CIT2114 · Redes de Datos

Guía de Estudio — Capítulo 1

Redes, Modelo de Capas, OSI y TCP/IP

Universidad Diego Portales
Ingeniería Civil en Informática y Telecomunicaciones

Elaborado para el curso
Semestre 1 · 2026

■ Esta guía complementa y amplía el contenido visto en clases. Utilízala junto a tus apuntes y el libro de Tanenbaum para consolidar los conceptos fundamentales de redes.

Contenidos

1. Fundamentos de Redes de Datos

Conceptos básicos sobre qué es y para qué sirve una red

¿Qué es una Red?	Conjunto de dispositivos **interconectados** diseñados para intercambiar información en tiempo real y, en la mayoría de los casos, de forma bidireccional. Está formada por **nodos** (equipos) y **medios de transmisión** (cables de cobre, fibra óptica, espacio libre).

1.1 Componentes esenciales de una red

Una red de datos se compone de tres elementos básicos que siempre deben estar presentes:

Componente	Descripción	Ejemplos
Nodos / Dispositivos	Equipos que generan, reciben o retransmiten información.	PC, servidor, router, switch, smartphone
Medios de transmisión	Canal físico o inalámbrico por el que viajan las señales.	Cable UTP, fibra óptica, Wi-Fi (radio), satélite
Protocolos	Reglas comunes que permiten a los dispositivos comunicarse.	Ethernet, IP, TCP, HTTP, Wi-Fi 802.11

1.2 Tipos de redes según alcance

Los tipos de redes se clasifican principalmente según la distancia que cubren y el contexto en que se despliegan:

Tipo	Alcance	Ejemplo
PAN	Hasta ~10 m	Bluetooth, USB
LAN	Edificio / campus	Red universitaria, red de una empresa
MAN	Ciudad / región metropolitana	Red de cable TV, redes municipales
WAN	País / continente / global	Internet, redes de operadoras

■ En el curso de Redes de Datos nos enfocaremos principalmente en las tecnologías de LAN y WAN, ya que son las más relevantes para la industria.

2. Codificación de la Información

Cómo se representa la información para ser transmitida

Toda la información que circula por una red —texto, imagen, audio, video— debe transformarse en una secuencia de bits (0s y 1s) para poder ser transmitida. Este proceso se llama **codificación**.

¿Cómo ocurre la codificación?

El ejemplo más clásico es el texto ASCII (American Standard Code for Information Interchange). Cada carácter tiene un valor numérico decimal y luego se convierte a binario (base 2). Por ejemplo, la letra "A" es el valor decimal 65, que en binario es `01000001`.

■ Además de ASCII, existen Unicode (UTF-8, UTF-16) para representar caracteres de cualquier idioma del mundo. Hoy en día UTF-8 es el estándar predominante en Internet.

Otros formatos de codificación

El texto es solo un tipo de datos. Las redes transportan muchos otros:

Formato	Tipo de dato	Observación
ASCII / UTF-8	Texto	Base de toda la comunicación de texto en redes
JPEG / PNG / GIF	Imágenes	Distintos niveles de compresión y calidad
MP3 / AAC	Audio comprimido	Usado en streaming de música y voz sobre IP (VoIP)
MPEG / H.264	Video	Compresión con pérdida, base de YouTube, Netflix
PDF	Documentos	Portabilidad de formato entre distintos SO

3. Modelo de Capas — Conceptos Clave

La abstracción que hace posible la comunicación universal

Antes de que existieran los modelos de capas, cada fabricante diseñaba sus propios protocolos propietarios. Un equipo IBM no podía hablar con uno de Digital Equipment. La solución fue crear una **arquitectura en capas**: dividir el problema de la comunicación en problemas más pequeños e independientes, cada uno resuelto por una capa.

Protocolo	Conjunto de reglas que definen la **sintaxis** (forma del mensaje), **semántica** (significado de los campos) y **sincronización** (temporización e intercambio). Pueden implementarse en hardware, software o ambos.
Arquitectura de red	Conjunto completo de capas y protocolos. Ejemplos: arquitectura OSI, arquitectura TCP/IP, Ethernet.
Pila de protocolos	Lista de protocolos utilizados por un sistema, uno por capa. Por ejemplo: HTTP / TCP / IP / Ethernet.

3.1 Principios del diseño en capas

■ Abstracción

Cada capa se "olvida" de los detalles internos de las capas inferiores. Solo le importa la interfaz que le exponen.

■ Encapsulamiento

Al bajar por la pila, cada capa agrega su propia cabecera (y a veces un trailer) al bloque de datos recibido de la capa superior.

■ Independencia

Un cambio en la implementación de una capa no afecta a las demás, siempre que la interfaz se mantenga igual.

■ Comunicación virtual

Lógicamente, cada capa parece comunicarse directamente con su homóloga en el otro extremo, aunque físicamente los datos deben descender y subir la pila completa.

✉ Analogía postal: cuando envías una carta, no sabes si el correo usa avión, camión o bicicleta. Tú solo interactúas con la "interfaz" de la oficina de correos. Lo mismo ocurre entre capas de red.

4. Diseño de las Capas

Problemas que debe resolver cada capa

Independientemente del modelo (OSI, TCP/IP u otro), cada capa debe resolver un conjunto de problemas recurrentes en toda comunicación digital:

■ Direccionamiento

Identificar emisores y receptores. En distintas capas se usan diferentes tipos de dirección: **MAC (capa 2)**, **IP (capa 3)**, **puerto (capa 4)**.

■ Control de errores

Los canales físicos no son perfectos. Se usan técnicas de **detección** (paridad, CRC, checksum) y **corrección** (Hamming, Reed-Solomon). Ambos extremos deben acordar qué método usar.

■ Fragmentación y reordenamiento

Los datos se dividen en unidades más pequeñas (tramas, paquetes). Como los canales no garantizan el orden de entrega, se numeran los fragmentos para que el receptor los reordene.

■ Control de flujo

Evita que un emisor rápido sature a un receptor lento. Se implementa mediante ventanas deslizantes (TCP) o señales de "back-pressure" en capas inferiores.

■ Multiplexación

Permite que múltiples conversaciones compartan el mismo canal físico simultáneamente (por ejemplo, varios navegadores abiertos usan el mismo cable de red usando distintos puertos).

■ Seguridad

Aunque no siempre fue parte del diseño original (el modelo OSI fue diseñado en otra época), hoy el cifrado (TLS), autenticación y control de acceso son fundamentales.

5. Modelo OSI — Las 7 Capas en Detalle

Open Systems Interconnection · ISO 1984

El modelo OSI fue propuesto por la ISO en 1984 como el **estándar universal** para las comunicaciones en red. Es un modelo de referencia: describe qué debe hacer cada capa, pero no especifica cómo implementarla. Tiene **7 capas**, numeradas del 1 (física) al 7 (aplicación).

■ Mnemotécnico para recordar las capas de arriba hacia abajo: "All People Seem To Need Data Processing" → Application, Presentation, Session, Transport, Network, Data Link, Physical.

Capa 7 Aplicación PDU: APDU

Proporciona a las aplicaciones acceso a los servicios de red. Define los protocolos que las aplicaciones usan para intercambiar datos. No es la aplicación en sí, sino la interfaz entre la app y la red.

Protocolos / ejemplos:

- HTTP/HTTPS (web)
- FTP (transferencia de archivos)
- SMTP / POP3 / IMAP (correo)
- DNS (resolución de nombres)
- SSH (shell remoto seguro)

Capa 6 Presentación PDU: PPDU

Maneja la representación y sintaxis de los datos. Su función es garantizar que información enviada en un formato sea comprensible en el otro extremo, aunque los sistemas usen representaciones internas distintas. También se encarga de cifrado y compresión.

Protocolos / ejemplos:

- Conversión ASCII ↔ EBCDIC
- Little-endian ↔ Big-endian
- Cifrado TLS/SSL (parcialmente)
- Compresión de datos (zlib)
- Codificación MIME

Capa 5 Sesión PDU: SPDU

Permite establecer, gestionar y finalizar sesiones entre aplicaciones. Una sesión es una conexión lógica de más alto nivel que la del transporte. Gestiona diálogos, tokens y puntos de sincronización (checkpoints).

Protocolos / ejemplos:

- Control de diálogo (half/full duplex)
- Administración de tokens (evita colisiones lógicas)
- Checkpoints en transferencias largas (resume tras caída)
- NetBIOS (Windows), RPC

Capa 4 Transporte PDU: TPDU / Segmento

Es la primera capa de extremo a extremo (end-to-end). Divide los datos en segmentos, los transmite a la capa de red y se asegura de que lleguen completos y ordenados. También gestiona multiplexación de aplicaciones mediante puertos.

Protocolos / ejemplos:

- TCP — orientado a conexión, confiable, control de flujo y congestión
- UDP — sin conexión, sin garantías, útil para tiempo real (video, VoIP)
- Puertos: HTTP=80, HTTPS=443, DNS=53, SSH=22
- Three-way handshake de TCP (SYN → SYN-ACK → ACK)

Capa 3 Red PDU: Paquete

Determina la ruta que seguirán los paquetes desde el origen hasta el destino, pudiendo atravesar múltiples redes intermedias. No garantiza entrega ni orden.

Protocolos / ejemplos:

- IP v4 / IPv6 — protocolo principal
- ICMP (ping, traceroute)
- Algoritmos de enrutamiento: OSPF, BGP, RIP
- Enrutamiento estático vs dinámico
- Fragmentación de paquetes IP

Capa 2 Enlace de Datos PDU: Trama (Frame)

Transforma el canal físico (ruidoso) en una línea libre de errores para la capa de red. Fragmenta los datos en tramas, agrega CRC para detección de errores y gestiona el acceso al medio compartido (MAC).

Protocolos / ejemplos:

- Ethernet (IEEE 802.3)
- Wi-Fi (IEEE 802.11)
- Direcciones MAC (48 bits)
- Subcapa MAC — CSMA/CD (Ethernet), CSMA/CA (Wi-Fi)
- Switches operan en esta capa

Capa 1 Física PDU: Bit

Transmite bits puros a través del medio físico. Define voltajes, frecuencias, conectores, distancias máximas y demás aspectos mecánicos, eléctricos y de temporización.

Protocolos / ejemplos:

- Señalización eléctrica (UTP) u óptica (fibra)
- Estándares: RS-232, IEEE 802.3 (100BASE-T)
- ¿Cuántos bits representa el carácter "1" en ASCII? (Respuesta: 8 bits → 00110001)
- Hubs, repetidores, cables, conectores RJ-45

6. Modelo TCP/IP — Las 4 Capas

El modelo que hace funcionar Internet

El modelo TCP/IP surgió de la red **ARPANET**, financiada por DARPA (Departamento de Defensa de EE.UU.) en la década de 1970. A diferencia del OSI, los **protocolos llegaron primero** y el modelo fue una descripción retroactiva de lo que ya funcionaba. Es el modelo que realmente usa Internet hoy.

Capa 4 Aplicación

Absorbe las funciones de las capas de Sesión y Presentación del modelo OSI. Aquí viven todos los protocolos con los que las aplicaciones interactúan directamente.

Protocolos: HTTP, HTTPS, FTP, SMTP, DNS, TELNET, SSH, SNMP, DHCP

Capa 3 Transporte

Equivalente a la capa de Transporte del OSI. Define dos protocolos fundamentales: **TCP** (orientado a conexión, confiable) y **UDP** (sin conexión, más rápido pero sin garantías).

Protocolos: TCP (confiable, control de flujo), UDP (rápido, sin garantías)

Capa 2 Interred (Internet)

Equivalente a la capa de Red del OSI. Define el protocolo **IP** (Internet Protocol) como el mecanismo universal de entrega de paquetes. Sin conexión, sin orden garantizado.

Protocolos: IP v4, IPv6, ICMP, ARP, RARP, IGMP

Capa 1 Acceso a la Red (Host-Red)

Combina las capas Física y de Enlace de Datos del OSI. No está bien especificada en el modelo TCP/IP original — su filosofía fue "usa lo que tengas" y que sea compatible con IP.

Protocolos: Ethernet, Wi-Fi, Token Ring, ATM, Frame Relay, DSL

■ TCP/IP no tiene capas de Sesión ni de Presentación. La experiencia práctica demostró que la mayoría de las aplicaciones no las necesitan como capas separadas, y cuando sí las necesitan (por ejemplo, cifrado TLS), se implementan dentro de la capa de Aplicación.

7. Comparación OSI vs TCP/IP

Similitudes, diferencias y para qué sirve cada uno hoy

Criterio	Modelo OSI	Modelo TCP/IP
N.º de capas	7	4
Origen	ISO 1984 · estándar teórico previo a protocolos	ARPANET/DARPA · modelo descriptivo posterior a protocolos
Separación interfaz / servicio / protocolo	Sí, bien definida	No claramente separada
Ocultamiento de protocolos	Alto — fácil reemplazo de implementaciones	Bajo — protocolos más expuestos y difíciles de reemplazar
Capa de Red	Soporta orientada Y no orientada a conexión	Solo no orientada a conexión (IP es sin conexión)
Capa de Transporte	Solo orientada a conexión	TCP (orientada) Y UDP (no orientada)
Capas Sesión / Presentación	Sí (capas 5 y 6)	No — absorbidas en Aplicación
Uso práctico hoy	Modelo de referencia y enseñanza	Protocolo real de Internet

■ ¿Por qué estudiar OSI si no se usa directamente? Porque es el lenguaje común de la industria. Cuando un ingeniero dice "opera en capa 3" o "el problema está en capa 2", se refiere al modelo OSI. Es la base conceptual indispensable.

8. Capa de Enlace de Datos

Direcciones MAC, Interfaces de Red y Control de Acceso al Medio

A lo largo de esta guía hemos visto que el **Modelo OSI** organiza la comunicación en 7 capas, y que la **Capa 2 — Enlace de Datos** es la responsable de tomar el canal físico ruidoso (capa 1) y entregárselo a la capa de red (capa 3) como si estuviera **libre de errores**. Para lograrlo, esta capa trabaja con **tramas** (frames), utiliza **direcciones MAC** para identificar dispositivos dentro de una misma red local, y gestiona quién puede transmitir y cuándo a través de su **subcapa MAC**.

■ Recuerda: en la tabla de PDUs vista en esta guía, la Capa 2 usa la Trama (Frame) como unidad de datos y la Dirección MAC como sistema de direccionamiento. Es la capa donde operan los switches y los bridges.

8.1 Función general de la Capa de Enlace

La capa de enlace de datos tiene tres responsabilidades principales que se relacionan directamente con los problemas de diseño de capas descritos en la sección 4 de esta guía:

Responsabilidad	Cómo se relaciona con el diseño de capas
Enmarcado (Framing)	Divide el flujo de bits de capa 1 en unidades llamadas tramas, con delimitadores de inicio y fin identificables.
Detección y corrección de errores	Implementa el control de errores visto en sección 4: agrega un CRC (Cyclic Redundancy Check) al final de cada trama para que el receptor detecte corrupciones.
Control de flujo y acceso al medio	Evita que un emisor rápido sature al receptor (control de flujo, sección 4) y coordina quién transmite en un canal compartido mediante la subcapa MAC.

8.2 Estructura de una Trama Ethernet

La trama es la PDU de la capa 2. En el estándar Ethernet (IEEE 802.3), que es el más usado en redes LAN modernas, cada trama tiene la siguiente estructura:

Preámbulo	MAC Destino	MAC Origen	EtherType / Long.	Datos (Payload)	Relleno (Pad)	CRC / FCS
8 bytes	6 bytes	6 bytes	2 bytes	46–1500 bytes	0–46 bytes	4 bytes

Figura 1: Estructura de una trama Ethernet II (IEEE 802.3)

- **Preámbulo (8 bytes)**

  Patrón de bits alternados (10101010...) que sirve para que el receptor sincronice su reloj con el del emisor. Los últimos 2 bits del octavo byte indican el inicio real de la trama (SFD: Start Frame Delimiter).

- **MAC Destino / MAC Origen (6 bytes c/u)**

  Direcciones físicas de 48 bits que identifican al destinatario y al emisor dentro de la red local. Se detallan en la sección 8.3.

- **EtherType (2 bytes)**

  Indica el protocolo encapsulado en el payload: 0x0800 = IPv4, 0x86DD = IPv6, 0x0806 = ARP. Permite que la capa 2 entregue el contenido a la capa 3 correcta (demultiplexación).

- **Datos / Payload (46–1500 bytes)**

  Contenido real: el paquete IP (o lo que sea) encapsulado. El mínimo de 46 bytes existe para garantizar que la trama sea suficientemente larga para que CSMA/CD funcione correctamente.

- **CRC / FCS (4 bytes)**

  Cyclic Redundancy Check: valor calculado sobre todos los campos de la trama. El receptor recalcula el CRC y lo compara; si no coincide, la trama se descarta silenciosamente.

■ El tamaño máximo de payload (1500 bytes) se conoce como MTU (Maximum Transmission Unit). Si un paquete IP es más grande, la capa de red debe fragmentarlo antes de enviarlo. En redes modernas (Jumbo Frames) el MTU puede llegar a 9000 bytes.

8.3 Direcciones MAC

Como vimos al estudiar el diseño de capas (sección 4), cada capa necesita un mecanismo de **direccionamiento** para identificar emisores y receptores. En la capa 2, ese mecanismo son las **direcciones MAC** (Media Access Control).

Dirección MAC	Identificador físico único de **48 bits (6 bytes)** asignado a cada interfaz de red por su fabricante. También llamada **dirección física** o **dirección de hardware**. Se representa en notación hexadecimal separada por dos puntos o guiones, por ejemplo: `00:1A:2B:CC:DD:EE`

Estructura de una dirección MAC

Los 48 bits se dividen en dos bloques de 24 bits. A continuación se muestra una dirección MAC real desglosada en sus dos partes:

← OUI (Organizationally Unique Identifier) · 24 bits · 3 bytes →			← NIC (Número de Serie del Fabricante) · 24 bits · 3 bytes →		
00	**1A**	**2B**	**CC**	**DD**	**EE**
Byte 1 bits 47–40	Byte 2 bits 39–32	Byte 3 bits 31–24	Byte 4 bits 23–16	Byte 5 bits 15–8	Byte 6 bits 7–0

Figura 2: Dirección MAC 00:1A:2B:CC:DD:EE — OUI 00:1A:2B (asignado por IEEE a Cisco) · NIC CC:DD:EE (número de serie del fabricante)

Bloque	Tamaño	Quién lo asigna	Significado
OUI	24 bits (3 bytes)	IEEE — organismo de normalización	Identifica al fabricante del chip de red. Cualquiera puede consultar el OUI en la base de datos pública de la IEEE para saber quién fabricó la tarjeta.
NIC ID	24 bits (3 bytes)	El propio fabricante	Número de serie único para cada tarjeta producida. La combinación OUI + NIC ID garantiza unicidad global: no existen dos NICs con la misma dirección MAC en el mundo.

Bits especiales dentro del OUI

Los dos bits menos significativos del primer byte del OUI tienen significado especial:

Bit	Nombre	Valor 0	Valor 1
Bit 0 del byte 1	**I/G (Individual / Group)**	Unicast (un solo destino)	Multicast / Broadcast (grupo o todos)
Bit 1 del byte 1	**U/L (Universal / Local)**	Asignada globalmente por el fabricante (quemada)	Asignada localmente por software (MAC virtual)

Tipos de direcciones MAC según destino

- **Unicast**
  Identifica a una única interfaz. El paquete es procesado solo por el dispositivo dueño de esa MAC. Ejemplo: `AA:BB:CC:DD:EE:FF`
- **Broadcast**
  Dirección especial `FF:FF:FF:FF:FF:FF`. Todos los dispositivos de la red local deben procesar la trama. Usada por ARP para descubrir a quién pertenece una IP.
- **Multicast**
  Identifica a un grupo de interfaces suscritas. El bit I/G = 1. Usada en IPv6 (prefijo `33:33:xx:xx:xx:xx`) y en protocolos como IGMP para streaming de vídeo.

■ Diferencia clave entre MAC e IP: la dirección MAC identifica el hardware dentro de un segmento de red local (no cambia al saltar de red). La dirección IP identifica lógicamente al host en Internet y puede cambiar. ARP es el protocolo que traduce IP a MAC dentro de una LAN.

8.4 Interfaces de Red (NIC)

Para que un dispositivo pueda participar en una red, necesita al menos una **interfaz de red** (NIC, Network Interface Card). La NIC es el punto físico donde el dispositivo se conecta al medio de transmisión. Desde el punto de vista de capas, la NIC implementa tanto la **capa física** (conversión de bits a señales eléctricas u ópticas) como la **capa de enlace** (gestión de tramas y dirección MAC).

Componentes y función de una NIC

- **Controlador (chipset)**
  Circuito integrado que implementa el protocolo Ethernet u otro estándar. Genera y procesa tramas, calcula el CRC y gestiona las colas de transmisión y recepción.
- **Buffer de memoria**
  Área de memoria dedicada que almacena temporalmente las tramas entrantes y salientes. Permite absorber diferencias de velocidad entre la red y el bus interno del equipo (relación con control de flujo, sección 4).
- **Transceptor (PHY)**
  Circuito que convierte las señales digitales del controlador en señales eléctricas (cable de cobre) u ópticas (fibra). Implementa los aspectos mecánicos y eléctricos de la capa física.
- **Conector físico**
  Puerto RJ-45 para Ethernet por cable, antena Wi-Fi para redes inalámbricas, o conector SFP para fibra óptica.
- **Dirección MAC grabada (BIA)**
  Burned-In Address: la MAC de fábrica guardada en una memoria ROM de la NIC. Puede ser sobreescrita por software (MAC spoofing) para casos de virtualización o pruebas de seguridad.

Ejemplo práctico: ver la MAC de tu equipo

En tu propio computador puedes inspeccionar las interfaces de red y sus MACs con los siguientes comandos:

Sistema Operativo	Comando	Qué muestra
Linux / macOS	`ip link show o ifconfig`	Nombre de interfaz, MAC, estado (UP/DOWN), MTU
Windows	`ipconfig /all o getmac`	Dirección física (MAC), IP, máscara, gateway
Cualquiera	`arp -a`	Tabla ARP: mapeo IP → MAC de vecinos conocidos en la LAN

8.5 Subcapa MAC y Control de Acceso al Medio

En redes de **difusión** (broadcast), como Ethernet o Wi-Fi, múltiples dispositivos comparten el mismo canal físico. Si dos transmiten al mismo tiempo ocurre una **colisión** y los datos se corrompen. La **subcapa MAC** (Media Access Control) es la parte inferior de la capa 2 que resuelve este problema definiendo reglas de acceso al canal.

CSMA/CD — Ethernet por cable (IEEE 802.3)

Carrier Sense Multiple Access with Collision Detection. Protocolo usado en Ethernet clásico (hubs). Su funcionamiento paso a paso:

1. **Escuchar (Carrier Sense)**
   Antes de transmitir, la NIC escucha el canal. Si detecta actividad (portadora), espera.
2. **Transmitir si libre**
   Si el canal está libre durante el tiempo de interframe (IFG = 96 bits de tiempo), comienza a transmitir.
3. **Detectar colisión (Collision Detection)**
   Mientras transmite, monitorea el cable. Si detecta que la señal recibida difiere de la enviada, hay colisión.
4. **Enviar jam signal**
   Transmite una secuencia de 32 bits para avisar a todos los nodos que hubo colisión y deben parar.
5. **Backoff exponencial**
   Espera un tiempo aleatorio (algoritmo de backoff exponencial binario) antes de reintentar. Con cada colisión, el rango de espera se duplica (hasta 16 intentos).

■ En redes Ethernet modernas con switches (full duplex), CSMA/CD ya no es necesario: cada dispositivo tiene su propio canal dedicado al switch y no hay colisiones posibles. Sin embargo, sigue siendo importante entenderlo como base histórica y para redes con hubs o segmentos half-duplex.

CSMA/CA — Redes Wi-Fi (IEEE 802.11)

Carrier Sense Multiple Access with Collision Avoidance. En redes inalámbricas no es posible detectar colisiones mientras se transmite (problema del nodo oculto), por lo que se usa un mecanismo de **evitación** en lugar de detección:

- Escucha el canal y espera un tiempo base (DIFS) más un backoff aleatorio antes de transmitir.
- Opcionalmente intercambia mensajes RTS/CTS (Request to Send / Clear to Send) para reservar el canal y mitigar el problema del nodo oculto.
- Requiere ACK explícito del receptor: si no llega, asume colisión y reintenta con backoff mayor.

8.6 Protocolo ARP — El Puente entre Capa 2 y Capa 3

Como vimos, la capa 3 usa **direcciones IP** y la capa 2 usa **direcciones MAC**. Para que IP pueda entregar un paquete en la red local, necesita conocer la MAC del destino. El **protocolo ARP** (Address Resolution Protocol) resuelve esta traducción.

Paso	Descripción
1. ARP Request	El host origen envía una trama Ethernet con MAC destino FF:FF:FF:FF:FF:FF (broadcast). Pregunta: "¿Quién tiene la IP X.X.X.X? Dile a Y.Y.Y.Y."

2. ARP Reply	Solo el host dueño de esa IP responde con un unicast: "La IP X.X.X.X está en la MAC AA:BB:CC:DD:EE:FF."
3. Caché ARP	El resultado se guarda en la tabla ARP del host por un tiempo (típicamente 20 min). Puedes verla con arp -a.

■ ARP Spoofing: un atacante puede enviar respuestas ARP falsas para asociar su MAC con la IP de otro host (por ejemplo, el gateway). Esto permite ataques Man-in-the-Middle. Es una vulnerabilidad clásica de la capa 2 y motivación para técnicas como Dynamic ARP Inspection en switches gestionados.

9. Tabla Resumen: PDU por Capa

Protocol Data Unit — el nombre que reciben los datos en cada capa

Cada vez que los datos bajan por la pila, la capa actual les agrega su propia cabecera (encapsulación). La unidad resultante recibe un nombre específico según la capa:

Capa OSI	PDU	Dispositivo típico	Dirección usada
7 · Aplicación	Mensaje / APDU	Gateway (app)	URL, nombre de dominio
6 · Presentación	PPDU	—	—
5 · Sesión	SPDU	—	—
4 · Transporte	Segmento (TCP) / Datagrama (UDP)	Firewall (L4)	Puerto (0-65535)
3 · Red	Paquete	Router	Dirección IP
2 · Enlace	Trama (Frame)	Switch, Bridge	Dirección MAC
1 · Física	Bit	Hub, repetidor, cable	N/A

■ Encapsulación: al enviar datos, cada capa "envuelve" el bloque de la capa superior añadiendo su cabecera (y a veces trailer). Al recibir, cada capa "desenvuelve" y entrega el contenido a la capa superior. Este proceso se llama desencapsulación.

10. Preguntas de Reflexión y Autoevaluación

Para consolidar los conceptos y prepararse para evaluaciones

1	¿Por qué es útil dividir las funciones de red en capas? ¿Cuál sería el problema si todo se implementara en una sola capa?
2	Explica la diferencia entre un protocolo y una interfaz de capa. ¿Por qué es importante esta distinción en el modelo OSI?
3	Si envías un correo electrónico, ¿qué protocolos intervienen en cada capa del modelo TCP/IP?
4	¿Por qué TCP/IP no tiene capas de Sesión ni de Presentación? ¿Quién cumple esas funciones en la práctica?
5	Un switch opera en capa 2 y un router en capa 3. ¿Cuál es la diferencia práctica? ¿Qué tipo de dirección usa cada uno para tomar decisiones de reenvío?
6	Explica la diferencia entre TCP y UDP. ¿En qué situación preferirías cada uno? Da un ejemplo de una aplicación que use cada protocolo.
7	¿Qué significa que la comunicación en el modelo de capas sea "horizontal virtual"? ¿Cómo es la comunicación real?
8	Describe el proceso de encapsulación y desencapsulación. ¿Qué ocurre en cada capa al enviar un paquete HTTP?
9	¿Cuál es la función de la subcapa MAC? ¿En qué situaciones es especialmente importante?
10	¿Por qué se dice que el modelo OSI llegó antes de los protocolos y el TCP/IP fue al revés? ¿Qué ventajas y desventajas implica cada enfoque?

■ Consejo: antes de buscar las respuestas, intenta responder de memoria. Luego verifica con tus apuntes y esta guía. La técnica de recuperación activa es la forma más eficaz de afianzar el conocimiento.