

Redes Wi-Fi

Introducción

Las redes inalámbricas o sin cables, conocidas como **Wi-Fi**, permiten la transmisión de datos sin necesidad de conexiones físicas entre dispositivos.

- Hasta hace unos años, la mayoría de redes eran por **cable (Ethernet)**.
- Las redes cableadas siguen siendo una buena opción si los dispositivos están **fijos y próximos entre sí**.
- Sin embargo, las redes **Wi-Fi** ofrecen mayor comodidad y flexibilidad al permitir movilidad y menos instalación física.

¿Qué es el Wi-Fi?

- Es una tecnología de **comunicación inalámbrica** que transmite señales digitales por el aire.
- Utiliza **ondas electromagnéticas de alta frecuencia** (GHz) para enviar y recibir datos.
- El proceso implica:
 - **Modulación**: codificar la información en la señal.
 - **Transmisión**: la señal se emite desde una antena emisora.
 - **Recepción**: otra antena la capta, la **demodula** y recupera los datos originales.

Comunicación por microondas

- Las redes Wi-Fi utilizan microondas, una forma de radiación electromagnética.
- La señal viaja por el espacio libre desde el transmisor al receptor.
- Durante el trayecto, **la señal se atenúa** (pierde fuerza), especialmente con la distancia o con obstáculos.

Intensidad de señal Wi-Fi

- La **intensidad de la señal** influye directamente en la **velocidad de transmisión** y la **estabilidad** de la conexión.
- Se mide mediante el indicador **RSSI** (*Received Signal Strength Indicator*).
- La unidad de medida es el **dBm (decibelios-milivatio)**.

Características de la escala en dBm

- Es una **escala logarítmica**, lo que significa:
 - **+3 dB** → Duplica la intensidad de la señal.
 - **+10 dB** → Multiplica por 10 la potencia recibida.
- Una señal débil reduce la calidad y velocidad de la conexión.

Conocer cómo funciona el Wi-Fi y cómo afecta la intensidad de la señal es clave para optimizar el rendimiento de nuestras redes inalámbricas.

Estándares Wi-Fi

Un **estándar** es un conjunto de normas técnicas que definen cómo debe funcionar una red para garantizar la compatibilidad entre dispositivos.

Estándar 802.11

- Las redes Wi-Fi se basan en el estándar **IEEE 802.11**.
- Existen diferentes versiones de este estándar, que se identifican por **letras** (a, b, g, n, ac, ax, etc.).
- Una red Wi-Fi debe cumplir con alguno de estos estándares para asegurar el funcionamiento correcto.

Certificación

- Los dispositivos Wi-Fi certificados por la **Wi-Fi Alliance** (organización fundada en 1999) garantizan **compatibilidad** y **seguridad**.
- Esta certificación asegura que los dispositivos de diferentes marcas puedan conectarse y comunicarse entre sí sin problemas.

Evolución de los estándares Wi-Fi

Para facilitar su comprensión, las versiones más recientes de Wi-Fi han adoptado una **nomenclatura más sencilla**:

Nombre técnico	Nombre comercial	Velocidad aproximada	Características principales
802.11n	Wi-Fi 4	Hasta 600 Mbps	Mayor alcance y uso de múltiples antenas (MIMO)
802.11ac	Wi-Fi 5	Hasta 3.5 Gbps	Alta velocidad en banda 5 GHz
802.11ax	Wi-Fi 6	Hasta 9.6 Gbps	Mejor rendimiento con muchos dispositivos
802.11ax (mejorado)	Wi-Fi 6E	Igual que Wi-Fi 6	Añade la nueva banda de 6 GHz
802.11be	Wi-Fi 7	> 30 Gbps (estimado)	Muy alta velocidad y baja latencia, ideal para aplicaciones futuras

Nota

- Hablar de **Wi-Fi 6** o **Wi-Fi ax** es equivalente (ambos hacen referencia al estándar **802.11ax**).
- Cada nueva versión mejora aspectos como la **velocidad**, la **cobertura**, la **eficiencia** y la **capacidad** para conectar múltiples dispositivos.

Dual Band en redes Wi-Fi

Los routers **Dual Band** permiten trabajar con **dos bandas de frecuencia** diferentes: **2.4 GHz** y **5 GHz**.

¿Qué es un router Dual Band?

- Gestiona **dos redes Wi-Fi separadas** al mismo tiempo.
- Puede ofrecer una única red con el **mismo nombre (SSID)** y contraseña para ambas bandas.

- Los **dispositivos eligen automáticamente** la mejor banda según la señal y el rendimiento.

Características de cada banda

● Banda de 2.4 GHz

- **Mayor cobertura** y mejor penetración en paredes y obstáculos.
- Ideal para dispositivos de **mayor alcance** o que no necesitan mucha velocidad:
 - Cámaras de seguridad
 - Dispositivos IoT (domótica)
 - Navegación web
 - Redes sociales

● Banda de 5 GHz

- **Mayor velocidad** y menor interferencia.
- Perfecta para actividades que requieren un buen ancho de banda:
 - Juegos en línea
 - Streaming en HD o 4K
 - Videollamadas
- Ideal para dispositivos **cercanos al router o punto de acceso**.

Ventajas del Dual Band

- **Flexibilidad:** los usuarios pueden elegir manualmente o dejar que los dispositivos seleccionen la mejor opción.
- **Rendimiento optimizado:** se reduce la congestión en la red y se mejora la experiencia de conexión.

Dispositivos Wi-Fi

Los dispositivos Wi-Fi permiten la conexión inalámbrica a redes. Dependiendo del tipo de equipo, existen distintas formas de incorporar conectividad Wi-Fi.

Adaptadores Wi-Fi externos

Se utilizan para añadir Wi-Fi a ordenadores que no tienen conexión inalámbrica integrada.

Tarjetas PCI / miniPCI:

- Se instalan en ordenadore de sobremesa.
- Ofrecen buena velocidad y estabilidad.

Tarjetas PCMCIA:

- Usadas en los primeros ordenadores portátiles.
- Hoy en día están obsoletas.

Adaptadores USB:

- Muy comunes en PCs de sobremesa y portátiles.
- Fácil instalación y portabilidad.

Dispositivos móviles

Los smartphones, tablets y portátiles modernos **ya integran adaptadores Wi-Fi** en sus placas internas.

Características:

- Incluyen **chips especializados** para conexión inalámbrica.
- Son **compactos y energéticamente eficientes**.
- Disponen de **antenas internas** para transmitir y recibir señal.
- Compatibles con:
 - Estándares Wi-Fi como **802.11ac** (Wi-Fi 5) y **802.11ax** (Wi-Fi 6).
 - Bandas de frecuencia **2.4 GHz** y **5 GHz**.
- Garantizan **alto rendimiento y compatibilidad** con las redes actuales.

Equipos de red

Son dispositivos diseñados para permitir la comunicación y conexión a internet en redes pequeñas, como en el hogar o en oficinas pequeñas.

1. Router inalámbrico

Dispositivo principal en muchas redes domésticas o de oficina. Cumple varias funciones:

- **Router:** Conecta la red local a Internet.
- **Punto de acceso:** Permite que los dispositivos se conecten a la red mediante Wi-Fi.
- **Switch:** Facilita la comunicación entre todos los dispositivos conectados por cable.
- **Antenas:** Transmiten y reciben señales de radiofrecuencia para la conexión Wi-Fi.

2. Repetidores

Dispositivos que amplían la cobertura de una red Wi-Fi existente:

- Reciben la señal Wi-Fi y la **retransmiten** para ampliar el alcance.
- Permiten que dispositivos fuera del alcance del router principal se conecten.
- Son útiles en **espacios grandes** o con **obstáculos** que bloquean la señal.
- Mejoran la conectividad y reducen las **zonas muertas** (donde no llega la señal).
- Generan una nueva red Wi-Fi a la que otros dispositivos pueden conectarse.
- Actúan como **punto** entre la red cableada (Ethernet) y dispositivos inalámbricos.
- Se pueden usar **múltiples repetidores o puntos de acceso** para crear una red uniforme y con buena cobertura.

3. Puntos de acceso (Access Point - AP)

Dispositivos que extienden la red inalámbrica en lugares grandes:

- Se colocan en ubicaciones estratégicas como **techos, pasillos o paredes**.
- Se conectan a la red central por **cables Ethernet**.
- Pueden recibir tanto **datos como energía eléctrica** a través de **Power over Ethernet (PoE)**.
- Permiten ampliar la cobertura Wi-Fi de manera eficaz y con menor interferencia.

Seguridad en redes Wi-Fi

Para proteger nuestra red inalámbrica y la información que transmitimos, es fundamental aplicar medidas de seguridad adecuadas.

¿Qué riesgos queremos evitar?

- **Accesos no autorizados:** Evitar que personas ajenas se conecten a nuestra red.
- **Espionaje:** Proteger los datos para que no puedan ser interceptados ni leídos.

Medidas de seguridad Wi-Fi

1. Control de acceso

- **Filtrado de direcciones MAC:** Solo los dispositivos cuya dirección MAC esté autorizada pueden conectarse a la red.
- **Ocultación del SSID:** El nombre de la red Wi-Fi no se muestra públicamente, dificultando su detección por usuarios no autorizados.

2. Protocolos de seguridad y cifrado

Los protocolos de seguridad protegen la información que se transmite a través de la red.

- **WEP:** Antiguo sistema de cifrado, actualmente obsoleto y no seguro.
- **WPA (Wi-Fi Protected Access):** Evolución de WEP. Existen diferentes versiones:
 - **WPA2-Personal**
 - **WPA3-Personal** (más seguro y actual)

Características:

- Utilizan un sistema de **clave precompartida** (*PSK - Pre-Shared Key*) para autenticarse.
- Cada dispositivo puede tener **claves de cifrado únicas**, especialmente con WPA2 y WPA3.
- Permiten cifrar los datos que se transmiten, impidiendo que terceros puedan leer la información incluso si están dentro del alcance de la señal Wi-Fi.

Aplicar estas medidas mejora significativamente la seguridad de una red inalámbrica y protege tanto el acceso como la privacidad de los usuarios.