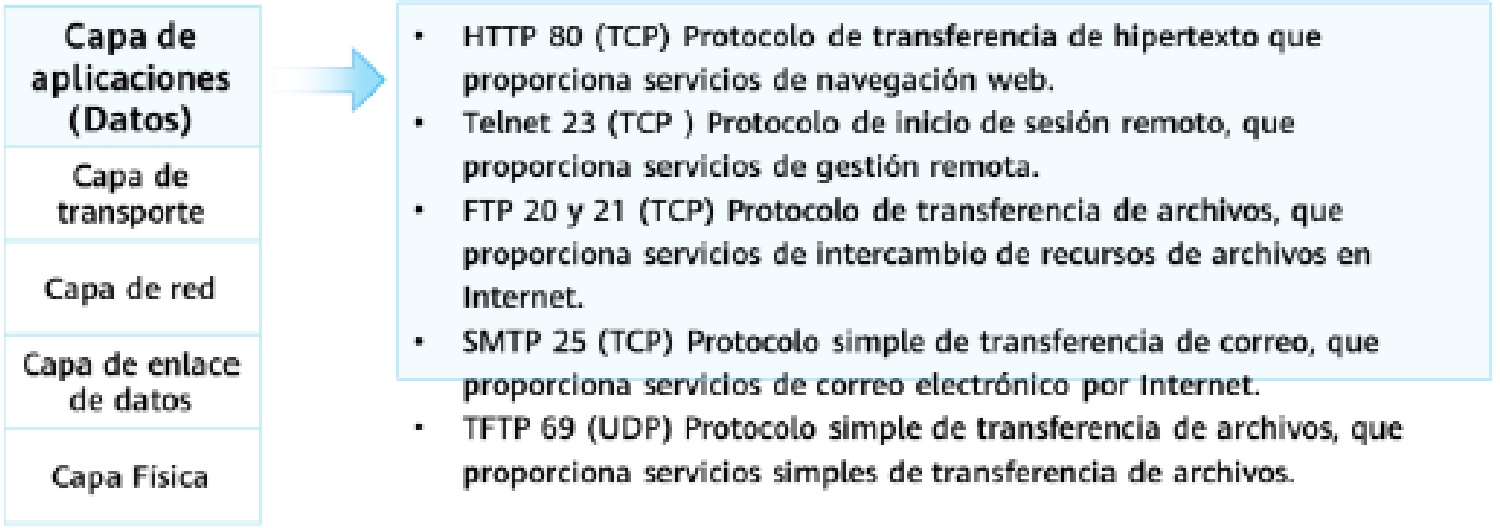
- Grupo de trabajo sobre ingeniería de Internet (IETF)
- Instituto de Ingenieros Eléctricos y Electrónicos (IEEE)
- Organización Internacional de Normalización (ISO)

Capa de aplicaciones

UNIVERSIDAD EAFIT

- La capa de aplicación proporciona interfaces para el software de aplicación de modo que las aplicaciones puedan utilizar servicios de red. El protocolo de la capa de aplicación designa los protocolos y puertos de la capa de transporte.

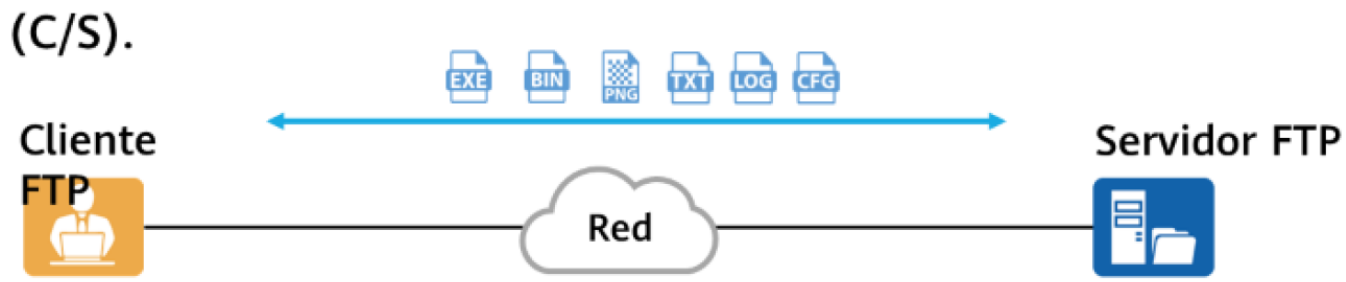
- Las PDU transmitidas en la capa de red se denominan datos.



Protocolos comunes de la Capa de aplicación - FTP

UNIVERSIDAD EAFIT

- El protocolo de transferencia de archivos (FTP) transfiere archivos de un host a otro para implementar la descarga y carga de archivos. Este protocolo adopta la estructura cliente/servidor (C/S).



Cliente FTP: Proporciona comandos para que los usuarios locales operen archivos en un servidor remoto. Un usuario puede instalar un programa cliente en un ordenador y establecer una conexión con un servidor FTP para operar los archivos en el servidor.

Servidor FTP: Dispositivo que ejecuta el servicio FTP. Proporciona las funciones de acceso y operación para los clientes remotos, permitiendo a los usuarios acceder al servidor FTP a través del programa cliente FTP y acceder a los archivos en el servidor.

Protocolos comunes de la Capa de aplicación - FTP

UNIVERSIDAD EAFIT

- Ejemplo 1: **Buscar servidores FTP públicos**

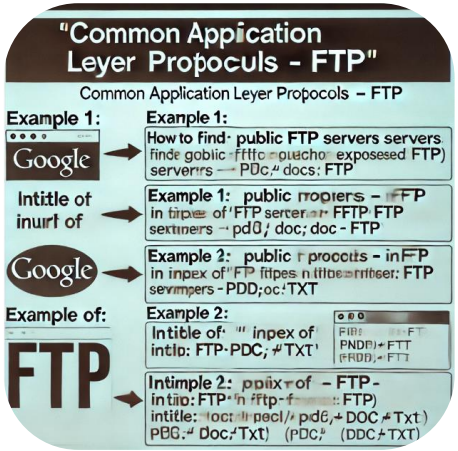
Esta búsqueda muestra directorios públicos de FTP indexados por Google. Puedes encontrar directorios que contienen archivos y carpetas expuestos al público.

intitle:"index of" inurl:ftp

- Ejemplo 2: **Buscar archivos específicos en servidores FTP**

Busca archivos PDF, DOC, o TXT en servidores FTP. Puedes cambiar los tipos de archivos según tus necesidades.

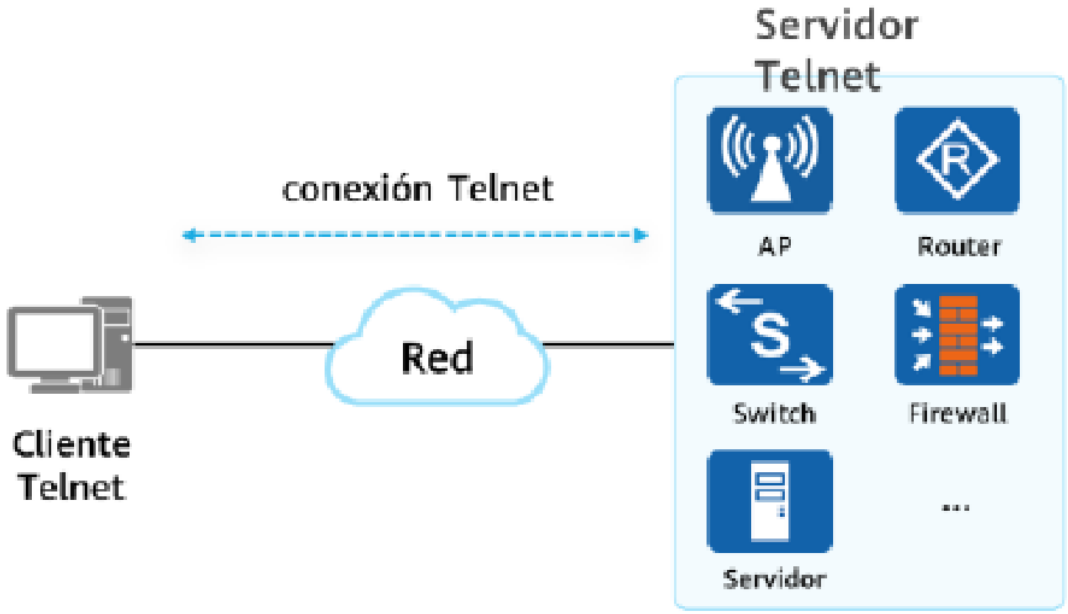
intitle:"index of" inurl:ftp inurl:(pdf|doc|txt)



Protocolos comunes de la Capa de aplicación - Telnet

UNIVERSIDAD EAFIT

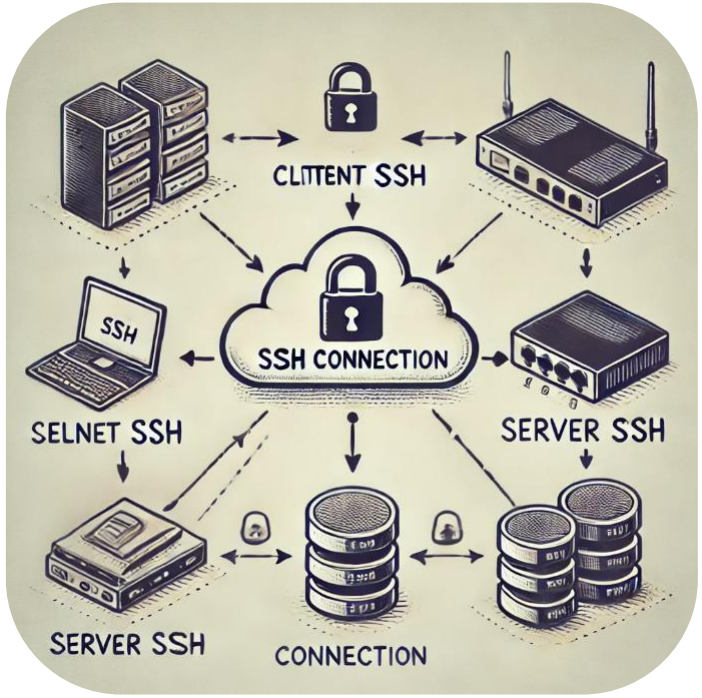
- Telnet es un protocolo estándar que proporciona servicios de inicio de sesión remoto en una red. Proporciona a los usuarios la capacidad de operar dispositivos remotos a través de PC locales.



Protocolos comunes de la Capa de aplicación - SSH

UNIVERSIDAD EAFIT

- SSH (Secure Shell) es un protocolo que permite el acceso remoto seguro a sistemas y servidores, cifrando la comunicación para proteger la transferencia de datos.



Protocolos comunes de la Capa de aplicación - HTTP

UNIVERSIDAD EAFIT

- Protocolo de transferencia de hipertexto: es uno de los protocolos de red más utilizados en Internet.

Protocolos comunes de la Capa de aplicación - HTTPS

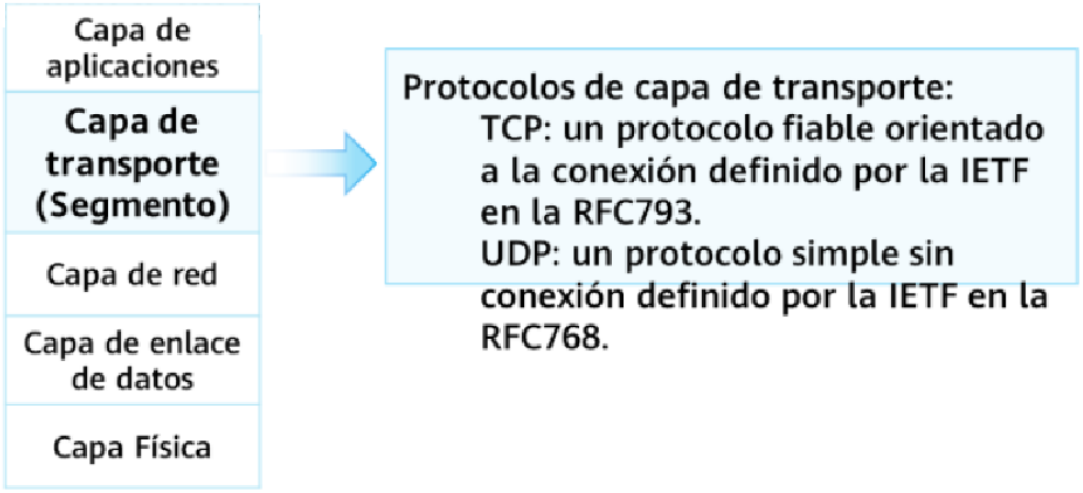
UNIVERSIDAD EAFIT

- Es una versión segura de HTTP que utiliza SSL/TLS para cifrar la comunicación entre el navegador del usuario y el servidor web, garantizando la confidencialidad e integridad de los datos transferidos en la capa de aplicación.

Capa de transporte

UNIVERSIDAD EAFIT

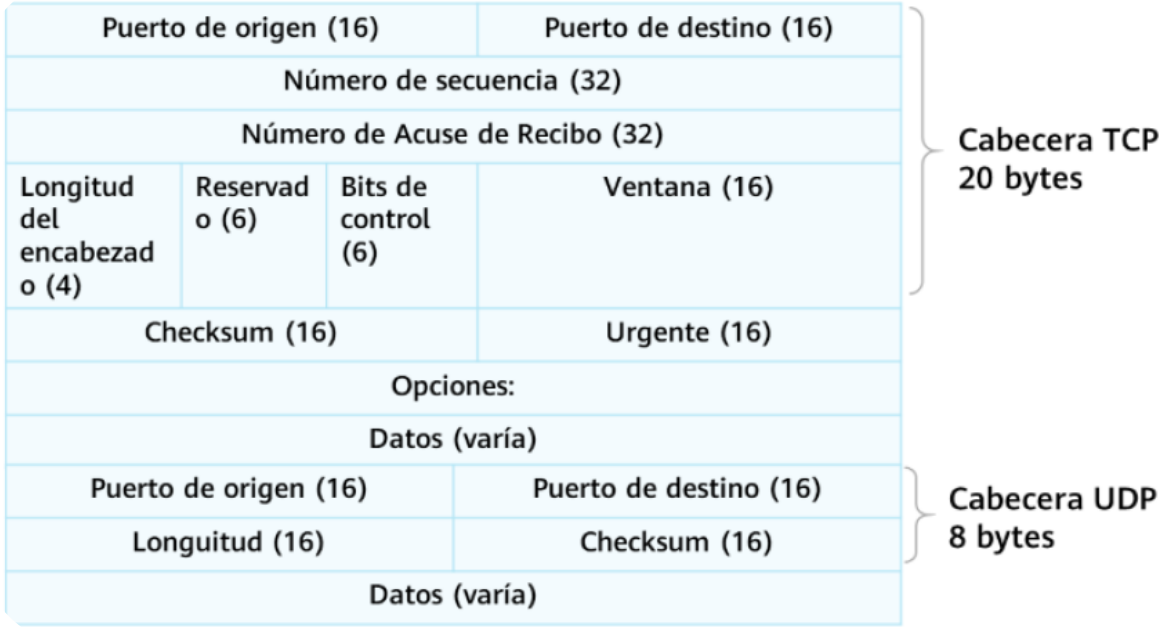
- Un protocolo de capa de transporte recibe datos de un protocolo de capa de encapsula los datos con el encabezado de protocolo de capa de correspondiente y ayuda a establecer una conexión de extremo a extremo (puerto).
- Las PDU transmitidas en la capa de transporte se denominan segmentos.



Formato de encabezados TCP y UDP

UNIVERSIDAD EAFIT

- **TCP** es un protocolo orientado a la conexión que garantiza la entrega fiable y ordenada de los datos. Su cabecera es más compleja debido a los mecanismos de control que implementa, como el control de flujo y el manejo de errores.
- **UDP** es un protocolo sin conexión que no garantiza la entrega de los datos, pero es mucho más rápido y eficiente para aplicaciones que pueden tolerar cierta pérdida de paquetes, como el streaming de video o VoIP.



Formato de encabezados TCP y UDP

UNIVERSIDAD EAFIT

- UDP (User Datagram Protocol) y TCP (Transmission Control Protocol) tienen un rango total de **65,536 puertos** cada uno, numerados del **0** al **65,535.**

- Los puertos efectivos que se pueden utilizar son del **1 al 65,535**.

- Propósitos del puerto 0:
  - Indicador de Error o Ausencia de Puerto.
  - Identificación de Proceso o Servicio No Especificado
  - Utilizado Internamente por Algunos Sistemas Operativos

Formato de encabezados TCP y UDP

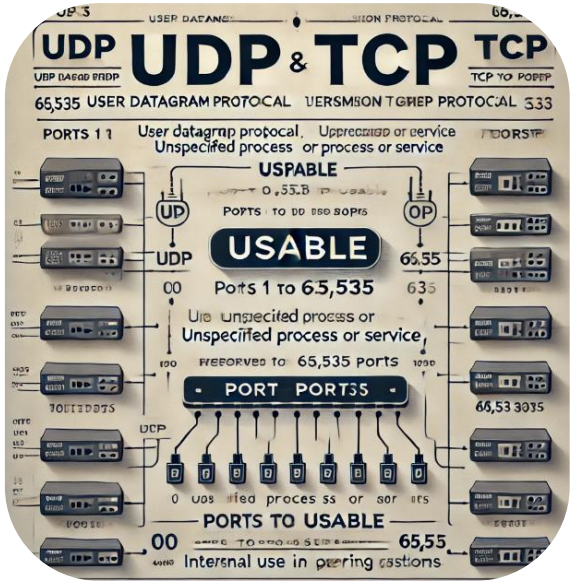
UNIVERSIDAD EAFIT

Los puertos están divididos en tres categorías:

- **Puertos bien conocidos (Well-Known Ports):**
  0 a 1023 - Reservados para servicios y aplicaciones muy utilizados, como HTTP (puerto 80) y FTP (puerto 21).

- **Puertos registrados (Registered Ports):**
  1024 a 49151 - Asignados para aplicaciones que no son tan comunes pero pueden ser utilizadas por cualquier usuario o proceso.

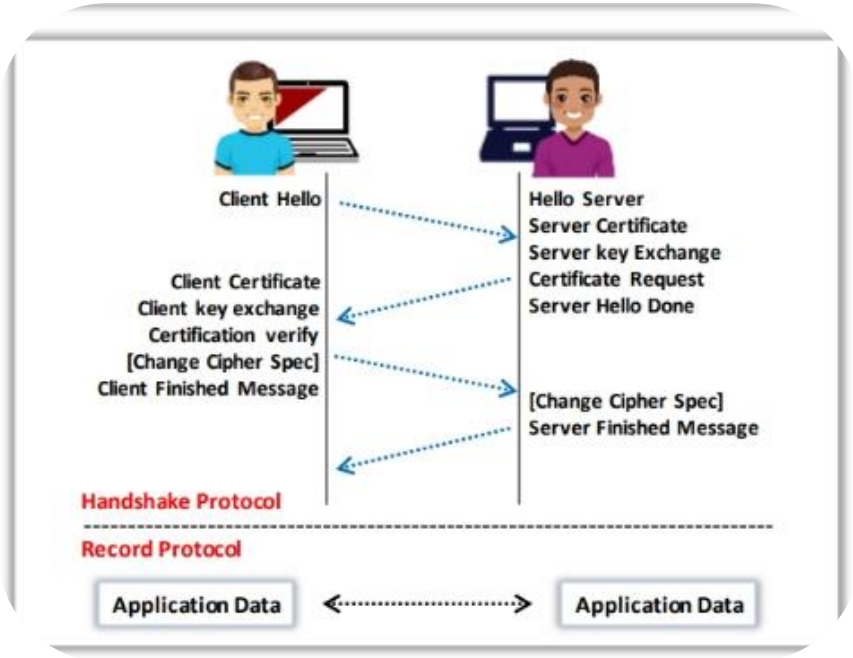
- **Puertos dinámicos o privados (Dynamic/Private Ports):**
  49152 a 65535 - Normalmente utilizados de forma temporal por aplicaciones cliente para realizar conexiones hacia un servidor.



Protocolos comunes de la Capa de Transporte - TLS

UNIVERSIDAD EAFIT

- Transport Layer Security (TLS) es un protocolo para **establecer una conexión segura** entre un cliente y un servidor y garantizar la privacidad e integridad de la información durante la transmisión.
- Utiliza el **algoritmo RSA** con potencias de 1024 y 2048 bits.

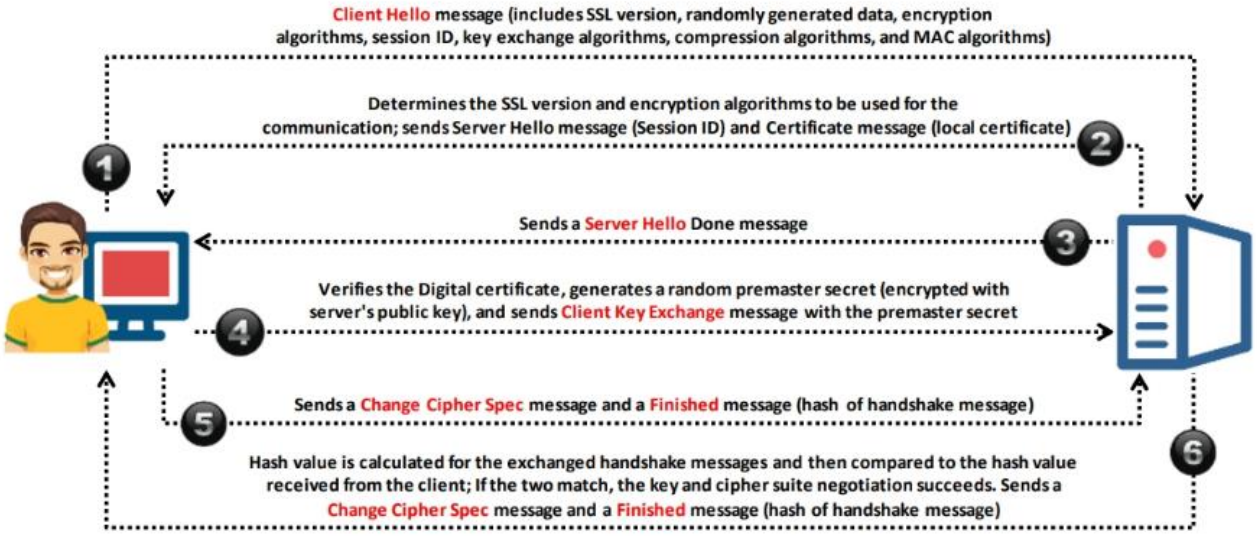


Protocolos comunes de la Capa de Transporte - SSL

UNIVERSIDAD EAFIT

- Secure Sockets Layer (SSL) es un protocolo para gestionar la seguridad de la transmisión de mensajes en Internet.

- Utiliza cifrado asimétrico RSA (clave pública) para cifrar los datos transferidos a través de conexiones SSL.

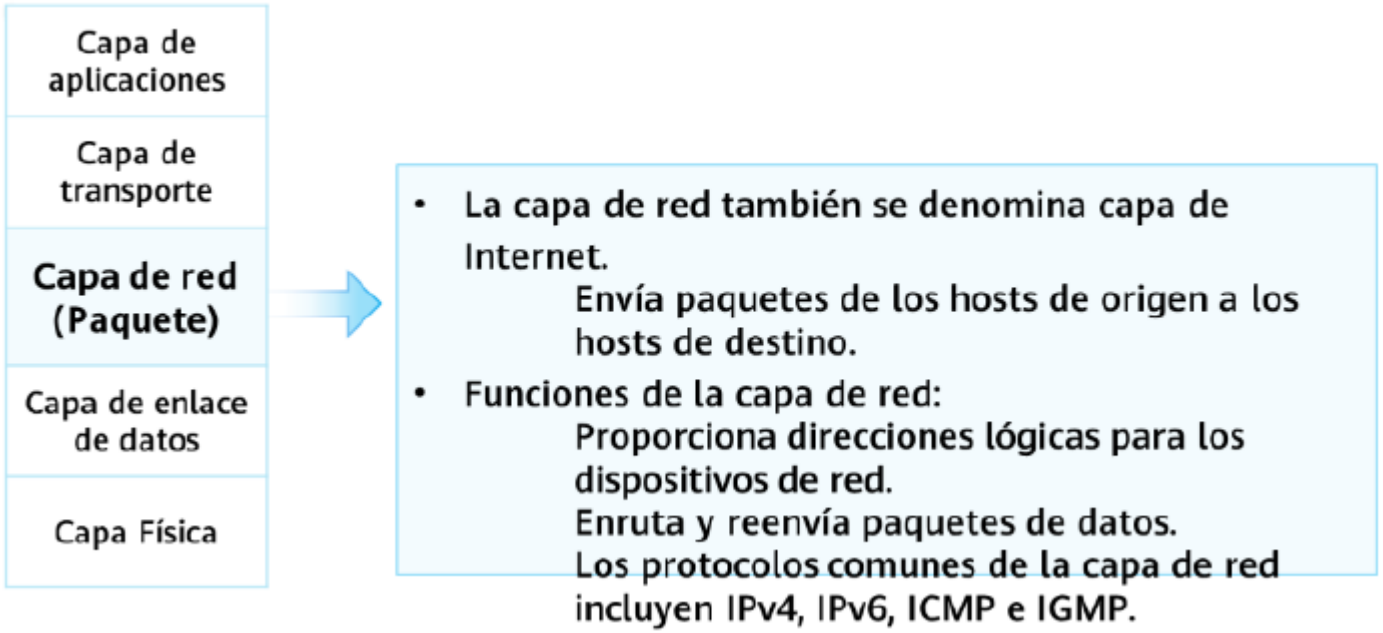


Capa de red

UNIVERSIDAD EAFIT

- La capa de transporte es responsable de establecer conexiones entre los procesos de los hosts, y la capa de red es responsable de transmitir datos de un host a otro.

- Las PDU transmitidas en la capa de red se denominan paquetes.



IPv4 (Internet Protocol version 4)

UNIVERSIDAD EAFIT

- IPv4 es el protocolo de direccionamiento más utilizado en telemática.
- Asigna direcciones IP de 32 bits, permitiendo la identificación única de dispositivos en una red.
- Utiliza un formato decimal con cuatro octetos (por ejemplo, 192.168.1.1).
- IPv4 tiene un espacio de direcciones limitado a 4.3 mil millones de direcciones, lo que ha llevado a la implementación de IPv6.

IPv6 (Internet Protocol version 6)

UNIVERSIDAD EAFIT

- IPv6 es la versión más reciente del protocolo de Internet, diseñado para superar las limitaciones de IPv4. Utiliza direcciones de 128 bits, lo que permite un número casi ilimitado de direcciones IP (3.4 x 10^38 direcciones).

- Utiliza un formato hexadecimal con ocho grupos de cuatro dígitos (por ejemplo, 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

- IPv6 no solo amplía el espacio de direcciones, sino que también mejora la eficiencia del enrutamiento y la configuración automática de direcciones (stateless autoconfiguration).

ICMP (Internet Control Message Protocol)

UNIVERSIDAD EAFIT

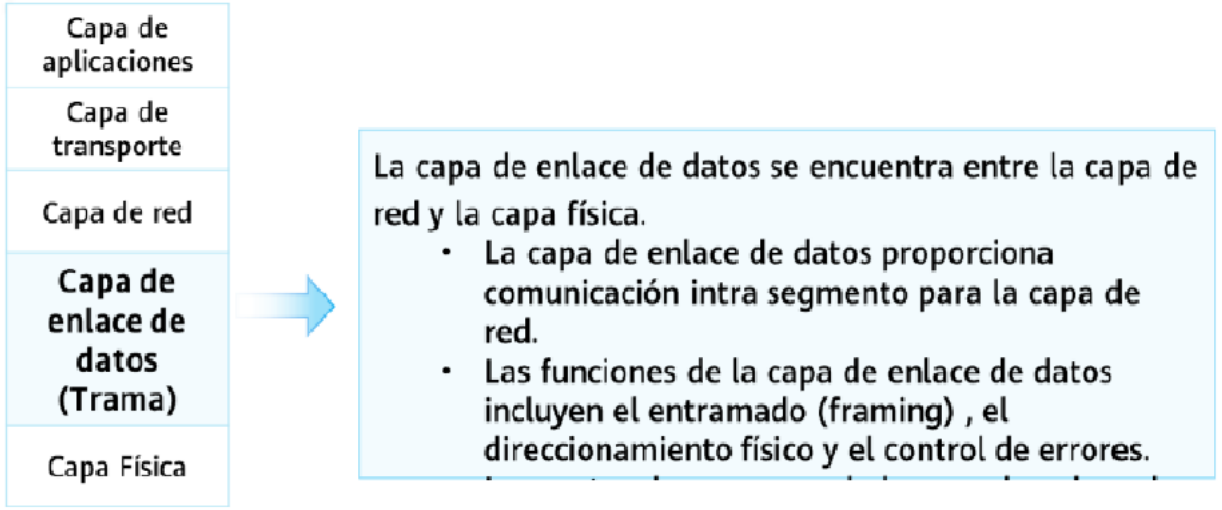
- ICMP es utilizado principalmente para enviar mensajes de error y diagnóstico en la red. No se utiliza para el envío de datos normales, sino para comunicar problemas como la inalcanzabilidad de una red o host, o para verificar si un host está activo mediante comandos como "ping".

- ICMP es fundamental en la resolución de problemas de red y en la gestión de la misma, proporcionando herramientas como el ping y traceroute.

Capa de enlace de datos

UNIVERSIDAD EAFIT

- La capa de enlace de datos se ubica entre la capa de red y la capa física y provee servicios para protocolos tales como IP e IPv6 en la capa de red.
- Las PDU transmitidas en la capa de enlace de datos se denominan tramas.
- Ethernet es el protocolo de capa de enlace de datos más común.



PPP (Point-to-Point Protocol)

UNIVERSIDAD EAFIT

- Es un protocolo utilizado para establecer una conexión directa entre dos nodos de red.
- Es comúnmente usado en conexiones de red punto a punto como las líneas seriales, las conexiones dial-up, y las conexiones de banda ancha.
- PPP incluye mecanismos para la autenticación de usuarios (mediante PAP o CHAP), la asignación de direcciones IP, la compresión de datos y la detección de errores.
- PPP es ampliamente utilizado para conectar a los usuarios a Internet a través de conexiones de módem y DSL, y también se utiliza en conexiones VPN.

PPPoE (Point-to-Point Protocol over Ethernet)

UNIVERSIDAD EAFIT

- PPPoE combina las características de PPP con la infraestructura de Ethernet, permitiendo que múltiples usuarios en una red Ethernet compartida puedan acceder a servicios de banda ancha como DSL mediante conexiones punto a punto virtuales.

- PPPoE establece una sesión punto a punto sobre una red Ethernet. Esta sesión se usa principalmente para la autenticación y facturación de usuarios en redes de banda ancha

- PPPoE es comúnmente implementado por proveedores de servicios de Internet (ISP) para conectar a sus usuarios a través de conexiones DSL, permitiendo la autenticación y la asignación de direcciones IP dinámicas

PPPoE (Point-to-Point Protocol over Ethernet)

UNIVERSIDAD EAFIT

- PPPoE combina las características de PPP con la infraestructura de Ethernet, permitiendo que múltiples usuarios en una red Ethernet compartida puedan acceder a servicios de banda ancha como DSL mediante conexiones punto a punto virtuales.

- PPPoE establece una sesión punto a punto sobre una red Ethernet. Esta sesión se usa principalmente para la autenticación y facturación de usuarios en redes de banda ancha

- PPPoE es comúnmente implementado por proveedores de servicios de Internet (ISP) para conectar a sus usuarios a través de conexiones DSL, permitiendo la autenticación y la asignación de direcciones IP dinámicas

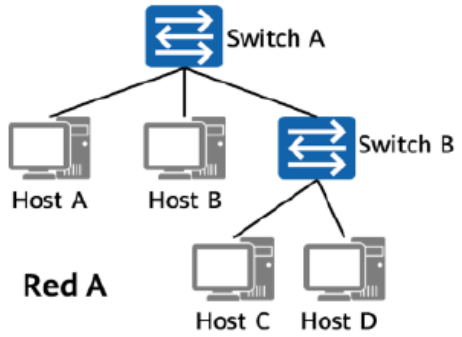
Ethernet

UNIVERSIDAD EAFIT

- Ethernet es el protocolo de capa de enlace de datos más ampliamente utilizado en redes de área local (LAN). Define cómo se estructuran los paquetes de datos (tramas) y cómo se transmiten sobre un medio físico (cables de cobre, fibra óptica, o incluso inalámbricamente).

- Ethernet utiliza un sistema de acceso múltiple con detección de portadora y detección de colisiones (CSMA/CD) en su versión cableada, lo que permite que múltiples dispositivos en la misma red puedan acceder al medio compartido de manera eficiente.

- Existen varias versiones y estándares de Ethernet, como **Fast Ethernet** (100 Mbps), **Gigabit Ethernet** (1 Gbps), y **10 Gigabit Ethernet** (10 Gbps).



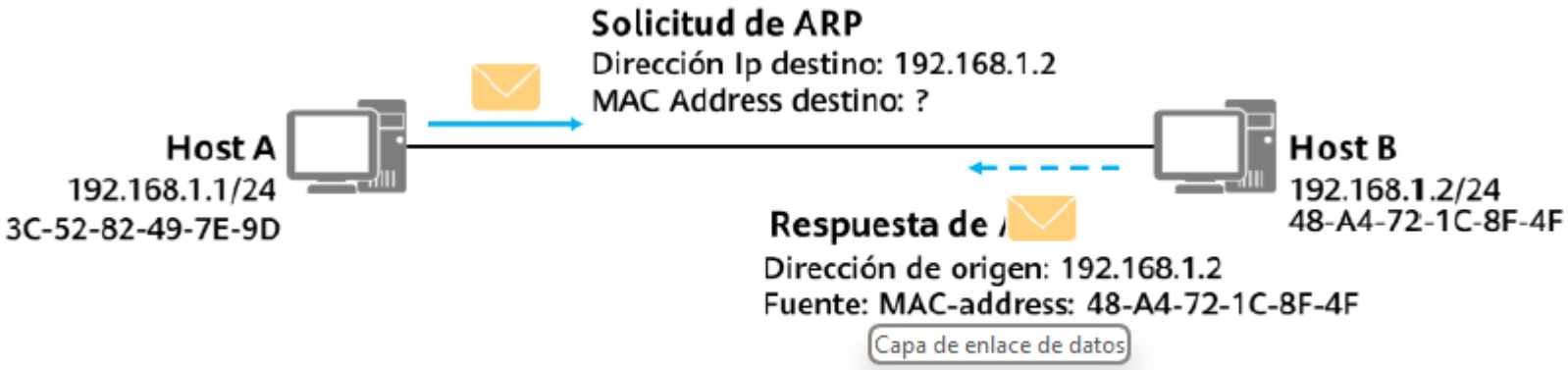
Dirección MAC de origen Ethernet

UNIVERSIDAD EAFIT

- Una dirección de control de acceso a los medios (MAC) identifica de forma única a un elemento de red en una red.
- Cada elemento de red requiere y tiene una dirección MAC exclusiva.
- Las direcciones MAC (MAC address) se utilizan para localizar dispositivos físicos específicos en un segmento de red IPs.
- Un dispositivo que funciona en la capa de enlace de datos, como un switch Ethernet, mantiene una tabla de direcciones MAC para guiar el reenvío de tramas de datos.

ARP

- Protocolo de resolución de direcciones:
  - Descubre la dirección MAC asociada a una dirección IP dada.



Servicio web: arquitectura, desarrollo de aplicaciones web y HTTP.

Protocolo HTTP (Hypertext Transfer Protocol)

¿Qué es HTTP?

Es el protocolo subyacente de la World Wide Web. Define cómo se deben estructurar y transmitir los mensajes entre los navegadores (clientes) y los servidores web.

HTTP es un protocolo **sin estado**, lo que significa que cada solicitud se realiza de manera independiente, sin recordar las solicitudes anteriores.

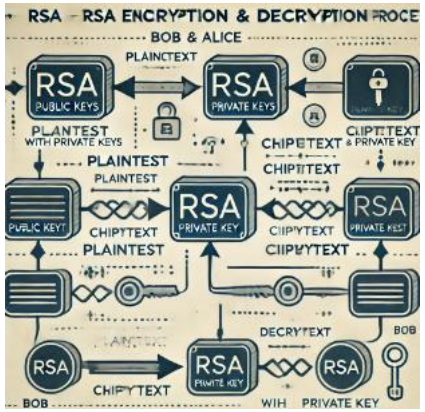
Introducción a los Servicios Web

UNIVERSIDAD EAFIT

Los **servicios web** permiten la interoperabilidad entre aplicaciones distribuidas.

Son componentes clave en la comunicación entre sistemas a través de la web, facilitando la integración de diferentes tecnologías, plataformas y lenguajes de programación.

Un servicio web se basa en estándares como **HTTP**, **XML**, **JSON**, y **SOAP** para enviar y recibir mensajes. En términos simples, es una tecnología que permite que una aplicación o sistema interactúe con otro de forma remota a través de internet.



Arquitectura de los Servicios Web

UNIVERSIDAD EAFIT

- La arquitectura de un servicio web sigue un modelo bien definido para asegurar su funcionamiento y escalabilidad. Este modelo se puede dividir en los siguientes componentes clave:
  - **Componentes de la Arquitectura de un Servicio Web**
  - **Tecnologías de Intercambio de Datos**
  - **Patrones de Comunicación**

Arquitectura de los Servicios Web

UNIVERSIDAD EAFIT

Componentes de la Arquitectura de un Servicio Web

Cliente: Es la aplicación que envía una solicitud al servicio web. Puede ser un navegador web o cualquier otro sistema que envíe peticiones HTTP.

Arquitectura de los Servicios Web

UNIVERSIDAD EAFIT

Componentes de la Arquitectura de un Servicio Web

Servidor Web: Es la parte que recibe las solicitudes del cliente. Procesa la solicitud y la dirige al **servidor de aplicaciones**.

Arquitectura de los Servicios Web

UNIVERSIDAD EAFIT

Componentes de la Arquitectura de un Servicio Web

Servidor de Aplicaciones: Aloja y ejecuta el código del servicio web. Su función es procesar la lógica del negocio y generar respuestas adecuadas a las solicitudes del cliente.

Arquitectura de los Servicios Web

UNIVERSIDAD EAFIT

Componentes de la Arquitectura de un Servicio Web

Base de Datos: Almacena la información necesaria para que el servicio web funcione correctamente. Puede ser consultada por el servidor de aplicaciones para enviar datos actualizados al cliente.

Arquitectura de los Servicios Web

UNIVERSIDAD EAFIT

Tecnologías de Intercambio de Datos

XML (eXtensible Markup Language): Un formato de datos utilizado en servicios web basados en **SOAP** para estructurar los datos.

Arquitectura de los Servicios Web

UNIVERSIDAD EAFIT

Tecnologías de Intercambio de Datos

JSON (JavaScript Object Notation): Un formato de intercambio de datos ligero que se usa comúnmente con servicios web **RESTful**. Es más eficiente y fácil de usar que XML.

Arquitectura de los Servicios Web

UNIVERSIDAD EAFIT

Patrones de Comunicación

Existen dos modelos principales de interacción en los servicios web:

SOAP (Simple Object Access Protocol)
REST (Representational State Transfer)

Arquitectura de los Servicios Web

UNIVERSIDAD EAFIT

Patrones de Comunicación

SOAP (Simple Object Access Protocol):
Un protocolo basado en XML que sigue un esquema más estricto y es altamente extensible.

Es utilizado en sistemas más complejos que requieren seguridad y transacciones robustas.

Arquitectura de los Servicios Web

UNIVERSIDAD EAFIT

Patrones de Comunicación

REST (Representational State Transfer): Un estilo arquitectónico que utiliza las operaciones básicas del protocolo HTTP (GET, POST, PUT, DELETE). REST es más sencillo, rápido y se usa ampliamente en aplicaciones web modernas, donde la eficiencia es prioritaria.

Desarrollo de Aplicaciones Web con Servicios Web

UNIVERSIDAD EAFIT

El desarrollo de aplicaciones web basadas en servicios web implica la creación de interfaces y la implementación de APIs para facilitar la interacción entre diferentes componentes del sistema.

APIs (Interfaz de Programación de Aplicaciones)
- APIs RESTfu
- APIs SOAP

Servidor Web vs Servidor de Aplicaciones
- Servidor Web
- Servidor de Aplicaciones

Patrones Arquitectónicos Comunes en Aplicaciones Web
- MVC (Modelo-Vista-Controlador)
- Microservicios

Desarrollo de Aplicaciones Web con Servicios Web

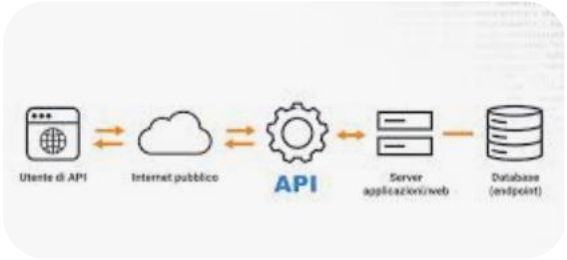
UNIVERSIDAD EAFIT

APIs (Interfaz de Programación de Aplicaciones)

Las **APIs** son esenciales en la creación de servicios web, ya que definen cómo los diferentes componentes interactúan entre sí.

Una API web expone funcionalidades de una aplicación para que otros sistemas puedan consumirlas de manera programática.

- **APIs RESTful:** Son las más utilizadas hoy en día. Siguen el estilo arquitectónico REST y permiten operaciones CRUD (Create, Read, Update, Delete) usando las operaciones HTTP.
- **APIs SOAP:** Son más estrictas en cuanto a la definición del protocolo y se utilizan en entornos donde es fundamental la seguridad y la transaccionalidad.



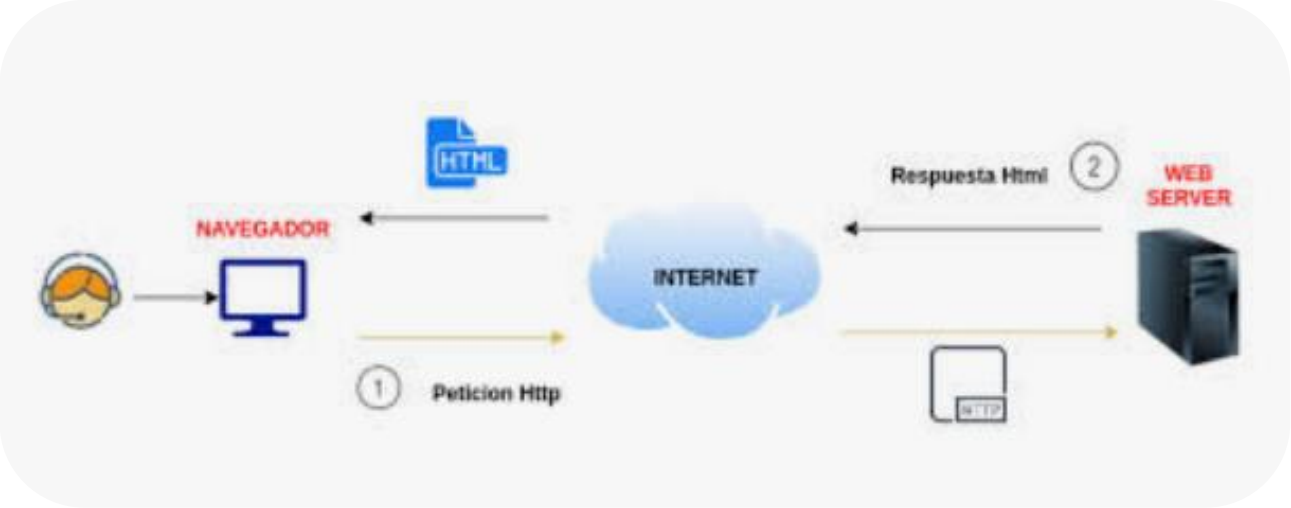
Desarrollo de Aplicaciones Web con Servicios Web

UNIVERSIDAD EAFIT

Servidor Web vs Servidor de Aplicaciones

En el desarrollo web, es fundamental entender la diferencia entre un servidor web y un servidor de aplicaciones:

- **Servidor Web**: Gestiona las solicitudes HTTP y sirve contenido estático como HTML, CSS y JavaScript. Ejemplos: **Apache**, **Nginx**.
- **Servidor de Aplicaciones**: Procesa la lógica de negocio, maneja conexiones con bases de datos, y sirve contenido dinámico. Ejemplos: **Tomcat**, **JBoss**.



Desarrollo de Aplicaciones Web con Servicios Web

UNIVERSIDAD EAFIT

Patrones Arquitectónicos Comunes en Aplicaciones Web

En el desarrollo web, es fundamental entender la diferencia entre un servidor web y un servidor de aplicaciones:

- **MVC (Modelo-Vista-Controlador):** Separa la lógica de negocio (Modelo), la interfaz de usuario (Vista), y el control de los datos (Controlador). Es uno de los patrones más populares en el desarrollo de aplicaciones web.
- **Microservicios:** Divide la aplicación en pequeños servicios independientes que pueden ser desplegados y escalados de forma individual. Es útil para sistemas de gran escala que requieren alta disponibilidad y resiliencia.

Consideraciones Técnicas para el Desarrollo de Aplicaciones Web

UNIVERSIDAD EAFIT

Seguridad

Autenticación y Autorización: Utilización de tokens (ej. JWT - JSON Web Tokens) o sistemas de autenticación como **OAuth** para garantizar que solo usuarios autorizados accedan a los servicios.

Cifrado: Uso de HTTPS para asegurar la transmisión de datos entre el cliente y el servidor.

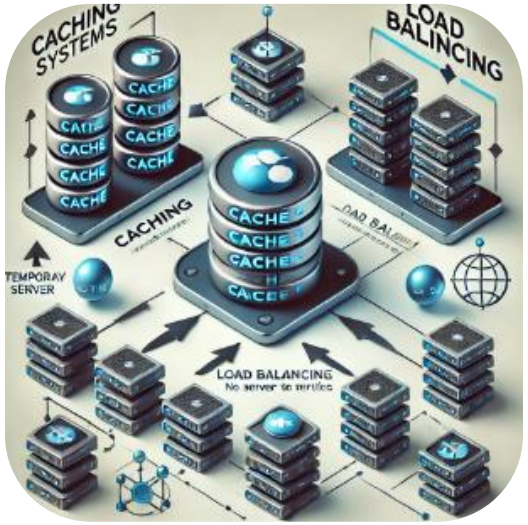
Consideraciones Técnicas para el Desarrollo de Aplicaciones Web

UNIVERSIDAD EAFIT

Escalabilidad y Desempeño

Caché: Implementación de sistemas de caché para almacenar temporalmente respuestas y reducir la carga sobre el servidor.

Balanceo de Carga: Distribución de las solicitudes entre varios servidores para evitar sobrecarga.



Consideraciones Técnicas para el Desarrollo de Aplicaciones Web

UNIVERSIDAD EAFIT

Tolerancia a Fallos

Circuit Breaker: Un patrón que interrumpe las solicitudes a un servicio cuando éste no está disponible para evitar fallos catastróficos en cascada.

Optimización web: redes de Distribución de Contenidos (CDN),

proxies , caché, desempeño

Redes de Distribución de Contenidos (CDN)

Es una red distribuida de servidores que se utilizan para entregar contenido web a los usuarios desde ubicaciones más cercanas a ellos geográficamente, con el fin de reducir la latencia, mejorar la velocidad de carga y optimizar el tráfico en la red.

Las CDNs son esenciales para mejorar el rendimiento de los sitios web y aplicaciones de alta demanda, como plataformas de streaming o grandes sitios de comercio electrónico.

Redes de Distribución de Contenidos (CDN)

Arquitectura de una CDN

Servidores de borde: Estos son los servidores ubicados en diferentes puntos geográficos cercanos a los usuarios finales. Almacenan en caché contenido estático y responden rápidamente a las solicitudes locales.

Servidores de origen: Son los servidores donde reside el contenido original. Estos servidores son contactados solo cuando un servidor de borde no tiene en caché el recurso solicitado.

Redes de Distribución de Contenidos (CDN)

Funcionamiento de una CDN

Cuando un usuario solicita un recurso (como una imagen o un archivo de video), la CDN redirige la solicitud a un servidor de borde cercano, si el recurso está en caché allí. Si no está disponible, el servidor de borde lo obtiene del servidor de origen y luego lo almacena localmente para futuras solicitudes.

Redes de Distribución de Contenidos (CDN)

Beneficios de las CDN

Reducción de la latencia: Al servir el contenido desde una ubicación más cercana al usuario, el tiempo de viaje de los datos se reduce significativamente.

Distribución de carga: Las CDN evitan la sobrecarga de los servidores de origen al distribuir las solicitudes en múltiples servidores de borde.

Mejora de la disponibilidad: Al contar con copias del contenido en diferentes ubicaciones, se garantiza la disponibilidad del servicio incluso en caso de fallo del servidor de origen.

Redes de Distribución de Contenidos (CDN)

Limitaciones de las CDN

Costos adicionales: La implementación y mantenimiento de una CDN puede ser costosa para pequeñas empresas.

Caché inconsistente: En algunos casos, la versión del contenido almacenada en el servidor de borde puede estar desactualizada, lo que requiere mecanismos para invalidar la caché.

Proxies

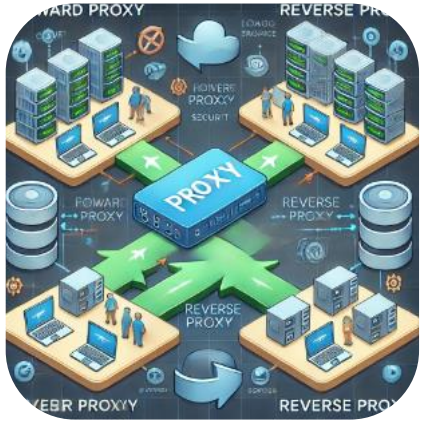
Es un intermediario entre un cliente y un servidor que maneja solicitudes en nombre del cliente. Los proxies son ampliamente utilizados en redes para mejorar el rendimiento y la seguridad.

Proxies

Tipos de Proxies

Proxy directo (Forward Proxy): Este proxy actúa en nombre de los clientes. Cuando un cliente desea acceder a un recurso en la web, el proxy reenvía la solicitud al servidor de destino y luego devuelve la respuesta al cliente. Este enfoque se usa a menudo para filtrar el tráfico o mejorar la seguridad.

Proxy inverso (Reverse Proxy): En este caso, el proxy está ubicado en el lado del servidor. El proxy inverso recibe las solicitudes del cliente en lugar del servidor, las procesa y luego responde al cliente. Es utilizado para balanceo de carga, seguridad y caché.



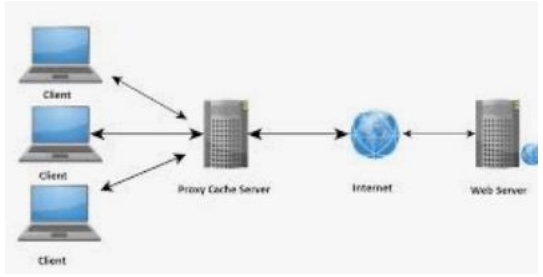
Proxies

Funciones de los Proxies en la Optimización Web

Caché: Los proxies pueden almacenar copias locales del contenido que los clientes solicitan con frecuencia, lo que reduce la latencia y el consumo de ancho de banda.

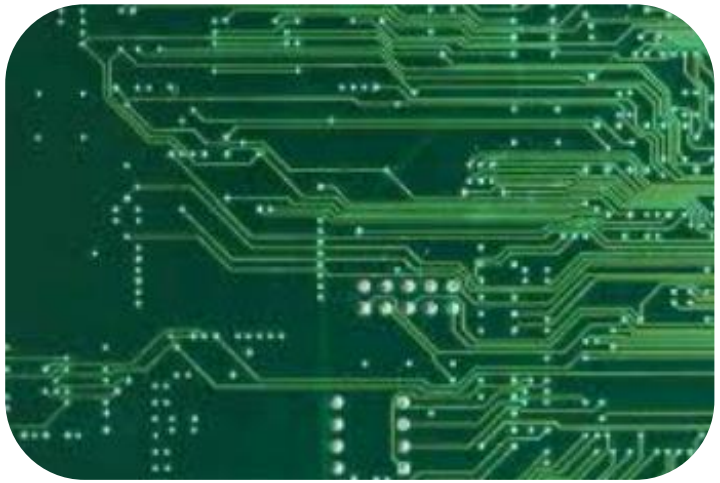
Balanceo de carga: Un proxy inverso puede distribuir las solicitudes entrantes entre varios servidores, lo que optimiza el uso de los recursos del servidor y evita cuellos de botella.

Seguridad: Los proxies pueden filtrar el tráfico no deseado y actuar como un firewall para proteger los servidores de ataques maliciosos.



Caché

Es un mecanismo de almacenamiento temporal de datos que permite un acceso más rápido a los recursos que se solicitan con frecuencia. Es uno de los componentes más importantes para optimizar el rendimiento de las redes y las aplicaciones web.



Caché

Tipos de Caché

Caché del navegador: Los navegadores web almacenan en caché recursos como imágenes, archivos CSS y JavaScript para evitar solicitarlos repetidamente al servidor.

Caché del servidor: Los servidores también pueden almacenar en caché las respuestas a las solicitudes de los clientes. Por ejemplo, si varios usuarios solicitan la misma página web, el servidor puede devolver una versión en caché en lugar de procesar nuevamente la solicitud desde cero.

Caché en proxy: Un proxy también puede implementar caché, lo que permite que múltiples clientes compartan una versión en caché de un recurso.

Caché

Funcionamiento de la Caché

Cada vez que un cliente realiza una solicitud, el sistema de caché verifica si una copia del recurso solicitado está disponible. Si el recurso está en caché y sigue siendo válido (dentro del tiempo de expiración definido por las políticas de caché), el sistema responde con la versión en caché. Si no, la solicitud es enviada al servidor de origen.

Caché

UNIVERSIDAD EAFIT

Ventajas de la Caché

Reducción de latencia: Al evitar solicitudes repetidas al servidor de origen, la caché acelera el tiempo de respuesta.

Ahorro de ancho de banda: Menos solicitudes al servidor original significan menor tráfico en la red.

Escalabilidad: Al reducir la carga sobre el servidor de origen, la caché permite que el sistema maneje más usuarios simultáneamente sin sacrificar el rendimiento.

Caché

Desventajas de la Caché

Invalidez de la caché: Si no se gestiona adecuadamente, la caché puede entregar contenido desactualizado a los usuarios.

Memoria limitada: El almacenamiento en caché requiere memoria, y los recursos en caché pueden ocupar espacio que podría utilizarse para otros fines.

Desempeño de la Red

UNIVERSIDAD EAFIT

Factores que Afectan el Desempeño

El desempeño de una red es un aspecto crítico de la optimización web. Hay varios factores que pueden influir en la velocidad y eficiencia con la que se entrega el contenido:

- **Latencia**: El retraso en el tiempo de viaje de los datos entre el cliente y el servidor. Las **CDN** y los **proxies** pueden reducir la latencia al acercar el contenido a los usuarios finales.

- **Ancho de banda**: La cantidad de datos que se pueden transmitir a través de una red en un tiempo determinado. Las limitaciones de ancho de banda pueden crear cuellos de botella en la entrega de contenido.

Desempeño de la Red

Factores que Afectan el Desempeño

El desempeño de una red es un aspecto crítico de la optimización web. Hay varios factores que pueden influir en la velocidad y eficiencia con la que se entrega el contenido:

- **Pérdida de paquetes**: Cuando los paquetes de datos se pierden en la transmisión, deben ser reenviados, lo que aumenta el tiempo de respuesta. La **caché** y el uso de **CDNs** pueden ayudar a mitigar el impacto de la pérdida de paquetes al reducir la cantidad de datos que necesitan ser transmitidos desde el servidor de origen.

- **Congestión de la red**: Cuando demasiados usuarios acceden a una red simultáneamente, puede haber una sobrecarga en los routers y switches, lo que disminuye la velocidad de entrega de los datos.

UNIVERSIDAD EAFIT

Desempeño de la Red

Técnicas de Optimización del Desempeño

Minificación de recursos: Reducir el tamaño de archivos JavaScript, CSS y HTML mediante la eliminación de espacios en blanco y comentarios innecesarios.

Compresión: Utilizar algoritmos como **GZIP** para comprimir archivos antes de transmitirlos, reduciendo la cantidad de datos que viajan por la red.

Prefetching: Anticipar las solicitudes de los usuarios y cargar recursos antes de que se necesiten, mejorando la percepción de velocidad.

HTTP/2: Implementar la última versión del protocolo HTTP, que permite la multiplexación de solicitudes y respuestas, lo que reduce la latencia y mejora el rendimiento.

UNIVERSIDAD EAFIT

Desempeño de la Red

Técnicas de Optimización del Desempeño

Minificación de recursos: Reducir el tamaño de archivos JavaScript, CSS y HTML mediante la eliminación de espacios en blanco y comentarios innecesarios.

Compresión: Utilizar algoritmos como **GZIP** para comprimir archivos antes de transmitirlos, reduciendo la cantidad de datos que viajan por la red.

Prefetching: Anticipar las solicitudes de los usuarios y cargar recursos antes de que se necesiten, mejorando la percepción de velocidad.

HTTP/2: Implementar la última versión del protocolo HTTP, que permite la multiplexación de solicitudes y respuestas, lo que reduce la latencia y mejora el rendimiento.

Servicio de Directorio (LDAP) y Servicio de Archivos de Red (NFS)

LDAP) y NFS

Los **servicios de red** como el **Servicio de Directorio (LDAP)** y el **Servicio de Archivos de Red (NFS)** son pilares fundamentales en entornos corporativos y sistemas distribuidos.

Ambos servicios permiten la centralización de la gestión de usuarios y recursos, optimizando la administración y el acceso a la información a través de redes.

En esta presentación, abordaremos los conceptos fundamentales de LDAP y NFS, cómo funcionan y su importancia en la infraestructura de red moderna

LDAP) y NFS

Los **servicios de red** como el **Servicio de Directorio (LDAP)** y el **Servicio de Archivos de Red (NFS)** son pilares fundamentales en entornos corporativos y sistemas distribuidos.

Ambos servicios permiten la centralización de la gestión de usuarios y recursos, optimizando la administración y el acceso a la información a través de redes.

Abordaremos los conceptos fundamentales de LDAP y NFS, cómo funcionan y su importancia en la infraestructura de red moderna

Servicio de Directorio (LDAP)

¿Qué es LDAP?

LDAP (Lightweight Directory Access Protocol) es un protocolo estándar que facilita el acceso y la gestión de un **servicio de directorio**.

Un servicio de directorio almacena información estructurada y jerárquica sobre usuarios, grupos, dispositivos y otros recursos de la red.

- **Directorio**: Es una base de datos especializada y optimizada para lecturas rápidas, en lugar de escrituras frecuentes. Se utiliza comúnmente para almacenar información de usuarios y grupos en redes corporativas.

- **LDAP**: Protocolo ligero basado en TCP/IP diseñado para acceder a directorios distribuidos a través de una red.

Servicio de Directorio (LDAP)

¿Estructura de un Servicio de Directorio LDAP

El servicio de directorio organiza los datos de forma jerárquica en una estructura de **árbol**.

En esta estructura, cada entrada tiene un **DN (Distinguished Name)** único que la identifica, y se organiza en una serie de **nodos** o **ramos**.

- **Nodo raíz**: Representa el nivel más alto de la jerarquía, usualmente una organización o dominio (por ejemplo, "dc=empresa, dc=com").
- **Ramas**: Agrupan elementos relacionados, como unidades organizacionales (ou=ventas, ou=recursos_humanos).
- **Hojas**: Representan los elementos finales, como los usuarios, dispositivos o aplicaciones.

Servicio de Directorio (LDAP)

UNIVERSIDAD EAFIT

¿Estructura de un Servicio de Directorio LDAP

El servicio de directorio organiza los datos de forma jerárquica en una estructura de **árbol**.

En esta estructura, cada entrada tiene un **DN (Distinguished Name)** único que la identifica, y se organiza en una serie de **nodos** o **ramos**.

- **Nodo raíz**: Representa el nivel más alto de la jerarquía, usualmente una organización o dominio (por ejemplo, "dc=empresa, dc=com").
- **Ramas**: Agrupan elementos relacionados, como unidades organizacionales (ou=ventas, ou=recursos_humanos).
- **Hojas**: Representan los elementos finales, como los usuarios, dispositivos o aplicaciones.

Cada entrada en el directorio contiene **atributos** (ej. nombre, correo electrónico, etc.) organizados mediante el uso de **schemas**, que definen el tipo de datos que se pueden almacenar y cómo se estructuran.

Servicio de Directorio (LDAP)

UNIVERSIDAD EAFIT

Operaciones Básicas en LDAP

LDAP define varias operaciones clave para interactuar con el servicio de directorio:

1. **Bind:** Autenticar y establecer una sesión con el servidor LDAP.
2. **Search:** Realizar búsquedas de entradas en el directorio.
3. **Compare:** Verificar si un atributo tiene un valor específico.
4. **Add/Delete/Modify:** Operaciones para agregar, eliminar o modificar entradas en el directorio.
5. **Unbind:** Finalizar la sesión.

Servicio de Directorio (LDAP)

Autenticación y Control de Acceso

LDAP se utiliza con frecuencia para **autenticar usuarios** en una red.

Los sistemas pueden integrarse con LDAP para centralizar la autenticación y el control de acceso.

Autenticación basada en LDAP: Los usuarios inician sesión en diferentes aplicaciones o sistemas utilizando las credenciales almacenadas en el directorio LDAP.

LDAP sobre SSL/TLS (LDAPS): Proporciona una capa de seguridad al cifrar las comunicaciones entre el cliente y el servidor LDAP.

UNIVERSIDAD EAFIT

Servicio de Archivos de Red (NFS)

Autenticación y Control de Acceso

NFS (Network File System) es un protocolo que permite compartir archivos entre sistemas a través de una red.

Desarrollado por **Sun Microsystems** en los años 80, permite que diferentes dispositivos accedan a archivos de manera remota como si estuvieran en su sistema de archivos local.

- **Arquitectura cliente-servidor**: NFS sigue una arquitectura cliente-servidor donde un servidor NFS exporta sistemas de archivos y los clientes pueden montarlos y acceder a ellos.

- **Acceso transparente**: Una de las principales ventajas de NFS es que permite que los usuarios accedan a archivos remotos de manera transparente, como si estuvieran en su propia máquina local.

Servicio de Archivos de Red (NFS)

Funcionamiento de NFS

NFS permite compartir directorios y archivos utilizando procedimientos de llamada remota (RPC) sobre el protocolo TCP/IP.

Los clientes pueden **montar** un directorio remoto compartido por el servidor NFS, lo que significa que los archivos de ese directorio aparecen en el sistema de archivos local del cliente.

Proceso de Montaje

1. El **servidor NFS** exporta un sistema de archivos y lo pone a disposición de los clientes.

2. El **cliente NFS** monta el sistema de archivos remoto en su propio sistema, asignándolo a un punto de montaje.

3. Los usuarios del cliente acceden a los archivos remotos de manera normal, sin darse cuenta de que están almacenados en un servidor remoto.

UNIVERSIDAD EAFIT

Servicio de Archivos de Red (NFS)

Versiones de NFS

NFSv2: Versión inicial de NFS, que utilizaba exclusivamente el protocolo UDP.

NFSv3: Introdujo soporte para TCP, mejorando la confiabilidad y el rendimiento.

NFSv4: La versión más reciente de NFS, que incluye mejoras en la seguridad y el rendimiento. NFSv4 incorpora autenticación mediante Kerberos y compatibilidad con firewalls.

Servicio de Archivos de Red (NFS)

Seguridad en NFS

Tradicionalmente, NFS utilizaba mecanismos de autenticación simples como el **UID/GID** del sistema de archivos Unix.

Sin embargo, NFSv4 añadió **Kerberos** para mejorar la autenticación y proporcionar seguridad en las conexiones entre cliente y servidor.

- **Autenticación Kerberos**: Utiliza tickets de autenticación para validar las conexiones de los usuarios de manera más segura.

- **Cifrado de datos**: Aunque NFSv4 soporta cifrado, muchas implementaciones modernas también utilizan VPNs o túneles seguros para proteger las transferencias de datos.

Desafíos y Consideraciones

Escalabilidad

LDAP: A medida que una organización crece, el número de usuarios, dispositivos y recursos gestionados por LDAP también crece. Se necesita una infraestructura robusta y bien configurada para soportar este crecimiento.

NFS: El tráfico y la latencia de la red pueden impactar el rendimiento del servicio. A medida que más usuarios acceden al servidor de archivos, puede volverse un cuello de botella.

Desafíos y Consideraciones

Seguridad

LDAP: Dado que LDAP maneja la autenticación, es esencial implementar medidas de seguridad como LDAPS (LDAP sobre SSL/TLS) para evitar ataques de tipo "man-in-the-middle" o robo de credenciales.

NFS: Aunque NFSv4 introduce mejoras en seguridad, las versiones anteriores de NFS carecían de mecanismos robustos de autenticación. La implementación de Kerberos o el uso de VPNs es recomendable.

UNIVERSIDAD EAFIT

Muchas gracias