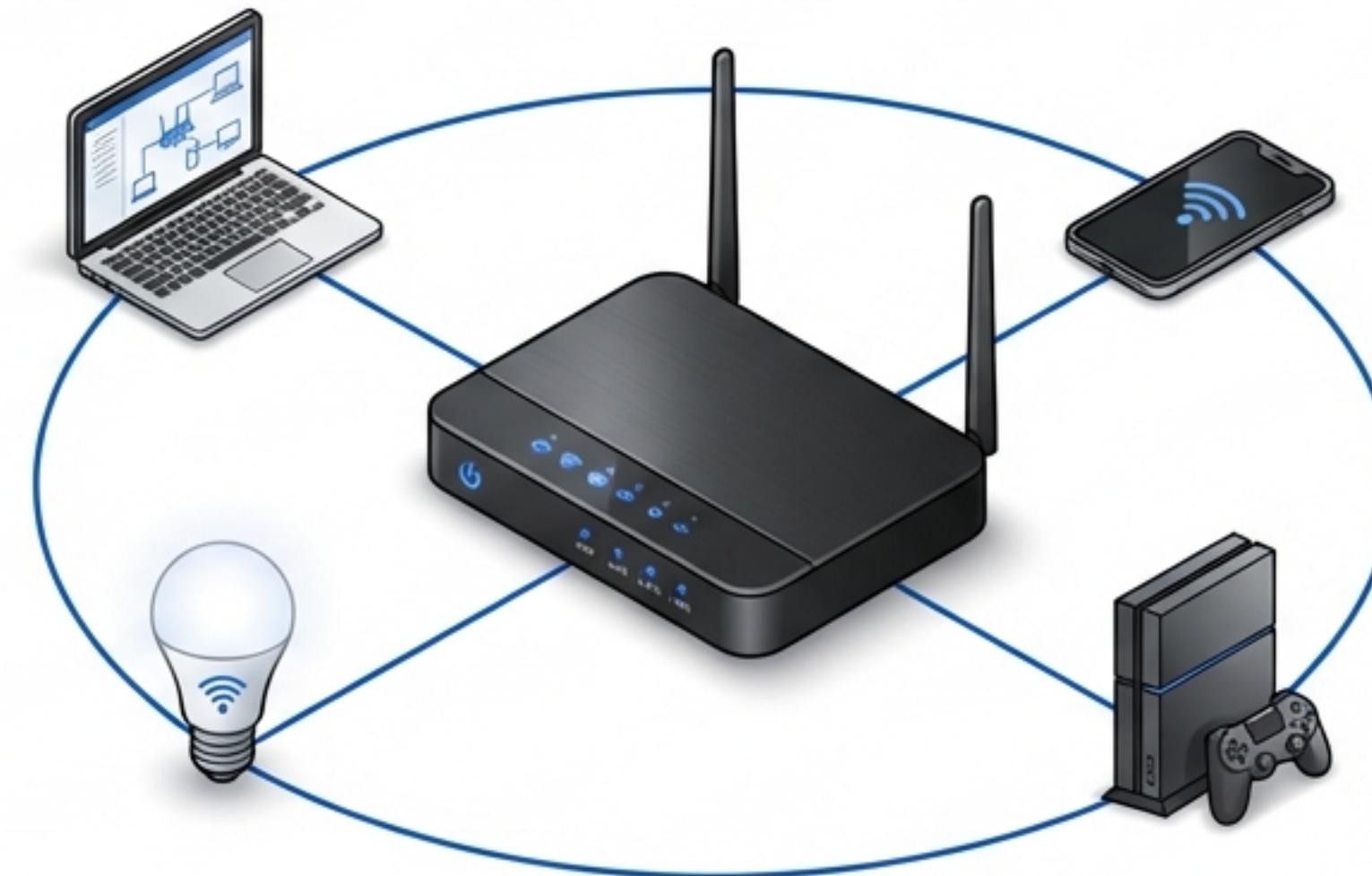


Tratamiento de la Información y Competencia Digital: El Router

Guía completa de configuración, arquitectura de red y seguridad cibernética

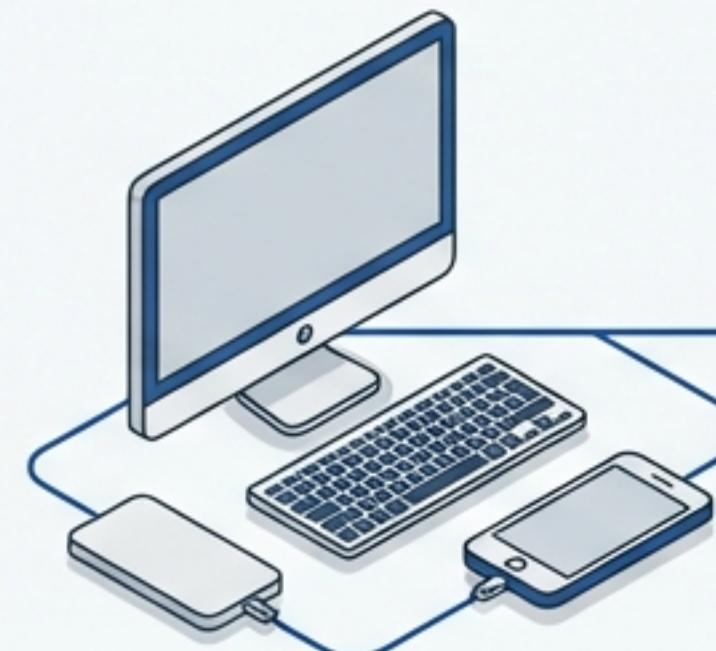


“El corazón de su red: De la caja de plástico a la fortaleza digital.”

Basado en “Configuración básica de routers” por Francisco Aldarias Raya (2026)

El Ecosistema: LAN vs. WAN

Red Local (LAN)



LAN (Red de Área Local)

- El tráfico dentro de casa (Oficina, aula, hogar).
- **IP Privada:** Identificador interno (ej. '192.168.1.10').

Internet (WAN)



WAN (Red de Área Extensa)

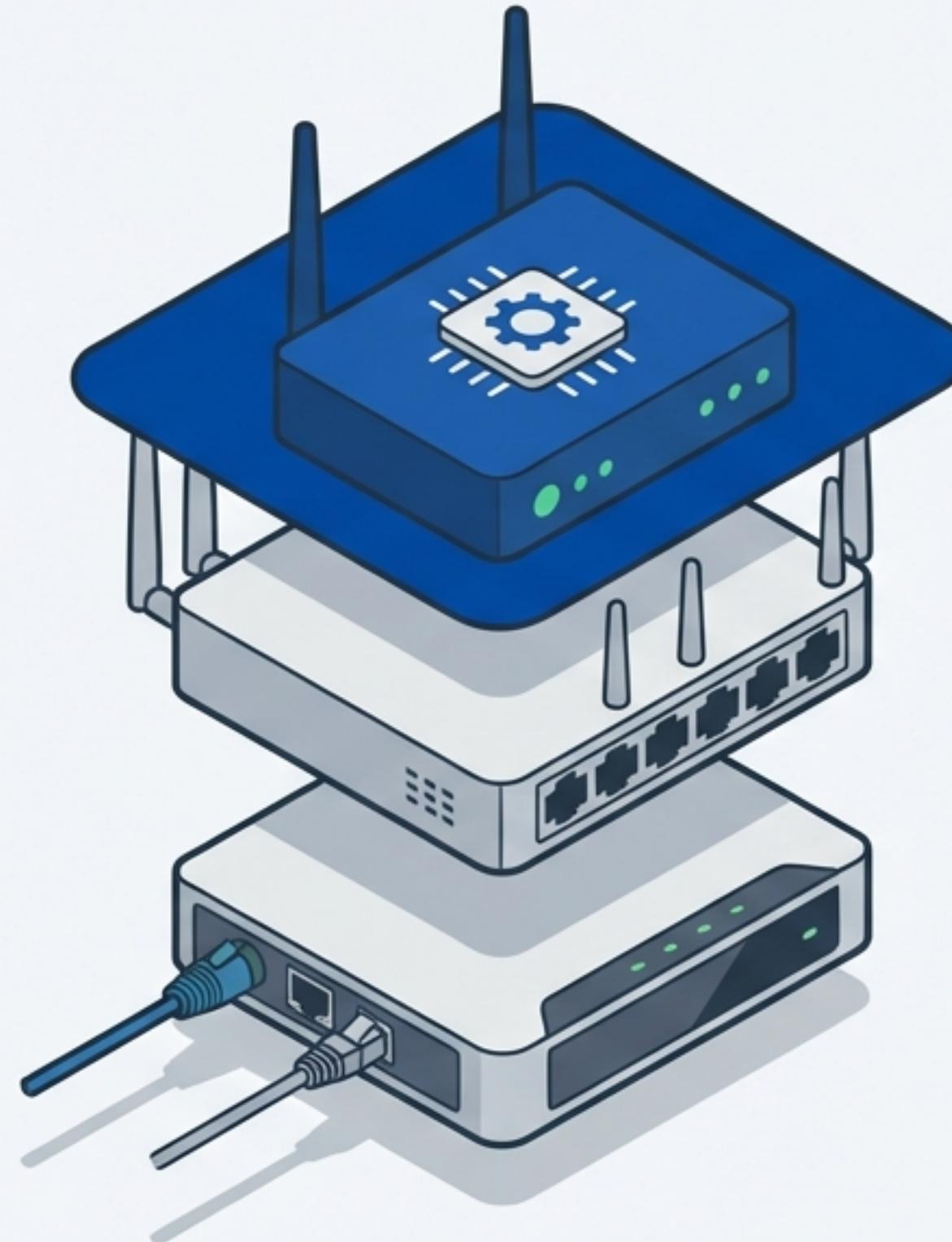
- Internet, la red gigante exterior.
- **IP Pública:** La matrícula visible en internet.

ROUTER

La Puerta de Enlace (Gateway)

La dirección IP del router (ej. '192.168.1.1') que actúa como la salida obligatoria hacia Internet.

Anatomía de una decisión: ¿Qué es un Router?



3. Router (Capa 3 OSI)

El director de tráfico.

2. Switch / Punto de Acceso

Conecta dispositivos
(Capa 2 Enlace de Datos).

1. Módem

Traduce la señal de
fibra/cable a digital.

La Función del Cerebro (Capa de Red)

El router lee la IP de destino de cada paquete y decide:

¿Esto es para el vecino de al lado (LAN)?
¿O para una ciudad lejana (WAN)?

Eligiendo la Herramienta Correcta

Domésticos



El "Todo en uno" estándar.

- Módem integrado.
- Configuración web simple.
- Para uso básico hogar/oficina.

Empresariales



Alto Tráfico.

- VLANs y VPNs robustas.
- Balanceo de carga.
- Configuración por consola/`SSH`.

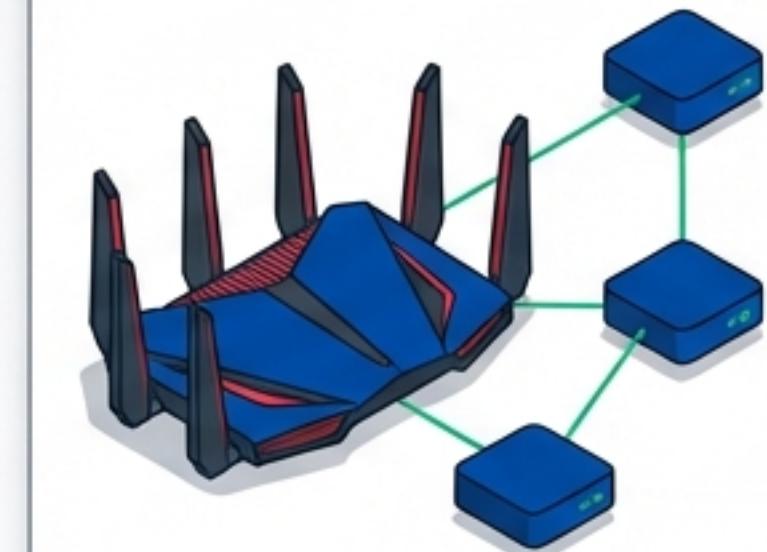
Neutros



Libertad y Potencia.

- Sin módem integrado (Requiere modo puente).
- Aislamiento de la red del proveedor.
- Wi-Fi superior.

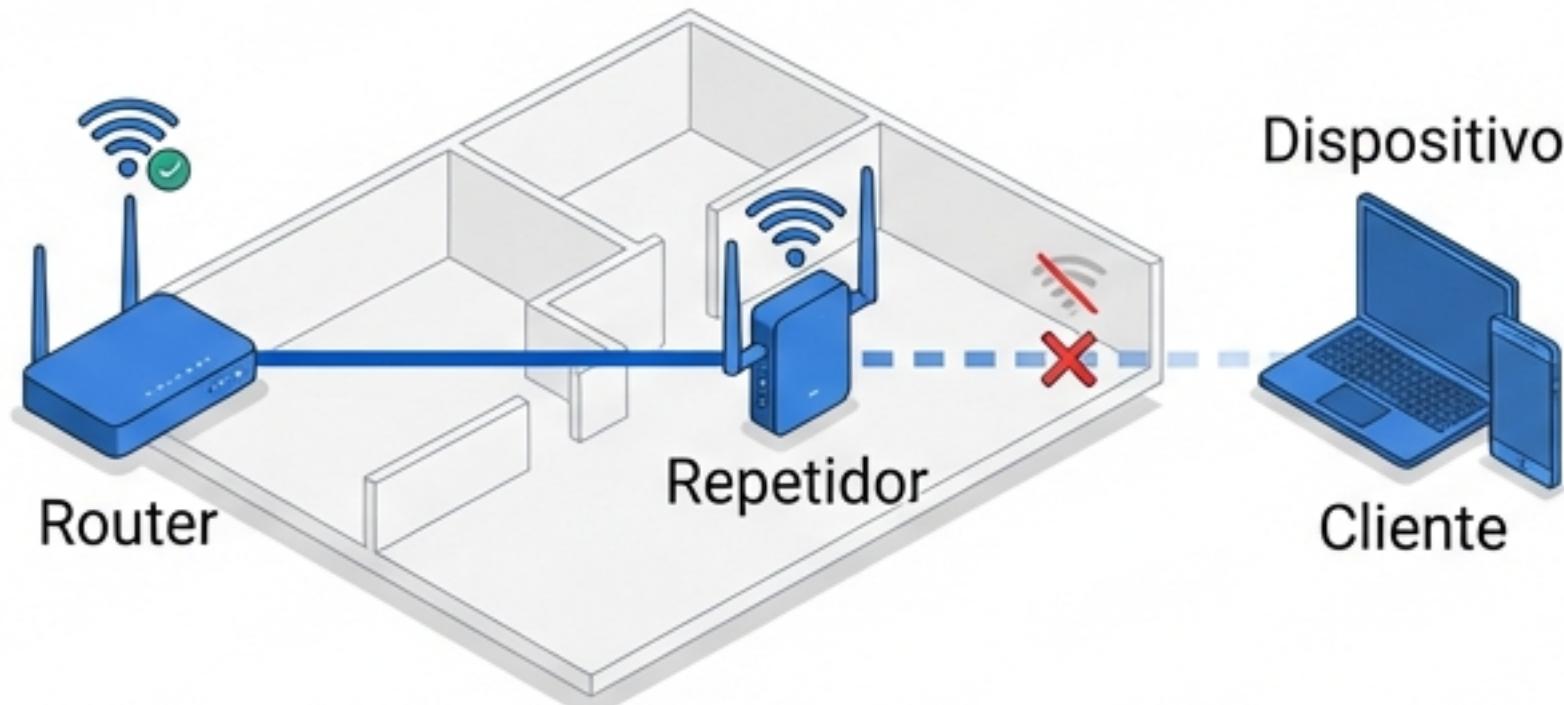
Gaming / Mesh



Nichos Específicos.

- Optimizado para baja latencia.
- Cobertura total (Mesh).

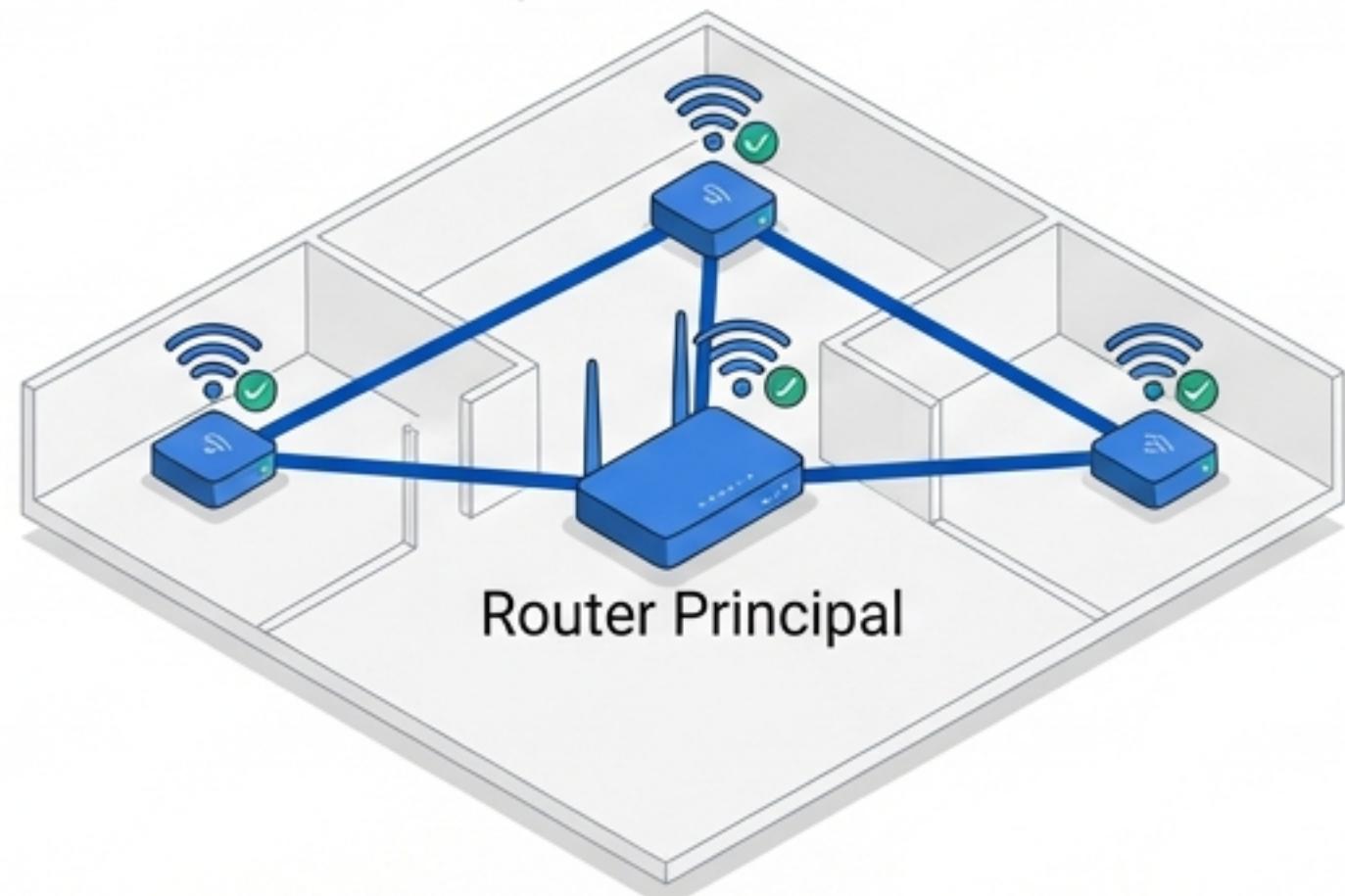
Arquitectura de Cobertura: Mesh vs. Repetidores



Repetidor (La solución antigua)

Recibe y retransmite.

Desventaja: Reduce el ancho de banda a la mitad (Half-duplex) y crea conflictos al moverse.



Sistema Mesh (La solución inteligente)

Malla única: Un solo SSID para toda la casa.

Roaming transparente: El móvil cambia de nodo sin cortar la llamada.

Gestión centralizada: Los nodos 'hablan' entre sí para buscar la ruta más rápida.

Tomando el Control: Acceso a la Gestión

1. Conexión Física

Conecte un PC al router vía cable Ethernet
(Recomendado).

2. Identificar la Puerta de Enlace

Windows: cmd > ipconfig

Mac/Linux: ifconfig o ip route

Busque: 'Puerta de enlace predeterminada'

3. El Navegador

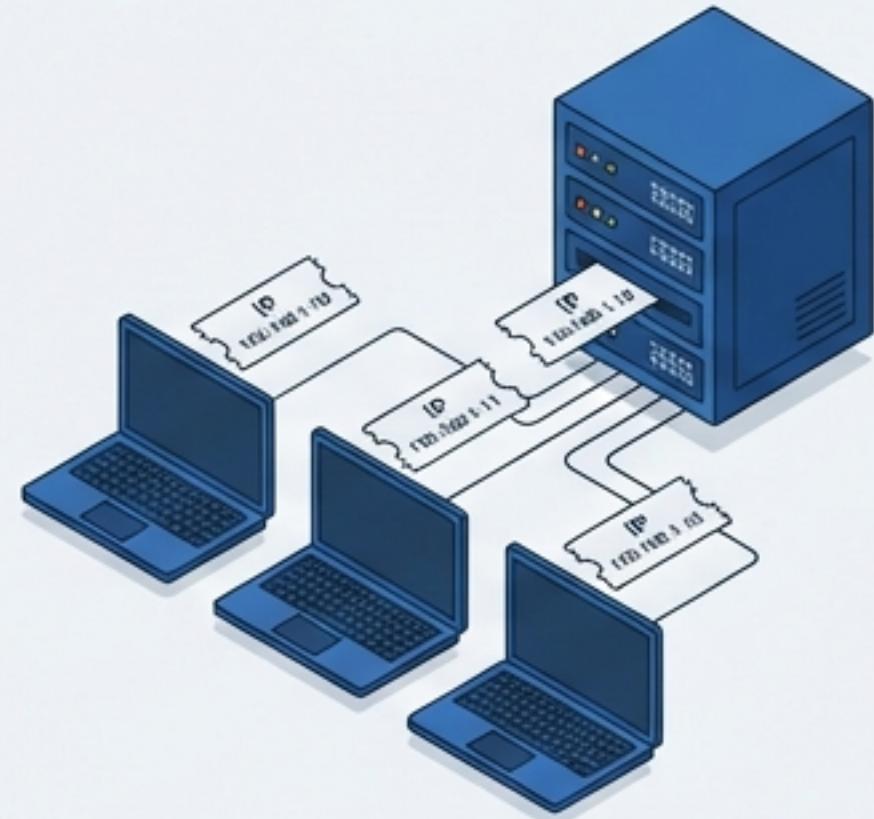
Escriba la IP en la barra de direcciones (ej.
<http://192.168.1.1>).

4. Autenticación

Usuario/Clave (Busque la etiqueta en la base
del router).

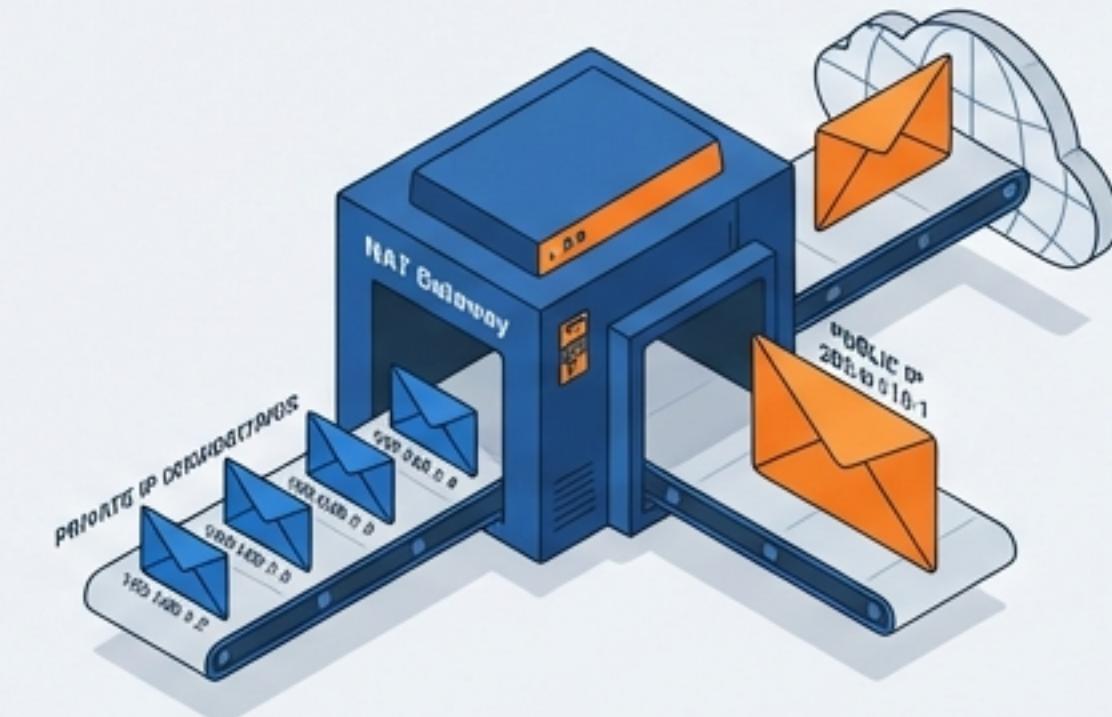


Servicios Invisibles I: Automatización y Traducción



DHCP (Dynamic Host Configuration Protocol)

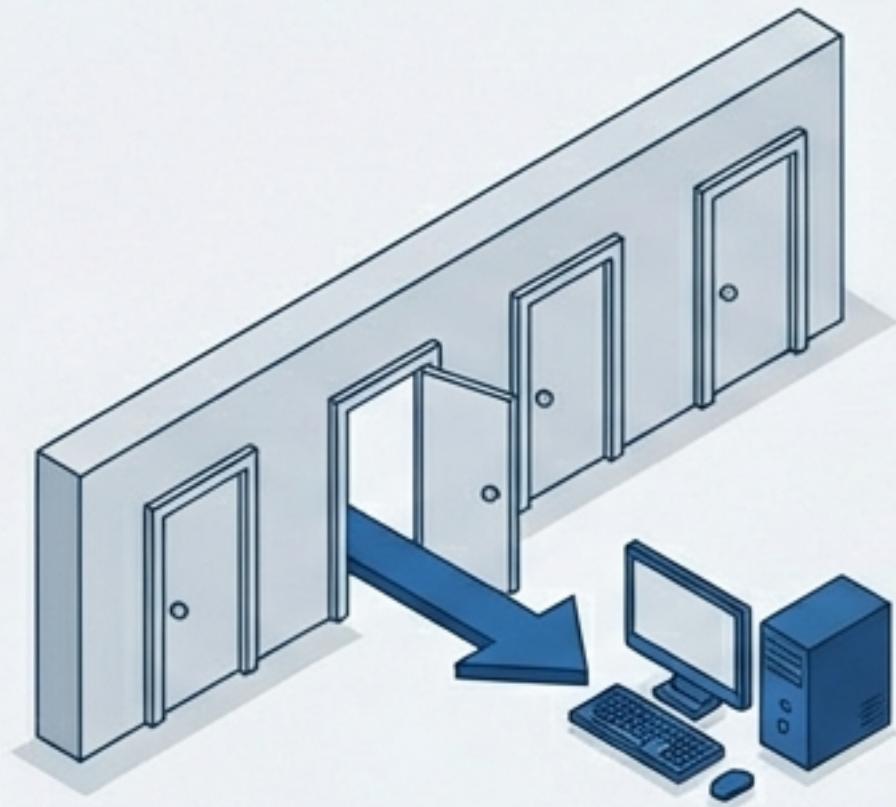
- **Función:** Asigna IPs, Máscara y DNS automáticamente.
- **Concepto Clave:** Lease Time (Tiempo de concesión) - el tiempo que un dispositivo 'alquila' una dirección.



NAT (Network Address Translation)

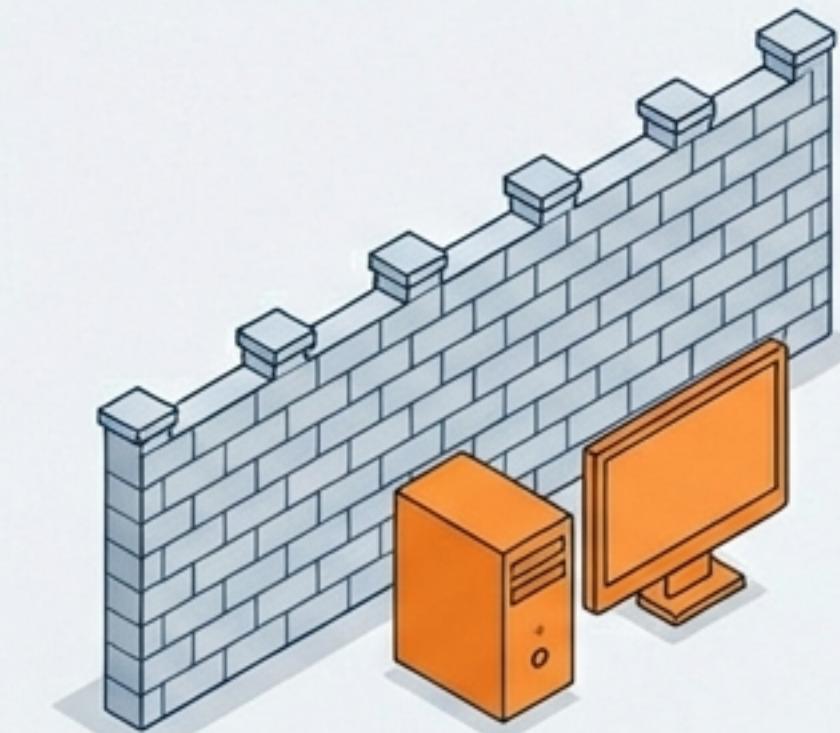
- **Función:** Permite que múltiples dispositivos (192.168.x.x) naveguen con una sola **IP Pública**.
- **Mecánica:** Reescribe los encabezados de los paquetes para enrutar la respuesta al dispositivo correcto.

Servicios Invisibles II: Accesibilidad y Riesgo



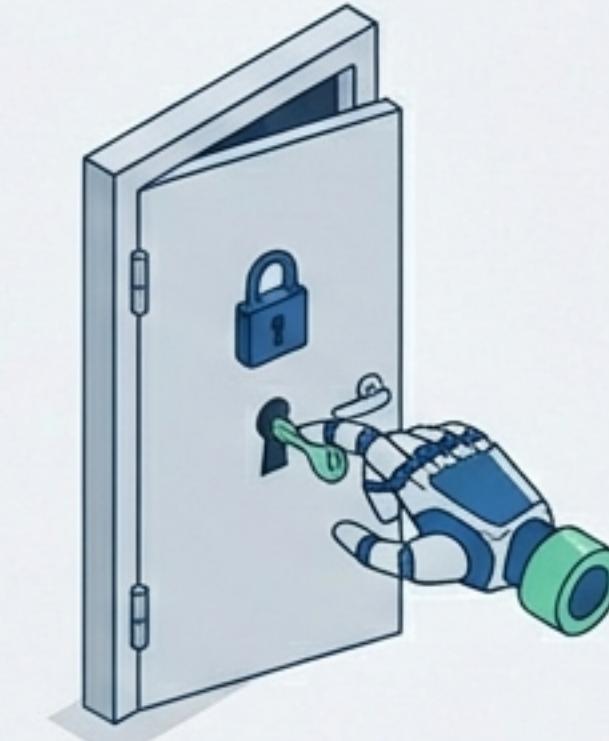
Redirección de Puertos

- Abrir caminos específicos. "Si tocan al timbre en el puerto 80, envíalos al PC del salón". Vital para servidores web o juegos.



DMZ (Zona Desmilitarizada)

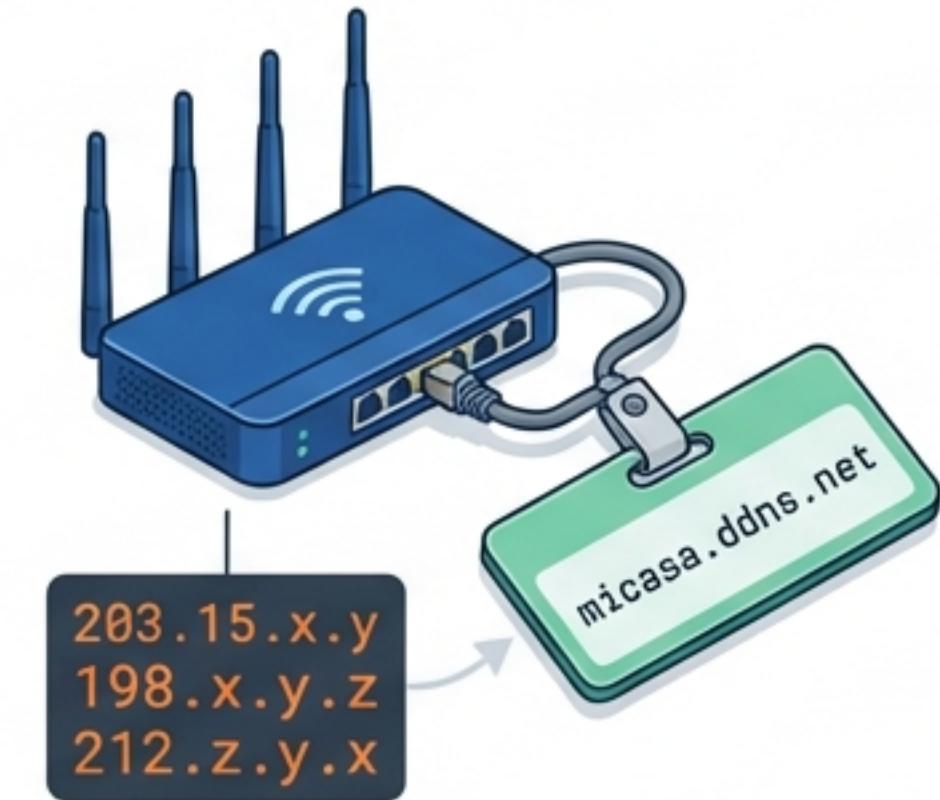
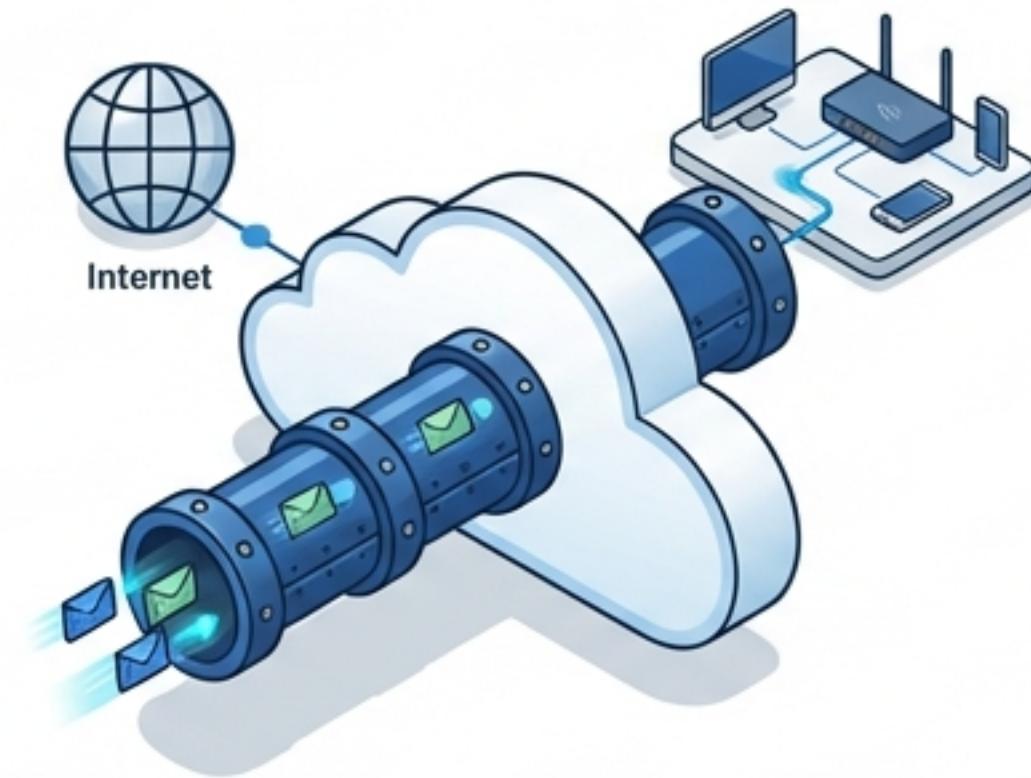
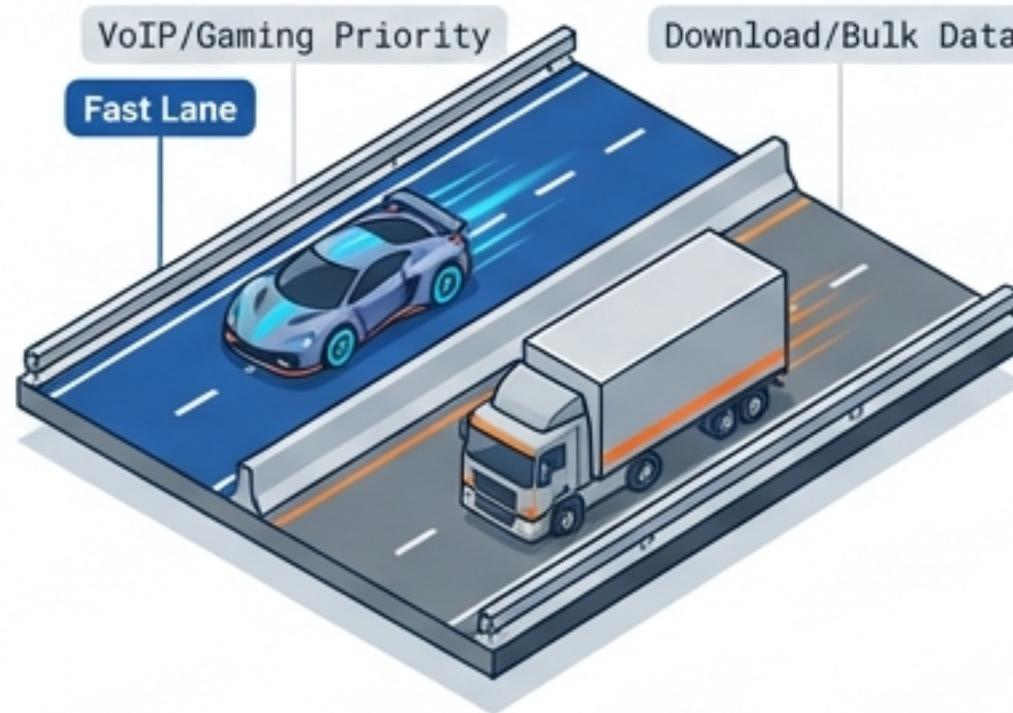
- **Advertencia:** Expone TODOS los puertos de un dispositivo a internet.
- Riesgo de seguridad extremo. Usar solo como último recurso.



UPnP (Universal Plug and Play)

- Permite a las apps abrir puertos automáticamente.
- **Consejo de Seguridad:** DESACTIVAR. El malware puede usarlo para abrir puertas traseras.

Servicios Avanzados: Prioridad y Acceso Remoto



QoS (Calidad de Servicio)

- Gestión inteligente de la tubería.
- Prioriza tráfico crítico (VoIP, Gaming) sobre descargas masivas.

VPN (Red Privada Virtual)

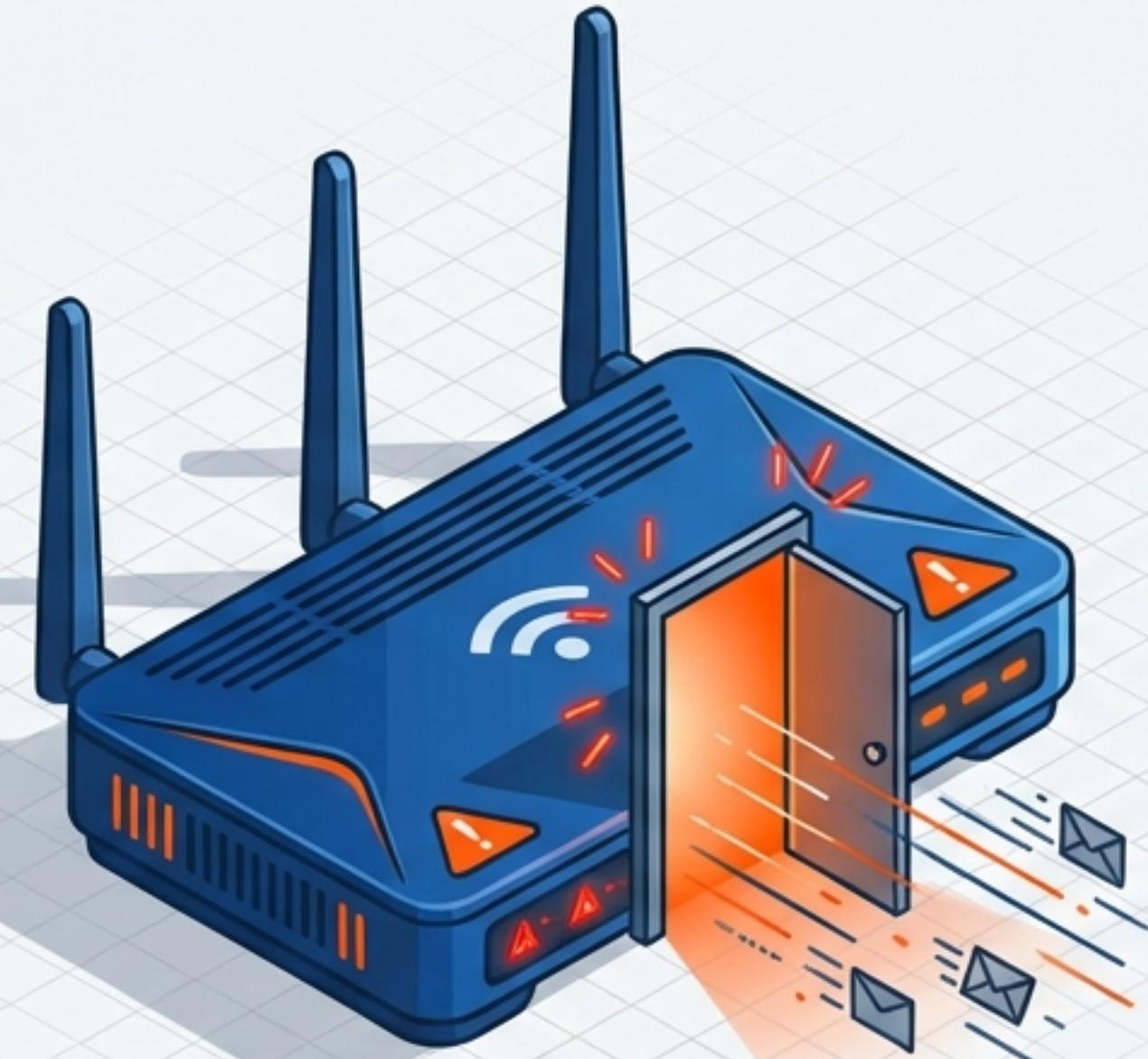
- **Server:** Acceso seguro a tu casa desde fuera.
- **Client:** Toda tu red navega cifrada hacia internet.

DDNS (Dominio Dinámico)

- Solución para IPs dinámicas.
- Asocia un nombre fijo a tu IP cambiante para localizar siempre tu router.

La Fortaleza Digital: ¿Por qué asegurar el router?

Riesgos de una configuración por defecto



1. Robo de Información

Interceptación de tráfico, acceso a cámaras IP privadas y robo de archivos en carpetas compartidas (NAS).



2. Responsabilidad Legal

Si un intruso usa su red para actividades ilícitas (ataques DDoS, descargas ilegales), la IP rastreada será la suya.



3. Degradación del Servicio

El "vampirismo" de Wi-Fi. Vecinos o intrusos consumiendo su ancho de banda reducen la velocidad de su hogar.

Un router mal configurado es una ventana abierta a su vida privada.

Seguridad Nivel 1: El 'Big 3' Obligatorio

Credenciales de Administración



Nunca dejar las credenciales de fábrica. Si alguien entra aquí, posee la red.

Identidad de la Red (SSID)



Cambiar nombres por defecto.
Evitar datos personales
(Nombre, Piso).
Opción: Ocultar SSID.

Firmware



El sistema operativo del router.
Actualizar periódicamente para obtener parches de seguridad críticos.

El Candado de la Red: Cifrado Wi-Fi

WEP (Obsoleto)



WEP (Obsoleto)

Inseguro. Nunca usar.

WPA2-PSK (AES) (Estándar)



WPA2-PSK (AES) (Estándar)

El estándar actual. Vulnerable a KRACK si no está parcheado.

WPA3 (Recomendado)



WPA3 (Recomendado)

Protección anti-diccionario. Autenticación SAE. Redes abiertas seguras.



ACCIÓN CRÍTICA: Desactivar WPS

El sistema de PIN es fácilmente hackeable por fuerza bruta. Es el agujero de seguridad más común.

Seguridad Nivel 2: Blindaje Avanzado

Filtrado MAC

Listas Blancas

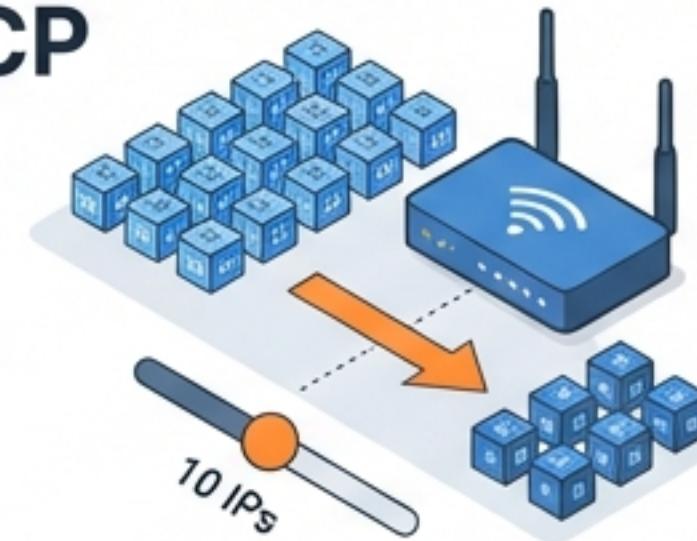
Configurar el router para que solo permita entrar a los dispositivos de una lista preprobada.



Minimización DHCP

Reducción de Superficie

Reducir el rango de IPs a las estrictamente necesarias (ej. solo 10 IPs disponibles).



Potencia Wi-Fi

Geolimitación Física

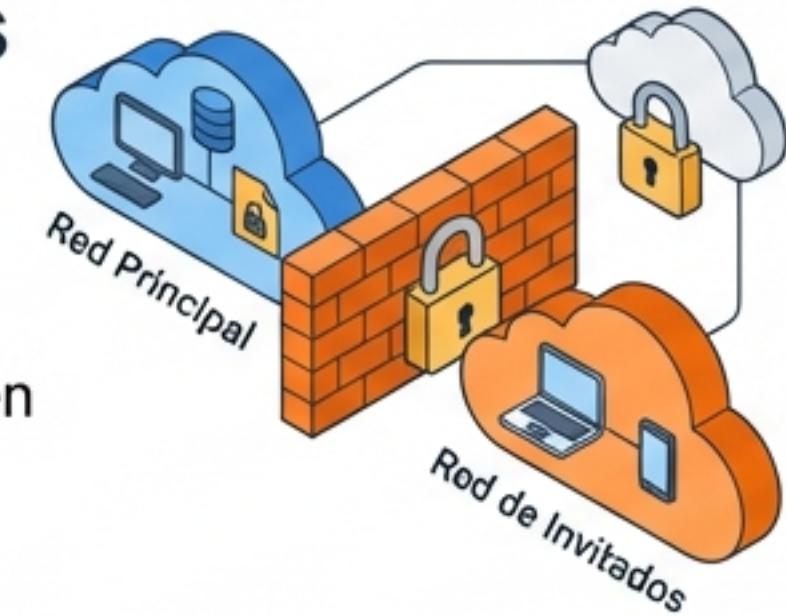
Bajar la intensidad de la antena para que la señal no llegue a la calle.



Red de Invitados

Aislamiento Total

Crear una VLAN/SSID separada para visitas. Tienen internet, pero no ven sus archivos ni dispositivos.



Checklist: Protocolo de Configuración Segura



Acceso Físico

Conectar por cable y entrar a la Gateway.



Identidad

Cambiar usuario y contraseña de admin.



Sistema

Buscar y aplicar actualización de Firmware.



Wireless

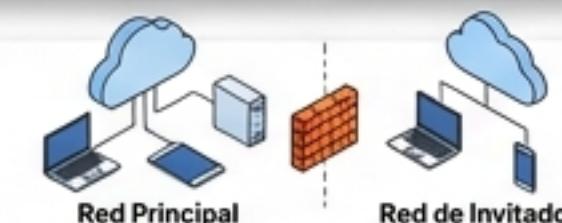
Configurar WPA3 (o WPA2-AES) + SSID Neutro.

Desactivar WPS.



Segregación

Activar Red de Invitados con aislamiento.



Hardening

Desactivar UPnP y Administración Remota.



Verificación

Revisar la lista de clientes conectados.



Resumen y Mantenimiento

Key Takeaways

- El router es el **dispositivo más crítico** de su infraestructura.
- **DHCP y NAT** son los motores invisibles; WPA3 y Firewall son los escudos.
- La seguridad no es un evento único, **es un hábito**: revise logs y dispositivos periódicamente.



Reflexión Final

Apagar el router cuando no se usa es la única seguridad infalible (Capa 0).