GENERALITAT VALENCIANA
Conselleria d'Educació, Cultura i Esport

ceedcv CENTRE ESPECÍFIC D'EDUCACIÓ A DISTÀNCIA DE LA COMUNITAT VALENCIANA

TRATAMIENTO DE LA INFORMACIÓN Y COMPETENCIA DIGITAL

Configuración básica de routers

Departament d'informàtica.
Autor: Francisco Aldarias Raya
Enero-2026

Preparació Proves d'Accés

ÍNDEX

Nomenclatura

A lo largo de este tema se utilizarán distintos símbolos para distinguir elementos importantes dentro del contenido. Estos símbolos son:

[Importante]

[Atención]

[Interesante]

1 Introducción

En la mayoría de hogares y pequeñas oficinas actuales existe una **red doméstica** que permite compartir la conexión a Internet entre varios dispositivos: ordenadores, móviles, tablets, televisores inteligentes, consolas, impresoras, etc. Una red doméstica suele ser una **red de área local (LAN)** que puede usar **cables Ethernet** y **Wi-Fi** simultáneamente.

En el centro de casi todas estas redes encontramos un dispositivo clave: **el router**. Cuando está mal configurado, puede convertirse en una puerta abierta para intrusos; cuando está bien configurado, es como una **muralla defensiva** que protege a todos los dispositivos.

En este tema vamos a estudiar:

- Qué es un router y qué tipos hay (doméstico, empresarial, **router neutro**, **router mesh**…).
- Qué es un **punto de acceso (AP)**, qué es un **repetidor** y en qué se diferencian.
- Cómo acceder al router y configurar sus servicios: **DHCP, NAT, DMZ, redirección de puertos, QoS, VPN, DDNS (actualizar IP con dominio)**.
- Comparación entre **WPA2 y WPA3**.
- Un bloque amplio de **medidas de seguridad** recomendadas para el router.
- Un ejemplo práctico de configuración segura.

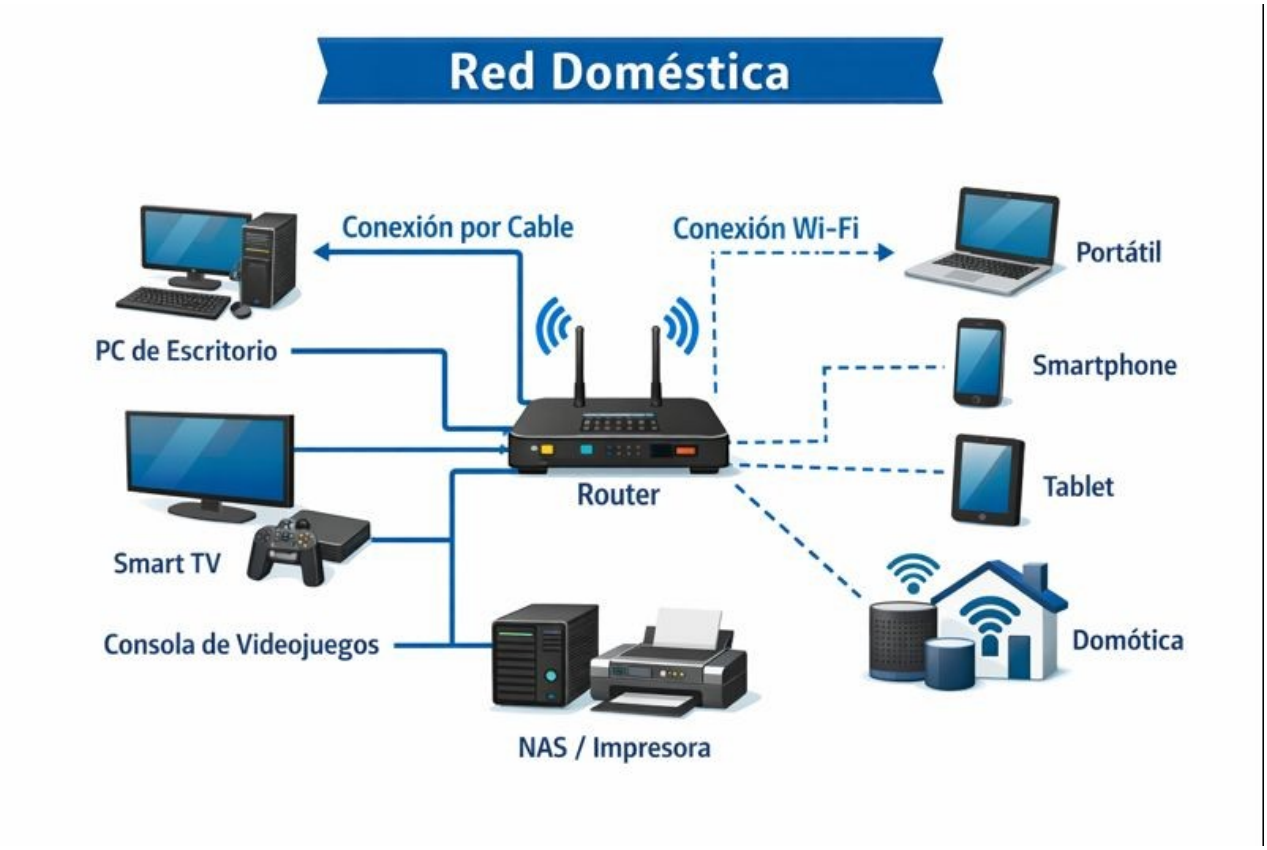

Figura 1: Red domestica con router y dispositivos conectados por cable y wifi

2 Conceptos básicos de redes

Antes de entrar en el router, repasamos algunos términos:

- **LAN (Local Area Network)**: red local. Normalmente está dentro de una casa, oficina o aula.
- **WAN (Wide Area Network)**: red extensa. Internet es una WAN gigante.
- **Dirección IP**: identificador numérico de cada dispositivo en la red (por ejemplo, 192.168.1.24).
- **Puerta de enlace (gateway)**: normalmente es la IP del router; es la "salida" hacia Internet.
- **Máscara de red**: indica qué parte de la IP identifica a la red y qué parte al host (ej. 255.255.255.0).
- **DNS (Domain Name System)**: servicio que traduce nombres como `www.ejemplo.com` a direcciones IP.

Estos conceptos se usan continuamente en la configuración del router.

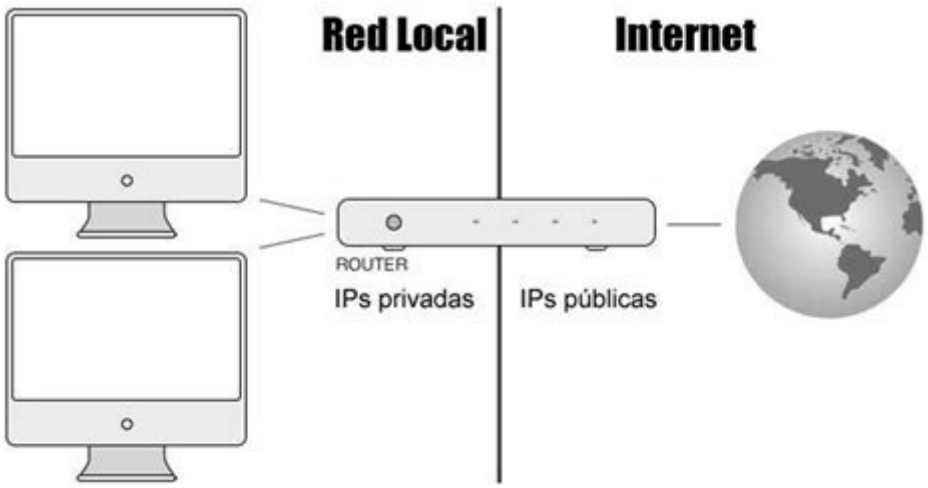

Figura 2: Diagrama de una LAN conectada a Internet

3 El modelo OSI y el papel del router

El **modelo OSI** divide las comunicaciones en 7 capas. El router trabaja principalmente en la **capa 3: Capa de Red**.

- La capa de red se encarga de **encaminar paquetes entre redes diferentes**.
- El router mira la **dirección IP destino** y decide por qué camino enviarla.

Podemos imaginar que:

- Las **capas 1 y 2** (física y enlace) son las calles de un barrio.

- La **capa 3 (red)** es el sistema de carreteras entre barrios y ciudades.
- El **router** es el encargado de escoger qué carretera usar para que el "paquete" llegue a otra ciudad.

En una red doméstica el router conecta:

- La **red local (LAN)** del hogar.
- La **red del proveedor de Internet (WAN)**.

Figura 3: El router está en el Modelo OSI nivel 3 de Red.

4 ¿Qué es un router?

Un **router** (encaminador, enrutador o puerta de enlace) es un dispositivo de red que:

1. **Conecta dispositivos** de una red local entre sí y con Internet.
2. **Asigna direcciones IP** a los dispositivos (mediante DHCP).
3. **Aplica medidas de seguridad**, como cortafuegos (firewall), filtrado, etc.
4. **Distribuye el ancho de banda** entre los diferentes equipos (Qos).

En la práctica, el router doméstico que nos entrega la operadora suele ser un **dispositivo "todo en uno"** que integra:

- Módem de fibra/ADSL/cable.
- Router IP.

- Punto de acceso Wi-Fi.
- Switch Ethernet con varios puertos.
- A veces, funciones extra: VoIP (Voz por Internet), servidor VPN, servidor de impresión conectando, etc.

Figura 4: Router Wifi

5 Tipos de routers

5.1 Routers domésticos

- Pensados para **hogares y pequeñas oficinas**.
- Suelen incluir **Wi-Fi**, un pequeño switch Ethernet y módem integrado.
- Interfaz de configuración simplificada (Web, a veces app de móvil).
- Orientados a facilidad de uso.

5.2 Routers empresariales

- Diseñados para **redes de empresa**, con muchos usuarios y tráfico intenso.
- Suelen incluir:
    - Soporte de **VLANs**, múltiples redes LAN.
    - Políticas avanzadas de firewall.
    - Servidores VPN para teletrabajo.
    - QoS avanzado, balanceo de carga, etc.

- Normalmente se configuran por **consola, SSH (conexión terminal remota segura) o interfaces web más complejas**.

5.3 Router neutro

Un router neutro es un dispositivo de red que compras tú mismo, no pertenece a ninguna compañía de internet (operadora), y te da más libertad y mejores prestaciones que el router básico que te dan con el contrato. Es "neutro" porque no está atado a un proveedor, permitiéndote elegir uno según tus necesidades para mejorar la cobertura WiFi, la velocidad y tener funcionalidades avanzadas, aunque generalmente se conecta al router de la operadora (que actúa como módem) para funcionar, ya que no tiene módem integrado

Un **router neutro** es un router que *no* incluye módem. Es decir, que el aparato **no puede conectarse directamente a la toma de internet** (la de la pared o la de fibra) por sí solo. Necesita "un traductor" en medio.

Se conecta a:

- Un módem de la operadora, o
- Directamente al ONT de fibra (en algunas configuraciones).
- En un punto de la red para aislarlo del resto de la red si se configura en una red diferente.

Características típicas:

- Mejores funciones Wi-Fi que el router del operador.
- Más opciones de configuración avanzada (control parental, QoS, redes de invitados, etc.).
- Permite crear una **subred separada** de la red de la operadora (aislamiento).

Se usa mucho cuando:

- El router del operador es limitado o inestable.
- Queremos un Wi-Fi más potente o más control sobre la red.

Figura 5: Router Neutro TP-Link AX1500 Wi-Fi 6

5.4 Routers Mesh

Un **router mesh** (o sistema Wi-Fi mesh) consta de:

- Un **router principal** conectado al módem.
- Uno o varios **nodos satélite** repartidos por la casa.

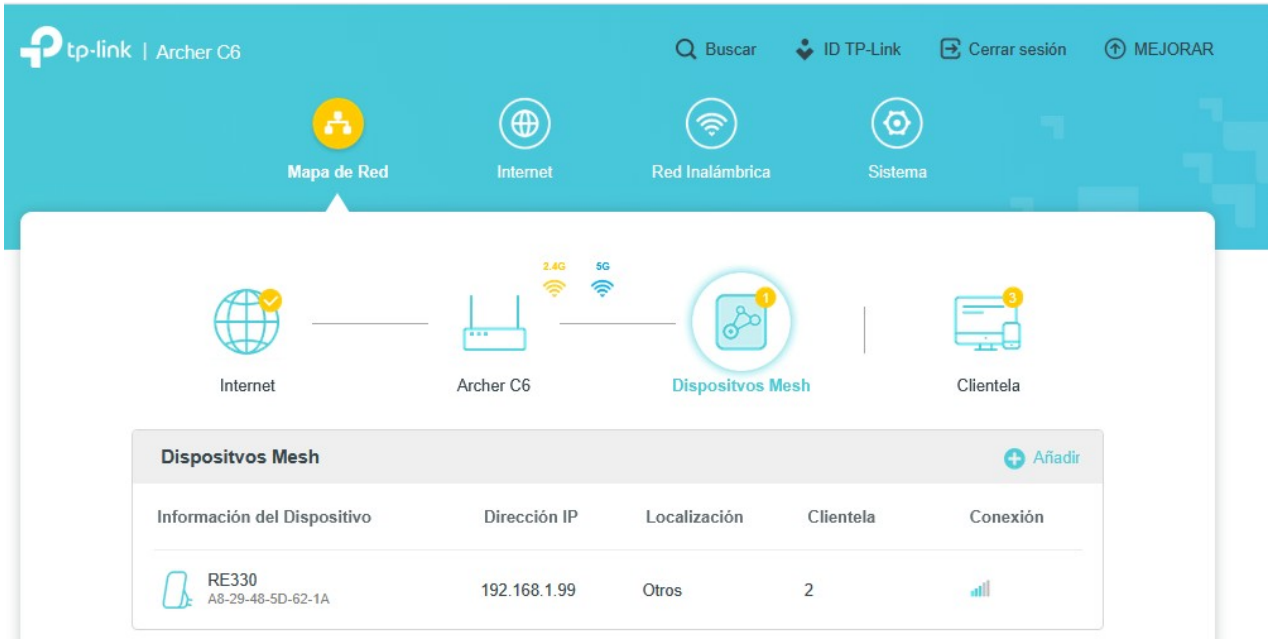

Figura 6: Router Principal Mesh. Router Mesh Wi-Fi 5 AC1200

Figura 7: Nodo Satelite Mes. Repetidor TPLINk RE330

Se pueden ver en las dos imágenes anterior que hay una red mesh estre el router mesh archer c6 y el nodo mesh repetidor RE330. La comexión se realiza por wifi con lo que hay perdida de señal.

Estos nodos forman una **malla** que se comunica entre sí. Ventajas:

- Mejor **cobertura Wi-Fi** en casas grandes o con muchas paredes.
- Los dispositivos se conectan al nodo que ofrece mejor señal.
- Roaming transparente: al moverte por la casa, el móvil cambia de nodo sin cortar la conexión.

Diferencias con un repetidor clásico:

- En mesh hay **coordinación central** y una única red lógica (mismo SSID).
- Los nodos se comunican de forma inteligente, optimizando el camino.

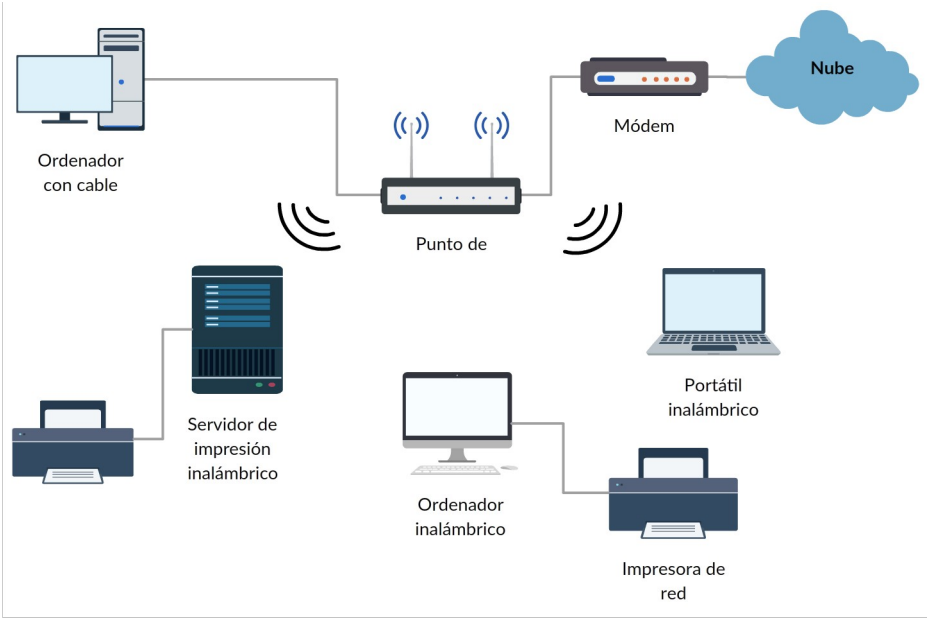

Figura 8: Red Wireless con router yu punto de acceso

5.5 Otras clasificaciones

- **Routers inalámbricos**: incluyen Wi-Fi (la mayoría hoy en día).
- **Routers 4G/5G**: se conectan a Internet por red móvil.
- **Routers "gaming"**: orientados a juegos online (QoS optimizado, baja latencia…).

El **QoS** (Quality of Service o Calidad de Servicio) es un conjunto de tecnologías y mecanismos que permiten gestionar el tráfico de una red para garantizar que las aplicaciones críticas reciban el ancho de banda y la prioridad que necesitan.

6 Punto de acceso (AP) y repetidor

6.1 Punto de acceso (Access Point, AP)

Un **punto de acceso** es un dispositivo que **crea una red Wi-Fi** a partir de una red cableada.

- Se conecta al router o a un switch mediante **cable Ethernet**.
- Emite uno o varios **SSIDs** (nombres de red Wi-Fi).
- Es ideal para:
    - Dar Wi-Fi en zonas donde el router no llega bien.
    - Redes profesionales con varios AP coordinados (ej. en un instituto).

En muchos routers domésticos, la parte Wi-Fi interna funciona como un AP.

6.2 Repetidor Wi-Fi

Un **repetidor** (o extensor Wi-Fi) es un dispositivo que:

- Recibe la señal Wi-Fi del router.
- La **repite** para ampliar la cobertura.

Ventajas:

- No necesita cableado: se coloca en un punto intermedio de la casa.
- Configuración sencilla.

Inconvenientes:

- Normalmente **reduce el ancho de banda efectivo** (porque recibe y retransmite en el mismo canal).
- Si la señal que recibe del router es mala, la que emite será aún peor.

6.3 Comparación AP vs Repetidor

Característica	Punto de acceso (AP)	Repetidor Wi-Fi
Conexión al router	Por cable	Por Wi-Fi
Rendimiento	Muy bueno, estable	Puede perder velocidad
Instalación	Requiere cableado	Solo enchufar y configurar
Número de saltos	1 (AP)	2 (router → repetidor → dispositivo)
Uso recomendado	Ampliar red en serio, oficinas	Solución rápida en casa pequeña/mediana

7 Cómo acceder a la configuración del router

Para configurar un router necesitamos:

1. Estar conectados a él (por cable o Wi-Fi).
2. Conocer su **dirección IP de gestión** (por ejemplo, 192.168.1.1).
3. Saber el **usuario y contraseña de administración**.

En sistemas Windows se puede obtener la puerta de enlace así:

1. Abrir el menú Inicio y buscar `cmd`.
2. Ejecutar el comando `ipconfig`.
3. Localizar la **"Puerta de enlace predeterminada"**: esa es la IP del router.

En macOS o Linux se puede usar:

- Utilidad de red / Preferencias de red, o
- El comando `ifconfig` / `ip route`.

Luego, basta con:

- Abrir un navegador y escribir la IP del router (`http://192.168.1.1`).
- Introducir usuario y contraseña (suele venir en una pegatina en la base del router).

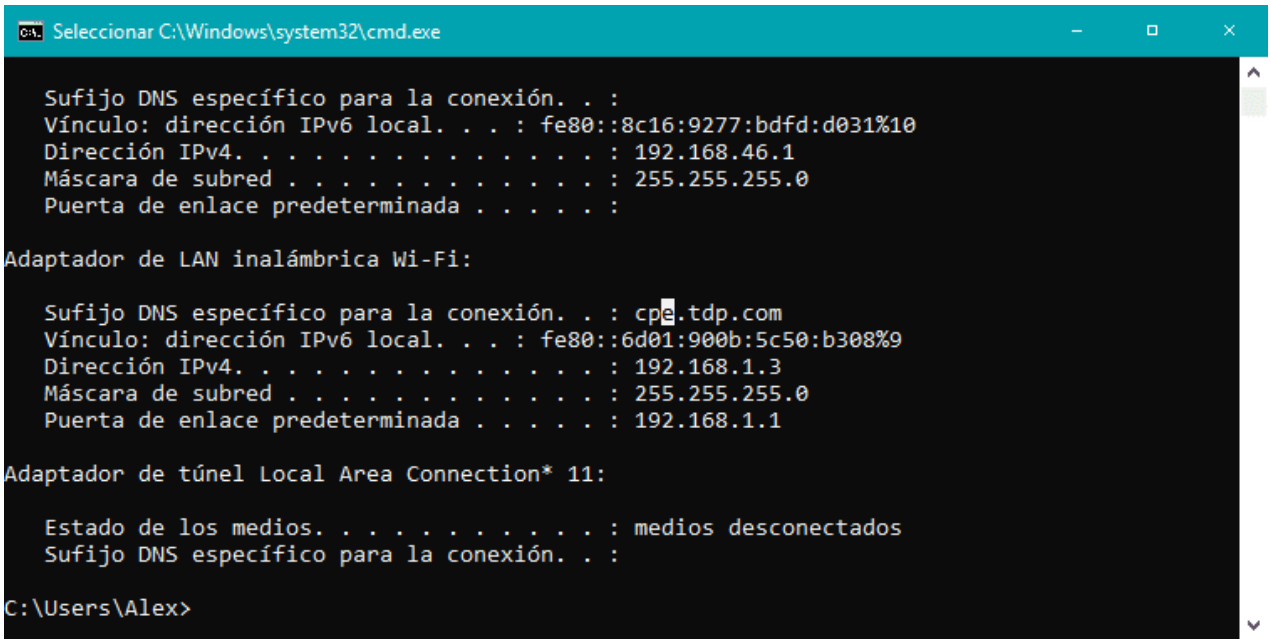

Figura 9: Comando ipconfig marcando la puerta de enlace

8 Servicios básicos del router

8.1 Servicio DHCP

El **DHCP (Dynamic Host Configuration Protocol)** permite que los dispositivos obtengan de forma automática:

- Dirección IP.
- Máscara de red.
- Puerta de enlace.
- Servidores DNS.

El **servidor DHCP** normalmente está en el router.

Parámetros típicos:

- **Rango de direcciones** (por ejemplo 192.168.1.20–192.168.1.200).
- **Tiempo de concesión** (lease time): cuánto tiempo se reserva una IP para un dispositivo.
- **Reservas DHCP**: asociar siempre la misma IP a una MAC concreta (útil para impresoras, servidores domésticos, etc.).

Ventajas:

- Evita errores de configuración manual.
- Facilita añadir nuevos dispositivos.

Riesgos si no se gestiona bien:

- Rango demasiado grande: deja muchas IP libres para intrusos.
- Otro dispositivo que actúe como servidor DHCP “pirata”.

8.2 NAT (Network Address Translation)

El **NAT** permite que muchos dispositivos de la red local (IPs privadas) compartan una sola **IP pública** al salir a Internet.

Ejemplo:

- Tu PC: 192.168.1.10
- Tu móvil: 192.168.1.11
- Router: IP pública 84.125.30.7

Cuando el PC se conecta a una web:

1. Envía un paquete desde 192.168.1.10:puerto12345 → 84.125.30.7 (router).
2. El router sustituye la IP origen por la IP pública y cambia el puerto (PAT).
3. La web responde a la IP pública del router, que luego reenvía la respuesta al PC correcto.

Ventajas:

- Ahorra direcciones IPv4.
- Aporta cierta **“ofuscación”** de la red interna (desde fuera no se ven las IP privadas).

Inconvenientes:

- Complica la conexión **desde Internet hacia dentro** (por eso hay que abrir puertos o usar DMZ/VPN).

8.3 Redirección de puertos (Port Forwarding)

La **redirección de puertos** consiste en decirle al router:

> “Cuando llegue una conexión de Internet al puerto X, mándala al dispositivo Y de mi red local”.

Ejemplo típico:

- Quiero acceder a un servidor web casero en mi PC 192.168.1.50.
- Configuro en el router:
    - Puerto externo 80 → 192.168.1.50 puerto 80.

Riesgos:

- Si abrimos un puerto a un dispositivo inseguro, lo exponemos a ataques.
- Es mejor abrir solo los puertos estrictamente necesarios.

Alternativas:

- Usar una **VPN** para entrar primero en la red local.
- Usar servicios de acceso remoto seguros.

8.4 DMZ (Zona Desmilitarizada)

En routers domésticos, activar la **DMZ** significa seleccionar un dispositivo interno cuya IP se va a **exponer totalmente** a Internet, sin pasar por el firewall del router.

Ventajas:

- Puede resolver problemas de conectividad en juegos online, servidores, etc.
- Es más sencillo que abrir muchos puertos manualmente.

Inconvenientes/riesgos:

- El equipo en DMZ queda prácticamente **sin protección** del router.
- Si es comprometido, podría servir de punto de entrada a la red interna.

Conclusión: **se usa solo como último recurso** y en dispositivos actualizados y reforzados (con su propio firewall y antivirus).

8.5 QoS (Quality of Service)

La **QoS** permite **priorizar cierto tipo de tráfico** sobre otro. Ejemplos:

- Dar prioridad a:
    - videollamadas y voz IP;
    - juegos online;
    - clases en streaming.
- Reducir prioridad a:
    - descargas P2P;
    - actualizaciones grandes.

Formas típicas de QoS:

- Por tipo de aplicación (VoIP, streaming, juegos…).
- Por dispositivo (por MAC o IP).
- Por puertos TCP/UDP.

Resultado: cuando la línea se satura, los servicios críticos siguen funcionando aceptablemente.

8.6 VPN en el router

Muchas veces el router permite actuar como:

- **Servidor VPN** (para conectarte desde fuera a tu casa/oficina), o
- **Cliente VPN** (para que toda tu red salga a Internet a través de un servidor remoto).

Ventajas de usar VPN:

- Cifrado de los datos de extremo a extremo.
- Protección en Wi-Fi públicas.
- En teletrabajo: acceso seguro a la red de la empresa.

Ventajas de que la VPN esté en el router:

- Todos los dispositivos se benefician sin instalar software.
- Menos carga en los equipos finales.

8.7 Dominio dinámicos (DDNS)

En la mayoría de conexiones domésticas, la IP pública es **dinámica**: el proveedor puede cambiarla.

Si queremos acceder siempre a nuestro router/casa desde fuera para RDP (Remote Desktop Protocol o Protocolo de Escritorio Remoto , servidores caseros, cámaras IP, etc.), es incómodo estar comprobando la IP.

Solución: **DNS dinámico (DDNS)**

- Registramos un nombre de dominio del estilo `mi-casa.ddns.net`.
- Configuramos en el router los datos del servicio DDNS.
- El router se encarga de ir **actualizando la IP** asociada al dominio cuando cambie.

Así, siempre podremos entrar con el mismo nombre, aunque la IP cambie.

9 Seguridad en el router: riesgos de una mala configuración

Un router mal configurado puede provocar:

1. **Robo de información confidencial**
   Intrusos conectados a nuestra red pueden:
   - Capturar tráfico.
   - Acceder a carpetas compartidas, cámaras, etc.
   - Instalar malware en nuestros dispositivos.
2. **Uso de nuestra red para actividades ilegales**
   Si alguien usa tu Wi-Fi para cometer delitos (por ejemplo, ataques DDoS, descarga de contenidos ilegales, etc.), las autoridades verán tu IP asociada a esas acciones. Aunque se demuestre que hubo intrusión, esto puede darte muchos problemas.
3. **Pérdida de ancho de banda**
   Cuantos más dispositivos (autorizados o no) haya conectados, más se reparte el ancho de banda y más lenta va la conexión.

Por todo ello, conviene aplicar con cuidado las medidas de seguridad que veremos a continuación.

10 Medidas de seguridad básicas

10.1 Cambiar la contraseña de acceso al router

Casi todos los routers traen una **contraseña por defecto** (a veces `admin/admin` o similar). Es fundamental cambiarla.

Pasos generales:

1. Acceder a la interfaz web del router.
2. Buscar la sección de **Administración** o **Sistema**.
3. Localizar la opción “Cambiar contraseña”, “Password”, etc.
4. Establecer una contraseña robusta.

Características de una **contraseña robusta**:

- Al menos 12 caracteres (mejor 16 o más).
- Mezcla de mayúsculas, minúsculas, números y símbolos.
- No usar nombres, fechas ni información obvia.
- No reutilizar la misma clave en otros sitios.

Motivo:

- Si alguien accede al **panel de administración**, puede cambiar toda la configuración, abrir puertos, registrar DNS dinámico a su favor, etc.

10.2 Cambiar el nombre de la red Wi-Fi (SSID)

El **SSID** por defecto suele indicar:

- Modelo del router.
- Operadora de Internet.

Esto da pistas a un atacante sobre:

- Qué vulnerabilidades podría explotar.
- Qué claves por defecto suele usar ese modelo.

Recomendación:

- Poner un SSID neutro que **no revele tu nombre, piso, operadora, etc.**.

Opción más avanzada:

- **Ocultar el SSID** (no emitir el nombre).
  – No es una protección absoluta (se puede descubrir con herramientas), pero añade una pequeña dificultad extra.

10.3 Elegir una buena contraseña Wi-Fi

No uses la clave Wi-Fi por defecto, aunque parezca compleja. Debe ser:

- Al menos 12 caracteres.
- Mezcla de letras, números y símbolos.
- No vigente en otros servicios.

La clave Wi-Fi protege el acceso a toda la red local; si es débil, cualquiera con un portátil cerca puede entrar.

10.4 Actualizar el firmware

El **firmware** es el software interno del router. Igual que un sistema operativo, puede tener fallos de seguridad.

Medidas:

1. Revisar periódicamente si hay nuevas versiones en:
    - La web del fabricante.
    - El propio menú de administración (a veces hay opción de “Actualizar firmware automáticamente”).
2. Aplicar las actualizaciones siguiendo las instrucciones.
3. No apagar el router durante el proceso.

Beneficios:

- Corrección de vulnerabilidades conocidas.
- Mejora de estabilidad y rendimiento.

10.5 Configurar cifrado WPA2 o WPA3

En el menú Wi-Fi del router, suele aparecer el tipo de **cifrado** de la red:

- WEP (muy antiguo e inseguro).
- WPA, WPA2, WPA3.

Es **imprescindible**:

- No utilizar nunca WEP.
- Usar al menos **WPA2-PSK (AES)**.
- Si el router y los dispositivos lo permiten, usar **WPA3**.

(La comparación detallada WPA2/WPA3 la veremos en el apartado 11.)

10.6 Desactivar WPS

El **WPS (Wi-Fi Protected Setup)** permite conectar dispositivos pulsando un botón o usando un PIN de 8 dígitos.

Problema:

- El PIN es relativamente fácil de atacar por fuerza bruta.
- Reducimos mucho la seguridad aunque la red esté en WPA2/3.

Recomendación:

- Desactivar WPS en el router.
- Conectar los dispositivos introduciendo la clave Wi-Fi manualmente o mediante códigos QR.

10.7 Crear una red Wi-Fi de invitados

Muchos routers permiten crear una **red para invitados**:

- Tiene su propio SSID y clave.
- Puede aislar a los invitados de la red local (no ven tus equipos).
- Ideal para visitas, clientes, alumnos, etc.

Ventajas:

- Si el dispositivo de un invitado está infectado, tiene menos posibilidades de atacar tu red.
- Puedes limitar el ancho de banda o programar horarios de uso.
- Puedes cambiar la clave de invitados sin afectar a la red principal.
-

11 Medidas de seguridad complementarias

11.1 Filtrado por dirección MAC

Cada tarjeta de red tiene una **dirección MAC** única. El router puede permitir solo determinadas MAC.

Pasos:

1. Obtener la MAC de cada dispositivo (con `ipconfig /all`, `ifconfig` o en ajustes de Wi-Fi del móvil).
2. Añadirlas a la lista blanca del router (sección “Control de acceso”, “MAC Filter”, etc.).

Ventajas:

- Añade otra capa de control: aunque alguien conozca la clave, si su MAC no está en la lista, no entra.

Limitaciones:

- Un atacante avanzado puede **suplantar (spoofear)** una MAC permitida.
- No debe ser la única medida de seguridad, sino un complemento.

11.2 Reducir el rango de direcciones IP permitidas

El servicio DHCP permite definir un rango (por ejemplo 192.168.1.20–192.168.1.200).

Medida de seguridad:

- Reducirlo al número de dispositivos que realmente usamos (ej. 192.168.1.30–192.168.1.40 para 10 dispositivos).
- Desactivar DHCP y asignar IPs manuales en entornos muy controlados.

Ventajas:

- Menos IPs disponibles para intrusos.
- Más control sobre quién se conecta.

11.3 Limitar la potencia de emisión Wi-Fi

Muchos routers permiten ajustar la **potencia** de las antenas Wi-Fi.

Idea:

- Si la señal no sale de tu casa, será más difícil que alguien desde la calle detecte y ataque tu red.

Practica:

- Bajar ligeramente la potencia hasta que tengas buena cobertura dentro, pero poca fuera.
- Comprobarlo midiendo la señal con el móvil en distintas zonas.

11.4 Deshabilitar la administración remota

La opción de **administración remota** permite acceder al router desde Internet (ej. desde la casa de un familiar).

Riesgos:

- Si alguien descubre la IP y usuario/contraseña, puede administrar tu router desde cualquier lugar.

Recomendación:

- Desactivarla si no es absolutamente necesaria.
- Si se necesita, usar conexiones seguras (HTTPS/VPN) y contraseñas robustas.

11.5 Controlar los equipos conectados

En el panel del router suele haber una sección tipo “Dispositivos conectados”.

Medida:

- Revisar periódicamente la lista:
  – Si ves un dispositivo que no reconoces, puede ser un intruso.

Figura 10: Control de equipos conectador al router wifi de DIGI ZXHN H298Q

Acciones en caso de sospecha:

- Cambiar inmediatamente la clave Wi-Fi.
- Revisar el cifrado (WPA2/WPA3).
- Comprobar si el firmware está actualizado.

11.6 Desactivar UpnP

El **UPnP (Universal Plug and Play)** permite que las aplicaciones abran puertos automáticamente en el router.

Riesgo:

- Si un programa malicioso se ejecuta en tu PC, podría abrir puertos sin que te enteres.

Recomendación:

- Desactivar UPnP.
- Abrir manualmente los puertos que realmente necesites.

11.7 Apagar el router cuando no se use

Es una medida sencilla pero eficaz:

- Por la noche, en vacaciones, etc., **apagar el router** elimina cualquier posibilidad de ataque remoto.

Además:

- Ahorra algo de energía.
- A veces ayuda a “limpiar” problemas de conexión.

12 Comparación WPA2 vs WPA3

El estándar **WPA (Wi-Fi Protected Access)** protege las redes Wi-Fi mediante cifrado y autenticación.

12.1 WPA2

- Es el estándar más extendido.
- Suele usarse con el modo **WPA2-PSK (AES)**.
- Ofrece buen nivel de seguridad siempre que:
    - El firmware esté actualizado.
    - La contraseña sea robusta.

Debilidad conocida:

- El ataque **KRACK** (Key Reinstallation Attack) afecta a ciertas implementaciones de WPA2, permitiendo descifrar tráfico en condiciones concretas.

12.2 WPA3

Surge como evolución de WPA2:

- Mejora la **resistencia frente a ataques de diccionario** (contraseñas probadas masivamente).
- Ofrece un modo llamado **SAE (Simultaneous Authentication of Equals)** que refuerza la fase de autenticación.
- Proporciona mejor protección incluso si la contraseña no es perfecta.
- Incluye mejoras para redes abiertas (modo “WPA3-Enterprise” y “Enhanced Open”).

12.3 Tabla comparativa

Característica	WPA2	WPA3
Estado	Muy extendido	Nuevo, en expansión
Cifrado recomendado	AES (CCMP)	AES mejorado + SAE
Protección frente diccionario	Buena (si la clave es fuerte)	Muy mejorada, más difícil de romper
Redes abiertas seguras	No	Sí (modo Enhanced Open con cifrado individual)

Característica	WPA2	WPA3
Ataque KRACK	Afecta a implementaciones antiguas	Diseñado para mitigarlo

Recomendación práctica:

- **Si todos tus dispositivos soportan WPA3, úsalo**.
- Si tienes dispositivos antiguos, puedes usar modo mixto **WPA2/WPA3**.
- Evita siempre WEP y **no uses redes abiertas sin cifrado**.

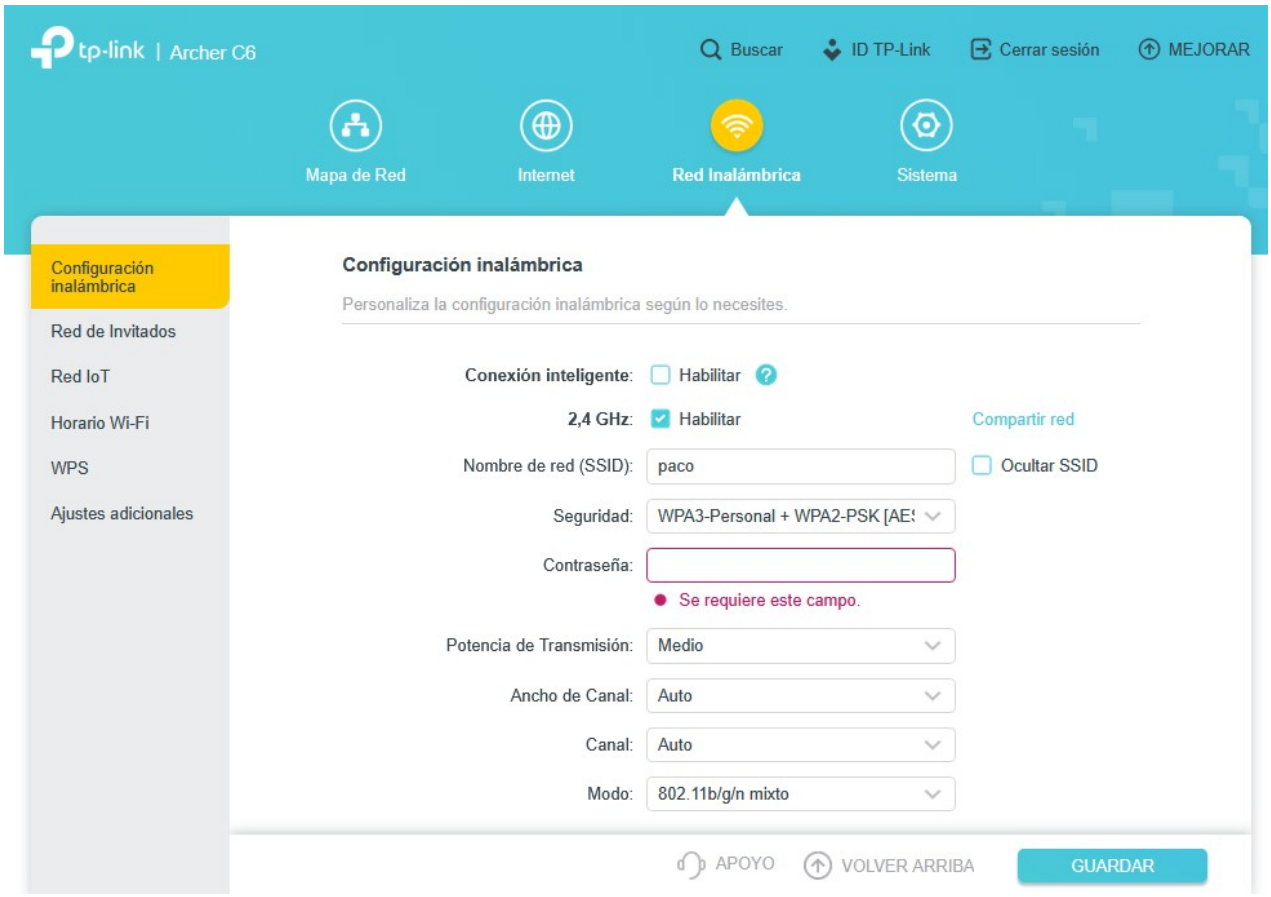

Figura 11: Router con wpa2 y wpa3

13 Más buenas prácticas de seguridad

Además de lo mencionado, es recomendable:

1. **Cambiar el usuario por defecto del router** (si lo permite), no solo la contraseña.
2. **Desactivar servicios que no uses** (servidor FTP, servidor de impresión, etc.).

3. **Hacer copia de seguridad de la configuración** del router cuando tengas un perfil seguro y estable.
4. **Activar registros (logs)**, si el router lo permite, y revisar de vez en cuando.
5. **Segregar redes**:
    - Red principal para tus equipos de confianza.
    - Red de invitados para móviles de visitas.
    - Si el router lo soporta, usar VLAN o varias SSID con distinto aislamiento.
6. **Proteger también los dispositivos de la red**:
    - Actualizar sistemas operativos y aplicaciones.
    - Usar antivirus en equipos Windows/Mac.
    - No instalar apps sospechosas en el móvil (pueden abrir puertas desde dentro).

14 Ejemplo práctico de configuración segura de un router doméstico

A continuación, un guion que podrías seguir en un examen práctico o en tu casa (no todos los routers tendrán exactamente las mismas opciones):

1. **Acceso inicial**
    - Conecta tu ordenador al router por cable.
    - Accede a `http://192.168.1.1` (o la puerta de enlace que corresponda).
    - Introduce usuario y contraseña inicial (pegatina del router).
2. **Cambiar credenciales de administración**
    - Entra en el menú “Administración” o “System”.
    - Cambia usuario (si es posible) y pon una contraseña robusta.
3. **Actualizar firmware**
    - Busca “Firmware update”.
    - Comprueba si hay una versión más reciente.
    - Actualiza siguiendo las instrucciones y reinicia el router.
4. **Configurar la LAN**
    - Asegúrate de que la IP del router sea algo común (ej. 192.168.1.1 o 192.168.0.1).
    - En el servidor DHCP:
        - Define un rango razonable (por ejemplo 192.168.1.50–192.168.1.100).
        - Crea reservas para impresoras u otros servidores internos si lo deseas.

5. **Configurar Wi-Fi principal**
    - Cambia el **SSID** por uno neutro (ej. “RedEstudio”).
    - Desactiva WPS.
    - Elige:
        - **Modo WPA2-PSK (AES)** o **WPA3-Personal** si está disponible.
    - Define una contraseña robusta.
6. **Crear red de invitados**
    - Activa la red para invitados.
    - Pon un SSID distinto (ej. “RedInvitados”).
    - Activa aislamiento de clientes (para que los invitados no vean la red principal).
    - Pon otra clave distinta, también segura.
7. **Filtrado MAC (opcional, como capa extra)**
    - Obtén las MAC de tus dispositivos.
    - Activa el filtrado en modo “lista blanca” y añade tus dispositivos.
8. **Desactivar UPnP y administración remota**
    - En el menú correspondiente, desactiva UPnP.
    - Desactiva administración remota por HTTP/HTTPS, a menos que la necesites.
9. **Ajustar potencia de emisión**
    - Reduce ligeramente la potencia (ej. al 70–80%).
    - Comprueba cobertura dentro y fuera de casa.
10. **Configurar port forwarding / DMZ (solo si hace falta)**
    - Si necesitas acceder a un servidor interno:
        - Crea reglas específicas de redirección de puertos.
    - Evita usar DMZ; si no hay más remedio, úsala solo con un dispositivo muy bien protegido.
11. **Configurar DDNS (opcional)**
    - Regístrate en un servicio de DNS dinámico (Por ejemplo Dyndns.com)
    - Introduce datos en el router y verifica que tu dominio se actualiza correctamente.
12. **Revisión final**
    - Comprueba la lista de dispositivos conectados.
    - Verifica desde el móvil que:

- Te conectas bien a la red principal.
- Te conectas a la red de invitados y no ves dispositivos de la principal.

- Guarda (si el router lo permite) un **backup** de la configuración.

13. **Comprobar si tienes comprometida tu red.**
    - Comprueba la lista de dispositivos conectados
    - Lleva el lista a la IA
    - Pidele un informe de máquinas conectadas , ips, dispositivos y posibles accesos no autorizados.

15 Resumen del tema

- Un **router** es el corazón de la red doméstica: conecta la LAN con Internet y dirige el tráfico.
- Existen distintos tipos: domésticos, empresariales, **routers neutros** y **sistemas mesh**.
- Un **punto de acceso (AP)** crea una red Wi-Fi a partir de una red cableada; un **repetidor** amplía la cobertura repitiendo la señal.
- El router ofrece servicios como **DHCP, NAT, redirección de puertos, DMZ, QoS, VPN y DNS dinámico**, esenciales para el funcionamiento y accesibilidad de la red.
- La seguridad es crítica: un router mal configurado puede provocar **robos de información, uso ilícito de la conexión y pérdida de rendimiento**.
- Medidas básicas:
    - Cambiar contraseña de administración.
    - Cambiar SSID.
    - Contraseña Wi-Fi robusta.
    - Firmware actualizado.
    - Cifrado **WPA2 o WPA3** y desactivar WPS.
    - Crear red de invitados.
- Medidas complementarias:
    - Filtrado MAC.
    - Rango de IPs limitado.
    - Potencia de emisión ajustada.
    - Administración remota y UPnP desactivados.
    - Supervisión de dispositivos conectados y apagado del router cuando no se use.

Si quieres, en otro mensaje puedo prepararte:

- Una **portada y índice** listos para imprimir.
- O un **ejercicio práctico** donde el alumno tenga que tomar capturas de pantalla de cada paso de configuración del router.

16 Bibliografía

- Aprende a configurar tu router. De forma segura paso a paso. Incibe.