UNIVERSIDAD SAN SEBASTIAN
Ilumina el futuro

Semana 03: Modelos de referencia y protocolos

Infraestructura TI

Ingeniería civil informática, semestre 2026

¿Cómo es posible que un mensaje enviado desde tu notebook llegue exactamente al servidor web de otra ciudad, pasando por múltiples redes y equipos diferentes, sin que tú tengas que configurar nada manualmente?

Es posible dado que existen **modelos de referencia** (OSI y TCP/IP)
y **protocolos** estandarizados que dividen la comunicación en capas, y cada capa se encarga de una parte específica del proceso de extremo a extremo.

Introducción

Al diseñar y entender redes de computadores se necesita un lenguaje común que permita describir qué hace cada parte de la comunicación, desde el cable o el Wi-Fi hasta la aplicación web o el correo electrónico. Los modelos de referencia OSI y TCP/IP cumplen esta función **“organizan la red en capas lógicas y asocian a cada capa un conjunto de protocolos que cooperan para lograr la comunicación extremo a extremo.”**

Estos modelos no son software en sí mismos, sino esquemas conceptuales que permiten estandarizar funciones, favorecer la interoperabilidad entre fabricantes y facilitar el diagnóstico, el diseño de redes. Sobre estos modelos se construyen protocolos concretos como Ethernet, IP, TCP, UDP, HTTP, DNS, SMTP, que son los que realmente implementan los servicios que se usan diariamente en Internet

Modelos de referencia y protocolos

Un **modelo de referencia** es una abstracción que divide el problema de la comunicación en subproblemas organizados en capas; cada capa ofrece servicios bien definidos a la capa superior y se apoya en los servicios de la capa inferior.

- Cada capa define: funciones, tipos de datos, interfaces de servicio y protocolos candidatos.
- La implementación concreta (sistema operativo, router, switch, firewall) puede agrupar varias capas o distribuir funciones de forma ligeramente distinta, pero el modelo sirve como guía y lenguaje común.

Modelos de referencia y protocolos

Un **protocolo** es un conjunto de reglas de formato, temporización, semántica y procedimientos para el intercambio de mensajes entre entidades de la misma capa en distintos nodos.

- Define cómo se construyen las unidades de datos (campos, cabeceras, longitudes, códigos de control).
- Define el comportamiento ante eventos: errores, reintentos, establecimiento y cierre de conexiones, control de flujo, etc.

Modelos de referencia y protocolos: Ventajas

- **Descomposición del problema**: la comunicación se vuelve abordable al separar transmisión física, direccionamiento, transporte, sesiones y aplicaciones.

- **Modularidad y reemplazo:** se puede cambiar un protocolo de una capa (por ejemplo, pasar de HTTP/1.1 a HTTP/2 o HTTP/3) sin alterar IP (Internet Protocol, o protocolo de capa de red de la pila TCP/IP; se encarga de direccionar y encaminar paquetes entre redes diferentes, permitiendo que los datos viajen de un host origen a un host destino a través de múltiples routers.) o Ethernet (Ethernet (IEEE 802.3) es el protocolo de capa de enlace de datos más usado en redes LAN cableadas; define cómo se forman y transmiten las tramas entre dispositivos en una red local).

- **Interoperabilidad**: fabricantes distintos implementan protocolos estándar (TCP, IP, Ethernet) y pueden comunicarse sin acuerdos privados adicionales.

- **Facilita troubleshooting (buscar la raíz del problema)**: al ubicar el problema en una “capa” (ej., capa 1: cable, capa 3: IP, capa 7: aplicación), se acota rápidamente la investigación.

Modelos de referencia y protocolos: Desventajas

- **Abstracción imperfecta:** algunas funciones se reparten entre varias capas, por ejemplo, la compresión en aplicación o en transporte.

- **Discrepancias con implementaciones reales:** el modelo OSI de 7 capas no coincide exactamente con la pila de protocolos real de Internet (TCP/IP), lo que puede confundir.

- **Superposición funcional:** mecanismos de control de errores aparecen en enlace, transporte y aplicación con distintos alcances.

Modelos de referencia y protocolos: Casos de éxito

- **La estandarización de Ethernet (IEEE 802.3) en casi todas las LAN del mundo, valiéndose del modelo en capas para evolucionar de 10 Mbps a 400 Gbps sin rediseñar toda la pila**, esto implica que la que la red ha podido evolucionar durante décadas cambiando tarjetas de red, switches y medios físicos para más velocidad, pero sin tener que rediseñar ni reemplazar todo el conjunto de protocolos y aplicaciones que dependen de Ethernet.

- **La adopción global de la pila TCP/IP, que gracias a su definición por capas permitió escalar desde redes militares y académicas a la Internet comercial y móvil actual**, esto hizo que redes muy distintas (militares, universitarias, de empresas, de operadores móviles) pudieran interconectarse sin cambiar toda su infraestructura.

Modelo OSI: Capas y Protocolos

El modelo OSI es un marco conceptual muy detallado que se creó para describir, de forma ordenada y universal**, todo lo que ocurre cuando dos sistemas se comunican a través de una red**. Divide la comunicación en siete capas lógicas, desde el hardware físico hasta las aplicaciones de usuario, de manera que cada capa tiene responsabilidades bien definidas y se apoya en los servicios de la capa inmediatamente inferior. Esta división permite que ingenieros, fabricantes hablen el mismo “idioma” al diseñar, implementar y analizar redes, sin atarse a una tecnología específica.

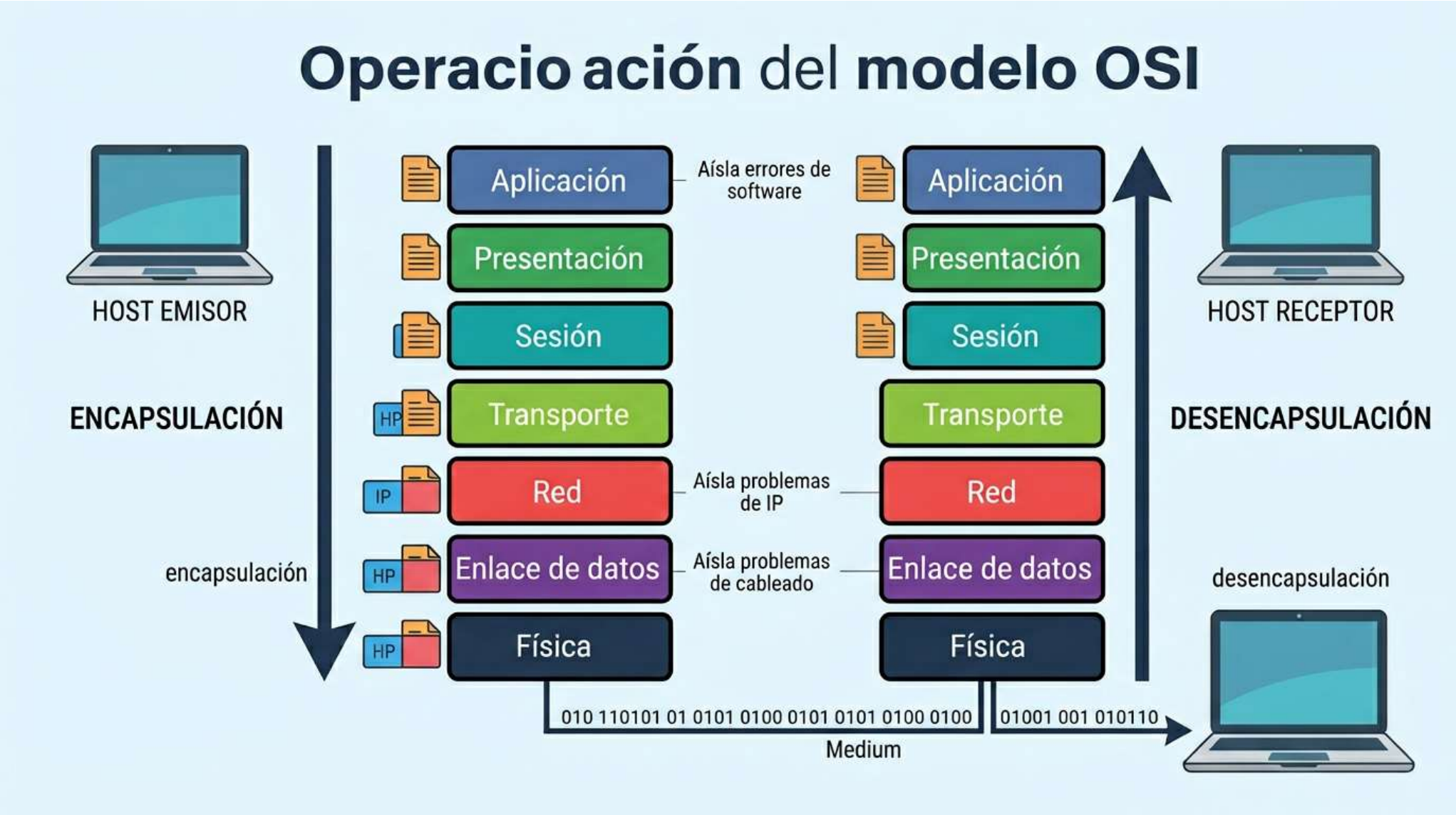
Modelo OSI: Capas y Protocolos

El modelo OSI (Open Systems Interconnection) define 7 capas, cada una con responsabilidades detalladas y tipos de PDU (paquete de datos) diferentes.

Modelo OSI: Capas y Protocolos

Conceptualmente, el modelo OSI funciona como una pila: cuando un host envía datos, estos descienden desde la capa de aplicación hasta la física, encapsulándose progresivamente (añadiendo cabeceras/trailers en cada nivel); cuando el host receptor recibe los bits, el proceso se invierte, desencapsulando capa por capa hasta entregar los datos a la aplicación destino. Esta visión por capas permite aislar problemas (por ejemplo, distinguir un fallo de cableado de un error de direccionamiento IP o de un bug en una aplicación) y también evoluciona de forma modular: se puede mejorar una tecnología de enlace o un formato de aplicación sin rediseñar todo el sistema. Por eso, aunque Internet real usa sobre todo la pila TCP/IP, el modelo OSI sigue siendo la referencia teórica central para enseñar y razonar sobre redes.

Modelo OSI: Capas y Protocolos



Modelo OSI: Capa 1 “Fisica”

Función general: transportar bits sin interpretar su significado lógico.

Define:

- características eléctricas, ópticas y de radiofrecuencia: voltajes, niveles de señal, modulación, sincronización de reloj.
- conectores físicos, topologías (bus, estrella, anillo) y velocidades de transmisión.
- PDU: bits (secuencias de 0 y 1).

Ventajas: diseño independiente del contenido de los datos, se puede aumentar velocidad sin cambiar capas superiores.

Desventajas: no corrige errores lógicos, solo define el medio; todo el control de errores se delega a capas superiores.

Ejemplos:

- Estándares Ethernet físicos (10BASE-T, 100BASE-TX, 1000BASE-T).
- Wi-Fi a nivel de señal (802.11 PHY), fibra óptica (1000BASE-LX), DSL.

Modelo OSI: Capa 2 “Enlace de datos”

Función general: crear un enlace fiable sobre un medio físico potencialmente ruidoso, entre nodos directamente conectados, esta se divide en:

- Subcapa LLC
  - Es la parte “superior” de la capa 2; hace de intermediaria entre la capa de red (IP, IPX, etc.) y la subcapa MAC.
  - Sus tareas principales son:
    - Indicar qué protocolo de capa 3 va dentro de la trama o paquete (multiplexación: IP, IPX, etc.).
    - Añadir información de control para que los datos lleguen a la MAC con el formato correcto.
- Subcapa MAC
  - Es la parte “inferior” de la capa 2; se pega a la capa física y trabaja directamente con la NIC y el medio (cable, Wi-Fi, etc.).
  - Sus tareas principales son:
    - Poner y leer las direcciones físicas (direcciones MAC) en las tramas.
    - Controlar quién puede usar el medio en cada momento por ejemplo CSMA/CD (por cable: escucha el medio si ocurre una colisión al transmitir, la detecta y reintenta tras un tiempo aleatorio), CSMA/CA (por `Wi-Fi: escucha el medio y usa esperas/mensajes de coordinación para evitar que dos nodos transmitan a la vez`)
    - Delimitar las tramas (saber dónde empieza y termina cada una) y, en muchos casos, incluir el FCS/CRC para detección de errores.

Modelo OSI: Capa 2 “Enlace de datos”

Ventajas:

- Aísla los errores físicos, reduciendo la carga de capas superiores.
- Permite compartir eficientemente un medio entre varios dispositivos.

Desventajas:

- Protocolos de control de acceso (como CSMA/CD) escalan mal a topologías muy grandes.
- La presencia de distintas tecnologías de enlace obliga a routers a trabajar más para interconectarlas.

Ejemplos de protocolos capa 2:

- Ethernet (802.3), Wi-Fi (802.11), PPP, HDLC, VLAN (802.1Q), STP (Spanning Tree Protocol).

Modelo OSI: Capa 3 “Red”

Función general: proporcionar direccionamiento lógico y enrutamiento entre múltiples redes, permitiendo el envío de paquetes desde un origen a un destino que no comparten el mismo medio físico, sus funciones típicas son:

- **Lógica de encaminamiento:**
  - Usa algoritmos de ruta más corta (por ejemplo, para elegir el mejor camino).
  - Mantiene tablas de enrutamiento.
  - Toma decisiones salto a salto (*hop-by-hop*), eligiendo el siguiente router en cada paso.
- **Fragmentación y reensamblado:**
  - Si un enlace intermedio tiene una MTU más pequeña, divide el paquete en fragmentos.
  - En el destino, esos fragmentos se vuelven a juntar para reconstruir el paquete original.
- **PDU: paquete o datagrama:**
  - Es la unidad de datos propia de la capa de red: lo que la capa 3 envía y recibe (por ejemplo, un paquete IP).

Modelo OSI: Capa 3 “Red”

Ventajas:

- Escalabilidad global mediante direccionamiento jerárquico (subredes, agregación de rutas).
- Independencia de la tecnología de enlace: IP trabaja sobre Ethernet, Wi-Fi, enlaces WAN, etc.

Desventajas:

- IP básico no garantiza entrega ni orden; se basa en mejores esfuerzos.
- Diseño original de IPv4 con espacio de direcciones limitado, lo que llevó a NAT y a complejidad adicional.

Ejemplos de protocolos capa 3:

- IP (IPv4, IPv6) como protocolo central de encaminamiento.
- ICMP para mensajes de error y diagnóstico (ej., ping, time exceeded).
- IGMP para gestión de grupos multicast.
- Protocolos de enrutamiento: OSPF, BGP, RIP, IS-IS.

Modelo OSI: Capa 4 “Transporte”

Función general: proporcionar transporte extremo a extremo entre procesos (no solo entre máquinas), con diferentes garantías de fiabilidad, orden, control de flujo y control de congestión, sus funciones típicas son:

- **Service-point addressing (direcciones de servicio):**
  - Uso de puertos (números como 80, 443, 5432) para identificar qué aplicación/proceso envía o recibe datos en cada host.
  - Permite que muchas aplicaciones compartan la misma IP al mismo tiempo.
- **Segmentación y reensamblado:**
  - Divide mensajes grandes en segmentos más pequeños que quepan en los paquetes IP.
  - En el destino, vuelve a juntar los segmentos en el mensaje original.

Modelo OSI: Capa 4 “Transporte”

- **Segmentación y reensamblado:**
  - Divide mensajes grandes en segmentos más pequeños que quepan en los paquetes IP.
  - En el destino, vuelve a juntar los segmentos en el mensaje original.
- **Control de flujo extremo a extremo:**
  - Ajusta cuánto se envía para no saturar los búferes del receptor.
  - Ejemplo típico: ventana deslizante de TCP.
- **Control de errores y congestión:**
  - Detecta pérdidas/errores, pide retransmisiones y confirma recepciones (ACKs).
  - En protocolos como TCP, adapta la tasa de envío según la congestión de la red.
- **PDU de la capa 4:**
  - Segmento cuando se usa TCP.
  - Datagrama de transporte cuando se usa UDP.

Modelo OSI: Capa 4 “Transporte”

Ventajas:

- Permite que las aplicaciones no tengan que implementar sus propios mecanismos de fiabilidad y control de flujo.
- Multiplexa muchas aplicaciones simultáneas sobre una misma conexión de red.

Desventajas:

- TCP añade latencia que puede ser problemática en aplicaciones de tiempo real.
- Seleccionar el protocolo de transporte adecuado (TCP vs UDP vs QUIC) requiere comprender muy bien las necesidades de la aplicación.

Ejemplos de protocolos capa 4:

- TCP: conexión orientada, fiable, con control de flujo y control de congestión.
- UDP: no orientado a conexión, sin garantías de entrega ni orden, pero con menor latencia y overhead.
- SCTP, QUIC como alternativas modernas con características de multipath, multistream y cifrado integrado.

Modelo OSI: Capa 5“Sesión”

Función general: gestionar sesiones de comunicación entre aplicaciones, sus funciones típicas son:

- **Establecimiento, mantenimiento y terminación de sesiones**
  - Establecimiento de sesión: proceso por el cual dos aplicaciones acuerdan empezar a comunicarse; suele incluir autenticación del usuario (login) y negociación de parámetros (por ejemplo, tipo de servicio, tiempo máximo inactivo).
  - Mantenimiento de sesión: mientras la sesión está activa, la capa de sesión se encarga de que siga “viva”: controla el diálogo (quién habla y cuándo), puede usar temporizadores, keep-alive, renovación de credenciales, etc.
  - Terminación de sesión: cierre ordenado cuando una de las partes finaliza la comunicación o expira un tiempo; libera recursos y, si corresponde, invalida el login/autorización asociados.

Modelo OSI: Capa 5“Sesión”

- **Sincronización mediante puntos de control (checkpoints)**
  - En transferencias largas (copias de archivos grandes, sesiones de aplicación extensas), la capa de sesión puede marcar puntos de control periódicos, que indican “hasta aquí todo llegó bien”.
  - Si ocurre un fallo en medio de la transferencia, en lugar de empezar desde cero, las aplicaciones pueden reanudar desde el último checkpoint, ahorrando tiempo y ancho de banda.

Ejemplos típicos de **protocolos o mecanismos que implementan funciones en la capa de sesión**: NetBIOS, RPC, y partes de PPTP y otros protocolos de túneles.

Modelo OSI: Capa 6 “Presentación”

Función general: asegurar que los datos enviados por una aplicación puedan ser interpretados correctamente por otra, independientemente de formatos internos, entres sus tareas tenemos:

- Traducir los datos de un formato a otro para que emisor y receptor los entiendan igual, por ejemplo:
  - Convertir texto entre ASCII y Unicode.
  - Ajustar cómo se representan enteros (big-endian / little-endian).
  - Transformar estructuras u objetos complejos a una representación estándar (por ejemplo, JSON, XML, ASN.1) y viceversa.
- Compresión y descompresión
  - Compresión: reduce el tamaño de los datos antes de enviarlos para consumir menos ancho de banda y acelerar la transmisión.
  - Descompresión: al recibir, vuelve a expandir esos datos a su forma original para que la aplicación pueda usarlos normalmente.

Modelo OSI: Capa 6 “Presentación”

- Cifrado y descifrado
  - Cifrado: transforma los datos a una forma ilegible para terceros, usando algoritmos y claves (por ejemplo, en un canal TLS/SSL).
  - Descifrado: en el extremo receptor, revierte ese proceso usando la clave adecuada para recuperar la información original, manteniendo confidencialidad e integridad durante el transporte.

Ejemplos: TLS/SSL, codificaciones JPEG, MPEG, ASN.1, JSON, XML como formatos de representación.

Modelo OSI: Capa 7 “Aplicación”

Función general: ofrecer servicios de red directamente a procesos de usuario, entres sus principales funciones tenemos:

- Interfaces de alto nivel (APIs, comandos)
  - Significa que la capa de aplicación ofrece métodos y comandos para que los programas usen la red sin preocuparse por los detalles bajos.
  - Ejemplos: funciones de una API para hacer peticiones web (HTTP), enviar correo (SMTP/IMAP), consultar DNS, acceder a archivos remotos, o comandos de una herramienta de administración de red.
- Control de acceso, logging y validación
  - Control de acceso: la propia aplicación puede pedir usuario/contraseña, tokens, roles y decidir qué operaciones permite a cada uno.
  - Logging: registrar quién hizo qué y cuándo (peticiones, errores, cambios de configuración) para auditoría y depuración.
  - Validación de datos: comprobar que los datos recibidos tienen formato y contenido correctos (por ejemplo, que un campo email tenga forma válida) antes de procesarlos o guardarlos.

Ejemplos: HTTP/HTTPS, FTP, SMTP, POP3, IMAP, DNS, DHCP, SNMP, Telnet, SSH.

Modelo OSI

Cabe señalar que el modelo OSI separa explícitamente las capas 5 (Sesión) 6 (Presentación) 7 (Aplicación), no obstante, en la práctica suelen agruparse en la capa de aplicación de TCP/IP.

Modelo TCP/IP: Capas y Protocolos

El modelo TCP/IP es un marco conceptual y práctico que se creó para describir y estandarizar cómo se comunican los sistemas en Internet y en la mayoría de las redes modernas.

Organiza la comunicación en cuatro capas lógicas, desde la interacción de las aplicaciones hasta el acceso al medio físico, de modo que cada capa se encarga de una parte específica del proceso y se apoya en los servicios de la capa inmediatamente inferior.

Esta estructura permite que miles de millones de dispositivos muy distintos (servidores, PCs, smartphones, routers, sensores) puedan intercambiar datos de forma confiable sobre una infraestructura global heterogénea, sin necesidad de que cada fabricante diseñe su propia arquitectura cerrada.

Modelo TCP/IP: Capas y Protocolos

A diferencia del modelo OSI, el modelo TCP/IP surgió directamente de las necesidades de ARPANET y de las primeras redes que dieron origen a Internet, por lo que está íntimamente ligado a protocolos concretos como IP, TCP y UDP.

Gracias a esta pila, es posible dividir el problema de la comunicación en funciones como direccionamiento y enrutamiento (capa Internet), transporte extremo a extremo (capa Transporte) y servicios de alto nivel como la Web, el correo o el streaming (capa Aplicación), manteniendo la independencia respecto de las tecnologías de enlace y de los medios físicos subyacentes (capa de Acceso a red).

Esta división ha permitido que la red escale desde unos pocos nodos académicos hasta la Internet global actual, incorporando nuevas tecnologías de enlace y nuevos servicios sin rediseñar desde cero todo el sistema.

Modelo TCP/IP: Capas y Protocolos

El modelo TCP/IP (Transmission Control Protocol/Internet Protocol) define una arquitectura de red práctica con una pila de 4 capas clave.

4 Aplicación	Servicios de red (HTTP, DNS, etc.)
3 Transporte	Transporte extremo a extremo (TCP, UDP)
2 Internet	Direccionamiento y enrutamiento IP
1 Acceso a red	Tramas, MAC y medio físico

Modelo TCP/IP: Capa 1 “Acceso a red”

La capa de Acceso a red (o “Network Access / Link”) es la parte de la pila TCP/IP que se encarga de cómo los paquetes IP se convierten en bits reales que viajan por un medio físico concreto (cobre, fibra, radio, etc.), y de cómo se comunican entre sí los nodos que comparten ese medio. Conceptualmente agrupa lo que en OSI serían las capas 1 (Física) y 2 (Enlace de datos)

Qué hace esta capa

- Define cómo se envían y reciben tramas sobre un medio físico:
  - Estructura de la trama (cabeceras, datos, FCS/CRC).
  - Reglas para detectar el inicio y el fin de cada trama.
- Gestiona el direccionamiento físico:
  - Uso de direcciones MAC u otros identificadores de enlace para saber a qué nodo de la red local va cada trama.
- Implementa el acceso al medio compartido:
  - Reglas para decidir quién transmite y cuándo (CSMA/CD en Ethernet clásico, CSMA/CA en Wi-Fi, TDMA u otros esquemas en WAN).

Modelo TCP/IP: Capa 1 “Acceso a red”

Qué hace esta capa

- Se ocupa de la transmisión de bits:
  - Codificación de señales eléctricas/ópticas o de radio.
  - Sincronización, niveles de voltaje, modulación, etc.
- Puede aportar detección de errores local (CRC/FCS) e incluso cierta recuperación local (retransmisiones en algunos enlaces punto a punto).

Funciones principales

- Encapsular paquetes IP en tramas adecuadas al medio, por ejemplo, Ethernet.
- Direccionar a nivel de enlace (MAC u otros identificadores).
- Controlar el acceso al medio cuando es compartido (evitar o gestionar colisiones).
- Transmitir y recibir bits de manera fiable a corta distancia (entre nodos directamente conectados).
- Detectar errores en la trama y descartarla o pedirla de nuevo (según el protocolo).

Modelo TCP/IP: Capa 1 “Acceso a red”

Ventajas que aporta esta capa

- Independencia del medio físico: se puede cambiar de cable de cobre a fibra, o de Ethernet cableado a Wi-Fi, sin modificar IP, TCP/UDP ni las aplicaciones.
- Modularidad: diferentes tipos de redes locales (LAN cableada, WLAN, enlaces WAN serie, PPP etc.) pueden transportar los mismos paquetes IP.
- Optimización local: cada tecnología de acceso puede usar sus propios mecanismos óptimos de acceso al medio y de codificación, sin impactar al resto de la pila.
- Interoperabilidad: al estandarizar protocolos de acceso (Ethernet, 802.11), dispositivos de distintos fabricantes pueden trabajar juntos en la misma red.

Protocolos típicos en esta capa

- En redes LAN y WLAN:
  - Ethernet (IEEE 802.3)
  - Wi-Fi (IEEE 802.11)
  - VLAN tagging (802.1Q), STP/RSTP/MSTP como protocolos de control de capa 2

Modelo TCP/IP: Capa 1 “Acceso a red”

Protocolos típicos en esta capa

- Enlaces punto a punto y acceso:
  - PPP (Point-to-Point Protocol)
  - HDLC, Frame Relay (históricos, aún presentes en algunas infraestructuras)
  - Enlaces seriales síncronos/asíncronos
- Tecnologías WAN y de agregación:
  - MPLS (en el borde puede verse como “por debajo” de IP)
  - Ethernet sobre fibra en MAN/WAN
  - Enlaces de radio microondas, LTE/5G en la parte más baja de la pila de los operadores

Esta capa, es la responsable de **“cómo” viaja físicamente** lo que IP y las capas superiores quieren enviar; si cambias el tipo de enlace o la tecnología de acceso, deberías poder mantener intacto el resto de la pila TCP/IP.

Modelo TCP/IP: Capa 2 “Internet”

La capa de Internet de la pila TCP/IP es la responsable de que los datos puedan viajar entre redes distintas, eligiendo rutas y usando direcciones IP. esta corresponde a la capa de red del modelo OSI

Qué hace esta capa

- Toma los datos que le envía la capa de transporte (segmentos TCP/UDP) y los encapsula en paquetes IP (datagramas IP).
- Añade direcciones IP de origen y destino, para que routers y equipos sepan de dónde viene y adónde va cada paquete.
- Hace que esos paquetes puedan atravesar múltiples redes intermedias con tecnologías físicas diferentes, hasta llegar al host destino.

Modelo TCP/IP: Capa 2 “Internet”

Funciones principales

- Direccionamiento lógico, asigna y usa direcciones IP para identificar hosts y redes.
- Encapsulado y formateo, encapsula segmentos de transporte en datagramas IP, añadiendo cabeceras con dirección, TTL, protocolo.
- Enrutamiento (routing), decide la ruta que seguirá cada paquete, salto a salto, usando tablas de enrutamiento en routers y hosts.
- Fragmentación y reensamblado, si un paquete es más grande que la MTU (tamaño máximo de paquete) de un enlace intermedio, puede fragmentarlo en trozos más pequeños, cada uno con su propia cabecera IP, el host de destino reensambla los fragmentos para reconstruir el paquete original.
- Gestión de errores y mensajes de control (vía ICMP), informa de problemas como “destino inalcanzable”, “TTL excedido”, etc., para ayudar a diagnosticar fallos de red.

Modelo TCP/IP: Capa 2 “Internet”

Ventajas que aporta esta capa

- Escalabilidad, permite interconectar miles de redes y millones de dispositivos usando un esquema común de direccionamiento (IPv4/IPv6) y routing.
- Independencia del medio, IP funciona sobre muchas tecnologías de acceso (Ethernet, Wi-Fi, enlaces WAN, etc.), sin requerir cambios en las capas superiores.
- Flexibilidad de enrutamiento, se pueden redefinir rutas, añadir routers y cambiar topologías sin modificar aplicaciones ni protocolos de transporte.
- Soporte para multicast y servicios especiales, mediante protocolos auxiliares (IGMP, ICMPv6/MLD) permite envío a grupos, autoconfiguración y descubrimiento de vecinos.

Modelo TCP/IP: Capa 2 “Internet”

Protocolos típicos en esta capa

- IPv4 (Internet Protocol version 4), protocolo IP clásico de 32 bits, todavía el más extendido.
- IPv6 (Internet Protocol version 6), sucesor de IPv4 con direcciones de 128 bits, mejor soporte para autoconfiguración y multicast.
- ICMP / ICMPv6 (Internet Control Message Protocol), envía mensajes de error y diagnóstico (por ejemplo, los usados por ping y traceroute).
- ARP (Address Resolution Protocol) – en IPv4, Traduce direcciones IP locales a direcciones MAC para poder enviar los paquetes sobre la red física (Ethernet, Wi-Fi, etc.).
- IGMP (Internet Group Management Protocol) – en IPv4, Gestiona la pertenencia a grupos multicast, informando a los routers de qué hosts quieren recibir tráfico para cada grupo.

En conjunto, la capa de Internet es la que convierte una colección de redes locales heterogéneas en una **red de redes unificada** “Internet”

Modelo TCP/IP: Capa 3 “Transporte”

Gestiona la comunicación de extremo a extremo entre aplicaciones, encima de IP. Conceptualmente es equivalente a la capa 4 del modelo OSI.

Qué hace esta capa

- Proporciona una conexión lógica entre procesos en el host origen y procesos en el host destino, independientemente de las redes intermedias.
- Toma los datos de la aplicación, los segmenta en unidades manejables, los numera y los pasa a la capa de Internet; en el receptor, los reensambla en el orden correcto.
- Usa puertos para identificar qué aplicación debe recibir cada flujo de datos, permitiendo que muchas aplicaciones compartan la misma IP.

Modelo TCP/IP: Capa 3 “Transporte”

Funciones principales

- Multiplexación/demultiplexación por puertos, varios flujos de distintas aplicaciones viajan simultáneamente sobre la misma dirección IP; la capa de transporte los distingue por el par (IP, puerto).
- Control de flujo extremo a extremo, evita que el emisor sature los búferes del receptor, ajustando cuánto puede enviar sin confirmación (ventanas deslizantes, etc.).
- Control de errores y fiabilidad, detección de pérdidas/errores, retransmisión, confirmaciones (ACKs), numeración de segmentos y reordenación en destino, según el protocolo.
- Control de congestión (en TCP y SCTP), ajusta dinámicamente la velocidad de envío según el estado de congestión de la red, para no colapsarla y aprovechar mejor el ancho de banda.
- Abstracción de sockets, para las aplicaciones, la comunicación se expone como un socket, un “extremo” de comunicación identificado por IP+puerto que permite enviar y recibir datos como si fuera un archivo.

Modelo TCP/IP: Capa 3 “Transporte”

Ventajas que aporta esta capa

- Independencia de la red subyacente, las aplicaciones no necesitan saber nada de routers, MTU, ni tipos de enlace; solo hablan con sockets.
- Fiabilidad opcional, se puede elegir entre transporte fiable (TCP, SCTP) o ligero/sin conexión (UDP) según las necesidades de la aplicación.
- Uso eficiente de recursos, el control de flujo y congestión reduce pérdidas y retransmisiones innecesarias, mejorando rendimiento global.

Modelo TCP/IP: Capa 3 “Transporte”

Protocolos típicos de la capa de Transporte

- TCP (Transmission Control Protocol), orientado a conexión, fiable, garantiza entrega en orden, sin duplicados, con control de flujo y de congestión. Ideal para web, correo, SSH, etc.
- UDP (User Datagram Protocol), no orientado a conexión, sin garantías fuertes de entrega ni de orden, pero muy ligero y con menor latencia; usado en DNS, VoIP, streaming, juegos en línea.
- SCTP (Stream Control Transmission Protocol), protocolo fiable y orientado a conexión, basado en mensajes, con soporte de multihoming y control de congestión; utilizado en telecomunicaciones y algunas aplicaciones de alta disponibilidad.

La capa de transporte es la que hace posible que las aplicaciones se comuniquen entre sí **de extremo a extremo**, escogiendo el equilibrio adecuado entre fiabilidad, control y rendimiento.

Modelo TCP/IP: Capa 4 “Aplicación”

Es la capa superior y reúne todo lo que, en OSI, serían las capas de sesión, presentación y aplicación. Es la que habla directamente con los programas de usuario (navegador, cliente de correo, etc.)

Qué hace esta capa

- Ofrece servicios de red concretos, web, correo, transferencia de archivos, resolución de nombres, administración, mensajería, etc.
- Define formatos de mensaje y reglas de diálogo para cada servicio, por ejemplo, cómo es una petición/respuesta HTTP, un mensaje SMTP, una consulta DNS).
- Encapsula la lógica de sesión (abrir/cerrar conversaciones lógicas), de presentación (formato, codificación, a veces compresión/cifrado) y de aplicación (semántica de cada operación).

Modelo TCP/IP: Capa 4 “Aplicación”

Funciones principales

- Interfaz para las aplicaciones, proporciona comandos, métodos y APIs para que las aplicaciones usen la red sin conocer detalles de TCP, IP o Ethernet.
- Formato y semántica de los datos, define cómo se estructuran las peticiones y respuestas (cabeceras, cuerpos, códigos de estado) y qué significan.
- Gestión de sesiones lógicas, para muchos protocolos, incluye mecanismos de login, autenticación, cookies, tokens, mantenimiento de sesión, etc.
- Funciones adicionales de seguridad y control, validación de datos, control de acceso por usuario/rol, registro de actividades (logging) y, en algunos casos, cifrado a nivel de protocolo (ej. HTTPS sobre TLS).

Modelo TCP/IP: Capa 4 “Aplicación”

Ventajas de esta capa

- Alineada con la Internet real, coincide con cómo las RFC (1122/1123 y posteriores) organizan los protocolos de usuario y de soporte, por servicios.
- Menos capas conceptuales arriba, simplifica diseño e implementación en sistemas operativos y equipos de red, porque muchas funciones de alto nivel se agrupan en un solo estrato.
- Alta extensibilidad, es fácil definir nuevos protocolos de aplicación (REST/HTTP-based, gRPC, nuevos servicios) sin tocar las capas inferiores siempre que se apoyen en TCP/UDP.
- Separación clara de responsabilidades, las aplicaciones negocian formatos y políticas aquí, mientras transporte e Internet se ocupan de mover bits y paquetes de forma fiable y eficiente.

Modelo TCP/IP: Capa 4 “Aplicación”

Protocolos típicos de la capa de Aplicación

- HTTP / HTTPS, navegación web y APIs REST; HTTPS añade cifrado TLS para seguridad.
- FTP, SFTP, TFTP, transferencia de archivos con distintos niveles de complejidad y seguridad.
- SMTP, POP3, IMAP, envío (SMTP) y recepción/gestión (POP3, IMAP) de correo electrónico.
- DNS (Domain Name System), traduce nombres de dominio legibles a direcciones IP.
- DHCP, asigna automáticamente direcciones IP y parámetros de red a los hosts.
- SSH, Telnet, acceso remoto a línea de comandos; SSH añade cifrado y autenticación fuerte.
- SNMP para gestión de red, NTP para sincronización de hora, LDAP para directorios, SIP para señalización de VoIP.

Tabla comparativa OSI vs TCP/IP

Aspecto	Modelo OSI	Modelo TCP/IP
N° de capas	7 capas (Física, Enlace, Red, Transporte, Sesión, Presentación, Aplicación).	4 capas (Acceso a red, Internet, Transporte, Aplicación).
Enfoque	Teórico, de referencia general.	Práctico, centrado en Internet.
Detalle funcional	Muy detallado, distingue sesión y presentación.	Más agregado; sesión y presentación integradas en aplicación.
Uso en la industria	Principalmente educativo y como marco conceptual.	Implementado en sistemas reales y protocolos de Internet.
Facilidad de aprendizaje inicial	Más complejo por las 7 capas.	Más simple y cercano a la práctica.
Ejemplos de protocolos superiores	HTTP, FTP, SMTP, DNS en capa 7.	HTTP, FTP, SMTP, DNS en capa de aplicación.
Mapeo entre modelos	Capas 1–2 OSI ≈ Acceso a red; 3 ≈ Internet; 4 ≈ Transporte; 5–7 ≈ Aplicación.	Igual relación, pero definidas originalmente desde la pila TCP/IP.

Protocolos básicos por capa

Capa OSI	Capa TCP/IP	Función principal	Ejemplos de protocolos
1 Física	Acceso a red	Transmisión de bits por el medio.	Señalización Ethernet, fibra, Wi-Fi.
2 Enlace de datos	Acceso a red	Tramas, MAC, detección de errores local.	Ethernet, PPP, HDLC.
3 Red	Internet	IP lógico y enrutamiento entre redes.	IPv4, IPv6, ICMP, OSPF, BGP.
4 Transporte	Transporte	Entrega extremo a extremo, puertos.	TCP, UDP, SCTP, QUIC.
5 Sesión	Aplicación	Gestión de sesiones y diálogo.	NetBIOS, RPC, PPTP, SOCKS.
6 Presentación	Aplicación	Formato, compresión,	TLS/SSL, JPEG,

UNIVERSIDAD
SAN SEBASTIAN

Ilumina el futuro

Santiago | Concepción | Valdivia | Puerto Montt

uss.cl