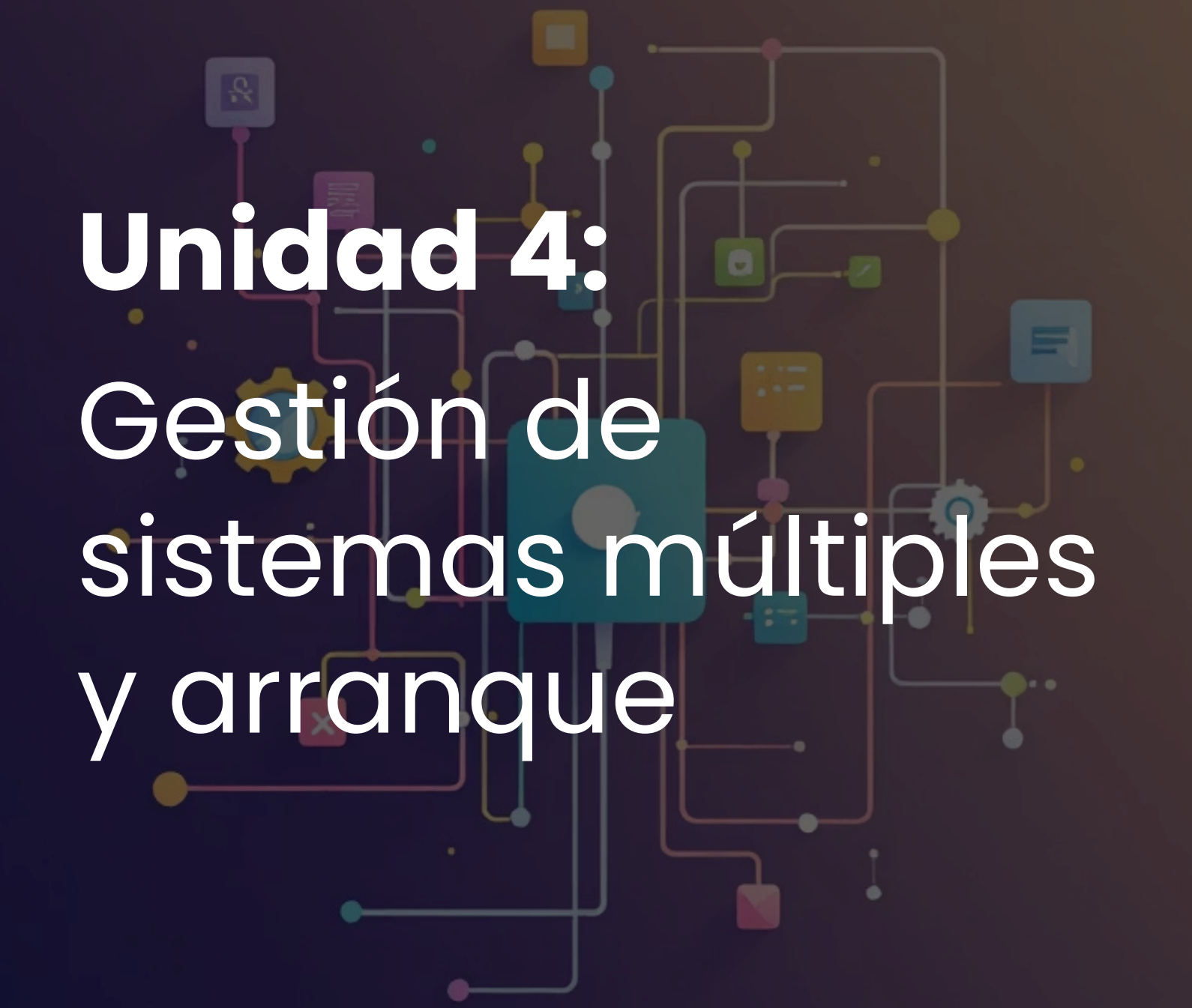
PROMETEO



Unidad 4:
Gestión de sistemas múltiples y arranque

Sistemas informáticos

Técnico Superior de DAM / DAW

El ADN de la conectividad digital

Cuando escribes una dirección como **www.google.com** en tu navegador y la página se abre en cuestión de segundos, detrás de ese acto aparentemente simple ocurre un proceso técnico sofisticado. Tres elementos lo hacen posible: el DNS (Domain Name System), el enrutamiento (routing) y la resolución de nombres. Comprender cómo funcionan es esencial para cualquier profesional que trabaje con redes, servidores o sistemas digitales, ya que forman la base invisible sobre la que se construye toda la comunicación en Internet.

El DNS: la agenda telefónica de Internet

El DNS es un sistema global que traduce los nombres de dominio (fáciles de recordar para los humanos) en direcciones IP (que los ordenadores y routers pueden entender). Por ejemplo, cuando escribes google.com, tu equipo consulta un servidor DNS para averiguar que su dirección IP es 142.250.184.142. Este proceso evita que tengas que memorizar largas cadenas numéricas.

Los servidores DNS están organizados jerárquicamente en varios niveles:

01

Servidores raíz (root servers)

el primer nivel de búsqueda. Existen solo 13 conjuntos distribuidos en todo el mundo.

02

Servidores de dominio de nivel superior (TLD servers)

gestionan extensiones como .com, .es o .org.

03

Servidores autoritativos

contienen los registros definitivos de un dominio concreto (por ejemplo, el DNS de Google).

El DNS no solo resuelve direcciones web. También se utiliza para correo electrónico (registros MX), verificación de identidad (TXT, SPF) y seguridad (DNSSEC). Es la base de la infraestructura digital moderna.

Enrutamiento: los caminos de los datos

Una vez que el DNS ha proporcionado la dirección IP del destino, entra en juego el enrutamiento, el proceso mediante el cual los routers determinan el mejor camino que deben seguir los paquetes de datos a través de la red para llegar al servidor correcto.

Los routers funcionan como señales de tráfico: analizan las rutas disponibles, el estado de la red y las políticas configuradas para decidir por dónde enviar los paquetes. Los protocolos más comunes son:

RIP (Routing Information Protocol)

usa saltos (hops) como métrica.

OSPF (Open Shortest Path First)

elige la ruta más corta según el ancho de banda y la latencia.

BGP (Border Gateway Protocol)

conecta grandes redes o "autónomos" en Internet, siendo el "GPS" de la red global.

Sin el enrutamiento, los datos no sabrían cómo ir de tu ordenador al servidor de destino. Y sin DNS, no sabrías a qué dirección enviar esos datos.

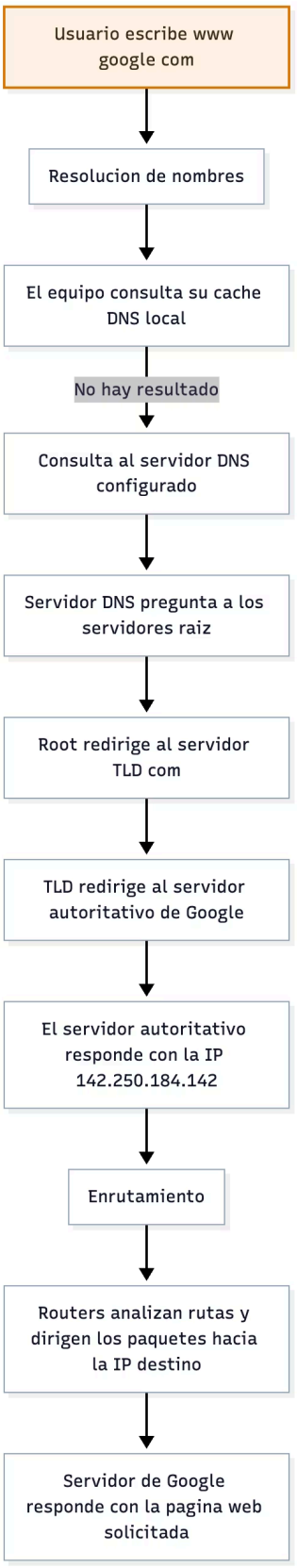
Resolución de nombres: la cadena de eventos

La resolución de nombres es el proceso completo por el que tu dispositivo traduce un dominio en una IP y establece conexión. A grandes rasgos, sigue estos pasos:

1. El usuario escribe un dominio (por ejemplo, google.com).
2. El sistema operativo busca en su caché local DNS para ver si ya tiene la IP almacenada.
3. Si no la tiene, consulta al servidor DNS configurado (por lo general, el del proveedor de Internet o uno público como Google DNS o Cloudflare).
4. Ese servidor, si tampoco tiene la respuesta, pregunta a los servidores raíz, que lo redirigen al servidor TLD y, finalmente, al autoritativo.
5. El servidor autoritativo devuelve la IP, y la respuesta se almacena temporalmente (cacheada) para acelerar futuras consultas.

Todo este proceso ocurre en milisegundos, pero su correcta configuración es esencial para garantizar la disponibilidad de cualquier servicio en línea.

Esquema visual: Del dominio al destino



El siguiente diagrama describe el flujo completo desde que un usuario escribe un dominio hasta que los datos llegan al servidor.

Descripción del diagrama:

- **Nodo A:** representa al usuario iniciando la solicitud.
- **Nodos B–H:** describen la resolución de nombres mediante el sistema DNS jerárquico.
- **Nodo I–J:** representa la etapa de enrutamiento, donde los routers determinan el mejor camino hacia el servidor.
- **Nodo K:** indica la entrega del contenido al navegador, cerrando el ciclo de comunicación.

Este flujo combina tres procesos: resolución de nombres, consulta de servidores DNS y enrutamiento de paquetes. Es la base funcional de todo el tráfico en Internet.

Caso de estudio: Cloudflare y la carrera por la velocidad y la privacidad

Contexto

Durante años, los proveedores de Internet controlaban los servidores DNS que usaban sus clientes, priorizando la estabilidad por encima de la velocidad o la privacidad. Sin embargo, con el aumento del tráfico cifrado y las crecientes preocupaciones sobre la vigilancia digital, surgió una nueva generación de servicios DNS públicos centrados en la rapidez y protección de datos.

Estrategia

En 2018, Cloudflare lanzó el servicio 1.1.1.1, que revolucionó el sector. Su promesa era simple: "El DNS más rápido y privado del mundo". Sus principales innovaciones fueron:

Velocidad récord

respuesta media de 13 milisegundos, frente a los 35–40 ms de otros proveedores.

Privacidad total

Cloudflare prometió no registrar direcciones IP ni historiales de búsqueda.

Seguridad reforzada

integración con DNS-over-HTTPS (DoH) y DNS-over-TLS (DoT), que cifran las consultas para evitar que terceros (como proveedores o gobiernos) las intercepten.

Infraestructura global

más de 300 centros de datos distribuidos en 100 países, asegurando baja latencia en casi cualquier ubicación.

Además, Cloudflare ofrece protección anti-DDoS: actúa como un escudo entre los usuarios y los servidores de las empresas, filtrando ataques de tráfico masivo.

Resultado

Cloudflare 1.1.1.1 se convirtió rápidamente en el DNS público preferido por millones de usuarios y empresas, superando a Google DNS (8.8.8.8) en muchos países en términos de rendimiento. La empresa fortaleció su imagen como referente de seguridad y rendimiento en Internet, mostrando que optimizar algo tan básico como el DNS puede tener un impacto directo en la velocidad y la confianza del usuario.

Herramientas y consejos

Cambia tus DNS para mejorar rendimiento y seguridad

Puedes configurar manualmente servidores DNS públicos como:

- Cloudflare: 1.1.1.1 y 1.0.0.1
- Google DNS: 8.8.8.8 y 8.8.4.4
- Quad9: 9.9.9.9 (orientado a seguridad)

Esta acción sencilla puede mejorar la velocidad de navegación y proteger tus datos frente a rastreos.

Usa herramientas de diagnóstico profesional

- **nslookup** (Windows/Linux/macOS): consulta la dirección IP de un dominio y verifica qué servidor DNS responde.
- **dig** (Linux/macOS): muestra información más detallada sobre el proceso de resolución (útil para administradores).
- **traceroute o tracert**: rastrea el camino que siguen los paquetes desde tu ordenador hasta el destino, mostrando los routers intermedios (ideal para detectar cuellos de botella).

Verifica rendimiento y disponibilidad global

- Plataformas como DNSPerf.com permiten comparar la velocidad y fiabilidad de distintos proveedores DNS en tiempo real.
- PingPlotter o MTR (My TraceRoute) combinan ping y traceroute en una sola herramienta para monitorear la estabilidad de la red.

Activa DNS cifrado (DNS over HTTPS)

En navegadores como Chrome, Firefox o Edge puedes activar DoH (DNS over HTTPS) en ajustes avanzados. Esto protege tus consultas de espionaje y mejora la privacidad en redes públicas.

Mitos y realidades

❌ Mito: "El DNS solo sirve para navegar por Internet."

→ **FALSO.** El DNS interviene en casi todos los servicios conectados: correo electrónico (registros MX), mensajería instantánea (SRV), autenticación de dominios (TXT, SPF, DKIM), videojuegos online e incluso aplicaciones móviles que verifican conexiones seguras. Sin DNS, muchos servicios simplemente no funcionarían.

❌ Mito: "Debo usar siempre el DNS de mi proveedor de Internet."

→ **FALSO.** Cualquier usuario puede cambiar sus DNS a servidores públicos o privados que sean más rápidos o seguros. De hecho, muchas empresas configuran sus propios DNS internos para controlar el tráfico y aplicar políticas de seguridad. Usar alternativas como Cloudflare o Google DNS mejora la privacidad y reduce la dependencia del proveedor.

Resumen final

- **DNS:** traduce dominios en direcciones IP (ej: google.com → 142.250.184.142).
- **Resolución de nombres:** proceso completo de consulta a servidores DNS.
- **Enrutamiento:** los routers deciden el mejor camino para los datos.
- **DNS públicos:** Cloudflare (1.1.1.1), Google (8.8.8.8), Quad9 (9.9.9.9).
- **Comandos útiles:** nslookup, dig, traceroute, ping.
- **Claves:** velocidad, privacidad, caché y cifrado DNS.

Sesión 14 – Herramientas de diagnóstico: ping, traceroute, Wireshark y Nmap

Diagnosticar la red, el primer paso hacia la estabilidad

Imagina que tu conexión a Internet empieza a fallar. No puedes acceder al servidor de la empresa, el correo deja de sincronizarse y las páginas cargan a medias. En ese momento, la diferencia entre un usuario y un profesional de sistemas es la capacidad de diagnosticar. El diagnóstico de red es el conjunto de técnicas y herramientas que permiten detectar, analizar y resolver problemas de conectividad, rendimiento o seguridad en una infraestructura digital. Cuatro de las herramientas más poderosas y universales para ello son ping, traceroute, Wireshark y Nmap.

Ping: la prueba de vida digital

El comando ping (del término Packet Internet Groper) es la forma más básica y eficaz de comprobar si un dispositivo responde en la red. Funciona enviando pequeños paquetes de datos (ICMP Echo Request) al destino y esperando su respuesta (ICMP Echo Reply). Si hay respuesta, el host está "vivo"; si no la hay, puede estar desconectado o filtrando el tráfico.

Además, ping mide:

- **Tiempo de respuesta (latencia):** cuántos milisegundos tarda el paquete en ir y volver.
- **Pérdida de paquetes:** porcentaje de mensajes que no llegan, indicador de congestión o cortes de red.

Un simple `ping google.com` puede confirmar si tienes conexión general a Internet, mientras que `ping 192.168.1.1` comprueba si el router local responde.

Traceroute: el mapa del viaje de los datos

Cuando un paquete de datos viaja desde tu ordenador a un servidor, puede atravesar decenas de routers. Si algo falla en el camino, traceroute (o tracert en Windows) te muestra dónde se detiene el tráfico.

Traceroute envía paquetes con un valor de "Tiempo de vida" (TTL) que aumenta en cada intento. Cada router que los recibe devuelve una respuesta, revelando su dirección IP. El resultado final es una lista ordenada de todos los "saltos" (hops) intermedios.

Este comando es clave para:

- Diagnosticar problemas de enrutamiento o latencia.
- Identificar si el fallo está en tu red local, en tu proveedor o en el servidor remoto.
- Visualizar la topología de conexión hasta un destino.

Por ejemplo, si traceroute muestra que los paquetes se detienen en un nodo de tu ISP, sabes que el problema no está en tu equipo, sino fuera de tu control.

Wireshark: ver lo invisible

Wireshark es el microscopio de la red. Permite capturar y analizar en detalle cada paquete de datos que circula por una interfaz (Ethernet, Wi-Fi, Bluetooth, etc.). Es una herramienta fundamental para:

- Diagnosticar problemas complejos de red o aplicaciones.
- Analizar protocolos (HTTP, DNS, TCP, etc.) y su comportamiento.
- Identificar ataques o fugas de información (ciberseguridad).

Cada paquete capturado puede verse capa por capa, desde la dirección MAC hasta el contenido de la solicitud HTTP. Por eso, Wireshark es utilizado tanto por administradores de red como por investigadores forenses digitales.

Nmap: el radar de los sistemas

Por último, Nmap (Network Mapper) es una herramienta de código abierto usada para explorar redes y detectar dispositivos activos, puertos abiertos y servicios en ejecución. No solo muestra si un equipo responde, sino también qué sistemas operativos, versiones de software o vulnerabilidades podrían existir.

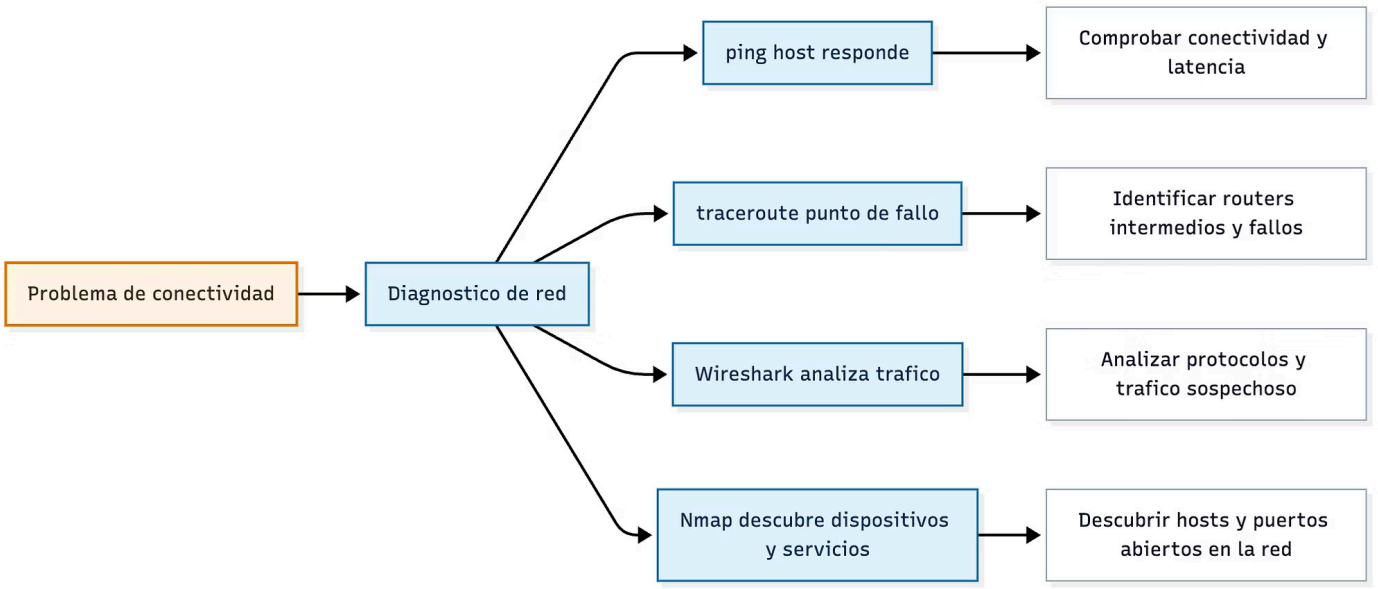
En ciberseguridad, Nmap se usa para auditorías de red; en entornos corporativos, para mantener inventarios actualizados y controlar la exposición de servicios.

La importancia del diagnóstico proactivo

Dominar estas herramientas no solo sirve para reaccionar ante fallos, sino para prevenir incidentes. Las empresas que monitorean activamente su red con estas utilidades reducen drásticamente los tiempos de inactividad y los riesgos de intrusión. En el entorno profesional actual, donde cada segundo de caída puede significar pérdidas económicas, saber usar ping, traceroute, Wireshark y Nmap es una competencia clave para técnicos, administradores y analistas.

Esquema visual: El flujo del diagnóstico de red

El siguiente diagrama muestra la relación y propósito de cada herramienta dentro del proceso de diagnóstico.



Explicación del esquema:

- Todo comienza con un problema de conexión o lentitud (nodo A).
- El proceso de diagnóstico de red (nodo B) se divide en cuatro fases complementarias.
- **Ping** determina si el destino está accesible.
- **Traceroute** identifica el punto exacto donde la conexión se interrumpe.
- **Wireshark** analiza el tráfico para encontrar errores de protocolo o congestión.
- **Nmap** mapea los dispositivos conectados y los servicios que ejecutan.

Estas herramientas, usadas de forma combinada, ofrecen una visión 360° de la salud de una red.

Caso de estudio: Wireshark Foundation y el poder del análisis profundo

Contexto

Desde su creación en 1998 (bajo el nombre Ethereal), Wireshark se ha convertido en el estándar mundial de análisis de tráfico de red. Actualmente, es mantenido por la Wireshark Foundation, una organización sin ánimo de lucro que impulsa la educación y la transparencia en la administración de redes.

Estrategia y funcionalidad

Wireshark permite capturar en tiempo real cada paquete que pasa por una interfaz de red, mostrando información de cada capa del modelo OSI (física, enlace, red, transporte, aplicación). Su poder reside en:

Filtros avanzados

puedes aislar tráfico de un protocolo concreto (por ejemplo, `tcp.port == 80` para HTTP o `dns` para consultas de nombres).

Desglose por capas

muestra encabezados, direcciones IP, puertos, tiempos de respuesta y contenido.

Análisis gráfico

calcula latencias, retransmisiones y conversaciones entre hosts.

Una función esencial es la detección de errores de configuración o retransmisiones TCP, que pueden ralentizar toda una red sin ser visibles desde la capa de aplicación.

Resultado

Wireshark es utilizado por empresas como Cisco, IBM y Microsoft en su formación técnica. También es una herramienta clave en certificaciones como CCNA o CompTIA Network+. Su impacto va más allá del diagnóstico técnico: ha permitido mejorar protocolos, identificar vulnerabilidades en tiempo real y formar a miles de profesionales. En definitiva, Wireshark democratizó el acceso a un análisis de red de nivel profesional.

Herramientas y consejos

Ping y Traceroute: tu punto de partida

- En Windows: `ping -t google.com` realiza un ping continuo hasta que lo detengas con Ctrl + C.
- En Linux/macOS: usa `ping -c 5` para limitar el número de paquetes enviados.
- `tracert` (Windows) o `traceroute` (Linux/macOS) permite ver la ruta de los paquetes. Si un salto muestra "Request timed out", probablemente hay un firewall intermedio.

Wireshark: domina la captura y filtrado

- Descárgalo en wireshark.org.
- Usa filtros de visualización:
  - `ip.addr == 8.8.8.8` para ver solo el tráfico hacia Google DNS.
  - `http` para analizar peticiones web.
- Guarda las capturas (.pcap) para documentar incidencias o compartir con otros técnicos.
- En entornos empresariales, combina Wireshark con TShark, su versión de línea de comandos, para automatizar análisis.

Nmap: el mapa de la red

- Instalación sencilla en Windows, Linux y macOS.
- Ejemplo básico: `nmap 192.168.1.0/24` escanea toda la red local.
- Ejemplo avanzado: `nmap -sS -sV -O 192.168.1.10` detecta servicios, versiones y sistema operativo.
- Usa Zenmap, su interfaz gráfica, si prefieres visualizar los resultados con gráficos y topologías.

Combina herramientas para un diagnóstico completo

1. Empieza con **ping** para verificar conexión.
2. Usa **traceroute** para localizar el fallo.
3. Ejecuta **Nmap** para descubrir dispositivos activos o puertos bloqueados.
4. Cierra con **Wireshark** para analizar el tráfico y confirmar la causa raíz.

Recomendaciones profesionales

- Siempre solicita permiso antes de escanear una red (Nmap puede ser considerado intrusivo).
- Documenta cada prueba con capturas y tiempos de respuesta.
- En entornos corporativos, complementa estas herramientas con soluciones como PRTG Network Monitor o Zabbix para monitorización continua.

Mitos y realidades

❌ Mito: "Si el comando ping falla, el servidor está caído."

→ **FALSO.** Muchos servidores y routers bloquean las respuestas ICMP por seguridad, evitando ataques de tipo ping flood. El hecho de no recibir respuesta no significa necesariamente que el servidor esté inactivo; puede estar operativo pero protegido por un firewall.

❌ Mito: "Usar Nmap es ilegal."

→ **FALSO.** Nmap es completamente legal y se usa en auditorías, mantenimiento de redes y formación en ciberseguridad. Solo es ilegal si se utiliza para escanear redes ajenas sin autorización. En entornos empresariales, forma parte de la rutina de seguridad preventiva.

Resumen final

- **Ping:** comprueba conectividad y mide latencia.
- **Traceroute:** muestra el recorrido de los paquetes hasta el destino.
- **Wireshark:** analiza protocolos y tráfico a nivel de paquete.
- **Nmap:** escanea redes y detecta hosts, puertos y servicios activos.
- **Uso combinado:** diagnóstico completo desde la conectividad básica hasta la inspección avanzada.

Recordatorio clave: un fallo en red puede deberse tanto a errores físicos como de configuración o seguridad. El diagnóstico correcto es la mitad de la solución.

Sesión 15 – Configuración de adaptadores de red en Windows y Linux

Conectividad controlada — cómo y cuándo asignar direcciones IP

Cada equipo conectado a una red —sea un ordenador, un móvil, una impresora o un servidor — necesita una dirección IP para comunicarse. Sin ella, no podría enviar ni recibir datos. Pero lo que diferencia a un usuario doméstico de un profesional es comprender cómo se asignan esas direcciones y cuándo conviene usar un método u otro. En esta sesión, aprenderás las dos formas principales de configurar una red: dinámica (DHCP) y estática (manual), así como su aplicación práctica en Windows y Linux.

Configuración dinámica (DHCP): simplicidad y automatización

El método DHCP (Dynamic Host Configuration Protocol) permite que los dispositivos obtengan automáticamente su dirección IP y otros parámetros de red (como la máscara de subred, la puerta de enlace y los servidores DNS) desde un servidor DHCP —habitualmente, el router.

Cuando un equipo se conecta, envía una solicitud ("DHCP Discover") a la red. El servidor DHCP responde asignando una dirección IP libre por un tiempo determinado (lease time).

Ventajas clave:

- **Configuración automática:** el usuario no necesita introducir datos manualmente.
- **Prevención de conflictos:** el servidor controla que no se dupliquen direcciones IP.
- **Ideal para redes grandes o cambiantes:** como oficinas, aulas o entornos con decenas de equipos conectados simultáneamente.

Ejemplo: un portátil que se conecta hoy al Wi-Fi del trabajo y mañana al de casa recibirá en cada lugar una IP distinta, sin intervención manual.

Configuración estática (manual): control absoluto

En la configuración estática, el técnico asigna manualmente los parámetros de red:

- Dirección IP (por ejemplo, 192.168.1.10)

- Máscara de subred (255.255.255.0)
- Puerta de enlace predeterminada (normalmente el router: 192.168.1.1)
- Servidor DNS (por ejemplo, 8.8.8.8 de Google)

Este tipo de configuración se usa en equipos que deben ser siempre accesibles con la misma dirección, como servidores, impresoras de red, cámaras IP o dispositivos de infraestructura (NAS, controladores de dominio, etc.).

Ventajas:

- **Conectividad predecible:** la IP nunca cambia, lo que facilita la gestión y monitorización.
- **Mayor estabilidad:** ideal para servicios críticos o automatizaciones que requieren rutas fijas.
- **Posibilidad de control remoto permanente:** mediante SSH, RDP o herramientas de administración.

Inconvenientes:

- Riesgo de conflictos si se repiten direcciones IP.
- Mantenimiento manual: cualquier cambio en la red requiere reconfiguración.

Reservas DHCP: el punto intermedio

Una alternativa muy usada es la reserva DHCP, disponible en la mayoría de routers empresariales. Permite asociar una dirección IP fija a una dirección MAC concreta, de modo que, aunque la red use DHCP, ese equipo reciba siempre la misma IP. Este método combina automatización con estabilidad, y es la opción preferida para pequeñas empresas o laboratorios con servidores internos.

Windows y Linux: enfoques diferentes, mismo propósito

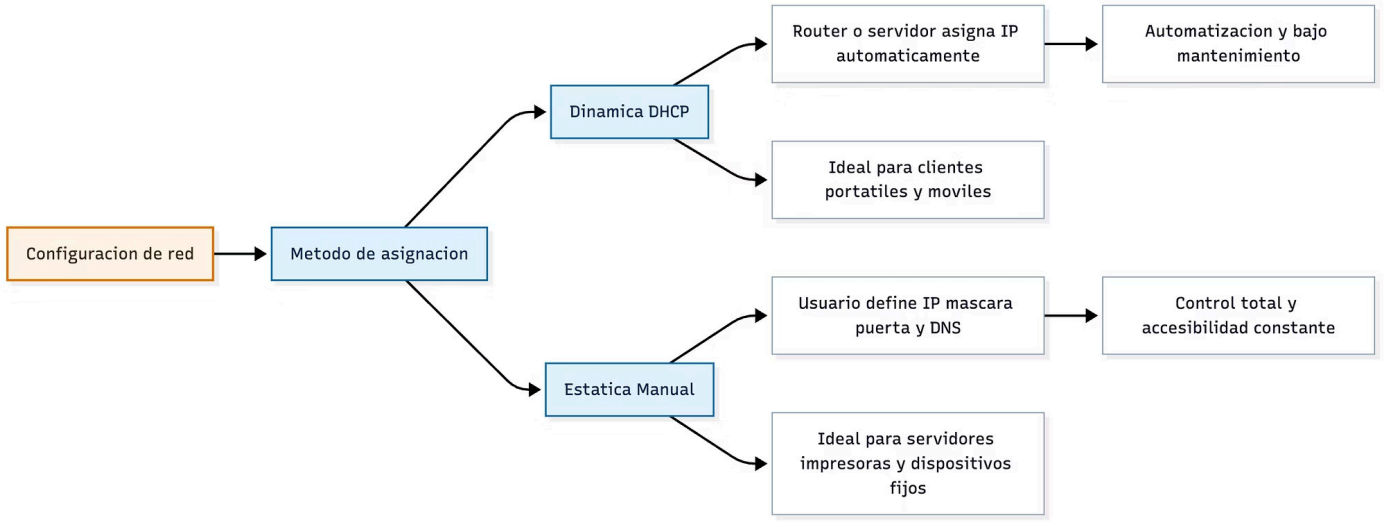
En **Windows**, la configuración puede hacerse desde la interfaz gráfica (Panel de control → Centro de redes → Propiedades del adaptador) o desde la terminal con el comando `netsh`.

En **Linux**, depende de la distribución: las más modernas (Ubuntu, Fedora, Debian) utilizan NetworkManager o el sistema Netplan, que permiten alternar entre DHCP y estática tanto desde GUI como por terminal (`nmcli`, `ip`, `ifconfig`, o edición de `/etc/netplan/`).

En ambos sistemas, el objetivo es el mismo: asegurar que el equipo tenga una dirección válida dentro del rango de la red y que pueda comunicarse correctamente con los demás dispositivos.

Esquema visual: Dinámica vs Estática

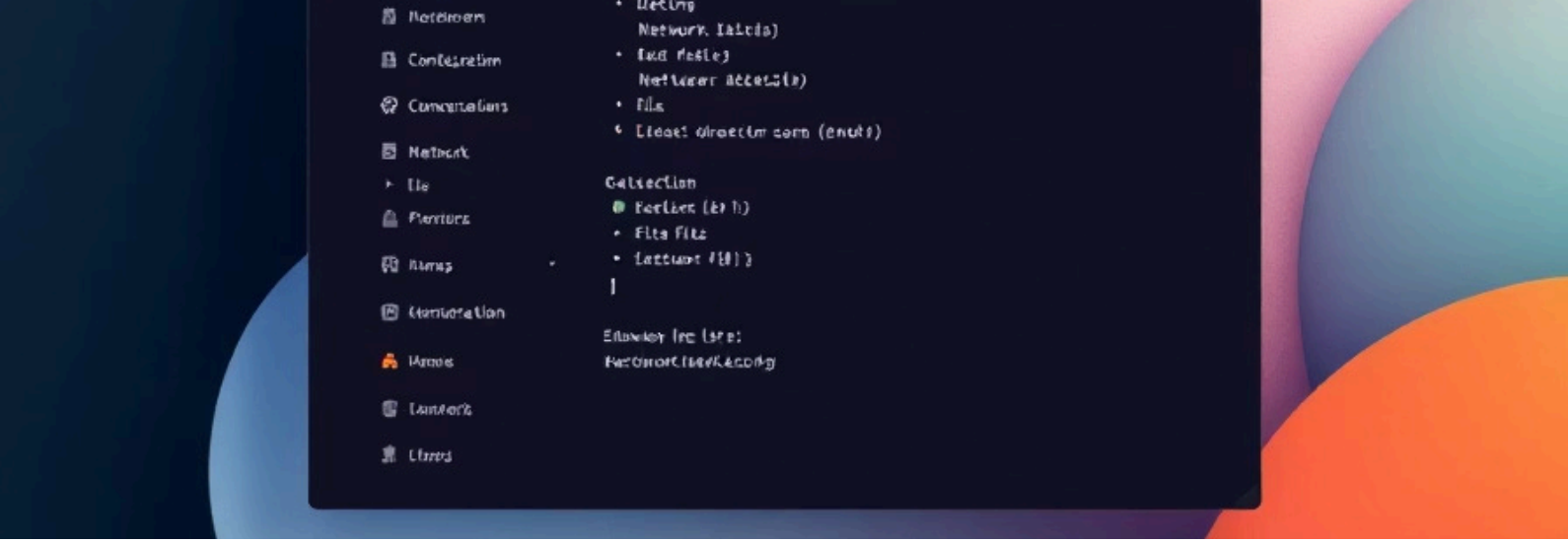
El siguiente diagrama muestra de forma conceptual cómo se configuran los adaptadores de red en ambos modos:



Descripción:

- **Nodo C (DHCP):** representa la asignación automática mediante un servidor.
- **Nodo D (Estática):** simboliza la configuración manual.
- **Nodo E–F–I:** ventajas del método dinámico (simplicidad y flexibilidad).
- **Nodo G–H–J:** ventajas del método estático (control y estabilidad).

El esquema deja claro que ambos métodos coexisten en la misma red: los equipos "móviles" suelen usar DHCP, mientras los "fijos" o críticos usan IP estáticas.



Caso de estudio: NetworkManager — la gestión moderna de redes en Linux

Contexto

Durante años, configurar redes en Linux implicaba editar archivos de texto y reiniciar servicios manualmente. Esto suponía un reto para usuarios menos técnicos. Para simplificar la administración y hacerla más accesible, las distribuciones modernas adoptaron un sistema unificado: NetworkManager.

Estrategia

NetworkManager es un servicio de Linux que detecta, configura y gestiona conexiones de red (Ethernet, Wi-Fi, VPN, módems, etc.) de forma automática. Sus ventajas más destacadas:

Gestión centralizada

unifica todas las interfaces en una sola herramienta.

Compatibilidad GUI/CLI

permite configurar desde entorno gráfico o mediante comandos (nmcli o nmtui).

Cambio flexible entre DHCP y estática

con un solo comando o clic, se puede alternar entre métodos.

Soporte para VPN, VLAN y proxy

integra funciones avanzadas sin necesidad de editar múltiples archivos.

Resultado

Gracias a NetworkManager, Linux se ha vuelto mucho más amigable para entornos corporativos y domésticos. Hoy en día, Ubuntu, Fedora y CentOS lo incluyen por defecto. Además, su versión de línea de comandos, nmcli, ha ganado popularidad entre administradores de sistemas porque permite automatizar configuraciones en servidores sin interfaz gráfica.

Ejemplo práctico:

```
# Ver conexiones activas
nmcli connection show

# Cambiar de DHCP a IP estática
nmcli connection modify "Wired connection 1" ipv4.method manual ipv4.addresses
192.168.1.50/24 ipv4.gateway 192.168.1.1 ipv4.dns 8.8.8.8
nmcli connection up "Wired connection 1"
```

Este proceso sería equivalente, en Windows, a editar las propiedades del adaptador y seleccionar "Usar la siguiente dirección IP".

Herramientas y consejos

En Windows: interfaz gráfica y comandos útiles

- Accede a la configuración desde: Panel de control → Redes e Internet → Centro de redes → Cambiar configuración del adaptador.
- Haz clic derecho sobre el adaptador → Propiedades → "Protocolo de Internet versión 4 (TCP/IPv4)".
- Puedes usar comandos:
  - `ipconfig /all` → muestra la configuración actual.
  - `ipconfig /release` y `ipconfig /renew` → renuevan la dirección DHCP.
  - `netsh interface ip set address "Ethernet" static 192.168.1.10 255.255.255.0 192.168.1.1` → asigna IP fija.

En Linux: flexibilidad total

- **NetworkManager (nmcli)** → línea de comandos moderna.
- **Netplan (Ubuntu 18.04+):** edita `/etc/netplan/01-netcfg.yaml` y aplica cambios con `sudo netplan apply`.
- Comandos clásicos:
  - `ip addr show` → lista interfaces y direcciones IP.
  - `sudo dhclient -r` → libera IP actual.
  - `sudo dhclient` → obtiene una nueva del servidor DHCP.

Reservas DHCP en el router: equilibrio perfecto

- En el panel de administración del router (normalmente 192.168.1.1), busca "DHCP" o "LAN Setup".
- Añade una reserva para que el dispositivo con MAC "00:1B:44:11:3A:B7" siempre reciba la IP 192.168.1.50.
- **Ventaja:** el dispositivo tiene IP fija sin perder la automatización del DHCP.

Buenas prácticas de red

- Evita mezclar direcciones estáticas dentro del rango DHCP del router.
- Documenta tus configuraciones en una hoja o planilla compartida.
- Usa servidores DNS confiables (Cloudflare 1.1.1.1, Google 8.8.8.8 o AdGuard 94.140.14.14).
- En entornos empresariales, aplica políticas de direccionamiento:
  - IPs bajas (1–100) → dispositivos fijos.
  - IPs altas (101–254) → asignaciones dinámicas.

Mitos y realidades

❌ Mito: "Una IP estática es más rápida."

→ **FALSO.** La velocidad de la conexión depende del ancho de banda, la calidad del cableado y la latencia del proveedor, no del tipo de configuración IP. Lo único que cambia es el método de asignación, no el rendimiento.

❌ Mito: "En Linux solo se configura la red por terminal."

→ **FALSO.** Aunque Linux es famoso por su potencia en línea de comandos, herramientas modernas como NetworkManager o Netplan ofrecen interfaces gráficas (y de texto) muy intuitivas. Hoy puedes configurar una red en Ubuntu con apenas dos clics o comandos.

Resumen final

- **Configuración dinámica (DHCP):** el router asigna automáticamente IP, máscara, puerta y DNS.
- **Configuración estática (manual):** el técnico introduce valores fijos.
- **Uso ideal:** DHCP → clientes móviles; Estática → servidores o impresoras.
- **Herramientas:**
  - Windows → Panel de control, ipconfig, netsh.
  - Linux → nmcli, Netplan, /etc/netplan/.
- **Reservas DHCP:** combinación óptima entre automatización y control.
- **Gestor clave en Linux:** NetworkManager.