Protocolos de la Capa de Aplicación

La capa de aplicación (Capa 7 del modelo OSI) es la más cercana al usuario. Proporciona los servicios y protocolos que las aplicaciones de software utilizan para comunicarse a través de la red.

HTTP (HyperText Transfer Protocol)

El Protocolo de Transferencia de Hipertexto es la base de la World Wide Web. Su función principal es transmitir recursos, principalmente documentos HTML, pero también imágenes, hojas de estilo (CSS), scripts (JavaScript) y otros archivos. Funciona bajo un modelo de solicitud-respuesta: un cliente (como un navegador web) envía una solicitud a un servidor, y el servidor responde con el recurso solicitado.

Puerto estándar: TCP 80.

Dato clave: Es un protocolo "sin estado", lo que significa que cada solicitud es independiente y el servidor no guarda información sobre las solicitudes anteriores del mismo cliente.

HTTPS (HyperText Transfer Protocol Secure)

El Protocolo Seguro de Transferencia de Hipertexto añade una capa de seguridad utilizando TLS (Transport Layer Security) o su predecesor SSL (Secure Sockets Layer). Esta capa se encarga de dos cosas fundamentales:

Cifrado: Protege la integridad y la confidencialidad de los datos intercambiados entre el cliente y el servidor, evitando que terceros puedan leer o modificar la información.

Autenticación: Verifica que te estás comunicando con el servidor legítimo que dice ser, previniendo ataques de suplantación de identidad (phishing).

Puerto estándar: TCP 443.

Dato clave: El "candado" que se ve en la barra de direcciones de tu navegador indica que la conexión está protegida mediante HTTPS.

FTP (File Transfer Protocol)

El Protocolo de Transferencia de Archivos se utiliza para mover archivos entre un cliente y un servidor en una red. Es uno de los protocolos más antiguos y permite subir (cargar) y bajar (descargar) archivos. Una de sus características distintivas es que utiliza dos conexiones separadas:

Conexión de control: Para enviar comandos (como listar archivos, cambiar de directorio).

Conexión de datos: Para transferir los archivos en sí.

Puertos estándar: TCP 21 (para control) y TCP 20 (para datos).

Dato clave: Aunque sigue en uso, a menudo se considera inseguro porque las credenciales (usuario y contraseña) viajan sin cifrar. Alternativas seguras como SFTP (SSH File Transfer Protocol) y FTPS (FTP over SSL/TLS) son más recomendables.

SMTP (Simple Mail Transfer Protocol)

Cuando envías un email, tu cliente de correo (Outlook, Gmail) usa SMTP para mandar el mensaje a tu servidor de correo. Luego, ese servidor utiliza SMTP para reenviar el mensaje a través de internet hasta llegar al servidor de correo del destinatario.

Puerto estándar: TCP 25. Puertos más modernos y seguros son el 587 y 465 (con SSL/TLS).

Dato clave: SMTP solo se encarga del envío. Para recibir y leer correos electrónicos se utilizan otros protocolos como POP3 (Post Office Protocol) e IMAP (Internet Message Access Protocol).

DNS (Domain Name System)

El Sistema de Nombres de Dominio funciona como la "agenda de contactos" de internet. Los humanos usamos nombres de dominio fáciles de recordar (como google.com), pero las computadoras se comunican mediante direcciones IP numéricas (como 142.250.184.174). DNS se encarga de traducir esos nombres de dominio a sus correspondientes direcciones IP para que los dispositivos sepa a qué servidor conectarse.

Puerto estándar: UDP 53 (principalmente, aunque también puede usar TCP 53 para transferencias de zona).

Dato clave: Sin DNS, tendríamos que memorizar las direcciones IP de todos los sitios web que visitamos, lo que haría la navegación por internet muy poco práctica.

SSH (Secure Shell)

Secure Shell es un protocolo de red criptográfico que permite operar servicios de red de forma segura sobre una red insegura. Sus aplicaciones más comunes son:

Acceso remoto: Permite a un usuario conectarse y controlar un ordenador remoto (como un servidor) a través de una línea de comandos, de forma totalmente cifrada.

Tunelización: Puede reenviar el tráfico de otros protocolos para asegurar sus comunicaciones.

Transferencia de archivos: Protocolos como SFTP se basan en SSH para transferir archivos de manera segura.

Puerto estándar: TCP 22.

Dato clave: SSH es la herramienta fundamental para la administración remota de servidores basados en Linux y otros sistemas UNIX. Reemplazó al antiguo y no seguro protocolo Telnet.