APUNTES DE SISTEMAS INFORMÁTICOS

UD4 - INTRODUCCIÓN A LOS SISTEMAS EN RED

Módulo: 0483. Sistemas informáticos
Ciclo Formativo: IF303 - Técnico Superior en Desarrollo de Aplicaciones Web
Profesora: María Paradela García

1. Introducción

1.1. La importancia de las redes en los sistemas informáticos

Vivimos conectados. Desde que enciendes tu ordenador o desbloqueas tu móvil, estás participando en una red. Cada mensaje que envías, cada búsqueda que realizas o cada archivo que compartes, viaja por una compleja infraestructura de equipos interconectados. En el corazón de los sistemas informáticos, las **redes de ordenadores** son el tejido que permite la comunicación, la colaboración y el acceso a la información a escala global.

En los primeros temas de este módulo hemos trabajado con el **hardware** y los **sistemas operativos** que conforman el entorno local de un equipo. Sin embargo, un sistema informático aislado tiene una utilidad limitada. Su verdadero potencial se alcanza cuando forma parte de una red que le permite **compartir recursos**, **intercambiar datos** y **acceder a servicios** ubicados en otros lugares.

Podríamos decir que un ordenador sin red es como un teléfono sin línea: funcional, pero incomunicado.

¿Por qué estudiar redes en un ciclo de Desarrollo de Aplicaciones Web?

Como futuros desarrolladores, vuestro trabajo no termina en escribir código. Las aplicaciones web necesitan **ser desplegadas en servidores**, **comunicarse con bases de datos remotas**, **consumir APIs** o **interactuar con usuarios distribuidos en todo el mundo**. Comprender los fundamentos de las redes os permitirá:

- Saber **cómo viaja la información** desde el navegador del cliente hasta el servidor.
- Diagnosticar **problemas de conectividad o rendimiento**.
- Configurar entornos de prueba y despliegue realistas.
- Trabajar de forma segura, conociendo las vulnerabilidades y buenas prácticas básicas.

1.2. Conceptos previos: nodo, enlace y recurso compartido

Antes de adentrarnos en los tipos de redes y sus componentes, conviene recordar algunos términos básicos que utilizaremos continuamente:

Concepto	Definición	Ejemplo práctico
Nodo	Cualquier dispositivo conectado a una red capaz de enviar o recibir información.	Un ordenador, una impresora o incluso una cámara IP.
Enlace	Medio físico o lógico que conecta dos nodos entre sí.	Un cable Ethernet o una conexión Wi-Fi.

Concepto	Definición	Ejemplo práctico
Recurso compartido	Elemento disponible para varios usuarios o equipos dentro de una red.	Una carpeta compartida, una impresora o una base de datos en línea.

Estos tres elementos —**nodos, enlaces y recursos**— constituyen la esencia de cualquier red, desde las más simples hasta las que sostienen Internet.

> **Curiosidad**
> El primer mensaje transmitido entre dos ordenadores se envió en 1969, dentro del proyecto ARPANET (precursor de Internet). El sistema falló al tercer carácter: el operador tecleó “LOGIN”, pero solo llegaron las letras “LO”. Paradójicamente, “LO” (en inglés “mira”) fue el primer mensaje de la historia de Internet.

Error común

Muchos estudiantes asocian el término “red” exclusivamente a Internet. En realidad, **Internet es solo una red más**, aunque la mayor y más interconectada de todas. Una red puede ser tan pequeña como dos ordenadores en la misma mesa, o tan grande como las infraestructuras que sostienen servicios globales como Google o Netflix.

En resumen

La evolución de los sistemas informáticos ha estado marcada por un objetivo constante: **comunicar**. En esta unidad aprenderás a entender cómo se estructuran las redes, qué elementos las forman, qué modelos las gobiernan y cómo diseñar tus propias conexiones de forma lógica y segura. Será el primer paso hacia la comprensión del funcionamiento de Internet y de las comunicaciones que sustentan cualquier aplicación web moderna.

2. Conceptos básicos de red

Si tuviéramos que definir una red informática en una frase sencilla, podríamos decir que es un conjunto de dispositivos interconectados que comparten información y recursos.

Pero quedarse ahí sería como decir que una ciudad son solo calles y edificios: cierto, pero incompleto. Detrás de una red hay toda una infraestructura física, lógica y organizativa que hace posible que los datos circulen de forma ordenada, segura y eficiente.

2.1. Qué es una red informática

En esencia, una red de ordenadores (o red informática) es un sistema que permite que varios dispositivos (ordenadores, impresoras, servidores, smartphones, cámaras IP, routers) se comuniquen entre sí mediante canales de transmisión que transportan datos codificados.

Para que esta comunicación sea posible, los dispositivos deben “hablar el mismo idioma”: seguir un conjunto de reglas o protocolos que definan cómo se formatean los datos, cómo se envían y cómo se interpretan al llegar a destino.

Podemos imaginar la red como una especie de autopista de la información:

- Las carreteras serían los cables o los medios inalámbricos.
- Los vehículos, los paquetes de datos que transportan información.
- Las señales y normas de tráfico, los protocolos de comunicación.
- Y los nodos (ordenadores, routers, servidores), las intersecciones donde la información se enruta o se detiene.

El objetivo final de cualquier red es facilitar la comunicación y el intercambio de recursos. Pero eso no siempre fue así: durante décadas, los ordenadores fueron islas. Cada empresa, cada universidad, cada usuario tenía su propio entorno cerrado. La revolución llegó cuando se entendió que conectar era multiplicar posibilidades.

2.2. Beneficios de las redes informáticas:

Las redes transformaron la informática de una herramienta individual a una infraestructura colectiva. Los beneficios son muchos, pero podemos destacar los siguientes:

Beneficio	Descripción	Ejemplo
Compartición de recursos	Permite que varios usuarios accedan a impresoras, archivos o conexiones a Internet comunes.	Una impresora compartida en una oficina o un disco NAS accesible desde todos los equipos.
Comunicación inmediata	Facilita la transmisión de mensajes y datos en tiempo real.	El correo electrónico, la mensajería instantánea o una videollamada.
Centralización y gestión eficiente	Los recursos y la seguridad se pueden administrar desde un punto central.	Un servidor de dominio que gestiona usuarios y permisos en toda una empresa.
Escalabilidad	Se pueden añadir nuevos equipos o servicios sin necesidad de reconstruir la red.	Añadir un nuevo ordenador a la red del aula sin modificar toda la configuración.
Reducción de costes	Compartir recursos reduce la inversión en hardware y mantenimiento.	Una sola conexión a Internet para todo un departamento, en lugar de una por equipo.

Colaboración y acceso remoto	Permite el trabajo en equipo desde lugares distintos.	Repositorios de código en GitHub o trabajo compartido en Google Drive.

> **Reflexión:** ¿Podríamos imaginar hoy un entorno de desarrollo web sin red? Sin acceso a repositorios, APIs o documentación online, nuestro trabajo sería prácticamente imposible.

2.3. Clasificación general de las redes

En toda red, independientemente de su tamaño, existen tres elementos clave:

1. Dispositivos o nodos: los equipos que generan, transmiten o reciben la información.
    - Ejemplo: ordenadores, impresoras, servidores, cámaras IP, routers, smartphones.
2. Medios de transmisión: los canales por los que viaja la información.
    - Ejemplo: cables Ethernet, fibra óptica, señales Wi-Fi, infrarrojos o incluso satélite.
3. Protocolos de comunicación: las reglas que garantizan que los datos lleguen correctamente.
    - Ejemplo: TCP/IP, HTTP, FTP, DNS, SMTP, entre otros.

Estos tres componentes son inseparables. Si falta uno, la red no existe.

Nota:

Cuando tu ordenador “no tiene Internet”, lo primero no es culpar al router: revisa la cadena completa.

- ¿Tu adaptador de red (dispositivo) está funcionando correctamente?
- ¿El cable o conexión Wi-Fi (medio) es estable?
- ¿Tienes una dirección IP válida o hay un problema en el protocolo TCP/IP?

Comprender cómo se encadenan estos elementos es el primer paso para diagnosticar problemas reales.

2.4. Tipos de conexión y direccionalidad

Toda red implica un flujo de información entre un emisor y un receptor. Ese flujo puede organizarse de varias formas:

Modo de transmisión	Descripción	Ejemplo
Simplex	La comunicación va en un único sentido.	Un monitor recibe información de la tarjeta gráfica, pero no envía nada de vuelta.
Semidúplex (Half-duplex)	La comunicación puede ir en ambos sentidos, pero no al mismo tiempo.	Los walkie-talkies: cuando uno habla, el otro escucha.

Modo de transmisión	Descripción	Ejemplo
Dúplex (Full-duplex)	La comunicación se produce simultáneamente en ambos sentidos.	Una llamada telefónica o la conexión entre un PC y un switch Ethernet moderno.

> En la mayoría de las redes informáticas actuales, las conexiones son full-duplex, lo que permite una comunicación fluida y simultánea. Sin embargo, en redes más antiguas o en ciertos protocolos inalámbricos, todavía se emplean modos half-duplex para evitar interferencias.

2.5. Clasificación general de las redes

Las redes pueden clasificarse desde muchos puntos de vista: por su alcance, por su tecnología, por su propósito o incluso por su propiedad. En esta unidad nos centraremos en las clasificaciones más prácticas:

Según la extensión geográfica:

- PAN (Personal Area Network): conexión de dispositivos personales, como el móvil y los auriculares Bluetooth.
- LAN (Local Area Network): red local de un aula, empresa o vivienda.
- MAN (Metropolitan Area Network): red que cubre un área urbana, como la red municipal de fibra o Wi-Fi pública.
- WAN (Wide Area Network): redes que abarcan grandes distancias, interconectando varias LAN, como Internet.

Según su propósito:

- **Intranet:** red privada interna, por ejemplo, la de un instituto o empresa.
- **Extranet:** red privada que permite acceso parcial a usuarios externos (clientes o proveedores).
- **Internet:** red pública global interconectada mediante protocolos TCP/IP.

Según la relación entre los equipos:

- **Redes cliente-servidor:** un equipo central (servidor) ofrece servicios o recursos al resto (clientes).
- **Redes entre iguales (peer-to-peer):** todos los nodos pueden actuar como clientes y servidores.

> **Ejemplo:** Cuando compartes un archivo por Airdrop o Bluetooth, estás creando una red P2P temporal. Pero cuando entras en tu correo web, estás accediendo a un servicio cliente-servidor: tu navegador envía una petición HTTP al servidor, y este responde con la página solicitada.

En resumen

Una red informática no es solo una conexión física entre máquinas: es un ecosistema organizado de dispositivos, medios y protocolos que hacen posible la comunicación digital.

Comprender sus componentes y clasificaciones es el primer paso para diseñar, configurar y administrar redes reales, una competencia imprescindible tanto para administradores como para desarrolladores web

3. Tipos de redes según su extensión

A menudo, cuando hablamos de “una red”, nos referimos de forma genérica a cualquier conexión entre dispositivos. Pero no todas las redes son iguales. No tiene nada que ver una red doméstica con tres ordenadores y un router Wi-Fi, con la red troncal de un proveedor de Internet que conecta países enteros.

La diferencia principal entre unas y otras está en su extensión, finalidad y tecnología utilizada.

3.1. De la red personal a internet

Podemos imaginar las redes como círculos concéntricos: en el centro está el individuo con sus dispositivos personales, y conforme nos alejamos, crece la escala hasta llegar a la red mundial. Estos niveles se resumen en cuatro grandes categorías:

Sigla	Nombre completo	Alcance aproximado	Ejemplo típico
PAN	*Personal Area Network*	1–10 metros	Conexión Bluetooth entre el móvil y unos auriculares.
LAN	*Local Area Network*	Hasta unos 100 m (una vivienda o aula)	Red doméstica o de oficina.
MAN	*Metropolitan Area Network*	Varios kilómetros	Red municipal de fibra óptica o WiMAX.
WAN	*Wide Area Network*	De cientos a miles de kilómetros	Internet o la red privada de una multinacional.

Cada tipo de red tiene su propio propósito, coste y complejidad técnica. Veámoslas una a una con más detalle.

3.2. PAN (Personal Area Network)

Una red de área personal (PAN) es la más pequeña de todas. Conecta dispositivos muy próximos entre sí, normalmente alrededor de una persona.

Ejemplo: Tu teléfono móvil conectado a un reloj inteligente, unos auriculares Bluetooth y un portátil está formando una red PAN. Estas redes suelen usar tecnologías inalámbricas de corto alcance como:

- **Bluetooth:** ideal para periféricos (ratones, teclados, auriculares).
- **NFC (Near Field Communication):** comunicación a pocos centímetros, usada en pagos móviles.

- **IrDA (Infrarrojos):** hoy casi en desuso, pero popular en portátiles y PDAs antiguas.

> **Dato curioso:** El término *Personal Area Network* fue acuñado por Thomas Zimmerman en los laboratorios de MIT Media Lab en los años 90, al experimentar con dispositivos "wearables" que se comunicaban a través del cuerpo humano mediante señales eléctricas de baja intensidad.

Ventajas:

- Sin cables ni configuración compleja.
- Bajo consumo y fácil sincronización.

Limitaciones:

- Muy corto alcance.
- Vulnerabilidad a interferencias y ataques por proximidad si no hay cifrado.

3.3. LAN (Local Area Network)

Una LAN (Local Area Network) es probablemente el tipo de red más conocido. Cubre un área limitada (una oficina, un aula, una vivienda) y conecta equipos que necesitan comunicarse rápidamente.

Ejemplo cotidiano: La red del aula de informática: cada ordenador está conectado a un switch, que a su vez enlaza con un router y este con Internet. Todo ocurre dentro de un mismo edificio, por lo que la distancia entre dispositivos es pequeña y las velocidades pueden ser muy altas (1 Gbps o más).

Las LAN suelen utilizar cables Ethernet (UTP, categoría 6 o 7) o conexiones Wi-Fi, y se basan en los protocolos TCP/IP.

Importancia técnica: Las LAN son el bloque fundamental de cualquier red más grande. De hecho, Internet no es más que una red global de LAN interconectadas.

Ventajas:

- Alta velocidad de transmisión.
- Coste relativamente bajo.
- Fácil mantenimiento.

Inconvenientes:

- Cobertura limitada.
- Dependencia de un administrador o de un router para conectarse al exterior.

> **Ejemplo real en cifras:** En una LAN doméstica típica con fibra óptica de 600 Mbps, el tráfico interno entre dispositivos (por ejemplo, copiar un archivo de un PC a otro) puede alcanzar más de 1 Gbps, es decir, más rápido que la propia conexión a Internet.

3.4. MAN (Metropolitan Area Network)

Las MAN (Metropolitan Area Networks) amplían el alcance de las LAN hasta cubrir una ciudad o zona metropolitana. Pueden conectar sedes de una misma empresa, centros educativos o edificios públicos separados por varios kilómetros.

> **Ejemplo real:** El Ayuntamiento de Zaragoza mantiene una red MAN que interconecta sus dependencias municipales y servicios digitales mediante fibra óptica y radioenlaces.

Las MAN suelen apoyarse en tecnologías de banda ancha como:

- Fibra óptica municipal.
- WiMAX (Worldwide Interoperability for Microwave Access).
- Redes de operadores locales (ISP).

> Dato histórico: El concepto de red metropolitana se popularizó en los años 80 con el estándar FDDI (Fiber Distributed Data Interface), que permitía conectar universidades y organismos dentro de una misma ciudad usando fibra óptica.

Ventajas:

- Alta capacidad y fiabilidad.
- Permite compartir recursos entre edificios o sedes.

Limitaciones:

- Coste elevado de instalación y mantenimiento.
- Requiere planificación profesional y equipamiento avanzado.

3.5. WAN (Wide Area Network)

La WAN (Wide Area Network) es el siguiente nivel de escala. Su propósito es interconectar redes locales situadas a grandes distancias: distintas ciudades, países o continentes.

El ejemplo por excelencia es Internet, la red de redes, que combina millones de LAN y MAN interconectadas mediante routers y protocolos comunes.

Otras WAN son privadas: por ejemplo, la red de una multinacional que conecta sus filiales de Madrid, Buenos Aires y Tokio a través de líneas dedicadas o túneles VPN.

Las tecnologías más habituales incluyen:

- Enlaces de fibra óptica de alta capacidad (backbones).
- Satélites de comunicaciones.
- Redes MPLS (Multiprotocol Label Switching).
- Conexiones 4G/5G o microondas para zonas remotas.

> **Ejemplo real:** Cuando haces una videollamada con alguien en otro país, los paquetes de datos pueden viajar por docenas de routers, cruzar océanos por cables submarinos de fibra y llegar a su destino en menos de 300 milisegundos.
>
> **Dato curioso:** El primer cable submarino de fibra óptica transatlántico (TAT-8) se desplegó en 1988 y transmitía apenas 280 Mb/s. Hoy, los cables modernos como el Grace Hopper (Google, 2021) alcanzan los 350 Tb/s, más de un millón de veces más rápidos.

Ventajas:

- Comunicación global.
- Conexión entre redes heterogéneas.

Desventajas:

- Latencias más altas.
- Complejidad en la gestión y la seguridad.

3.6. Comparativa general

Tipo de red	Alcance	Medio típico	Velocidad	Ejemplo real
PAN	1–10 m	Bluetooth, NFC	1–100 Mb/s	Conexión móvil–auriculares
LAN	Hasta 100 m	Ethernet, Wi-Fi	100 Mb/s–10 Gb/s	Red de oficina o aula
MAN	Hasta 50 km	Fibra, WiMAX	10 Mb/s–1 Gb/s	Red municipal de fibra
WAN	Ilimitado	Fibra, satélite, 5G	1 Mb/s–100 Tb/s	Internet o red corporativa global

3.7. Una visión integradora

Podemos pensar las redes como capas de conectividad:

- Tu dispositivo personal forma parte de una PAN.
- Esa PAN se conecta a una LAN doméstica o de empresa.
- Varias LAN dentro de una ciudad se agrupan en una MAN.
- Y todas ellas se enlazan finalmente a través de una WAN, la infraestructura global de Internet.

Cada nivel aporta más alcance y complejidad, pero también más posibilidades. Sin esta jerarquía, Internet no podría existir.

En resumen

Los tipos de red según su extensión nos permiten entender la escala del sistema de comunicaciones que sostiene nuestra vida digital. Desde la conexión inalámbrica de tus auriculares hasta los servidores que alojan tu aplicación web, todos forman parte de un ecosistema interdependiente que une miles de millones de dispositivos bajo un mismo lenguaje: los protocolos de red.

4. Topologías de red

Una red no es solo un conjunto de cables y dispositivos. También tiene una estructura, una forma de interconexión que determina cómo fluye la información, qué ocurre si se interrumpe un enlace y qué tan fácil resulta ampliarla o mantenerla. A esa estructura la llamamos topología.

Podemos entender la topología como el “plano arquitectónico” de una red: define quién está conectado con quién, y por qué camino viajan los datos.

4.1. Concepto de topología física y lógica

Existen dos formas de describir la estructura de una red:

Tipo de topología	Definición	Ejemplo
Física	Representa la disposición real de los cables, dispositivos y conexiones.	En una LAN del aula, el switch central y los cables hacia cada PC.
Lógica	Describe cómo circulan los datos, independientemente de la disposición física.	Una red Wi-Fi en modo infraestructura: todos los datos pasan por el punto de acceso.

En muchas ocasiones, la topología física y la lógica no coinciden. Por ejemplo, una red Wi-Fi físicamente parece una estrella (todos conectan al router), pero lógicamente funciona como un bus: todas las transmisiones comparten el mismo canal de radio.

4.2. Topología en bus

La topología en bus fue una de las primeras en utilizarse en redes locales. Todos los equipos se conectan a un mismo cable principal o troncal por el que circulan los datos en ambos sentidos. Cada mensaje viaja por ese cable hasta llegar al destino indicado.

> **Ejemplo histórico:** Las primeras redes Ethernet (años 80) usaban cable coaxial y conectores tipo T. Cada ordenador pinchaba literalmente en el cable común.

Ventajas:

- Sencillez y bajo coste.
- Consumo mínimo de cable.

Inconvenientes:

- Si el cable principal se corta, toda la red deja de funcionar.
- Dificultad para detectar averías.
- Colisiones de datos frecuentes (dos equipos transmiten a la vez).

> **Curiosidad:** Las primeras LAN de oficinas se montaban con topología en bus porque solo requerían un único cable coaxial y terminadores en los extremos. Si alguien desconectaba un conector mal, podía dejar sin red a toda la planta —y nadie sabía por qué.

4.3. Topología en anillo

En la topología en anillo, los equipos se conectan uno tras otro formando un círculo cerrado. Los datos viajan en una sola dirección, pasando por cada nodo hasta llegar al destino.

> **Ejemplo clásico:** La red Token Ring de IBM, muy popular en los años 90, utilizaba este sistema con una señal especial (token) que se iba pasando de un equipo a otro para evitar colisiones.

Ventajas:

- Tráfico ordenado y sin colisiones.
- Rendimiento predecible.

Inconvenientes:

- Si un nodo o conexión falla, se interrumpe todo el anillo.
- Dificultad para añadir o quitar equipos.

Analogía: Imagina un tren que da vueltas por una vía circular. Cada estación representa un ordenador. El tren (el token) solo puede estar en un lugar a la vez, y solo quien lo tiene puede “hablar”. Ordenado, pero poco flexible.

4.4. Topología en estrella

La **topología en estrella** es la más común hoy en día. Todos los equipos se conectan a un dispositivo central (switch, hub o punto de acceso) que actúa como intermediario.

> **Ejemplo real:** La red del aula de informática: cada ordenador se conecta mediante cable al switch central, que se encarga de reenviar los datos al destinatario correcto.

Ventajas:

- Fácil de instalar y mantener.

- Si un cable falla, solo se desconecta un equipo, no toda la red.
- Permite detectar fallos y aislar dispositivos fácilmente.

Inconvenientes:

- Dependencia total del nodo central: si el switch falla, la red se cae.
- Requiere más cableado que una red en bus.

> **Curiosidad tecnológica:** Las redes domésticas Wi-Fi también son en estrella: el router central es el punto de conexión común. Por eso, cuando el router "se cuelga", parece que todos los dispositivos fallan a la vez.

4.5. Topología en malla

En una topología en malla, cada dispositivo está conectado a varios otros dispositivos. Esto proporciona redundancia, es decir, múltiples rutas posibles para los datos. Si un enlace se rompe, la información puede tomar otro camino.

> Ejemplo: Las redes troncales de Internet y las redes Wi-Fi malladas (Mesh) domésticas. En estas últimas, varios puntos de acceso distribuidos por la casa se comunican entre sí, asegurando cobertura en todas las zonas sin depender de un solo router.

Ventajas:

- Alta fiabilidad y tolerancia a fallos.
- Excelente rendimiento en redes críticas.

Inconvenientes:

- Muy costosa y compleja de implementar.
- Difícil de escalar en grandes instalaciones (número de conexiones crece exponencialmente).

Dato técnico: En una red completamente mallada de n nodos, cada uno necesita ($n-1$) conexiones. Por ejemplo, con 5 nodos habría 10 enlaces; con 10 nodos, ¡45! Por eso, en la práctica, se usan mallas parciales, con enlaces redundantes solo en los puntos clave.

4.6. Topología en árbol

La topología en árbol combina características de la estrella y del bus. Se organiza jerárquicamente: un nodo raíz (normalmente un switch o router principal) se conecta a otros dispositivos que, a su vez, pueden actuar como concentradores secundarios.

> **Ejemplo:** Una red de instituto donde el switch principal del servidor se conecta a los switches de cada aula, y cada uno de estos a los ordenadores del alumnado.

📊 **Ventajas:**

- Fácil expansión: se pueden añadir ramas.
- Organización lógica y segmentada.
- Aísla fallos locales sin afectar al resto de la red.

Inconvenientes:

- Si falla el nodo raíz, la red queda inutilizada.
- Requiere planificación jerárquica.

> **Analogía:** Como un árbol genealógico: el tronco principal reparte la "información" hacia ramas y hojas. Cada rama depende de las anteriores, pero las hojas no se comunican directamente entre sí.

4.7. Topologías híbridas

En la práctica, las redes reales no siguen una única topología pura. Suelen combinar varias para adaptarse a las necesidades del entorno. Por ejemplo:

- Una empresa puede tener una topología en estrella en cada departamento y conectarlas entre sí mediante un anillo o una malla parcial.
- En una vivienda moderna, los routers Wi-Fi forman una malla, mientras los dispositivos cableados siguen una estrella.

Ventaja: Flexibilidad. Las topologías híbridas aprovechan las ventajas de cada tipo y reducen sus desventajas.

> **Ejemplo:** Las redes de campus universitarios combinan distintas topologías: los edificios se interconectan en anillo o malla, pero dentro de cada planta se usa estrella para los puestos de trabajo.

4.8. Comparativa general

Topología	Ventajas principales	Desventajas principales	Uso típico
Bus	Económica, simple	Colisiones, poco fiable	Redes antiguas, coaxial
Anillo	Ordenado, sin colisiones	Poco flexible, sensible a fallos	Token Ring, redes industriales
Estrella	Fácil mantenimiento, fiable	Dependencia del nodo central	LAN modernas
Malla	Muy robusta, tolerante a fallos	Costosa, compleja	Backbone de Internet, redes Mesh

Topología	Ventajas principales	Desventajas principales	Uso típico
Árbol	Escalable, estructurada	Falla del nodo raíz afecta al resto	Grandes instalaciones educativas o empresariales
Híbrida	Flexible, adaptable	Difícil de documentar	Redes corporativas o domésticas mixtas

La topología de red es una decisión estratégica: condiciona el rendimiento, el coste y la fiabilidad del sistema.

- En un entorno pequeño, estrella suele ser la mejor opción.
- En infraestructuras críticas, malla o árbol jerárquico aportan redundancia.
- En instalaciones modernas, lo habitual es una topología híbrida, que combina seguridad, simplicidad y escalabilidad.

En la próxima sección entraremos en los modelos OSI y TCP/IP, que explican *cómo viaja realmente la información dentro de esas topologías*, capa a capa.

5. Modelos de referencia OSI y TCP/IP

Hasta ahora hemos visto cómo se organizan físicamente las redes y qué tipos existen según su extensión. Sin embargo, aún no sabemos cómo se comunican los equipos entre sí, cómo un mensaje pasa del teclado de un ordenador a la pantalla de otro, ni qué ocurre en ese trayecto.

Responder a esas preguntas nos lleva a los modelos de referencia de red, auténticas guías conceptuales que explican *cómo se construye la comunicación paso a paso, de forma ordenada y estandarizada*.

5.1. ¿Por qué se necesitan modelos de red?

Imagina que un ordenador con Windows necesita enviar un archivo a un servidor Linux. Ambos sistemas operativos son diferentes, hablan “idiomas informáticos” distintos… pero deben entenderse. ¿Cómo lo consiguen?

A lo largo de los años, la comunidad técnica internacional comprendió que era necesario un lenguaje común, una forma de estructurar la comunicación para que cualquier dispositivo, independientemente de su fabricante o sistema operativo, pudiera conectarse a cualquier otro.

De esa necesidad nacieron dos modelos fundamentales:

1. El modelo OSI (Open Systems Interconnection), teórico y muy detallado.
2. El modelo TCP/IP, más simple y práctico, en el que se basa Internet.

5.2. Modelo OSI: capas, funciones y ejemplos

El modelo OSI fue desarrollado por la ISO (Organización Internacional de Normalización) en los años 80.

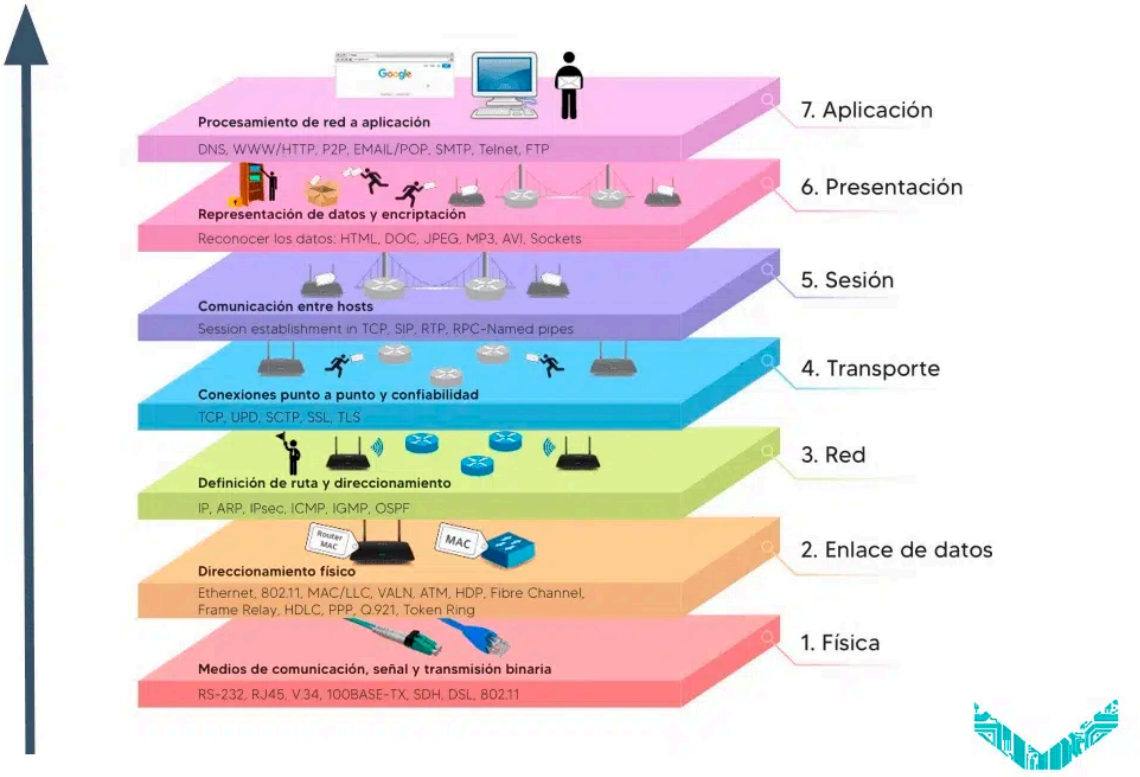
Su objetivo era definir un marco general que describiera todas las etapas que sigue la información en una comunicación de red.

Dividió ese proceso en siete capas, cada una con una función específica.

Capa (nº)	Nombre	Función principal	Ejemplo
7	**Aplicación**	Interfaz con el usuario o con el software.	Navegador web, cliente de correo.
6	**Presentación**	Traduce los datos (formato, codificación, cifrado).	Compresión, SSL/TLS, ASCII, JPEG.
5	**Sesión**	Controla las conexiones entre dispositivos.	Establecer, mantener y finalizar sesiones.
4	**Transporte**	Divide los datos en segmentos y garantiza su entrega.	TCP, UDP.
3	**Red**	Gestiona direcciones y rutas de los paquetes.	IP, ICMP, routers.
2	**Enlace de datos**	Detecta errores y controla el acceso al medio físico.	Ethernet, Wi-Fi (802.11), switches.
1	**Física**	Transmite bits a través del medio físico.	Cables, señales eléctricas, conectores RJ45.

Cada capa ofrece servicios a la capa superior y utiliza los servicios de la inferior.

Esto se llama **encapsulación**: los datos descienden capa a capa, añadiendo información de control en cada paso.



5.3. Analogía con el correo postal

Una forma sencilla de entender el modelo OSI es imaginar que enviamos una carta por correo tradicional:

Etapa real	Equivalente en OSI	Qué ocurre
Escribes el mensaje y lo metes en un sobre.	Capa de Aplicación / Presentación	Preparas la información.
Añades la dirección del destinatario y tu remitente.	Capa de Red	Asignas direcciones IP.
Entregas la carta en la oficina de correos.	Capa de Enlace / Física	Se transmite por cables o señales.
El cartero la transporta y la entrega al buzón correcto.	Capa de Transporte	Se asegura de que llegue completa.
El destinatario abre la carta y la lee.	Capas superiores	Se interpreta y muestra la información.

En informática, el proceso es similar, pero la carta es digital y viaja en paquetes de datos.

Cada capa añade su propio “sobre” con instrucciones específicas: dirección, tipo de protocolo, control de errores, etc.

Al llegar al destino, las capas se van retirando en orden inverso, hasta entregar el mensaje original a la aplicación.

5.4. Encapsulación y desencapsulación

El concepto más importante del modelo OSI es la encapsulación de datos. Cuando un mensaje viaja por la red, cada capa añade su propio encabezado (y, en algunos casos, una cola) con información de control.

Proceso de envío:

1. La aplicación genera los datos (por ejemplo, una solicitud HTTP).
2. La capa de transporte los divide en segmentos.
3. La capa de red encapsula esos segmentos en paquetes con direcciones IP.
4. La capa de enlace los convierte en tramas con direcciones físicas (MAC).
5. Finalmente, la capa física los transmite como bits por el cable o el aire.

Cuando llegan al destino, el proceso se desencapsula en sentido inverso: los encabezados se eliminan capa a capa hasta reconstruir el mensaje original.

Dato técnico: Cada capa tiene su propia unidad de datos:

- Capa 1 (Física): bits
- Capa 2 (Enlace): tramas
- Capa 3 (Red): paquetes
- Capa 4 (Transporte): segmentos
- Capas 5–7: datos

5.5. Modelo TCP/IP: la base de Internet

Mientras la ISO elaboraba su modelo teórico OSI, el Departamento de Defensa de EE. UU. desarrolló otro modelo más pragmático para sus redes militares y académicas: el modelo TCP/IP (Transport Control Protocol / Internet Protocol). Su éxito fue tal que acabó convirtiéndose en el estándar de facto de Internet.

El modelo TCP/IP agrupa las funciones del OSI en cuatro capas principales:

Capa TCP/IP	Equivalente OSI	Función principal	Ejemplos
Aplicación	5, 6, 7	Interacción con el usuario y los programas.	HTTP, FTP, DNS, SMTP, SSH.
Transporte	4	Comunicación extremo a extremo.	TCP, UDP.

Capa TCP/IP	Equivalente OSI	Función principal	Ejemplos
Internet	3	Encaminamiento y direccionamiento.	IP, ICMP, ARP.
Acceso a la red	1 y 2	Transmisión física y enlace de datos.	Ethernet, Wi-Fi, PPP.

Diferencia clave:

El modelo TCP/IP no separa tanto las funciones como el OSI, pero describe con precisión cómo funcionan las redes reales.

Es el que se utiliza para configurar direcciones IP, diseñar protocolos y entender la comunicación entre navegadores, servidores y servicios web.

5.6. Ejemplo de comunicación: desde el navegador hasta el servidor

Supongamos que introduces en tu navegador la dirección:

https://www.wikipedia.org

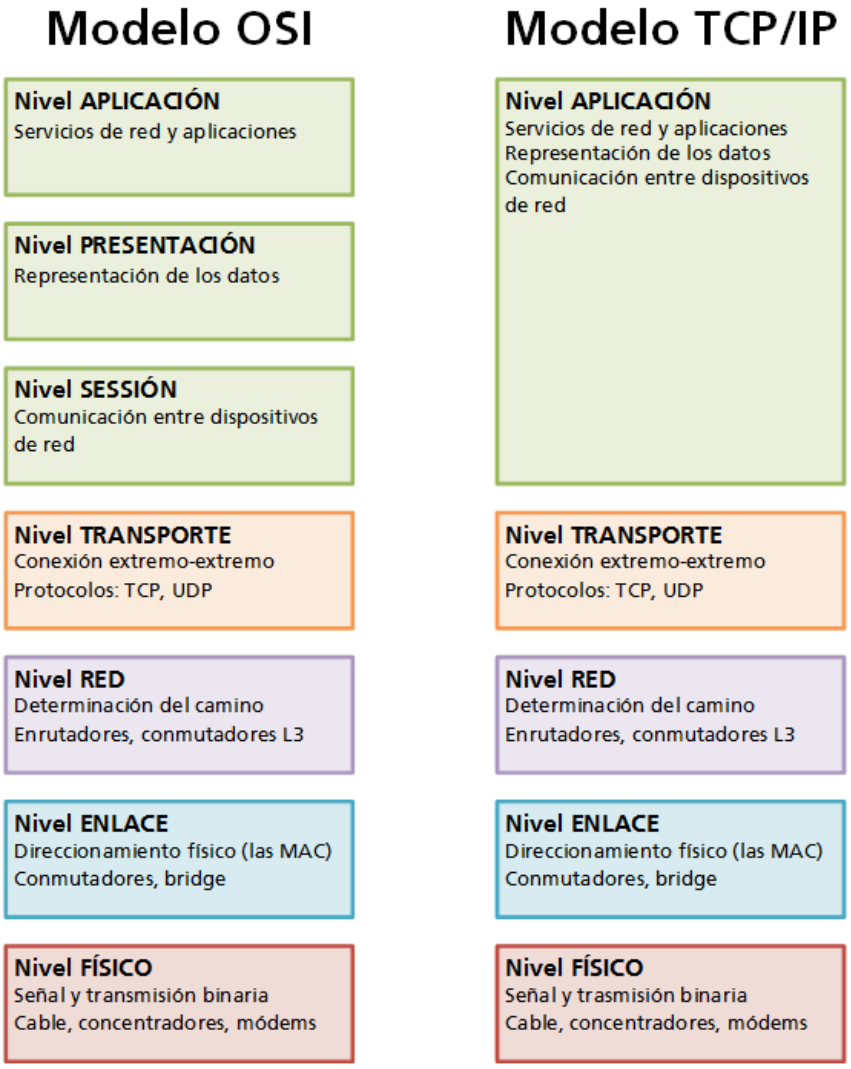
1. **Capa de Aplicación:** El navegador genera una solicitud HTTP (con cifrado HTTPS) para pedir la página web.
2. **Capa de Transporte:** TCP divide esa solicitud en segmentos numerados y garantiza que todos lleguen al servidor sin errores.
3. **Capa de Internet:** IP añade las direcciones de origen y destino (tu IP pública y la del servidor).
4. **Capa de Acceso a la red:** Ethernet encapsula los datos en tramas y los envía por tu cable o Wi-Fi hasta el router.
5. En el destino, el servidor **desencapsula** las capas, interpreta la solicitud y responde con los datos de la página.

> **Dato:** En una simple carga de una web moderna, pueden viajar cientos de paquetes TCP/IP, cruzando routers, switches y firewalls de varios países, todo en menos de un segundo.

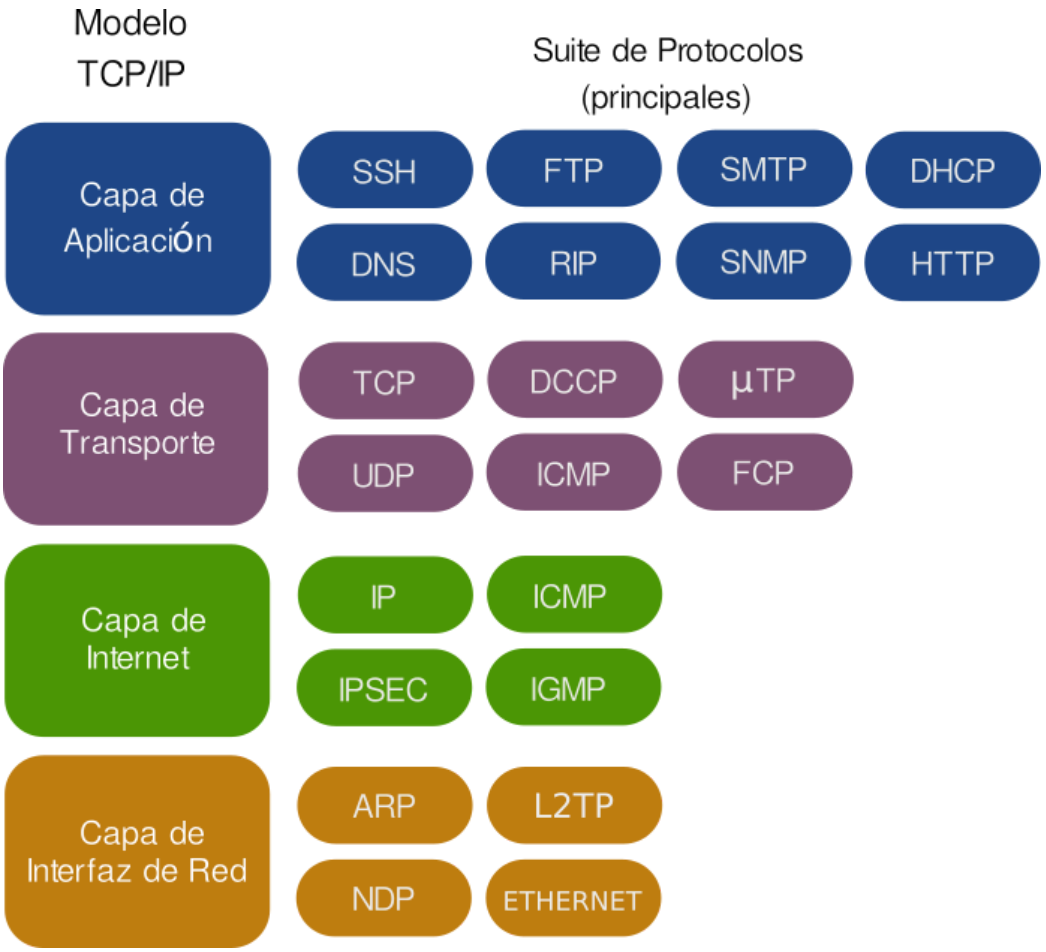
5.7. Correspondencia OSI vs TCP/IP

Modelo OSI (7 capas)	Modelo TCP/IP (4 capas)	Ejemplo de protocolo
Aplicación	Aplicación	HTTP, FTP, SMTP
Presentación	Aplicación	SSL/TLS, JPEG, ASCII
Sesión	Aplicación	NetBIOS, RPC
Transporte	Transporte	TCP, UDP

Modelo OSI (7 capas)	Modelo TCP/IP (4 capas)	Ejemplo de protocolo
Red	Internet	IP, ICMP, ARP
Enlace de datos	Acceso a la red	Ethernet, Wi-Fi
Física	Acceso a la red	Cables, señales, conectores



5.8. Protocolos más comunes



5.9. Reflexión: ¿por qué es importante conocer las capas?

Para un desarrollador web, entender los modelos de red no es un capricho teórico: es una herramienta práctica. Saber qué ocurre en cada capa permite:

- Diagnosticar dónde se rompe una conexión.
- Comprender errores como “Timeout”, “DNS no encontrado” o “Conexión reiniciada por el servidor”.
- Implementar servicios web seguros y eficientes.
- Comunicarte con administradores de sistemas “en su idioma”.

> **Ejemplo:** Cuando haces un `ping` a una dirección IP, estás probando la capa 3 (Red) mediante el protocolo ICMP. Si haces un `tracert`, analizas las rutas que sigue el paquete a través de los routers. Y si inspeccionas una conexión HTTPS con las herramientas de desarrollo del navegador, estás viendo cómo interactúan las capas 4 a 7.

Conclusión:

- El **modelo OSI** explica *cómo debería funcionar* una red, capa a capa, de forma teórica y ordenada.
- El **modelo TCP/IP** describe *cómo funciona realmente Internet*.
- Ambos modelos nos ayudan a entender, diseñar y depurar redes complejas dividiendo el problema en partes manejables.

> **Idea para recordar:** Si una red es como una empresa, las capas son sus departamentos: cada uno cumple su función, se comunica con el de arriba y el de abajo, y juntos hacen que todo el sistema funcione.

6. Componentes de una red informática

Una red informática no es una entidad abstracta: está formada por equipos, dispositivos y medios físicos que hacen posible la comunicación entre nodos.

Podemos imaginarla como un sistema de transporte: los dispositivos son los vehículos, los medios de transmisión son las carreteras, y los protocolos son las normas de tráfico que evitan el caos.

6.1. Clasificación general

Los componentes de una red pueden dividirse en tres grandes grupos:

1. Dispositivos de red: permiten la conexión, gestión o encaminamiento de datos.
2. Medios de transmisión: transportan la información de un punto a otro.
3. Software de red: los protocolos, servicios y programas que gestionan la comunicación.

En este punto nos centraremos en los dispositivos y medios físicos, los elementos tangibles que encontramos en cualquier aula o empresa.

6.2. Dispositivos de red

a) Tarjeta de interfaz de red (NIC)

La Network Interface Card (NIC) o tarjeta de red es el componente que permite a un equipo conectarse a la red. Puede ser:

- Integrada en la placa base (lo habitual hoy).
- PCIe (interna) o USB (externa), para añadir conectividad adicional.

Cada tarjeta tiene una dirección física única, llamada dirección MAC (Media Access Control), formada por 48 bits (12 dígitos hexadecimales). Ejemplo: `00-1A-92-4F-7B-AC`

> **Dato curioso:** Los tres primeros pares identifican al fabricante (OUI – *Organizationally Unique Identifier*), y los tres últimos son un número de serie único. Esto significa que no existen dos tarjetas en el mundo con la misma dirección MAC.

Importancia práctica:

- La NIC se encarga de enviar y recibir tramas (nivel 2 OSI).
- Gestiona la conversión de bits eléctricos o de radio en información digital interpretable.

b) Concentradores o *hubs*

Los hubs fueron los primeros dispositivos que permitían conectar varios equipos entre sí dentro de una red local. Funcionan de forma muy básica: cuando un equipo envía una trama, el hub la replica a todos los puertos, sin distinguir destinatarios.

- **Ventajas:** sencillos y baratos.
- **Desventajas**: ineficientes y poco seguros (todo el tráfico es visible para todos los equipos).

Resultado: Hoy están prácticamente en desuso, sustituidos por switches, que ofrecen un funcionamiento mucho más inteligente.

c) Conmutadores o *switches*

El switch es el corazón de la mayoría de las redes locales modernas. A diferencia del hub, analiza la dirección MAC de destino de cada trama y la envía solo al puerto correspondiente, evitando colisiones.

Ventajas principales:

- Aumenta la velocidad y la eficiencia de la red.
- Permite segmentar tráfico (VLANs en entornos avanzados).
- Aporta más seguridad y control sobre el flujo de datos.

Tipos comunes:

- **No gestionables:** plug and play, sin configuración.
- **Gestionables:** permiten configurar VLANs, prioridades, estadísticas, seguridad, etc.

> **Ejemplo real:** En el aula, el switch central al que se conectan todos los ordenadores actúa como intermediario entre ellos y el router. Si un equipo quiere comunicarse con otro, el switch se encarga de enviar la trama directamente, sin molestar a los demás.

d) Enrutadores o *routers*

El router (enrutador) conecta redes diferentes entre sí y decide la mejor ruta para los paquetes de datos. Trabaja en la capa 3 (Red) del modelo OSI, interpretando direcciones IP y tablas de encaminamiento.

Funciones principales:

- Conectar la red local (LAN) con la red exterior (WAN).
- Asignar direcciones IP (mediante DHCP).
- Traducir direcciones internas a externas (NAT).

- Filtrar tráfico mediante cortafuegos integrados.

Ejemplo: Tu router de casa no solo da Internet, también actúa como servidor DHCP, NAT y firewall. Cuando tu PC pide una página web, el router envía la solicitud a Internet usando su IP pública y traduce las respuestas hacia tu equipo.

> **Dato técnico:** Los routers actuales suelen integrar un switch (para las conexiones cableadas) y un punto de acceso Wi-Fi. Por eso, aunque solo veas una "cajita", dentro hay tres dispositivos en uno.

e) Puntos de acceso inalámbrico (*Access Points*)

Los Access Points (AP) permiten conectar dispositivos Wi-Fi a una red cableada. Funcionan en la capa 2, retransmitiendo las tramas entre el medio inalámbrico y el cableado.

Tipos de AP:

- **Independientes:** se configuran uno a uno.
- **Controlados:** gestionados desde un controlador central (útiles en empresas o centros educativos).

Ejemplo real: Los puntos de acceso distribuidos por el instituto forman una red Wi-Fi común. Cada uno cubre una zona diferente, y los dispositivos se conectan automáticamente al más cercano.

> **Curiosidad:** Los routers domésticos integran un AP interno, pero en instalaciones grandes se usan varios AP conectados a un mismo switch para dar cobertura completa.

f) Servidores y clientes

En una red, los equipos no son todos iguales. Algunos proporcionan recursos o servicios (**servidores**), mientras otros los utilizan (**clientes**).

Tipo de servidor	Función principal	Ejemplo
Servidor de archivos	Almacena y comparte datos.	NAS, servidor Samba.
Servidor web	Aloja sitios web.	Apache, Nginx.
Servidor DNS	Traduce nombres de dominio en direcciones IP.	Servidores raíz de Internet.
Servidor DHCP	Asigna direcciones IP automáticamente.	Integrado en routers.
Servidor de impresión	Gestiona colas de impresión compartidas.	Servidor Windows o CUPS en Linux.

Ejemplo: En una red de empresa, el servidor DHCP asigna IPs a los equipos, el servidor de archivos almacena documentos y el servidor web aloja la intranet corporativa. Cada cliente accede a ellos según sus permisos de usuario.

g) Cortafuegos (*firewalls*)

El **firewall** es el guardián de la red. Controla qué tráfico puede entrar o salir según reglas definidas. Puede ser:

- **Software:** integrado en el sistema operativo (Windows Defender Firewall, UFW en Linux).
- **Hardware:** dispositivos dedicados que filtran el tráfico antes de entrar en la LAN.

Ejemplo: Bloquear el puerto 21 (FTP) en un cortafuegos impide que se establezcan conexiones de ese tipo, protegiendo la red de accesos no deseados.

> **Dato curioso:** El término *firewall* proviene de las paredes cortafuegos que impiden que un incendio se propague de una sección a otra: la idea es la misma, pero con datos en vez de llamas.

6.3. Medios de transmisión: cobre, fibra óptica, radiofrecuencia

Los medios de transmisión son las “carreteras” por las que circula la información. Podemos clasificarlos en guiados (con cable) e inalámbricos.

a) Medios guiados (con cable)

1. **Par trenzado (UTP/STP):**
   - El más común en redes Ethernet.
   - Los pares de cables están trenzados para reducir interferencias.
   - Se usa con conectores **RJ45**.
   - Categorías más usadas: **Cat 5e, 6, 6A, 7, 8**, que determinan velocidad y alcance.
2. **Cable coaxial:**
   - Utilizado antiguamente en redes en bus.
   - Hoy se usa más en televisión por cable e Internet de operadoras (DOCSIS).
3. **Fibra óptica:**
   - Transmite datos mediante pulsos de luz.
   - Ofrece **altas velocidades (hasta 100 Gbps)** y gran inmunidad a interferencias.
   - Se usa en redes troncales y conexiones de alta capacidad.

Comparativa rápida:

Medio	Velocidad típica	Distancia máxima	Uso principal
UTP Cat 6	1 Gbps	100 m	LAN doméstica o de oficina
Fibra óptica	>10 Gbps	Hasta 40 km	Enlaces troncales, ISP
Coaxial	100 Mb/s	500 m	Red de TV o Internet por cable

b) Medios no guiados (inalámbricos)

- **Radiofrecuencia (Wi-Fi, Bluetooth):** transmisión de datos mediante ondas.
- **Infrarrojos:** comunicación por luz no visible; actualmente en desuso.
- **Satélite:** conexión a Internet o transmisión de datos a gran distancia.
- **Microondas:** enlaces punto a punto en zonas rurales o empresariales.

> **Ejemplo:** Las redes Wi-Fi de los institutos o las redes 5G urbanas son medios no guiados. El aire, en este caso, actúa como medio de transmisión.

6.4. Direccionamiento físico (MAC) y lógico (IP)

Cada dispositivo conectado a la red necesita una **identidad** para comunicarse.

- **Dirección MAC:** Fija, grabada en la tarjeta de red. Identifica al dispositivo físicamente (capa 2)
  Ejemplo: `00:1A:2B:3C:4D:5E`
- **Dirección IP:** Asignada dinámicamente o fija (capa 3). Identifica el dispositivo dentro de una red lógica.
  Ejemplo: `192.168.1.25` (IPv4) o `fe80::1a2b:3c4d:5e6f` (IPv6).

Analogía: La dirección MAC sería el *DNI* del dispositivo, mientras que la dirección IP sería su *domicilio actual*. Un ordenador puede cambiar de red (y por tanto de IP), pero seguirá teniendo la misma MAC.

6.5. Herramientas básicas de diagnóstico

Conocer los componentes está bien, pero saber cómo verificar que funcionan es aún mejor. Algunas herramientas universales para cualquier técnico son:

Comando	Función	Ejemplo
`ipconfig` (Windows) / `ifconfig` (Linux)	Muestra la configuración IP de las interfaces.	`ipconfig /all`
`ping`	Comprueba conectividad entre dos dispositivos.	`ping 8.8.8.8`
`tracert` / `traceroute`	Muestra la ruta que siguen los paquetes hasta un destino.	`tracert www.google.com`
`arp -a`	Muestra la tabla de direcciones IP ↔ MAC.	—
`netstat`	Lista conexiones activas y puertos abiertos.	`netstat -an`

En resumen

Los componentes de red forman el **ecosistema físico y lógico** que sostiene cualquier comunicación digital.

- Las **tarjetas de red** son las puertas de entrada y salida.
- Los **switches y routers** son las intersecciones y autopistas.
- Los **medios de transmisión** son las carreteras que transportan los datos.
- Y las **direcciones MAC e IP** son las matrículas que identifican a cada vehículo.

Dominar estos conceptos te permitirá **diagnosticar, diseñar y configurar** redes reales, además de comprender mejor lo que ocurre bajo la superficie de Internet.

7. Redes inalámbricas 802.11

Las redes inalámbricas son, sin duda, la forma de conexión más utilizada en la actualidad.

En casa, en clase, en un bar o en el transporte público, nos conectamos a Internet sin cables y casi sin pensar en cómo funciona ese proceso.

Pero detrás de esa aparente simplicidad hay tecnología de precisión, protocolos estandarizados y un complejo sistema de frecuencias y seguridad.

7.1. Concepto general

Una red inalámbrica (Wireless LAN o WLAN) es un tipo de red local que utiliza ondas electromagnéticas para transmitir datos entre dispositivos, en lugar de cables. Los estándares que la regulan pertenecen a la familia IEEE 802.11, publicada por el Institute of Electrical and Electronics Engineers, y actualizada periódicamente para mejorar velocidad, cobertura y estabilidad.

> **Idea clave:** El Wi-Fi no es una tecnología única, sino un conjunto de estándares que evolucionan constantemente. Cada versión de 802.11 introduce mejoras en velocidad, frecuencia y eficiencia energética.

7.2. Elementos de una red inalámbrica

Una red inalámbrica típica está compuesta por:

Elemento	Función principal
Punto de acceso (AP)	Dispositivo que emite la señal Wi-Fi y conecta los equipos inalámbricos con la red cableada.
Clientes inalámbricos	Ordenadores, móviles, tablets o dispositivos IoT que se conectan al AP.

Elemento	Función principal
SSID (Service Set Identifier)	Nombre de la red Wi-Fi visible para los usuarios.
Canal	Frecuencia dentro de la banda utilizada (2.4 o 5 GHz) por la red.
Modo de operación	Define si el punto de acceso actúa como infraestructura (centralizada) o ad-hoc (equipo a equipo).

Ejemplo:

Cuando abres el móvil y ves “RIOARBA”, estás visualizando un SSID emitido por un punto de acceso del centro.

Al conectarse, los dispositivos negocian parámetros como velocidad, canal, cifrado y dirección IP antes de tener acceso real a Internet.

7.3. Estándares 802.11 y sus características

Cada versión de la norma 802.11 define un conjunto de mejoras.

En la práctica, todos los dispositivos modernos son retrocompatibles, pero la velocidad final dependerá del estándar más lento implicado.

Estándar	Frecuencia	Velocidad máxima teórica	Año	Notas destacadas
802.11b	2,4 GHz	11 Mb/s	1999	Primera versión popular; interferencias con microondas y Bluetooth.
802.11g	2,4 GHz	54 Mb/s	2003	Compatible con b; mejora la modulación.
802.11n	2,4 / 5 GHz	600 Mb/s	2009	Introduce MIMO (múltiples antenas).
802.11ac (Wi-Fi 5)	5 GHz	>1 Gb/s	2013	Usa canales anchos y MU-MIMO; estándar doméstico durante una década.
802.11ax (Wi-Fi 6)	2,4 / 5 / 6 GHz	Hasta 9,6 Gb/s	2019	Más eficiente con muchos usuarios conectados; base del Wi-Fi actual.
802.11be (Wi-Fi 7)	6 GHz	>30 Gb/s	2024	En fase de adopción; orientado a entornos de alta densidad y baja latencia.

Ejemplo práctico: Una red Wi-Fi 6 de aula puede gestionar más de 50 dispositivos simultáneamente, algo impensable con Wi-Fi 4 o anteriores.

> **Dato curioso:** El nombre “Wi-Fi” no significa *Wireless Fidelity*, como mucha gente cree. Fue una marca comercial creada por la Wi-Fi Alliance en 1999 para facilitar la difusión del estándar 802.11b. El término no tiene traducción técnica: simplemente sonaba bien.

7.4. Bandas de frecuencia y canales

Los puntos de acceso Wi-Fi emiten en bandas de frecuencia específicas, asignadas internacionalmente:

Banda	Ventajas	Inconvenientes
2,4 GHz	Mayor alcance, buena penetración en paredes.	Solo 3 canales no solapados (1, 6 y 11); interferencias con otros dispositivos.
5 GHz	Más velocidad y menos interferencias.	Alcance menor; más sensible a obstáculos.
6 GHz (Wi-Fi 6E y 7)	Canales amplios, baja congestión.	Poca penetración; dispositivos compatibles aún escasos.

> **Consejo técnico:** En redes saturadas (bloques de viviendas o aulas con muchos routers), cambiar el canal de emisión puede mejorar drásticamente el rendimiento sin necesidad de más potencia.

7.5. Modos de funcionamiento

Modo	Descripción	Uso típico
Infraestructura	Todos los dispositivos se conectan a un AP central.	Redes domésticas, empresariales, centros educativos.
Ad-hoc	Los equipos se comunican directamente entre sí, sin AP.	Conexiones temporales o entre portátiles.
Mesh (malla)	Varios AP se interconectan, compartiendo señal y cobertura.	Hogares o edificios con múltiples zonas de acceso.

Ejemplo real: En una red Wi-Fi mesh doméstica, cada nodo (punto de acceso) se comunica con los demás. Esto permite moverte por la casa sin perder conexión: tu móvil cambia automáticamente al nodo más cercano.

7.6. Seguridad en redes inalámbricas

La libertad del Wi-Fi tiene un precio: la seguridad. Al no existir un cable físico, las transmisiones pueden ser captadas por cualquiera dentro del alcance de la señal. Por ello, los estándares 802.11 incluyen mecanismos de autenticación y cifrado que han evolucionado con los años.

Protocolo de seguridad	Año	Tipo de cifrado	Nivel de seguridad	Estado actual
WEP (Wired Equivalent Privacy)	1999	RC4 (estático)	Bajo	Obsoleto; fácilmente vulnerable.
WPA (Wi-Fi Protected Access)	2003	TKIP	Medio	Transitorio; ya en desuso.
WPA2	2004	AES	Alto	Estándar predominante durante años.
WPA3	2018	SAE (Simultaneous Authentication of Equals)	Muy alto	Actual estándar recomendado.

Ejemplo real: Si una red pública sigue usando WEP, cualquier persona con un portátil y herramientas básicas podría descifrar su clave en minutos. Por eso, en instalaciones educativas o domésticas, siempre se recomienda WPA2 o WPA3.

> **Curiosidad tecnológica:** El protocolo WPA3 implementa un método llamado *Handshake Dragonfly*, que protege incluso si el atacante captura la comunicación inicial entre el cliente y el AP. Es tan robusto que impide los ataques de diccionario (probando contraseñas una a una).

7.7. Buenas prácticas de seguridad Wi-Fi

1. **Usar siempre WPA2 o WPA3.** Evita WEP y WPA, que son vulnerables.
2. **Cambiar la contraseña por defecto del router.**
   Las claves de fábrica suelen estar publicadas en bases de datos.
3. **Ocultar el SSID** (opcional). No impide el acceso, pero evita conexiones accidentales.
4. **Actualizar el firmware del router.** Los fabricantes corrigen vulnerabilidades periódicamente.
5. **Filtrar por dirección MAC.** Permite aceptar solo dispositivos autorizados.
6. **Desactivar WPS (Wi-Fi Protected Setup).** Aunque cómodo, es un vector de ataque común.
7. **Segregar redes.** Usa una red “de invitados” para dispositivos no seguros (IoT, móviles externos).

Ejemplo práctico: En una empresa, las redes Wi-Fi están segmentadas:

- “PERSONAL” para personal (segura y cifrada).
- “VISITAS” sin acceso a recursos internos.

Esto evita que un alumno, por ejemplo, pueda acceder a impresoras o servidores administrativos.

7.8. Diagnóstico y análisis de redes Wi-Fi

Herramientas útiles para analizar el rendimiento y la seguridad de una red inalámbrica:

Herramienta	Uso principal	Plataforma
inSSIDer / Acrylic Wi-Fi	Escaneo de SSID y canales.	Windows.
Wireshark	Captura y análisis de tramas 802.11.	Multiplataforma.
Aircrack-ng	Auditoría de seguridad (uso ético).	Linux.
Analizador de redes de Android	Intensidad de señal y canal óptimo.	Móvil.

En resumen

Las redes inalámbricas son una combinación magistral de física, electrónica y lógica. Nos permiten movilidad y comodidad, pero exigen conocimiento y responsabilidad.

- Los estándares 802.11 definen las velocidades, frecuencias y modos de operación.
- Las bandas de 2,4 GHz, 5 GHz y 6 GHz ofrecen distintos equilibrios entre alcance y rendimiento.
- La seguridad evoluciona: de WEP a WPA3, cada versión ha corregido las debilidades de la anterior.
- Un diseño Wi-Fi eficiente requiere elegir el canal correcto, cifrar adecuadamente y mantener el hardware actualizado.

8. Diseño básico de una red doméstica

Una red doméstica es el laboratorio perfecto para entender cómo funciona cualquier sistema de comunicaciones.

En ella se combinan todos los conceptos aprendidos: dispositivos, medios de transmisión, direcciones IP, Wi-Fi, seguridad, topología y protocolos.

Diseñarla correctamente significa lograr una red estable, rápida y segura, capaz de conectar múltiples dispositivos sin conflictos.

8.1. Objetivos del diseño

Cuando se diseña una red, incluso pequeña, hay que tener claros tres objetivos fundamentales:

1. **Conectividad:** todos los dispositivos deben poder comunicarse entre sí y con Internet.
2. **Rendimiento:** la red debe soportar el tráfico generado sin saturarse.
3. **Seguridad:** solo los usuarios y dispositivos autorizados deben tener acceso.

> **Ejemplo práctico:** Una vivienda con dos plantas, tres ordenadores, una Smart TV, varios móviles y una impresora Wi-Fi requiere un diseño distinto al de una oficina con 20 equipos cableados y un servidor interno. El proceso, sin embargo, sigue las mismas fases.

8.2. Fases del diseño de red

1. Análisis de necesidades

Antes de colocar cables o encender el router, hay que evaluar qué se necesita conectar:

- ¿Cuántos dispositivos habrá?
- ¿Cuáles se conectarán por cable y cuáles por Wi-Fi?
- ¿Dónde se colocará el router principal?
- ¿Qué tipo de cobertura se requiere (toda la casa, una planta, jardín…)?

2. Elección de la topología

En entornos domésticos, la topología estrella es la más habitual:

- El router actúa como nodo central.
- A él se conectan ordenadores, consolas, televisores o puntos de acceso adicionales.
- Si se necesitan más puertos, se añade un switch como ampliación.

3. Selección de los medios de transmisión

En la práctica, conviene combinar cableado y Wi-Fi para aprovechar lo mejor de cada tecnología:

Dispositivo	Tipo de conexión recomendado	Motivo
Ordenador de sobremesa	Cable (Ethernet Cat 6)	Mayor velocidad y estabilidad.
Portátil o móvil	Wi-Fi	Movilidad.
Smart TV o consola	Cable si es posible	Evita cortes en streaming o juego online.
Impresora o IoT (domótica)	Wi-Fi	Menor consumo y flexibilidad.

> **Regla de oro:** Si el dispositivo no se mueve y tiene puerto Ethernet, mejor cable que Wi-Fi. El Wi-Fi se reserva para lo que realmente necesita movilidad.

4. Dirección IP y esquema lógico

Cada dispositivo necesita una dirección IP única dentro de la red local (LAN). El router suele actuar como servidor DHCP, asignando direcciones automáticamente dentro de un rango.

Ejemplo de direccionamiento típico:

```
Red local: 192.168.1.0/24

Router: 192.168.1.1

Rango DHCP: 192.168.1.100 – 192.168.1.200

Equipos fijos (estáticos): 192.168.1.10 – 192.168.1.20

Máscara de subred: 255.255.255.0

Puerta de enlace: 192.168.1.1

DNS: 8.8.8.8 (Google) o el del proveedor
```

Interpretación: Todos los dispositivos dentro de esa red comparten los tres primeros octetos (192.168.1), lo que significa que pueden comunicarse directamente entre sí.

Ejemplo práctico en Packet Tracer:

- Asigna IP 192.168.1.10 al PC1,
- 192.168.1.11 al PC2,
- 192.168.1.1 al router.

Haz `ping` entre ambos para comprobar conectividad.

5. Configuración del router

El router es el cerebro de la red. Sus funciones principales son:

- Actuar como puerta de enlace entre la LAN y la red exterior (Internet).
- Servir direcciones IP por DHCP.
- Gestionar el Wi-Fi (SSID, canal, cifrado, contraseña).
- Implementar NAT (Network Address Translation), que traduce las IP internas a una sola IP pública.

> **Ejemplo real:** Cuando varios dispositivos del aula navegan por Internet, todos usan la misma IP pública del centro, gracias a NAT. Sin NAT, cada equipo necesitaría su propia IP pública: inviable y caro.

Curiosidad: La mayoría de routers domésticos permiten acceder a su configuración mediante la dirección `192.168.1.1` en el navegador. Desde ahí puede cambiarse la contraseña, canal Wi-Fi o rango DHCP.

6. Seguridad del Wi-Fi doméstico

La red inalámbrica es el punto más vulnerable. Para asegurarla:

1. Cambiar el nombre del SSID por uno propio (evita revelar el modelo del router).
2. Usar cifrado WPA2 o WPA3.
3. Desactivar WPS, que facilita ataques por fuerza bruta.
4. Limitar el número de dispositivos conectados simultáneamente.
5. Revisar la lista de equipos conectados periódicamente.

Ejemplo real: Muchos routers permiten ver los dispositivos conectados desde una app móvil. Si aparece uno que no reconoces, alguien está usando tu Wi-Fi sin permiso.

7. Plan de mantenimiento básico

Una red doméstica no se “instala y olvida”. Conviene realizar tareas periódicas de mantenimiento:

Tarea	Frecuencia	Objetivo
Reiniciar router y switches	1 vez al mes	Liberar memoria y renovar conexiones.
Actualizar firmware	Trimestral	Corregir vulnerabilidades y mejorar rendimiento.
Cambiar contraseña Wi-Fi	Cada 6-12 meses	Reforzar seguridad.
Revisar cables y conectores	Anualmente	Evitar pérdidas o interferencias.

> **Consejo profesional:** Un cable deteriorado o un conector flojo puede provocar “microcortes” difíciles de detectar. Revisar físicamente el cableado a veces soluciona lo que parece un fallo misterioso de software.

8.3. Ejemplo de diseño completo

Supongamos que queremos diseñar una red doméstica para una vivienda de dos plantas.

- Requisitos:
- 2 ordenadores fijos.
- 3 móviles.
- 1 impresora Wi-Fi.
- 1 Smart TV.
- Cobertura completa en ambas plantas.

Diseño propuesto:

- Topología: estrella jerárquica.
- Router principal: planta baja, conectado al punto de entrada de fibra.
- Switch: para conectar los dos ordenadores y la TV.
- Punto de acceso adicional: planta superior, conectado al switch mediante cable Ethernet.

- Direcciones IP:
    - Router: 192.168.0.1
    - PC1: 192.168.0.10
    - PC2: 192.168.0.11
    - TV: 192.168.0.20
    - Impresora Wi-Fi: 192.168.0.30
    - Móviles: IP dinámica por DHCP.

Configuración Wi-Fi:

- SSID: “CasaParadela”
- Seguridad: WPA3-Personal
- Contraseña: segura, alfanumérica y larga
- Canal: 6 (libre de interferencias tras análisis con aplicación móvil)

Ventajas del diseño:

- Cobertura completa en ambas plantas.
- Red estable para streaming y juegos online.
- Gestión centralizada del tráfico y direcciones IP.
- Segmentación sencilla si se desea añadir red de invitados.

8.4. Buenas prácticas en redes domésticas

1. Ubicación estratégica del router: céntrica y elevada; evita esquinas o muebles metálicos.
2. Evitar solapamiento de canales Wi-Fi: especialmente en edificios con muchos vecinos.
3. Usar nombres de dispositivos claros: `PC-Salon`, `TV-Planta2`, etc.
4. Hacer copias de seguridad periódicas: de archivos compartidos o NAS.
5. Desactivar servicios no utilizados: administración remota, puertos abiertos o servidores innecesarios.

En resumen

Diseñar una red doméstica es un ejercicio práctico de ingeniería:

- Combina diseño físico (topología, cableado) y diseño lógico (direcciones, protocolos).
- Requiere equilibrio entre rendimiento, seguridad y facilidad de uso
- Aplicando unas pocas reglas básicas, se puede obtener una red doméstica robusta y profesional.

> **Frase para recordar:** *Una buena red no se nota cuando funciona, pero se echa mucho de menos cuando falla.*

9. Práctica integradora: simulación de una red

Una cosa es entender la teoría, y otra muy distinta ver cómo circulan realmente los datos entre los equipos.

El objetivo de esta práctica es construir y configurar una red local doméstica completa similar a la que podrías tener en casa o en un pequeño despacho, verificándola en Packet Tracer paso a paso.

9.1. Objetivos de la práctica

Al finalizar, deberías ser capaz de:

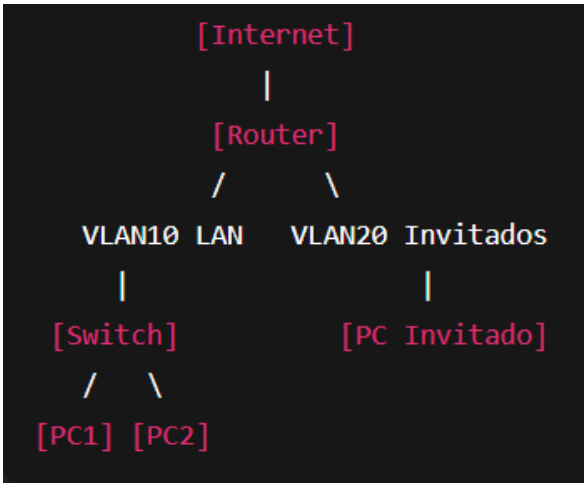
- Diseñar la topología de una red doméstica con router, switch y varios equipos.
- Asignar direcciones IP estáticas y dinámicas.
- Configurar la conectividad entre subredes (red principal y red de invitados).
- Verificar la comunicación mediante comandos de diagnóstico (`ping`, `ipconfig`, `tracert`).
- Entender cómo fluye la información a través de los dispositivos intermedios.

9.2. Escenario de trabajo

Situación inicial:

Vamos a simular una vivienda con:

- 1 **router doméstico** (con dos interfaces: una hacia Internet y otra hacia la LAN).
- 1 **switch** conectado al router.
- 2 **PCs de la red principal**.
- 1 **PC de invitados** (en subred separada).
- Conexión simulada a Internet (nube).



9.3. Paso 1: Crear la topología en Packet Tracer

Abre Cisco Packet Tracer.

Añade los siguientes dispositivos:

- 1 router Cisco 1941.
- 1 switch 2960.
- 3 PCs (PC1, PC2, PC-Invitado).
- 1 nube “Internet” (opcional, para estética).

Conecta los cables:

- Router → Switch (GigabitEthernet0/0 → Fa0/1)
- Switch → PC1 (Fa0/2)
- Switch → PC2 (Fa0/3)
- Router → PC-Invitado (GigabitEthernet0/1)

> **Consejo**: usa cables cobre directo entre dispositivos diferentes (PC–switch, switch–router) y cruzado solo si conectas iguales (router–router o switch–switch).

9.4. Asignar direcciones IP

Red principal (LAN)

- Dirección de red: 192.168.0.0/24
- Router: 192.168.0.1
- PC1: 192.168.0.10
- PC2: 192.168.0.11
- Máscara: 255.255.255.0
- Puerta de enlace: 192.168.0.1

Red de invitados

- Dirección de red: 192.168.10.0/24
- Router: 192.168.10.1
- PC Invitado: 192.168.10.10
- Máscara: 255.255.255.0
- Puerta de enlace: 192.168.10.1

9.5. Configurar el router

a) Activar interfaces

Entra en modo privilegiado y configura las IPs:

```
Router> enable
```

```
Router# configure terminal

Router(config)# interface g0/0

Router(config-if)# ip address 192.168.0.1 255.255.255.0

Router(config-if)# no shutdown

Router(config-if)# exit

Router(config)# interface g0/1

Router(config-if)# ip address 192.168.10.1 255.255.255.0

Router(config-if)# no shutdown

Router(config-if)# exit
```

> **Explicación:** Ahora el router tiene dos puertas: una para la red principal y otra para la de invitados. Actúa como frontera entre ambas.

b) Habilitar rutas hacia Internet (opcional)

Simula el acceso a Internet con una ruta por defecto:

```
Router(config)# ip route 0.0.0.0 0.0.0.0 g0/0
```

9.6. Configurar los PCs

En PC1 y PC2:

- IP: `192.168.0.10 / 192.168.0.11`
- Máscara: `255.255.255.0`
- Puerta de enlace: `192.168.0.1`

En PC-Invitado:

- IP: `192.168.10.10`
- Máscara: `255.255.255.0`
- Puerta de enlace: `192.168.10.1`

9.7. Comprobación de conectividad

Abre la línea de comandos de cada PC y ejecuta:

Conectividad interna:

```
ping 192.168.0.11   # Desde PC1 a PC2
```

Si responde, la red principal funciona correctamente.

Conectividad entre subredes:

```
ping 192.168.10.10   # Desde PC1 a PC Invitado
```

Si no responde, perfecto: significa que están aisladas.

Conectividad a la puerta de enlace:

```
ping 192.168.0.1
```

```
ping 192.168.10.1
```

Deben responder ambos, porque ambos pertenecen al mismo router.

9.8. (Opcional) Aislamiento mediante ACL

Para reforzar la segmentación, se pueden añadir listas de control de acceso (ACL) en el router.

Ejemplo: bloquear el tráfico de invitados hacia la red principal.

```
Router(config)# access-list 10 deny 192.168.10.0 0.0.0.255
```

```
Router(config)# access-list 10 permit any
```

```
Router(config)# interface g0/1
```

```
Router(config-if)# ip access-group 10 in
```

```
Router(config-if)# exit
```

Resultado: los invitados pueden navegar por Internet (si lo simulamos), pero no acceder a `192.168.0.x`.

9.9. Guardar la configuración

```
Router# write memory
```

Consejo: ahora es el momento de escribir un pequeño documento de red con direcciones IP, conexiones y observaciones, tal como haría un técnico real.

9.10. Resultado esperado

Red funcional con dos segmentos:

- La red principal (`192.168.0.0/24`) tiene conectividad total.
- La red de invitados (`192.168.10.0/24`) accede solo al router y (simuladamente) a Internet.
- Se puede visualizar la comunicación en Packet Tracer con el modo Simulation, observando el recorrido de los paquetes.

En resumen

Esta práctica integra todo lo aprendido en la UD4:

- Tipos de red y topologías.
- Direccionamiento IP y subredes.
- Componentes físicos: router, switch, tarjetas.
- Seguridad y segmentación lógica.

10. Resumen y cierre de la unidad

Durante esta unidad hemos recorrido el camino que va desde el concepto más básico de conexión entre dos equipos hasta el diseño y simulación de una red doméstica completa.

Hemos aprendido que una red informática no es solo un conjunto de cables o dispositivos, sino un ecosistema complejo y estructurado que permite la comunicación entre millones de sistemas en todo el planeta.

10.1. Síntesis de contenidos

Bloque temático	Conceptos esenciales
Conceptos básicos de red	Nodo, enlace, recurso compartido, beneficios de las redes, modos de transmisión.
Tipos de redes	PAN, LAN, MAN y WAN según extensión; redes cliente-servidor y P2P.
Topologías	Bus, anillo, estrella, malla, árbol e híbridas. Ventajas e inconvenientes de cada una.
Modelos de referencia	OSI (7 capas) y TCP/IP (4 capas): funciones, correspondencia y encapsulación.
Componentes de red	NIC, switch, router, punto de acceso, servidor, firewall; medios de transmisión guiados y no guiados.
Redes inalámbricas	Estándares 802.11, bandas de frecuencia, seguridad (WPA3) y buenas prácticas.
Diseño de red doméstica	Topología estrella, direccionamiento IP, router, DHCP, NAT y seguridad Wi-Fi.

Bloque temático	Conceptos esenciales
Segmentación y práctica	Separación de redes principal e invitados, subredes/VLAN, ACLs y simulación con Packet Tracer.

10.2. Reflexión final

Internet, esa red inmensa que usamos a diario, no es más que la combinación de miles de millones de pequeñas redes interconectadas, cada una construida con los mismos principios que acabas de estudiar. Los cables que ves en un aula, los routers que gestionan tu Wi-Fi o los servidores que alojan una web funcionan siguiendo reglas universales, basadas en los modelos OSI y TCP/IP.

Saber cómo se construyen y configuran estas redes es la diferencia entre usar la tecnología y entenderla. Y en el mundo del desarrollo web, comprender las redes es tan esencial como dominar un lenguaje de programación:

- Si un sitio no carga, puede ser un error en la capa de transporte.
- Si un formulario no responde, puede deberse a un fallo en la capa de aplicación.
- Si una API no devuelve datos, quizás haya un problema de DNS en la capa de red.

Cada vez que haces clic, hay siete capas (al menos) trabajando en armonía.

10.3. Curiosidades tecnológicas

El correo electrónico existía antes de Internet. En 1971, Ray Tomlinson envió el primer email en ARPANET… y eligió la @ para separar usuario y máquina. Cincuenta años después, sigue siendo el símbolo universal de la comunicación digital.

El Wi-Fi se inventó por accidente. Un equipo liderado por el australiano Dr. John O'Sullivan estaba desarrollando técnicas para detectar radiación cósmica, pero descubrió que podían aplicarse a la transmisión inalámbrica de datos. Ese hallazgo derivó en la patente del Wi-Fi moderno. Aunque sus raíces se remontan mucho antes: en 1942, la actriz e inventora Hedy Lamarr, junto al compositor George Antheil, patentó un sistema de comunicación secreta basado en el salto de frecuencia. Este principio de transmisión segura inspiró décadas después las tecnologías de espectro ensanchado que utilizan el Wi-Fi, Bluetooth y GPS.

Los cables submarinos son la auténtica Internet. Más del 95 % del tráfico global no viaja por satélite, sino por fibra óptica submarina. Solo un par de centímetros de grosor, pero miles de kilómetros de longitud, cruzando océanos enteros.

La dirección IPv4 se agotó en 2019. Con 4.300 millones de direcciones, parecía imposible quedarse sin ellas. Hoy, la transición a IPv6 (con 340 sextillones de direcciones posibles) está en marcha, aunque todavía no completa.

10.4. Autoevaluación y repaso

Preguntas de repaso (respuesta breve):

1. ¿Qué tres elementos básicos forman cualquier red informática?
2. ¿Qué diferencia principal hay entre una LAN y una WAN?
3. ¿Qué función cumple un switch en una red?
4. ¿Qué significa que una red use topología en estrella?
5. ¿Por qué es importante la capa de transporte en el modelo OSI?
6. ¿Qué protocolos pertenecen a la capa de aplicación del modelo TCP/IP?
7. ¿Qué diferencia hay entre dirección MAC y dirección IP?
8. ¿Por qué el cifrado WEP ya no es seguro?
9. ¿Qué ventajas aporta WPA3 frente a WPA2?
10. ¿Qué función cumple el NAT en un router?

Test de autoevaluación:

1. En una topología en bus, si se rompe el cable principal:
   a) Solo falla un equipo
   b) La red completa deja de funcionar
   c) No ocurre nada
2. La capa del modelo OSI encargada de decidir la ruta que siguen los paquetes es:
   a) Capa de red
   b) Capa de transporte
   c) Capa de enlace
3. El estándar Wi-Fi más reciente (2025) es:
   a) 802.11ac
   b) 802.11ax
   c) 802.11be
4. En una red doméstica, el router suele:
   a) Asignar IPs mediante DHCP
   b) Solo transmitir Wi-Fi
   c) Actuar como servidor web
5. En una red segmentada para invitados:
   a) Todos los dispositivos comparten recursos
   b) Los invitados solo acceden a Internet
   c) No hay seguridad adicional

Preguntas de reflexión abierta

1. Si tuvieras que diseñar la red de un instituto, ¿qué tipo de topología y segmentación usarías?
2. ¿Por qué crees que el modelo OSI sigue siendo relevante aunque Internet use TCP/IP?
3. ¿Qué riesgos implicaría dejar una red Wi-Fi abierta sin contraseña?

4. ¿Qué criterios seguirías para decidir qué dispositivos deben conectarse por cable y cuáles por Wi-Fi?
5. ¿Qué aprendiste en esta unidad que podrías aplicar en tu vida cotidiana?