ARQUITECTURA Y SISTEMAS OPERATIVOS

ACTIVIDAD III: Sockets, Zonificación DNS, Latencia, HTTPS

1. Introducción

En esta actividad abordaremos conceptos que, aunque no hemos discutido en profundidad en actividades anteriores, son fundamentales para comprender el funcionamiento de las redes y servicios de internet. Estos temas les ayudarán a tener una visión más completa de cómo interactúan los dispositivos y los servicios en un entorno conectado. Comprenderlos no solo les será útil para resolver problemas o configurar sistemas, sino también para tomar decisiones informadas al utilizar tecnologías y servicios de la red.

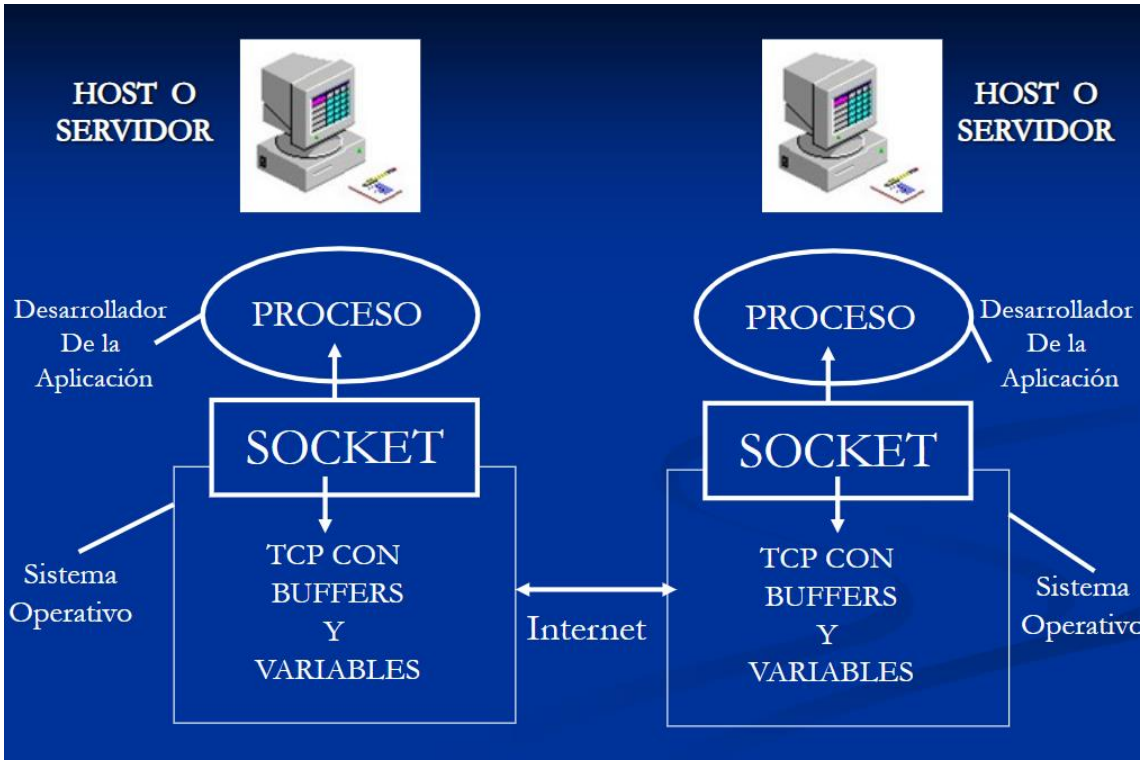
2. Sockets

Un **socket** es el mecanismo que permite que dos programas (en la misma computadora o en diferentes dispositivos) se comuniquen entre sí a través de una red. Piensa en los sockets como un "enchufe virtual" que conecta una aplicación con la red para enviar y recibir datos.

Imagina que los sockets son como las "líneas telefónicas" de una red. Cada extremo tiene un "teléfono" (socket) y, al marcar el "número" (dirección IP y puerto), puedes comunicarte con alguien, en este caso otro proceso o aplicación en la red.

Importancia para programadores

Para los programadores, los sockets son esenciales porque permiten crear aplicaciones que pueden comunicarse en red. Esto incluye desde servidores web hasta aplicaciones de mensajería o juegos online. Al trabajar con sockets, los programadores deben manejar aspectos como conexiones, envío/recepción de datos y protocolos de transporte (TCP o UDP).



En qué capa están los sockets

Los sockets funcionan en la **Capa de Transporte (Capa 4)** del modelo OSI. Se encargan de gestionar la comunicación de datos entre aplicaciones utilizando protocolos como TCP y UDP.

Ejemplo práctico

Cuando desarrollas una aplicación de chat, usas sockets para establecer conexiones entre los usuarios. Por ejemplo, un socket TCP puede enviar mensajes de texto en tiempo real.

3. Zonificación DNS

La zonificación DNS organiza el sistema de nombres de dominio en "zonas", que son partes de la base de datos DNS responsables de una porción específica de la jerarquía de árbol de dominios. Esto permite:

- Delegar la administración de dominios a diferentes servidores o entidades.
- Hacer más eficiente y escalable la gestión del sistema DNS.

Ejemplo

En este árbol, la raíz representa el nivel más alto, y a partir de allí, se dividen distintos niveles en subdominios. Por ejemplo, en el caso de www.ejemplo.com, la jerarquía sería:

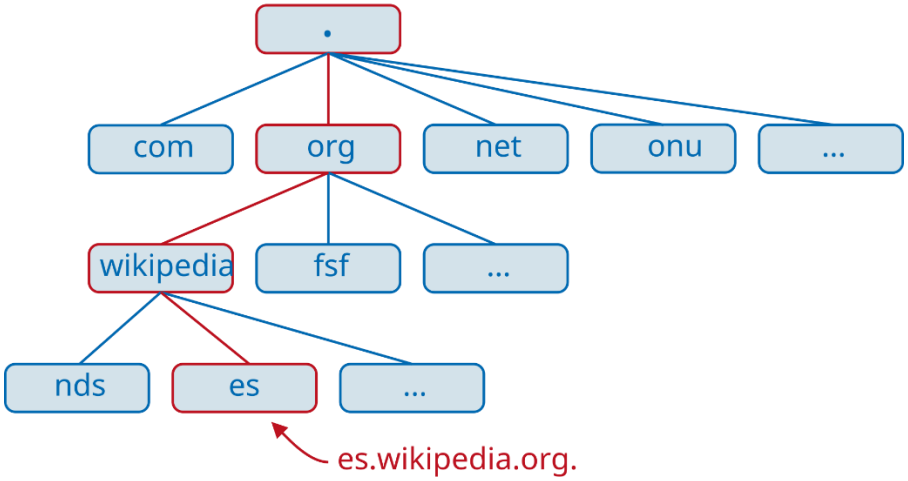
'.' (Raíz): Nivel superior del sistema DNS.

'.com': Dominio de nivel superior (TLD - Top Level Domain).

'ejemplo.com': Dominio registrado dentro del TLD.

'www.ejemplo.com': Subdominio específico que apunta a un servicio web.

Cada nivel en este árbol puede delegar la administración de sus subniveles a servidores específicos. Así, la gestión de 'ejemplo.com' puede delegarse a un servidor de nombres distinto del que gestiona '.com', lo que permite distribuir la carga y hacer más eficiente el funcionamiento de internet.



4. Latencia vs. Ancho de banda

Latencia

Es el tiempo que tarda un paquete de datos en viajar desde tu dispositivo hasta el destino y regresar. Se mide en milisegundos (ms). La latencia se relaciona directamente con el tiempo de respuesta de un ping, que mide cuánto tarda en enviarse un paquete y recibir su respuesta. Por ejemplo, al usar el comando ping en la consola, puedes ver el tiempo en milisegundos que tarda en completarse la conexión.

Razones para tiempos altos de respuesta en un ping:

- **Distancia geográfica:** Si los datos tienen que viajar a un servidor muy lejano, la latencia será mayor.
- **Congestión de la red:** Cuando hay mucho tráfico en la red, los paquetes tardan más en llegar.
- **Problemas en el servidor:** Si el servidor está sobrecargado o tiene problemas técnicos, la respuesta será más lenta.

- **Interferencias en conexiones inalámbricas:** En redes Wi-Fi, factores como la distancia al router o las interferencias pueden aumentar la latencia.

Ancho de banda

Es la cantidad máxima de datos que pueden transferirse por segundo a través de una red. Se mide en megabits por segundo (Mbps).

Analogía para comprender la relación

Imagina una carretera:

- La **latencia** es el tiempo que tarda un auto (es decir, un paquete IP) en ir y volver por la carretera.
- El **ancho de banda** es cuántos autos pueden circular al mismo tiempo (es decir, cuantos paquetes pueden transferirse en un tiempo determinado).

Ejemplo práctico

- Si tienes alta latencia (por ejemplo, 200 ms), las videollamadas se retrasarán, incluso si tienes buen ancho de banda, ya que los paquetes demoran en llegar, verías la pantalla de a saltos.
- Si tienes poco ancho de banda (por ejemplo, 1 Mbps), no podrás ver videos en alta definición, aunque la latencia sea baja. Los paquetes llegan rápido, pero llegan pocos por segundo.

Relación con los juegos en línea

En juegos en línea, la latencia (conocida como "ping") afecta directamente la experiencia del jugador. Un ping alto (mayor a 100 ms) puede causar retrasos en las acciones, como disparar o moverse, haciendo que el juego parezca lento o desincronizado.

Un ping bajo (menor a 50 ms) asegura respuestas rápidas y sincronizadas, lo que es crucial para juegos competitivos como los shooters en primera persona o los juegos de estrategia en tiempo real.

5. HTTP vs. HTTPS

HTTP (HyperText Transfer Protocol): Es el protocolo usado para transferir información en la web. Sin embargo, no es seguro, ya que los datos viajan sin cifrar.

HTTPS (HTTP Secure): Es la versión segura de HTTP. Utiliza cifrado para proteger la información que se transmite entre tu navegador y el servidor. Los datos enviados se encriptan en tu navegador y se desencriptan en el servidor, haciendo imposible que alguien que esté en un punto intermedio (como una red Wi-Fi pública) pueda leerlos.

HTTPS funciona gracias a protocolos de cifrado como **SSL (Secure Sockets Layer)** o su versión más moderna, **TLS (Transport Layer Security)**. Estos protocolos aseguran que los datos viajen de manera segura.

HTTPS opera en la **Capa de Aplicación (Capa 7)** del modelo OSI, ya que se encarga de cómo se presenta la información a los usuarios.

HTTPS es esencial para garantizar la seguridad en transacciones comerciales, como cuando ingresas tus datos de tarjeta de crédito o contraseñas en un sitio web.

Si vas a comprar algo en línea, asegúrate de que la dirección del sitio web comience con https://. Esto asegura que tus datos están protegidos y no pueden ser interceptados.

6. VPN (Virtual Private Network)

Una VPN es una tecnología que crea una conexión segura y cifrada entre tu dispositivo e internet. Esto protege tu privacidad y permite que tu tráfico de red viaje a través de un "túnel" seguro.

Por qué puedes ver Netflix como si estuvieras en otro país

Una VPN te asigna una dirección IP del país que elijas como ubicación, lo que hace que servicios como Netflix crean que estás físicamente en ese país.

Esto es posible porque todo tu tráfico pasa primero por el servidor VPN en el país seleccionado antes de llegar a su destino.

Si estás en Argentina pero usas una VPN conectada a un servidor en Estados Unidos, Netflix creerá que estás en Estados Unidos y te mostrará el catálogo de ese país, incluyendo series o películas no disponibles en tu región.

Si usas Wi-Fi público en un café, una VPN evita que otras personas en la red vean lo que estás haciendo (por ejemplo, tus contraseñas o mensajes). Además, te permite acceder a contenido restringido por ubicación, como el catálogo de Netflix de otros países.

¿Cómo funciona?

Cuando activas la VPN, tu dispositivo crea una conexión segura y cifrada con un servidor VPN.

Todo el tráfico que generas (navegación, mensajes, contraseñas) viaja dentro de un túnel seguro, lo que impide que otras personas en la misma red Wi-Fi puedan verlo.

Aunque un atacante intente capturar los datos, verá información encriptada e ilegible.

Como contracara, puede haber una demora en la transmisión de datos de entre un 10 y un 50% de acuerdo a la calidad del servicio de VPN.