PROTOCOLOS DE LA CAPA DE APLICACIÓN

Christian Hernández Mares

Redes de Computadoras II
Ing. en Computación
7mo Semestre
Grupo 704

Octubre 20, 2025

Protocolos de la capa de aplicación

• HTTP (Hypertext Transfer Protocol)

El Protocolo de Transferencia de Hipertexto (HTTP) es la columna vertebral de la World Wide Web, funcionando como el lenguaje principal para la comunicación entre los navegadores de los usuarios (clientes) y los servidores web. Su operación se basa en un modelo de solicitud-respuesta, donde un cliente pide un recurso, como una página HTML o una imagen, y el servidor responde entregando dicho recurso o un código de estado que indica el resultado de la petición. Una característica fundamental de HTTP es que es un protocolo "sin estado", lo que significa que cada transacción es independiente. Para mantener sesiones de usuario, como en los inicios de sesión, se utilizan cookies, que permiten al servidor recordar al cliente en solicitudes posteriores. La evolución más crítica de este protocolo ha sido la transición a **HTTPS (HTTP Seguro)**, que no es más que HTTP operando sobre una capa de cifrado SSL/TLS. Esta capa protege la integridad y confidencialidad de los datos transmitidos, siendo esencial para proteger información sensible como contraseñas y datos de tarjetas de crédito, y se ha convertido en el estándar de facto para toda la web moderna.

• Telnet (Telecommunication Network)

Telnet es uno de los protocolos de red más antiguos, diseñado para proporcionar acceso remoto a la interfaz de línea de comandos de una computadora a través de una red, actuando como un terminal virtual. Permite a un usuario conectarse a un sistema remoto y ejecutar comandos como si estuviera físicamente presente, transmitiendo las pulsaciones de teclado al servidor y recibiendo la salida de texto. En los inicios de Internet, fue una herramienta indispensable para la administración de sistemas. Sin embargo, su principal y fatal defecto es la total ausencia de seguridad. Toda la comunicación, incluyendo nombres de usuario y contraseñas, se transmite en texto plano, sin ningún tipo de cifrado. Esto lo hace extremadamente vulnerable a la interceptación de datos en cualquier red no segura. Debido a este riesgo inaceptable, Telnet se considera obsoleto para la administración remota y ha sido reemplazado casi universalmente por Secure Shell (SSH), que ofrece las mismas funcionalidades pero sobre un canal de comunicación cifrado.

• FTP (File Transfer Protocol)

El Protocolo de Transferencia de Archivos (FTP) es un estándar de red diseñado específicamente para el intercambio de archivos entre un cliente y un servidor. Su arquitectura es única, ya que utiliza dos conexiones TCP separadas para funcionar: una **conexión de control** (en el puerto 21) para enviar comandos y recibir respuestas (como iniciar sesión o listar directorios), y una **conexión de datos** (en el puerto 20) para la transferencia real de los archivos. Esta separación permite una gestión eficiente de la sesión. El FTP tradicional requiere autenticación con nombre de usuario y contraseña, pero su principal debilidad es la seguridad, ya que tanto las credenciales como los archivos se transmiten en texto plano, sin cifrar. Para abordar esta vulnerabilidad, se desarrollaron extensiones seguras como **FTPS** (FTP sobre SSL/TLS) y **SFTP** (SSH File Transfer Protocol), que cifran la comunicación para proteger los datos en tránsito.

• TFTP (Trivial File Transfer Protocol)

El Protocolo de Transferencia de Archivos Trivial (TFTP) es una versión deliberadamente simplificada y ligera de FTP, diseñada para transferencias de archivos básicas con un mínimo de recursos. A diferencia de FTP, que utiliza el fiable protocolo TCP, TFTP opera sobre UDP (Protocolo de Datagramas de Usuario) en el puerto 69, lo que lo hace más rápido pero sin garantías de entrega. Su simplicidad conlleva importantes limitaciones: no tiene mecanismos de autenticación ni de cifrado, y no permite listar el contenido de los directorios. Por estas razones, TFTP es completamente inseguro para su uso en redes abiertas como Internet. Sin embargo, su pequeño tamaño y facilidad de implementación lo hacen ideal para tareas específicas y automatizadas dentro de redes locales de confianza, como el arranque de estaciones de trabajo sin disco, la actualización del firmware de dispositivos de red como routers y switches, o la copia de seguridad de sus configuraciones.

• SMTP (Simple Mail Transfer Protocol)

El Protocolo Simple de Transferencia de Correo (SMTP) es el estándar fundamental de Internet para la **transmisión** de correo electrónico. Su función principal es "empujar" (push) los mensajes de correo desde un cliente de correo (como Outlook) a un servidor de correo, y luego retransmitir esos mensajes entre diferentes servidores a través de Internet hasta que llegan al servidor del destinatario. SMTP opera sobre una conexión TCP y se comunica mediante una serie de comandos de texto para especificar el remitente, el destinatario y el cuerpo del mensaje. El protocolo original carecía de seguridad, lo que lo hacía vulnerable al spam. Por ello, se introdujo el SMTP Extendido (ESMTP), que soporta extensiones como **SMTP AUTH** para la autenticación del usuario y **STARTTLS** para cifrar la conexión, garantizando que los correos se envíen de forma segura y privada. SMTP solo se encarga del envío; para la recepción se usan protocolos como POP o IMAP.

• DNS (Domain Name System)

El Sistema de Nombres de Dominio (DNS) es un protocolo esencial que funciona como la "guía telefónica de Internet". Su propósito principal es traducir los nombres de dominio legibles por humanos en las direcciones IP numéricas que las computadoras utilizan para identificarse y comunicarse en una red. El sistema no es una base de datos centralizada, sino una red jerárquica y distribuida globalmente, compuesta por servidores raíz, servidores de dominio de nivel superior (TLD) y servidores autoritativos. Esta arquitectura garantiza su escalabilidad y resiliencia. Para optimizar el rendimiento, el DNS utiliza masivamente el almacenamiento en caché, guardando temporalmente las respuestas a las consultas para acelerar futuras solicitudes. La mayoría de las consultas usan el protocolo UDP por su velocidad, aunque puede cambiar a TCP para transferencias de datos más grandes y fiables.

• NFS (Network File System)

El Sistema de Archivos de Red (NFS) es un protocolo de sistema de archivos distribuido que permite a un usuario en una computadora cliente acceder y manipular archivos a través de una red como si estuvieran en su propio disco duro local. A diferencia de FTP, donde se debe iniciar una transferencia explícita, NFS abstrae la ubicación de la red. Un servidor "exporta" uno o más de sus directorios, y un cliente los "monta", integrándolos de forma transparente en su propio árbol de directorios. Esto permite que las aplicaciones interactúen con los archivos remotos utilizando las mismas operaciones estándar del sistema operativo. Las primeras versiones de NFS tenían una seguridad limitada, pero las versiones más recientes, como NFSv4, han incorporado mecanismos robustos como la autenticación Kerberos y el cifrado de datos para proteger la comunicación en redes no seguras.

• POP (Post Office Protocol)

El Protocolo de Oficina de Correos (POP), en su versión más común POP3, es un protocolo de la capa de aplicación diseñado para que los clientes de correo electrónico **recuperen** los mensajes de un servidor de correo. A diferencia de SMTP, que se encarga de enviar correos, POP es un protocolo de "extracción" (pull). Su modelo de funcionamiento tradicional se conoce como "descargar y eliminar": el cliente se conecta al servidor, descarga todos los mensajes nuevos a la máquina local y, por defecto, los borra del servidor. Este paradigma fue diseñado para una época en la que los usuarios accedían a su correo desde un único dispositivo. Su principal desventaja en el entorno actual es la falta de sincronización; si se descarga un correo en un dispositivo, ya no estará disponible en otros. Por esta razón, ha sido en gran medida suplantado por IMAP, que mantiene los correos en el servidor y sincroniza su estado en todos los dispositivos.

• NTP (Network Time Protocol)

El Protocolo de Tiempo de Red (NTP) es un protocolo de Internet fundamental y de larga data, diseñado para sincronizar con precisión los relojes de los sistemas informáticos a través de redes de latencia variable. La sincronización horaria es crítica para el funcionamiento de la tecnología moderna, ya que es esencial para la correlación de archivos de registro en investigaciones de seguridad, el correcto funcionamiento de sistemas de autenticación como Kerberos y la integridad de las transacciones en bases de datos distribuidas. NTP utiliza una arquitectura jerárquica de "estratos", donde los servidores de tiempo se organizan en niveles según su proximidad a una fuente de tiempo de alta precisión, como un reloj atómico (Estrato 0). Un cliente NTP ajusta su reloj intercambiando paquetes con varios servidores para calcular el retardo de la red y el desfase horario, logrando una precisión de milisegundos y proporcionando una base de tiempo consistente y fiable para toda la red.

• NNTP (Network News Transfer Protocol)

El Protocolo de Transferencia de Noticias en Red (NNTP) es el protocolo de aplicación que sustenta Usenet, un sistema de discusión global y distribuido que fue uno de los precursores de los foros de Internet modernos. Usenet está organizado en miles de "grupos de noticias" temáticos, y NNTP se utiliza para transportar los "artículos" (mensajes) entre los servidores de noticias y para permitir que los clientes de los usuarios finales lean y publiquen dichos artículos. Cuando un usuario publica un artículo en un servidor, NNTP se encarga de propagarlo a través de una vasta red de servidores interconectados, asegurando su distribución a nivel mundial. El protocolo define un conjunto de comandos que permiten a un cliente listar grupos, descargar cabeceras de mensajes, recuperar artículos completos y publicar nuevas contribuciones, facilitando así la comunicación asíncrona a gran escala.

• SSH (Secure Shell)

Secure Shell (SSH) es un protocolo de red criptográfico que proporciona una forma segura de acceder y gestionar computadoras a través de una red no segura, como Internet. Fue diseñado como un reemplazo directo del inseguro protocolo Telnet, que transmitía toda la información, incluidas las contraseñas, en texto plano. SSH utiliza una arquitectura cliente-servidor y establece un canal de comunicación cifrado que protege la confidencialidad e integridad de los datos. Su seguridad se basa en una combinación de criptografía asimétrica para la autenticación inicial y el intercambio de claves, criptografía simétrica para el cifrado rápido de la sesión, y algoritmos de hash para verificar la integridad de los mensajes. Además del acceso a la línea de comandos, SSH es una plataforma versátil que soporta la transferencia segura de archivos (SFTP) y la creación de túneles cifrados para proteger otros protocolos de red.

• SNMP (Simple Network Management Protocol)

El Protocolo Simple de Administración de Red (SNMP) es un estándar de Internet para recopilar información y gestionar dispositivos en redes IP, como routers, switches, servidores e impresoras. Su arquitectura se basa en un "gestor" (el sistema de monitoreo), "agentes" (software en los dispositivos gestionados) y una "Base de Información de Gestión" (MIB), que es una base de datos de variables de estado y configuración en el agente. El gestor puede solicitar datos de un agente, modificar su configuración o recibir notificaciones asíncronas no solicitadas llamadas "Traps" cuando ocurren eventos importantes, como un error. La seguridad de SNMP ha evolucionado significativamente: mientras que las versiones iniciales eran inseguras, **SNMPv3** introdujo un modelo robusto con autenticación para verificar la identidad y cifrado para garantizar la privacidad de los datos, siendo el estándar recomendado para la gestión de redes moderna.