

Curso Completo de Redes (Networking)

Autor: Esteban

lucasegaacademy.com

*Guía completa con explicaciones extensas por unidad,
prácticas y examen final.*

Curso Completo de Redes (Networking)

Autor: Esteban

lucasegaacademy.com

Publicado por Colibrí Editorial EGA

© 2026 Esteban. Todos los derechos reservados.

Queda prohibida la reproducción total o parcial de esta obra
sin autorización escrita del autor.

ÍNDICE

PRÓLOGO	4
UNIDAD 1: Fundamentos de las redes	7
UNIDAD 2: El modelo OSI y TCP/IP	33
UNIDAD 3: Medios físicos, cableado y topologías	60
UNIDAD 4: Direccionamiento IPv4	84
UNIDAD 5: Subneteo, CIDR y VLSM	109
UNIDAD 6: Switches, routers y ruteo	136
UNIDAD 7: DHCP, DNS y NAT	163
UNIDAD 8: IPv6 y redes inalámbricas	189
UNIDAD 9: Seguridad de redes	213
UNIDAD 10: Diagnóstico y resolución de problemas	237
EXAMEN FINAL	261

PRÓLOGO

Bienvenido a "Curso Completo de Redes (Networking)", el libro de Lucas EGA Academy para aprender desde cero cómo funcionan las redes que conectan al mundo. Este libro nació del curso en video de 30 clases de la academia, pero aquí tienes todo explicado con mucho más detalle: conceptos a fondo, analogías de la vida real, errores comunes de principiantes, buenas prácticas de la industria, ejemplos paso a paso con comandos reales para probar en tu computadora, prácticas con soluciones explicadas y un examen final para medir lo que aprendiste.

Cada vez que mandas un mensaje por WhatsApp, que ves un video en YouTube o que pagas con tu tarjeta en una terminal, hay una red haciendo magia detrás. Los datos viajan por cables bajo el mar, por fibra óptica en tu colonia y por ondas de radio hasta tu celular. Entender cómo ocurre eso es entender el sistema nervioso de la civilización moderna. Y lo mejor: es una habilidad que se paga muy bien.

Las redes son la base de casi todo en tecnología. Sin redes no hay internet, no hay nube, no hay aplicaciones móviles, no hay trabajo remoto. Quien entiende redes entiende cómo se comunican las computadoras, y eso abre puertas en soporte técnico, administración de sistemas, ciberseguridad, desarrollo de software y telecomunicaciones. Es una de las áreas con más demanda laboral y con rutas claras de certificación.

A quién va dirigido este libro

Este libro es para ti si empiezas desde cero en tecnología y quieres una base sólida que te sirva para todo lo demás. Es para ti si ya programas, como en Python o JavaScript, y quieres entender qué pasa cuando tu código se conecta a un servidor. Es para ti si trabajas dando soporte técnico y quieres dejar de adivinar y empezar a diagnosticar con método. Es para ti si sueñas con certificaciones como las de Cisco o CompTIA y necesitas los fundamentos bien puestos.

No necesitas saber programar ni tener equipo caro. Con tu computadora, tu conexión a internet de casa y las herramientas gratuitas que ya trae tu sistema operativo puedes hacer casi todos los ejercicios. Si tienes acceso a un router casero, mejor: podrás entrar a su configuración y ver con tus propios ojos conceptos como DHCP, DNS y NAT.

Si vienes de otros cursos de Lucas EGA Academy, este libro encaja perfecto: ya sabes crear páginas y programas, y ahora aprenderás cómo viajan esos programas y datos por la red hasta llegar a los usuarios.

Por qué las redes son la habilidad invisible mejor pagada

Hablemos de frente: casi nadie ve las redes, pero todos dependen de ellas. Cuando el internet de una empresa se cae, se detiene todo: ventas, atención a clientes, producción. Por eso las empresas pagan bien a quién sabe mantenerlas funcionando y protegerlas. Administradores de red, ingenieros de soporte, analistas de ciberseguridad: todos comparten la misma base que vas a construir aquí.

Además, las redes son el prerrequisito silencioso de la ciberseguridad, el campo de moda. No puedes proteger lo que no entiendes: antes de hablar de hackers y defensas hay que saber qué es una dirección IP, cómo viaja un paquete y dónde se puede interceptar. Este libro te da exactamente esa base, con un enfoque defensivo y ético desde el primer capítulo.

Otra ventaja: es un conocimiento muy estable. Los fundamentos de TCP/IP tienen décadas y siguen vigentes. Lo que aprendas aquí te servirá por muchos años, a diferencia de herramientas que cambian cada dos años.

Qué vas a aprender: recorrido por las 10 unidades

El libro está organizado en 10 unidades, cada una agrupa 3 de las 30 clases originales del curso en video. Cada unidad sigue la misma estructura:

- Introducción: que verás y por qué importa.
- Explicación detallada: conceptos a fondo, analogías, errores comunes y buenas prácticas.
- Ejemplos paso a paso: comandos y configuraciones reales para probar en tu computadora, explicados línea por línea.
- Práctica: ejercicios con soluciones explicadas paso a paso. Las redes se aprenden practicando, no solo leyendo.
- Resumen de la unidad: los puntos clave para repasar.

Las unidades 1 a 3 construyen tu vocabulario: qué es una red, los modelos OSI y TCP/IP, cables y topologías. Las unidades 4 y 5 son el corazón matemático: direccionamiento IPv4, subneteo, CIDR y VLSM. Las unidades 6 y 7 te muestran los dispositivos y servicios que hacen funcionar todo: switches, routers, DHCP, DNS y NAT. La unidad 8 mira al futuro y al aire: IPv6 y Wi-Fi. La unidad 9 te enseña a proteger todo lo anterior. Y la unidad 10 te convierte en detective: diagnóstico y resolución de problemas con herramientas profesionales.

Al final encontrarás el examen final de 50 preguntas con todas las respuestas explicadas. Úsalo con honestidad: primero responde sin ver las soluciones y luego revisa cada explicación, incluso las que acertaste.

Cómo estudiar este libro para sacarle el máximo provecho

Primero, no te saltes la práctica. Leer sobre ping no es lo mismo que hacer ping. Abre tu terminal y ejecuta cada comando que veas en los ejemplos. Rompe cosas en tu red casera (con cuidado) y arreglalas: así se aprende de verdad.

Segundo, dibuja. Las redes son visuales: haz diagramas de tus topologías, escribe las direcciones IP de tus ejercicios, traza la ruta de un paquete con flechas. Un cuaderno lleno de diagramas vale más que cien páginas subrayadas.

Tercero, repite el subneteo hasta que te salga dormido. Es la parte que más traba a los principiantes y también la que más aparece en exámenes y entrevistas. Hay ejercicios de sobra en la unidad 5: hazlos todos.

Cuarto, arma un laboratorio mental: cada vez que aprendas un concepto nuevo, pregúntate dónde lo has visto en tu vida. El DHCP es lo que te da internet al conectarte al Wi-Fi del café. El DNS es lo que traduce google.com. El NAT es por lo que toda tu casa sale con una sola IP pública. Conectar la teoría con tu día a día la hace inolvidable.

Quinto, estudia en sesiones cortas y constantes. Una unidad por semana, con sus ejercicios, te lleva de cero a un nivel sólido en menos de tres meses. La constancia le gana a las maratones.

Empecemos. La red te estaba esperando.

UNIDAD 1: Fundamentos de las redes

Bienvenido al curso completo de redes de Lucas EGA Academy. Esta primera unidad es la base de todo: si entiendes bien qué es una red, para qué sirve y cómo se conecta a Internet tu casa en México, el resto del libro te va a parecer mucho más fácil. Muchos cursos brincan esta parte porque parece "demasiado sencilla", pero en la práctica, la mayoría de los problemas de redes que vas a resolver en tu trabajo se diagnostican con los conceptos de esta unidad. Así que tomala en serio.

En esta unidad vas a ver tres cosas grandes. Primero, qué es una red: la definición exacta, para qué sirven las redes y cuales son sus componentes básicos (nodos, medios y protocolos). Segundo, los tipos de redes que existen: LAN, WAN, MAN, PAN, WLAN y CAN, con ejemplos reales de tu vida diaria; además vas a aprender la diferencia entre las redes cliente-servidor y las redes punto a punto, que es una decisión de diseño que todo administrador de red toma tarde o temprano. Tercero, una breve historia de las redes: cómo nació ARPANET, cómo se convirtió en Internet, qué es la web (y por qué no es lo mismo que Internet) y cómo llega Internet hasta tu casa en México paso a paso, desde el proveedor de Internet (ISP) hasta tu teléfono.

Por qué importa esto en la vida real? Piensa en un día normal. Te despiertas y revisas tu teléfono: ahí hay una red. Enciendes la computadora de tu oficina y abres el correo: otra red. Pasas por un cyber o una papelería con Internet y conectas tu laptop: una red más. Entrás a una empresa y tu computadora usa la impresora que está al otro lado del edificio sin que tengas que mover ningún cable: una red local bien configurada. Todo eso que parece magia es infraestructura, y alguien tiene que instalarla, configurarla y mantenerla. Ese alguien puedes ser tu.

En el trabajo, saber redes es una habilidad que paga. Un técnico de soporte que entiende redes resuelve en minutos problemas que otros tardan horas en adivinar. Un programador que entiende redes escribe aplicaciones más rápidas y sabe depurar cuando "la app no conecta". Un administrador de sistemas que domina redes es indispensable en cualquier empresa, desde un despacho contable pequeño hasta una empresa de telecomunicaciones. Y si quieres trabajar como técnico independiente, ofreciendo servicios a negocios pequeños (instalar la red de un consultorio, configurar el WiFi de un restaurante, conectar las computadoras de una oficina), esta unidad es tu primer día de escuela.

En México tienes ejemplos por todas partes. Cuando contratas Internet con Telmex o Totalplay, te instalan un módem u ONT en tu casa: ese aparato es la puerta entre tu red local y la red gigante del proveedor. En un cyber, docenas de computadoras comparten la misma

conexión y el dueño necesita que nadie pueda ver los archivos de otra máquina: eso se resuelve con tipos de red y permisos. En una oficina, el servidor guarda los archivos de todos y las computadoras son clientes: ese es el modelo cliente-servidor que vas a estudiar aquí. Todo esto que ves todos los días tiene nombre técnico, y al terminar esta unidad vas a poder nombrar cada pieza.

Un consejo para estudiar esta unidad: no te limites a leer. Cada vez que mencione un concepto, busca su equivalente en tu entorno. Abre la configuración de WiFi de tu teléfono y mira el nombre de tu red: es una WLAN. Mira cuantos dispositivos están conectados a tu módem: son nodos de tu LAN. Pregunta a tu proveedor si tu servicio es por fibra o por cable coaxial: eso es el medio de transmisión. Aprender redes con los ojos abiertos, viendo las redes que ya te rodean, hace que todo se quede grabado.

Explicación detallada

Qué es una red

Una red es un conjunto de dispositivos conectados entre si para compartir recursos e intercambiar información. Esa es la definición formal, pero vamos a desarmarla palabra por palabra porque cada una importa.

"Conjunto de dispositivos": no se necesita mucho. Dos computadoras conectadas ya forman una red. Tu teléfono y tu computadora compartiendo archivos por Bluetooth también son una red. Una empresa con 500 computadoras es una red más grande, pero la idea es la misma: dispositivos conectados.

"Conectados entre si": la conexión puede ser por cable (cobre o fibra óptica) o inalámbrica (WiFi, Bluetooth, datos móviles). El medio cambia, el concepto no. Lo importante es que exista un camino por dónde puedan viajar los datos.

"Compartir recursos": este es el motivo número uno por el que existen las redes. Antes de las redes, si querias pasar un archivo de una computadora a otra, tenias que copiarlo en un disquete o una memoria USB y llevarlo físicamente. Con una red, el archivo viaja en segundos. Los recursos que se comparten incluyen archivos, impresoras, conexión a Internet, aplicaciones instaladas en un servidor y hasta potencia de procesamiento.

"Intercambiar información": más allá de compartir archivos, las redes permiten comunicación: correos, mensajes, videollamadas, juegos en línea. Todo eso son datos viajando por una red.

Una analogía útil: piensa en una red como el sistema de carreteras de una ciudad. Las carreteras son los medios (cables, ondas de radio). Los carros son los datos. Las casas y negocios son los nodos (computadoras, teléfonos, impresoras). Y las reglas de tránsito (quién tiene el paso, por qué carril se circula, qué significan los semáforos) son los protocolos. Sin carreteras no hay transporte; sin reglas, hay caos. Las redes funcionan igual: necesitan infraestructura física y reglas acordadas.

Para qué sirven las redes

Las redes existen por razones muy prácticas. Estas son las principales, con ejemplos que seguro has vivido:

Compartir archivos y datos. En una oficina, el contador guarda las facturas en una carpeta compartida y el gerente las revisa desde su computadora sin pedirle nada a nadie. En tu casa, ves en tu teléfono las fotos que tomaste con tu cámara porque están sincronizadas por la red. Sin red, cada dispositivo sería una isla.

Compartir hardware. Una impresora conectada a la red puede ser usada por 50 personas. Sin red, necesitarías 50 impresoras o tendrías que pasar el archivo en USB a la computadora que sí tiene impresora. Lo mismo pasa con escáneres y discos duros de respaldo.

Compartir la conexión a Internet. Contratas un solo servicio de Internet y lo reparten entre todos los dispositivos de la casa u oficina. El módem o router hace ese reparto. En un cyber, una sola línea de Internet alimenta 30 computadoras.

Comunicación. Correo electrónico, mensajería instantánea, videollamadas, redes sociales: todo es comunicación sobre redes. La llamada que haces por WhatsApp viaja como datos por Internet, no por la red telefónica tradicional.

Centralizar la administración. En una empresa, el administrador puede instalar un programa una sola vez en el servidor y todos los empleados lo usan. Puede hacer respaldos de toda la información en un solo lugar. Puede controlar quién entra a qué carpetas. Sin red, tendría que ir computadora por computadora.

Ahorro de dinero. Todo lo anterior se resume en esto: menos equipos duplicados, menos tiempo perdido, menos errores. Por eso hasta el negocio más pequeño se beneficia de tener una red bien puesta.

Componentes básicos: nodos, medios y protocolos

Toda red, desde la más pequeña hasta Internet completo, se puede describir con tres componentes: los nodos (quiénes se conectan), los medios (por dónde viajan los datos) y los protocolos (las reglas del juego).

Nodos

Un nodo es cualquier dispositivo conectado a la red que puede enviar, recibir o reenviar datos. Los nodos se dividen en dos grandes grupos: dispositivos finales y dispositivos intermedios.

Dispositivos finales: son los que están en los extremos de la red, los que usan las personas (o los que generan o consumen la información). Ejemplos: computadoras de escritorio y laptops, teléfonos celulares, tabletas, impresoras de red, televisores inteligentes, cámaras de seguridad IP, consolas de videojuegos. Si un aparato se conecta a la red para usarla, es un dispositivo final.

Dispositivos intermedios: son los que están en medio, conectando a los dispositivos finales entre si y dirigiendo el tráfico. El usuario normal casi no los ve, pero sin ellos no hay red. Ejemplos: switches (conectan varios dispositivos dentro de una red local), routers (conectan redes distintas entre si, por ejemplo tu casa con Internet), puntos de acceso inalámbricos (dan WiFi), módems u ONT (conectan tu casa con el proveedor). En unidades posteriores vas a estudiar cada uno a fondo; por ahora quedate con la idea: los finales usan la red, los intermedios la hacen funcionar.

Error común de principiante: llamar "módem" a todo. En México mucha gente le dice "módem" al aparato que da WiFi, pero casi siempre ese aparato es un router con WiFi integrado, y a veces también incluye el módem. No es solo un tema de vocabulario: si llamas a tu proveedor diciendo "mi módem no da WiFi", el técnico puede malinterpretar el problema. Aprende a distinguir: el módem (u ONT de fibra) traduce la señal del proveedor; el router reparte la conexión entre tus dispositivos y normalmente es el que genera la red WiFi.

Medios

El medio es el camino físico (o inalámbrico) por dónde viajan los datos. Hay dos familias: medios guiados (cables) y medios no guiados (inalámbricos).

Medios guiados:

1. Cable de par trenzado (UTP). Es el cable de red clásico, el que tiene un conector parecido al del teléfono pero más grande (conector RJ45). Dentro lleva 8 hilos de cobre trenzados en 4 pares. El trenzado no es decoración: reduce la interferencia electromagnética. Es el cable más usado en oficinas y casas para conectar computadoras al router o switch.

Barato, fácil de instalar, y con las categorías modernas (Cat5e, Cat6) alcanza velocidades de 1 Gbps o más en distancias cortas. Su límite típico es 100 metros por tramo.

2. Cable coaxial. Es el cable grueso que antes se usaba para la televisión por cable, con un conector metálico roscado. En México, muchos servicios de Internet por cable (como algunos paquetes de Totalplay o de cableras regionales) llegan a tu casa por coaxial hasta el módem. Todavía se usa mucho en la infraestructura de los proveedores.
3. Fibra óptica. En lugar de electricidad, transmite pulsos de luz por un hilo de vidrio o plástico del grosor de un cabello. Es el medio más rápido y el que menos interferencia sufre, y puede llevar datos a kilómetros de distancia sin perder calidad. Por eso los proveedores la usan para sus redes troncales y cada vez más para llevar el servicio hasta tu casa (cuando te ofrecen "Internet por fibra", la fibra llega hasta un aparato llamado ONT en tu domicilio). Su desventaja: es más cara y más delicada de instalar (no se puede doblar bruscamente).

Medios no guiados (inalámbricos):

1. WiFi. Usa ondas de radio para conectar dispositivos sin cables en distancias cortas (una casa, una oficina, un café). Es el medio más cómodo, pero también el más variable: paredes, distancia e interferencia de otras redes afectan la velocidad. En esta unidad lo verás como WLAN; sus detalles técnicos vienen en otra unidad.
2. Bluetooth. Ondas de radio de muy corto alcance (unos 10 metros) para conectar accesorios: audífonos, bocinas, teclados, o para pasar archivos entre teléfono y computadora.
3. Datos móviles (3G, 4G, 5G). Tu teléfono se conecta a las antenas de tu compañía telefónica por ondas de radio. Es una red inalámbrica de área amplia: funciona en toda la ciudad.
4. Enlaces de microondas y satelitales. Se usan para llevar Internet a lugares donde no llega el cable ni la fibra: comunidades rurales, por ejemplo. Un plato apunta a una antena lejana o a un satélite. Tienen más latencia (retardo), sobre todo los satelitales, porque la señal viaja muchísima distancia.

Buena práctica de la industria: el medio se elige según distancia, velocidad necesaria, presupuesto y entorno. Para una oficina pequeña, UTP a cada escritorio y WiFi para los móviles es la combinación ganadora. Para conectar dos edificios, fibra óptica. Para un rancho sin infraestructura, enlace inalámbrico o satelital. No existe "el mejor medio" en abstracto; existe el adecuado para cada caso.

Error común de principiante: pensar que WiFi e Internet son lo mismo. No lo son. WiFi es solo el medio inalámbrico entre tu dispositivo y tu router. Internet es la red global más allá de tu router. Por eso puedes tener "WiFi conectado pero sin Internet": tu teléfono habla bien con el router, pero el router no logra salir a Internet (se cayó el servicio del proveedor, por ejemplo). Este diagnóstico básico (separar el problema local del problema del proveedor) te va a ahorrar horas en soporte técnico.

Protocolos

Un protocolo es un conjunto de reglas que define cómo se comunican los dispositivos en una red: que formato tienen los mensajes, en qué orden se envían, que hacer si algo falla. Sin protocolos, cada fabricante hablaría su propio idioma y nada sería compatible.

La analogía clásica: dos personas que quieren hablar por teléfono necesitan acordar el idioma, quien habla primero, como saludar y como despedirse. Si uno habla español y el otro solo chino, no hay comunicación aunque la línea funcione perfecto. Los protocolos son ese acuerdo previo, pero escrito con precisión matemática para que lo ejecuten máquinas.

Protocolos que vas a estudiar en este libro (mencionados aquí, explicados a fondo después):

- TCP/IP: la familia de protocolos base de Internet. Incluye IP (direccionamiento y ruteo), TCP (entrega confiable de datos) y UDP (entrega rápida sin garantías).
- HTTP/HTTPS: el protocolo de la web (las páginas que ves en el navegador).
- DNS: traduce nombres como `www.ejemplo.com` a direcciones IP.
- DHCP: asigna automáticamente direcciones IP a los dispositivos de una red local.
- Ethernet: el protocolo de las redes locales cableadas.
- WiFi (estándares 802.11): el protocolo de las redes locales inalámbricas.

Por qué importan los protocolos para ti como técnico? Por qué la mayoría de las fallas de red son fallas de protocolo o de configuración de protocolo: un equipo con IP mal configurada, un DNS que no responde, un DHCP que no asigna direcciones. Entender que hace cada protocolo te permite diagnosticar por capas en lugar de adivinar.

Tipos de redes por alcance

Las redes se clasifican por su tamaño o alcance geográfico. Esta clasificación no es caprichosa: el alcance determina que tecnologías se usan, quien la administra y cuanto cuesta. Memoriza estas siglas porque las vas a ver en ofertas de trabajo, cotizaciones y exámenes de certificación.

PAN (Personal Área Network, red de área personal)

La red más pequeña: alcance de unos pocos metros, centrada en una persona. Ejemplo: tu teléfono conectado por Bluetooth a tus audífonos y a tu smartwatch. O tu laptop pasando archivos a tu teléfono. Son redes personales, normalmente inalámbricas y de baja velocidad, para conectar tus propios dispositivos entre sí.

LAN (Local Área Network, red de área local)

Una red que cubre un área pequeña: una casa, una oficina, un piso de un edificio, una escuela, un cyber. Es el tipo de red que más vas a instalar y administrar. Características: alta velocidad, baja latencia (los datos llegan rapidísimo porque todo está cerca), y normalmente la administra el dueño (tú en tu casa, el departamento de sistemas en una empresa).

Ejemplo mexicano típico: el cyber de la esquina. Tiene 20 computadoras conectadas a un switch, el switch conectado al router, y el router al módem del proveedor. Todas las máquinas comparten la impresora y la conexión a Internet. Eso es una LAN de libro.

CAN (Campus Área Network, red de área de campus)

Un conjunto de LANs interconectadas dentro de un área limitada pero más grande que un solo edificio: un campus universitario, un parque industrial, un hospital con varios edificios, una plaza comercial. Cada edificio tiene su LAN y todas se conectan entre sí, normalmente con fibra óptica. La administra una sola organización.

MAN (Metropolitan Área Network, red de área metropolitana)

Cubre una ciudad o zona metropolitana. Ejemplo: la red de fibra óptica de un proveedor de Internet dentro de la Ciudad de México, o la red que interconecta las sucursales de un banco dentro de Guadalajara. También entran aquí algunas redes de gobierno municipal (cámaras de seguridad de la ciudad, por ejemplo). Las MAN suelen usar fibra óptica y las opera un proveedor o una institución grande.

WAN (Wide Área Network, red de área amplia)

Cubre áreas grandes: un país, un continente, el mundo entero. Internet es la WAN más grande que existe: una red de redes que conecta millones de LANs en todo el planeta. Las WAN usan infraestructura de proveedores (fibra submarina, enlaces satelitales, redes troncales) y tienen mayor latencia que las LAN porque los datos recorren miles de kilómetros.

Ejemplo: una empresa con oficinas en Ciudad de México, Monterrey y Bogotá conecta sus tres LANs a través de una WAN (contratada a un proveedor o construida sobre Internet con VPN) para que trabajen como si fuerán una sola red.

WLAN (Wireless Local Área Network, red de área local inalámbrica)

Es una LAN pero inalámbrica: la red WiFi de tu casa, de un café, de un aeropuerto. Técnicamente es un tipo de LAN (mismo alcance, misma función), pero se clasifica aparte porque usa tecnología de radio en vez de cables y tiene sus propios retos (seguridad, interferencia, cobertura). Cuando configuras el WiFi de un restaurante para los clientes, estás montando una WLAN.

Tabla mental para no confundirte: PAN = tu cuerpo y tus aparatos (metros). LAN = un local (decenas de metros). CAN = varios edificios juntos (kilómetros). MAN = una ciudad (decenas de kilómetros). WAN = países y el mundo (miles de kilómetros). WLAN = LAN sin cables.

Error común de principiante: decir "la red WAN de mí casa". Tu casa tiene una LAN (y una WLAN si hay WiFi); la WAN es la del proveedor, a la que tu router se conecta. Ubicar dónde termina tu red y dónde empieza la del proveedor es el primer paso de cualquier diagnóstico: si falla tu LAN, el problema es tuyo; si falla más allá de tu router, es del proveedor.

Redes cliente-servidor vs punto a punto

Además del alcance, las redes se clasifican por cómo se organizan los equipos para compartir recursos. Esta decisión afecta la seguridad, el costo y la facilidad de administración.

Red punto a punto (peer-to-peer, P2P)

En una red punto a punto, todos los equipos son iguales: cada uno puede compartir sus recursos y usar los de los demás. No hay un equipo "jefe". Es como un grupo de amigos donde todos aportan algo a la mesa y todos pueden servirse.

Ejemplo: en un despacho pequeño de 5 personas, cada computadora comparte una carpeta con sus archivos y las demás la pueden abrir. La impresora está conectada a la computadora de la recepcionista y las demás imprimen a través de ella.

Ventajas: barata (no necesitas un servidor dedicado), fácil de instalar, no requiere un administrador especializado. Ideal para redes de hasta unas 10 computadoras.

Desventajas: cada equipo se administra por separado (si cambias una contraseña, la cambias en cada máquina), la seguridad es débil (depende de cada usuario), y si la computadora que comparte la impresora se apaga, nadie imprime. No escala: con 30 equipos se vuelve un caos.

Red cliente-servidor

Aquí hay equipos con roles definidos. El servidor (o servidores) es una computadora potente, siempre encendida, que ofrece servicios: guarda archivos, maneja el correo, corre la base de

datos, controla quién puede entrar. Los clientes son las computadoras de los usuarios, que piden servicios al servidor. Es como un restaurante: los clientes piden y el cocinero (servidor) prepara.

Ejemplo: en una empresa de 100 empleados hay un servidor de archivos donde están todos los documentos, un servidor de correo y un servidor que controla usuarios y contraseñas. Cuando un empleado enciende su computadora, inicia sesión contra el servidor, que verifica quién es y qué permisos tiene.

Ventajas: administración centralizada (un solo lugar para usuarios, permisos, respaldos), mejor seguridad, mejor rendimiento con muchos equipos, escala a cientos o miles de nodos.

Desventajas: más cara (servidores, licencias, personal capacitado), y si el servidor falla, todos se quedan sin servicio (por eso se usan respaldos y servidores redundantes).

En la práctica moderna, casi todo lo que usas en Internet es cliente-servidor: tu teléfono (cliente) le pide videos a los servidores de YouTube, tu navegador (cliente) le pide páginas a servidores web. Las redes punto a punto sobreviven en oficinas muy pequeñas y en algunas aplicaciones específicas (como ciertos sistemas de intercambio de archivos).

Buena práctica de la industria: para un negocio, la regla general es punto a punto hasta ~10 equipos con necesidades simples; cliente-servidor a partir de ahí, o antes si manejan información delicada (un consultorio médico, un despacho contable) porque la seguridad centralizada lo justifica.

Breve historia: de ARPANET a tu casa

Entender de dónde vienen las redes te ayuda a entender por qué son como son. Muchas decisiones técnicas que parecen raras tienen su origen en esta historia.

Los orígenes: ARPANET (1969)

A finales de los años 60, en plena Guerra Fría, el Departamento de Defensa de Estados Unidos financiaba investigación en varias universidades, cada una con computadoras caras y distintas. Surgió una pregunta práctica: ¿y si las computadoras pudieran comunicarse entre sí para compartir recursos? Así nació ARPANET, la abuela de Internet.

El 29 de octubre de 1969 se envió el primer mensaje entre dos computadoras: una en la UCLA y otra en Stanford. Querían escribir "LOGIN" pero el sistema se cayó al llegar a "LO". Ese "LO" es oficialmente el primer mensaje de la historia de las redes. Para 1971 ya había 15 nodos, y en 1972 se hizo la primera demostración pública, incluyendo el correo electrónico, que rápidamente se convirtió en la aplicación más popular.

Dos ideas de ARPANET siguen vivas hoy. Primera: la conmutación de paquetes. En lugar de abrir un circuito dedicado para cada comunicación (como las llamadas telefónicas de antes), los datos se cortan en pedazos pequeños (paquetes), cada uno viaja por su cuenta y se rearma al llegar. Si una ruta falla, los paquetes toman otra. Esta idea es la que hace a Internet resistente: no hay un solo punto cuya caída tumbe todo. Segunda: una red descentralizada, sin un control central único. Nadie "es dueño" de Internet, igual que nadie era dueño de ARPANET más allá de su financiamiento.

El nacimiento de Internet: TCP/IP (1983)

Al principio, ARPANET usaba un protocolo llamado NCP, que solo servía para esa red. El problema: empezaron a aparecer otras redes (de universidades, de otros países) y no podían hablar entre sí. La solución la crearon Vint Cerf y Bob Kahn en los años 70: un conjunto de protocolos diseñado para interconectar redes distintas, llamado TCP/IP.

El 1 de enero de 1983, ARPANET adoptó oficialmente TCP/IP. Esa fecha se considera el nacimiento de Internet como tal: ya no era una sola red, era una red de redes. Cualquier red que hablara TCP/IP podía unirse. Este es el momento en que Internet se volvió escalable por diseño: no importaba qué tecnología usara cada red por dentro (satélite, cable, radio), mientras hablara TCP/IP hacia afuera.

Dato para dimensionar: en 1983 había unos cientos de computadoras conectadas. Hoy hay miles de millones de dispositivos. El protocolo diseñado hace más de 40 años sigue siendo la base, lo cual habla de lo bien pensado que estaba.

La web: Internet se vuelve popular (1990s)

Ojo con esto, porque es una confusión muy común: Internet y la web no son lo mismo. Internet es la infraestructura (las redes, los protocolos TCP/IP). La web (World Wide Web) es un servicio que corre sobre Internet, inventado por Tim Berners-Lee en 1989-1990 en el CERN: páginas enlazadas que se ven en un navegador usando el protocolo HTTP.

La analogía: Internet es la red de carreteras; la web es el servicio de paquetería que usa esas carreteras. Sobre Internet también corren el correo electrónico, la mensajería, los videojuegos en línea, el streaming: cada uno es un servicio distinto usando la misma infraestructura.

En los 90, la web hizo que Internet dejará de ser cosa de universidades y militares. Aparecieron los navegadores gráficos, las empresas empezaron a tener páginas, y la gente común empezó a contratar "Internet" (casi siempre queriendo decir: acceso a la web y al correo). En México, los primeros proveedores comerciales aparecieron en esa década, y conectarse significaba oír el chillido del módem telefónico marcando a un número: el famoso dial-up, lento y que bloqueaba la línea telefónica mientras navegabas.

Cómo llega Internet a tu casa en México

Vamos a seguir el camino completo de los datos desde Internet hasta tu teléfono, porque este recorrido resume media unidad en un ejemplo real.

1. La red troncal (backbone). Internet tiene "autopistas" de fibra óptica que cruzan países y océanos (cables submarinos). Los grandes proveedores se conectan a ellas en puntos de intercambio.
2. El ISP (Internet Service Provider, proveedor de servicios de Internet). En México los más conocidos son Telmex (Infinitum), Totalplay, Izzi, Megacable y otros regionales. El ISP compra o renta capacidad en la red troncal y la revende a hogares y empresas. Tiene su propia MAN/WAN de fibra y equipos en centrales distribuidas por la ciudad.
3. La última milla. Es el tramo final desde la infraestructura del ISP hasta tu domicilio, y es la parte más cara de llevar a cada casa. Tecnologías comunes en México: fibra óptica hasta el hogar (FTTH: la fibra llega a tu casa y termina en un ONT), cable coaxial (HFC: fibra hasta el nodo de la colonia y coaxial hasta tu casa, típico de cableras), par de cobre telefónico (ADSL: usa la línea telefónica de Telmex; cada vez menos común), y en zonas rurales, enlaces inalámbricos o satelitales.
4. El equipo en tu casa. Según la tecnología, el ISP te instala un módem (ADSL/cable) o un ONT (fibra). Muchas veces ese aparato ya trae router y WiFi integrados; si no, conectas tu propio router. Este equipo es la frontera: de un lado está la red del proveedor (WAN), del otro tu red local (LAN/WLAN).
5. Tu red local. El router crea tu LAN: asigna direcciones IP privadas a tus dispositivos (por DHCP), les da WiFi, y traduce todo el tráfico hacia Internet. Tus dispositivos (teléfono, laptop, tele, consola) son los nodos finales.

Cuándo abres una página en tu teléfono, la petición sale por WiFi a tu router, el router la manda al equipo del ISP, de ahí viaja por la red del proveedor hasta la troncal, cruza hasta el servidor de la página (que puede estar en otro país), y la respuesta hace el camino de regreso. Todo en fracciones de segundo. En la unidad 2 vas a ver exactamente cómo se empaqueta esa petición capa por capa.

Error común de principiante: culpar al WiFi de todo. Si tu Internet está lento, antes de mover antenas verifica: es solo un dispositivo o todos? Si es uno solo, el problema es ese dispositivo o su conexión WiFi. Si son todos, reinicia el equipo del ISP y prueba con cable: si con cable va bien y por WiFi no, el problema es tu WLAN; si con cable también va mal, el problema es del proveedor (o de la última milla). Ese árbol de decisión tan simple resuelve el 80% de los reportes de "Internet lento".

Buenas prácticas generales de esta unidad

Para cerrar la explicación, algunas prácticas que distinguen a un técnico profesional desde el día uno:

Documenta tus redes. Un diagrama simple (qué equipos hay, cómo se conectan, qué IPs usan) vale oro cuando algo falla a las 2 de la mañana o cuando otro técnico tiene que continuar tu trabajo. No confíes en tu memoria.

Ponle nombre y contraseña decente a tu red WiFi. La red abierta del café es cómoda, pero en tu casa u oficina una WLAN sin contraseña es una puerta abierta. Usa WPA2 o WPA3 (los detalles de seguridad vienen en otra unidad).

Separa lo tuyo de lo del proveedor. Cuando reportes una falla, llega con datos: "con cable directo al módem tampoco hay Internet, el foco de LOS está en rojo" vale más que "no sirve el Internet". Los técnicos de Telmex o Totalplay te van a tomar más en serio.

Piensa en crecimiento. Si vas a cablear una oficina, deja cables y puertos de sobra. Poner un cable extra hoy cuesta poco; romper paredes mañana cuesta mucho.

Y la más importante: entiende antes de configurar. Cada pantalla de configuración de un router tiene sentido si sabes qué es una LAN, qué es DHCP, qué es una IP. Esta unidad te dio ese mapa; las siguientes te enseñan a moverte en él.

Topologías de red: cómo se conectan los nodos

La topología es la forma en qué los nodos están conectados entre sí: el "plano" de la red. Hay topologías físicas (cómo van los cables en la realidad) y lógicas (cómo viajan los datos, que no siempre coincide con lo físico). Estas son las clásicas:

Topología de bus. Todos los nodos comparten un solo cable troncal, como focos conectados a un mismo cable de luz. Barata y fácil de instalar, pero con un defecto mortal: si el cable troncal se rompe, toda la red cae. Además, solo un equipo puede transmitir a la vez. Fue popular en los 80 y 90 (cable coaxial), hoy está obsoleta para LANs nuevas. La mencionamos porque todavía aparece en exámenes y porque entender su debilidad te hace apreciar las demás.

Topología de anillo. Cada nodo se conecta con sus dos vecinos formando un círculo cerrado, y los datos viajan en una dirección pasando por cada equipo. Si un nodo falla, puede romper el anillo (aunque existen variantes con doble anillo para respaldo). Se usó en redes Token Ring de IBM; hoy casi no se instala nueva, pero la idea del anillo reaparece en redes de fibra metropolitanas con protección.

Topología de estrella. Todos los nodos se conectan a un equipo central (un switch o un router). Es la reina actual de las LANs: si se rompe el cable de una computadora, solo esa computadora se queda sin red; las demás siguen trabajando. Fácil de instalar, fácil de diagnosticar (sigues el cable hasta el switch) y fácil de crecer (agregas otro switch). Prácticamente toda oficina, cyber o casa con cableado usa estrella.

Topología de malla (mesh). Cada nodo se conecta con varios otros, creando múltiples caminos. Si una ruta falla, los datos toman otra automáticamente. Es cara (mucho cable o muchos radios), pero es la más resistente. Se usa en redes troncales de proveedores, en centros de datos y en sistemas WiFi de malla para casas grandes (esos kits de 2 o 3 aparatos que cubren toda la casa: cada aparato se conecta con los demás formando una malla inalámbrica).

Topología híbrida. Combinación de las anteriores, y es lo más común en la vida real: una empresa tiene estrella dentro de cada oficina, las oficinas se conectan en estrella al switch principal, y las sucursales se unen por una WAN. Internet misma es una malla gigantesca a nivel global.

Error común de principiante: confundir el diagrama físico con el lógico. Puedes tener cables en estrella (todo al switch) pero que los datos se comporten como bus (todos escuchan todo, como pasaba con los hubs antiguos). Para diagnosticar fallas te importa lo físico (que cable se rompió); para entender rendimiento y seguridad te importa lo lógico (quién puede ver el tráfico de quién).

Ancho de banda, velocidad, latencia y throughput

Estos cuatro términos se confunden todo el tiempo, incluso entre técnicos. Vamos a dejarlos claros con una analogía de tubería de agua:

Ancho de banda (bandwidth). Es el grosor de la tubería: la capacidad máxima de la conexión, medida en bits por segundo (bps, Kbps, Mbps, Gbps). Un plan de "100 megas" de Totalplay significa un ancho de banda de 100 Mbps. Ojo: son megabits, no megabytes; 100 Mbps equivalen a unos 12.5 megabytes por segundo en el mejor de los casos, porque 1 byte = 8 bits. Esta confusión bits vs bytes es causa del 90% de los reclamos de "me llegan menos megas de los contratados": el cliente mide en MB/s y el proveedor vende en Mbps.

Velocidad de transferencia real (throughput). Es cuanta agua sale realmente de la tubería: los datos útiles que logras mover por segundo en condiciones reales. Siempre es menor que el ancho de banda porque hay overhead (encabezados de protocolos), interferencia, congestión y límites del servidor destino. Si tu plan es de 100 Mbps y descargas a 90 Mbps, eso es normal y bueno; si descargas a 20 Mbps, hay algo que revisar.

Latencia. Es el tiempo que tarda un dato en ir y volver (retardo), medido en milisegundos (ms). En la analogía del agua, sería el tiempo que tarda una gota en recorrer la tubería. Depende sobre todo de la distancia y del medio: a un servidor en México tendrás 20-50 ms; a uno en Europa, 150-200 ms; por satélite, 500 ms o más. La latencia no la arregla contratar más megas: una conexión de 500 Mbps al otro lado del mundo seguirá teniendo 200 ms de latencia.

Por qué importa la diferencia? Para ver Netflix necesitas ancho de banda (muchos datos por segundo). Para jugar en línea o hacer videollamadas necesitas baja latencia (que cada dato llegue rápido, aunque sean pocos). Un gamer con 50 Mbps y 15 ms de latencia juega mejor que uno con 500 Mbps y 300 ms. Cuando un cliente se queja, pregunta primero que hace: si descarga lento, sospecha ancho de banda; si el juego "se traba" o la llamada se corta, sospecha latencia o pérdida de paquetes.

Jitter. Es la variación de la latencia: si tus paquetes llegan unos en 20 ms y otros en 200 ms, hay jitter alto, y las videollamadas se oyen robóticas aunque el promedio se vea bien. Mencionado aquí para que lo reconozcas cuando aparezca en herramientas de diagnóstico.

El modelo básico de comunicación

Toda comunicación en red, por compleja que sea, sigue cinco elementos. Entenderlos te ayuda a ubicar dónde falla algo:

1. Emisor: quién envía (tu laptop).
2. Receptor: quién recibe (el servidor de YouTube).
3. Mensaje: los datos (el video).
4. Medio: por dónde viaja (WiFi, fibra, etc.).
5. Protocolo: las reglas (TCP/IP, HTTP, etc.).

Cuándo algo no funciona, recorre la lista: el emisor está encendido y bien configurado? El receptor existe y responde? El mensaje está bien formado? El medio tiene continuidad? Ambos hablan el mismo protocolo? Este checklist mental es la versión sencilla del diagnóstico por capas que harás toda tu carrera.

Una primera mirada al direccionamiento IP

En la unidad 3 (o la que corresponda a direccionamiento) vas a estudiar las direcciones IP a fondo, pero necesitas la idea general desde ya porque aparece en cada ejemplo.

Una dirección IP es el "domicilio" de un dispositivo en la red: un número que lo identifica para qué los datos sepan a dónde ir. La versión más usada, IPv4, se escribe como cuatro números separados por puntos, por ejemplo 192.168.1.45. Cada número va de 0 a 255.

Hay dos clases de direcciones que debes distinguir desde hoy:

Direcciones privadas. Se usan dentro de las LANs y no existen en Internet público. Los rangos reservados son 10.0.0.0 a 10.255.255.255, 172.16.0.0 a 172.31.255.255 y 192.168.0.0 a 192.168.255.255. La IP 192.168.1.45 de tu laptop es privada: sirve dentro de tu casa, pero en Internet nadie te encuentra con ella. Por eso millones de casas pueden usar 192.168.1.1 para su router sin conflicto: cada una es un mundo privado separado.

Direcciones públicas. Son únicas en todo Internet y las asignan los proveedores. Tu router tiene una IP pública en su lado hacia el ISP (la puedes ver buscando "cuál es mi ip" en Google) y una privada en su lado hacia tu casa. El router traduce entre ambas (un proceso llamado NAT, que estudiarás después): así, todos tus dispositivos salen a Internet compartiendo una sola IP pública.

Analogía: tu casa tiene un número interior (el cuarto 3) que solo sirve dentro del edificio, y el edificio tiene una dirección en la calle que usa el cartero. La IP privada es el número interior; la pública, la dirección de la calle; el router es el conserje que reparte la correspondencia.

También existe IPv6, la versión nueva con direcciones larguissimas en hexadecimal (como 2001:db8::1), creada porque las IPv4 se están agotando. Muchos proveedores mexicanos ya la ofrecen junto con IPv4. No necesitas memorizar su formato hoy; solo recuerda que existe y que convive con IPv4.

Los ISP en México y los tipos de conexión

Ya viste el camino general de Internet a tu casa; ahora el detalle mexicano, porque como técnico te van a preguntar "que compañía me conviene" y "por qué mi conexión es así".

ISP (proveedor de servicios de Internet) es la empresa que te vende el acceso. Los principales en México: Telmex (marca Infinitum), Totalplay, Izzi, Megacable, y operadores regionales y locales más pequeños. Todos revenden capacidad que compran (o construyen) en redes troncales; la diferencia entre ellos está en la última milla y en la calidad de su red.

Tipos de conexión residencial y de pequeños negocios en México:

1. Fibra óptica hasta el hogar (FTTH). La fibra llega físicamente a tu domicilio y termina en un ONT. Es la mejor opción disponible: velocidades simétricas o casi (misma subida que bajada en muchos planes), latencia baja, estable. Telmex y Totalplay la ofrecen en

muchas ciudades. Si un cliente puede contratar fibra, casi siempre es la recomendación número uno.

2. Cable coaxial (HFC). Fibra hasta el nodo de la colonia, coaxial hasta la casa. Lo usan Izzi y varias cableras. Velocidades de bajada buenas, pero la subida suele ser mucho menor (planes asimétricos) y el coaxial compartido con los vecinos puede saturarse en horas pico.
3. ADSL por línea telefónica. Usa el par de cobre de Telmex. Velocidades modestas y muy dependientes de la distancia a la central: mientras más lejos vivas, más lento. Tecnología en retirada, pero todavía existe en zonas donde no ha llegado la fibra.
4. Inalámbrico fijo y satelital. Para zonas rurales o donde no hay cableado: una antena en el techo apunta a una torre cercana, o un plato apunta al satélite. Funciona, pero con más latencia y normalmente con límites de datos. Es la única opción en muchas comunidades, así que no la desprecies: mal Internet es mejor que nada.
5. Datos móviles (4G/5G). El teléfono como módem o un router con chip celular. Práctico y móvil, pero con planes limitados y latencia variable. Sirve como respaldo cuando se cae la conexión fija de una oficina pequeña.

Buena práctica profesional: cuando cotices o recomiendes, pregunta por la subida (upload), no solo la bajada. Un negocio que hace videollamadas todo el día o sube respaldos a la nube sufre con 10 Mbps de subida aunque tenga 200 de bajada. Y verifica la latencia con un ping al DNS del proveedor antes de firmar nada: es la prueba de 30 segundos que revela la calidad real.

Protocolos: cómo se ponen de acuerdo las máquinas

Profundicemos un poco más en los protocolos, porque son el corazón invisible de las redes. Un protocolo define sintaxis (formato de los mensajes), semántica (que significa cada campo) y temporización (en qué orden y a qué velocidad se intercambian). Los organismos que los estandarizan (como el IETF, que publica los RFC, y el IEEE, que estandariza Ethernet y WiFi) garantizan que un router chino, una laptop americana y un teléfono coreano se entiendan.

Los protocolos trabajan en familia y por capas (adelanto de la unidad 2): cada protocolo resuelve un problema específico y se apoya en otros. Ejemplo cotidiano: para abrir una página web se usan DNS (traduce el nombre a IP), TCP (conexión confiable), IP (lleva los paquetes), Ethernet o WiFi (los mueve por tu red local) y HTTP (pide y entrega la página). Si la página no abre, el técnico experimentado prueba cada protocolo por separado: ping para IP, nslookup para DNS, el navegador para HTTP. Esa es la mentalidad que este libro quiere formarte.

Error común de principiante: reinstalar drivers o formatear ante cualquier falla de red. El 90% de las fallas de red son de configuración o de un protocolo específico, no del sistema operativo. Aprende a diagnosticar por partes (como en los ejemplos con ping) y formatearás diez veces menos.

Ejemplos paso a paso

Vamos a bajar la teoría a la práctica con comandos reales. No necesitas ser experto: sigue cada ejemplo en tu propia computadora y compara las salidas. Los comandos varían un poco entre Windows y Linux; aquí verás los dos.

Ejemplo 1: ver tu conexión con ipconfig (Windows)

Abre el símbolo del sistema (tecla Windows, escribe "cmd", Enter) y ejecuta:

```
C:\Users\esteban> ipconfig
```

Salida típica (simplificada):

```
Adaptador de LAN inalámbrica Wi-Fi:

    Sufijo DNS específico para la conexión. . . : lan
    Dirección IPv4. . . . . : 192.168.1.45
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.1.1
```

Línea por línea:

- "Adaptador de LAN inalámbrica Wi-Fi": estás viendo la configuración de tu tarjeta WiFi. Si tuvieras cable, verías otro adaptador para Ethernet.
- "Dirección IPv4: 192.168.1.45": es la dirección IP privada de tu computadora dentro de tu LAN. Es tu "domicilio" dentro de la red local; ningún otro dispositivo de tu casa debe tener la misma.
- "Máscara de subred: 255.255.255.0": define que parte de la dirección es la red y que parte es el equipo. Con esta máscara, tu red es 192.168.1.0 y puede tener hasta 254 dispositivos. (El detalle de máscaras y subredes es tema de otra unidad; por ahora quedate con la idea general.)

- "Puerta de enlace predeterminada: 192.168.1.1": es la dirección de tu router, la "puerta" por la que sale el tráfico hacia Internet. Casi siempre termina en .1.

Prueba útil: si la dirección IPv4 empieza con 169.254, significa que tu equipo no pudo obtener IP del router (el DHCP fallo). Eso ya te dice dónde buscar el problema.

Ejemplo 2: ver tu conexión con ip addr (Linux)

En una terminal de Linux (Ubuntu, por ejemplo):

```
esteban@laptop:~$ ip addr show wlan0
```

Salida típica (simplificada):

```
3: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500  
    inet 192.168.1.45/24 brd 192.168.1.255 scope global dynamic wlan0
```

Línea por línea:

- "wlan0": es el nombre de tu interfaz inalámbrica (en cable suele ser eth0 o enp0s3).
- "UP, LOWER_UP": la interfaz está activa y con enlace físico (o radio, en WiFi). Si dijera DOWN, la tarjeta estaría apagada o desconectada.
- "inet 192.168.1.45/24": tu dirección IP y la máscara en notación corta (/24 equivale a 255.255.255.0).
- "brd 192.168.1.255": la dirección de broadcast de tu red, usada para mensajes a todos los equipos de la LAN.
- "dynamic": la IP la asignó el DHCP del router, no la configuraste a mano.

Ejemplo 3: probar conectividad con ping

El comando ping envía pequeños paquetes a un destino y mide si responden y cuanto tardan. Es la primera herramienta de diagnóstico de todo técnico de redes.

```
C:\Users\esteban> ping 192.168.1.1
```

Salida:

```
Haciendo ping a 192.168.1.1 con 32 bytes de datos:  
Respuesta desde 192.168.1.1: bytes=32 tiempo<1m TTL=64  
Respuesta desde 192.168.1.1: bytes=32 tiempo<1m TTL=64  
Respuesta desde 192.168.1.1: bytes=32 tiempo<1m TTL=64  
Respuesta desde 192.168.1.1: bytes=32 tiempo<1m TTL=64
```

Estadísticas de ping para 192.168.1.1:

Paquetes: enviados = 4, recibidos = 4, perdidos = 0 (0% perdidos),

Qué hiciste aquí? Le hiciste ping a tu router (la puerta de enlace que viste en ipconfig). Si responde con tiempo menor a 1 ms y 0% de pérdida, tu conexión local (tu WLAN o tu cable hasta el router) funciona bien. Si esté ping falla, el problema está en tu red local: revisa el WiFi, el cable o reinicia el router.

Ahora prueba más allá de tu red:

```
C:\Users\esteban> ping 8.8.8.8
```

8.8.8.8 es un servidor DNS público de Google, y hacer ping a una IP numérica (no a un nombre) prueba la conectividad a Internet sin depender del DNS. Si el ping al router funciona pero este falla, tu LAN está bien y el problema está en el proveedor o en la salida a Internet. Si esté funciona, prueba con un nombre:

```
C:\Users\esteban> ping www.google.com
```

Si la IP responde pero el nombre no, tu conexión a Internet funciona pero el DNS no resuelve nombres (falla el "directorio telefónico" de Internet). Tres pings, tres diagnósticos distintos: así trabaja un profesional, descartando por partes.

En Linux, ping funciona igual pero no se detiene solo (manda paquetes sin parar); deténlo con Ctrl+C:

```
esteban@laptop:~$ ping -c 4 8.8.8.8
```

La opción -c 4 le dice que envíe solo 4 paquetes, como en Windows.

Ejemplo 4: ver la ruta con tracert / traceroute

Cuando los datos van a un servidor lejano, pasan por varios equipos intermedios (routers). El comando tracert (Windows) o traceroute (Linux) te muestra cada salto del camino.

```
C:\Users\esteban> tracert www.google.com
```

Salida típica (simplificada):

```
Traza a la ruta a www.google.com [142.250.0.4]
sobre un maximo de 30 saltos:
```

1	<1 ms	<1 ms	<1 ms	192.168.1.1
2	12 ms	10 ms	11 ms	10.20.0.1
3	14 ms	13 ms	15 ms	200.10.50.1
4	38 ms	40 ms	39 ms	142.250.0.4

Línea por línea:

- Salto 1 (192.168.1.1): tu router. Menos de 1 ms, normal en una LAN.
- Saltos 2 y 3: equipos dentro de la red de tu proveedor (fijate en los tiempos: 10-15 ms, ya hay distancia).
- Salto 4: llegaste al servidor destino (38-40 ms: cruzo parte del país o llego a un servidor cercano).

Para qué sirve? Si una página tarda en cargar, un tracert te dice dónde se atora: si los tiempos se disparan en el salto 2, el problema es de tu proveedor; si todo va bien hasta el último salto, el problema es del servidor destino. También es la prueba visual perfecta de los conceptos de la unidad: ves tu LAN (salto 1), la red del proveedor (saltos intermedios, parte de una MAN/WAN) y el destino final.

En Linux:

```
esteban@laptop:~$ traceroute www.google.com
```

Hace lo mismo con formato ligeramente distinto.

Ejemplo 5: tu red vista cómo diagrama

Junta todo lo anterior en el mapa de tu propia casa. Con los datos de ipconfig ya puedes dibujar tu LAN:

```

[Internet / WAN del proveedor]
    |
    (fibra o coaxial)
    |
    [ONT o modem] <- equipo del ISP, frontera de tu red
    |
    [Router 192.168.1.1] <- puerta de enlace, da WiFi (WLAN)
    /      |      \
[Laptop .45] [Telefono .46] [Impresora .50]
(nodo final)  (nodo final)  (nodo final)

```

Este dibujo tan simple es exactamente lo que un técnico documenta al llegar a un cliente. Cada vez que algo falle, vuelve a él: el problema está en un nodo? en el router? más allá del módem? Con la teoría de esta unidad y estos cuatro comandos (ipconfig, ping, tracert, y su equivalente en Linux) ya puedes diagnosticar la mayoría de los problemas caseros y de oficina pequeña.

Ejemplo 6: medir tu velocidad real y entender el resultado

Abre en tu navegador un medidor como speedtest.net y corre la prueba con cable y luego por WiFi. Un resultado típico en un plan de 100 Mbps por fibra podría verse así:

```

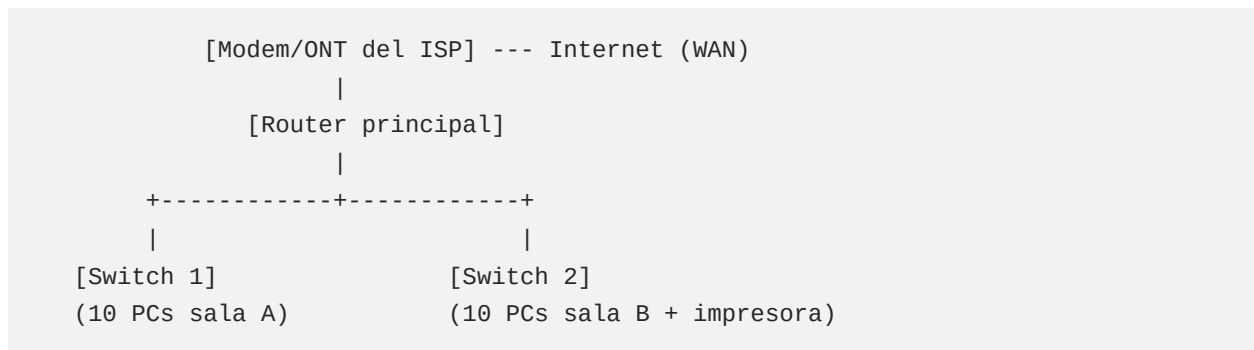
Descarga: 94.2 Mbps
Subida:   92.8 Mbps
Ping:     8 ms

```

Cómo leerlo: la descarga y la subida están cerca de lo contratado (nunca llegan al 100% por el overhead de protocolos; 90-95% es excelente). El ping de 8 ms indica que el servidor de prueba está cerca (probablemente en tu misma ciudad o en la red de tu proveedor): latencia buenisima. Si repites la prueba por WiFi desde el cuarto más lejano y obtienes 35 Mbps con ping de 60 ms, ya sabes que el limite no es tu plan contratado sino tu WLAN: interferencia, distancia o un router mal ubicado. Esa comparación cable vs WiFi es el diagnóstico más rápido para reclamos de "Internet lento" y usa directamente los conceptos de ancho de banda, throughput y latencia de esta unidad.

Ejemplo 7: topología estrella en un cyber

Imagina que vas a montar la red de un cyber con 20 computadoras. Aplicando lo aprendido, el diseño sería:



Cada PC se conecta por cable UTP a su switch (topología estrella dentro de cada sala), los switches suben al router (estrella de nuevo), y el router sale al módem. Si se dana el cable de la PC 7, solo cae la PC 7. Si falla el Switch 1, cae solo la sala A. El único punto crítico es el router: si cae, todo el cyber se queda sin Internet, por eso se elige un equipo de calidad y se deja bien ventilado. Este diagrama es el que dibujarías en la cotización del cliente, y cada decisión (estrella, UTP, switches separados por sala) viene de los conceptos de esta unidad.

Práctica

1. Dibuja el diagrama de la red de tu casa u oficina. Identifica cada dispositivo y clasifícalo como nodo final o dispositivo intermedio, e indica el medio que usa cada conexión (UTP, WiFi, fibra, etc.).

SOLUCIÓN: Empieza listando todo lo que se conecta: teléfonos, laptops, televisión, impresora, consola. Esos son nodos finales. Luego identifica los intermedios: el módem u ONT del proveedor y el router (a veces son el mismo aparato físico; anótalo así: "módem-router de Telmex/Totalplay, hace las dos funciones"). Dibuja el router al centro: de un lado, una línea hacia "Internet (ISP)" marcada con el medio de la última milla (fibra, coaxial o cobre); del otro lado, líneas hacia cada dispositivo marcadas con su medio (WiFi para los móviles, UTP si hay computadora con cable). Agrega las IPs si las conoces (las ves con ipconfig): el router suele ser 192.168.1.1 o 192.168.0.1. El objetivo del ejercicio no es que el dibujo quede bonito, sino que puedas señalar con el dedo dónde termina tu red y dónde empieza la del proveedor, porque esa frontera es lo primero que se verifica cuando algo falla.

2. Clasifica estas situaciones como PAN, LAN, CAN, MAN, WAN o WLAN y justifica tu respuesta: a) tus audífonos Bluetooth conectados a tu teléfono; b) la red de un cyber con 25 computadoras; c) la red de fibra de un proveedor que cubre toda la ciudad de Puebla; d) el WiFi de un aeropuerto; e) la red que conecta los edificios de una universidad; f) Internet.

SOLUCIÓN: a) PAN: son tus dispositivos personales a centímetros de distancia, red de área personal. b) LAN: un solo local, unas decenas de metros, administrada por el dueño del cyber. c) MAN: cubre una ciudad completa, operada por el proveedor. d) WLAN: es una LAN inalámbrica (mismo alcance que una LAN, pero por radio). e) CAN: varias LANs (una por edificio) interconectadas en un campus, una sola organización. f) WAN: la red de redes global. Fijate que el criterio no es la tecnología (cable o WiFi) sino el alcance y quien la administra: por eso el WiFi del aeropuerto es WLAN y no MAN, aunque le de servicio a mucha gente.

3. Un consultorio dental tiene 6 computadoras y una impresora. El dueño quiere compartir archivos e impresora con el menor costo posible y no tiene personal de sistemas. Recomienda red punto a punto o cliente-servidor y explica por qué.

SOLUCIÓN: Red punto a punto. Con 6 equipos y necesidades simples (archivos e impresora), una red punto a punto es suficiente: no requiere comprar un servidor dedicado ni pagar licencias o un administrador. Cada computadora comparte su carpeta y todas imprimen por la red. La desventaja (administración equipo por equipo, seguridad básica) es aceptable a esta escala. Se le debe advertir al dueño el límite: si el consultorio crece a más de 10 equipos o empieza a manejar información muy sensible con requisitos estrictos, convendra migrar a cliente-servidor. Buena práctica: aún en punto a punto, configura contraseñas en las carpetas compartidas y haz respaldos periódicos en un disco externo.

4. En tu computadora ejecuta ipconfig (Windows) o ip addr (Linux) y responde: cuál es tu dirección IPv4?Cuál es tu puerta de enlace? Que significaría si tu dirección empezará con 169.254?

SOLUCIÓN: La dirección IPv4 será algo como 192.168.1.x o 192.168.0.x (una IP privada de tu LAN, asignada por el DHCP del router). La puerta de enlace será la IP de tu router, típicamente 192.168.1.1 o 192.168.0.1. Si la dirección empezará con 169.254.x.x, significaría que tu equipo no pudo contactar al servidor DHCP y Windows/Linux se asignó una dirección automática privada (APIPA). En la práctica eso indica: el router está apagado o fallando, el cable está desconectado, o estás conectado a un WiFi que no da servicio DHCP. Pasos a seguir: verifica el cable o reconecta el WiFi, reinicia el router, y si persiste, prueba con otro dispositivo para saber si el problema es tu equipo o la red.

5. Haces ping a tu router (192.168.1.1) y responde perfecto (0% perdido). Haces ping a 8.8.8.8 y falla todo (100% perdido). Dónde está el problema y qué harías?

SOLUCIÓN: El problema NO está en tu red local: el ping al router demuestra que tu computadora, el medio (cable o WiFi) y el router funcionan. El problema está más allá: en la conexión del router hacia el proveedor (la última milla) o en el servicio del ISP. Que hacer, en orden: 1) reinicia el módem/ONT y el router (desconectalos 30 segundos); 2) revisa los focos del equipo del proveedor (un foco de LOS en rojo en fibra, o el foco de Internet apagado, indica falla del proveedor); 3) prueba con cable directo al módem para descartar tu router; 4) si nada funciona, llama al ISP y reporta con datos: "mi red local funciona, el ping a mí puerta de enlace responde, pero no hay salida a Internet; el foco X está en tal estado". Este es el diagnóstico por descarte que aprendiste en la unidad: separar tu LAN de la WAN del proveedor.

6. Explica con tus palabras la diferencia entre Internet y la web, y da un ejemplo de un servicio de Internet que NO sea la web.

SOLUCIÓN: Internet es la infraestructura: la red global de redes interconectadas con TCP/IP, los cables, los routers, los protocolos base. La web es un servicio que corre sobre Internet: páginas enlazadas que ves en el navegador usando HTTP/HTTPS, inventada por Tim Berners-Lee. La analogía: Internet son las carreteras, la web es un servicio de paquetería que las usa. Ejemplos de servicios de Internet que no son la web: el correo electrónico (SMTP/IMAP), la mensajería de WhatsApp, los videojuegos en línea, las videollamadas, la transferencia de archivos por FTP. Todos usan Internet, ninguno es "la web".

7. Un cliente te dice: "contrate 200 megas pero las descargas me llegan a 22 MB/s, me están robando". Explica si tiene razón usando bits vs bytes, y que le recomendarías verificar.

SOLUCIÓN: No necesariamente le están robando. Los proveedores venden en megabits por segundo (Mbps) y los programas de descarga muestran megabytes por segundo (MB/s); 1 byte = 8 bits, así que $200 \text{ Mbps} / 8 = 25 \text{ MB/s}$ teóricos, y con el overhead de protocolos unos 22-23 MB/s reales son un resultado excelente (más del 90% de lo contratado). Explicación para el cliente: multiplica lo que ve en el programa por 8 para comparar con su plan. Que verificar: 1) hacer la prueba con cable directo al módem, no por WiFi (el WiFi casi siempre da menos); 2) que ningún otro dispositivo este descargando al mismo tiempo; 3) probar en un medidor como speedtest.net contra un servidor cercano. Si con cable da, por ejemplo, 190 Mbps, el servicio está bien y el límite es su red local o el servidor de descarga.

8. Clasifica estas direcciones como privadas o públicas y explica por qué importa la diferencia: 192.168.1.1, 8.8.8.8, 10.0.0.5, 172.16.4.20, 200.100.50.25.

SOLUCIÓN: Privadas: 192.168.1.1 (rango 192.168.0.0 a 192.168.255.255), 10.0.0.5 (rango 10.0.0.0 a 10.255.255.255) y 172.16.4.20 (rango 172.16.0.0 a 172.31.255.255). Públicas: 8.8.8.8 y 200.100.50.25 (no están en los rangos reservados). Importa porque las privadas solo existen dentro de tu LAN: tu router las traduce a tu IP pública para salir a Internet (NAT). Por eso puedes tener 192.168.1.1 en tu casa y tu vecino también, sin conflicto: son redes privadas separadas. Y por eso desde Internet nadie puede entrar directo a tu laptop con su IP privada: primero tendría que pasar por tu router.

Resumen de la unidad

9. Vas a cablear una oficina nueva con 12 computadoras distribuidas en dos cuartos. Que topología usarías, que medió elegirías y que equipo central pondrías? Justifica cada decisión.

SOLUCIÓN: Topología estrella: cada computadora con su cable hasta un switch central, porque si falla un cable solo cae una máquina y es fácil diagnosticar siguiendo el cable. Medio: cable UTP categoría 5e o 6, barato y suficiente para 1 Gbps en esas distancias cortas; además agregaría un punto de acceso WiFi para laptops y teléfonos (los móviles no se cablean). Equipo central: un switch de al menos 16 puertos (12 para las PCs más puertos libres para crecer y para el enlace al router), y un router que conecte todo al módem del ISP y reparta IPs por DHCP. Si los dos cuartos están lejos, un switch por cuarto unidos entre si también es válido (estrella extendida). Todo esto sale directo de la unidad: estrella por tolerancia a fallas, UTP por costo y velocidad en corta distancia, y separación clara entre la LAN propia y la WAN del proveedor.

Una red es un conjunto de dispositivos conectados para compartir recursos e intercambiar información. Sus tres componentes básicos son los nodos (dispositivos finales como computadoras y teléfonos, y dispositivos intermedios como switches y routers), los medios (cables: UTP, coaxial, fibra óptica; inalámbricos: WiFi, Bluetooth, datos móviles, satélite) y los protocolos (las reglas de comunicación, como TCP/IP, HTTP, DNS y DHCP).

Por alcance, las redes se clasifican en PAN (tus dispositivos personales), LAN (una casa u oficina), CAN (un campus), MAN (una ciudad), WAN (países y el mundo; Internet es la WAN mayor) y WLAN (una LAN inalámbrica). Por organización, pueden ser punto a punto (equipos iguales, baratas, hasta ~10 nodos) o cliente-servidor (servidor central, administración y seguridad centralizadas, escalables).

La historia empezó con ARPANET en 1969, que aportó la conmutación de paquetes y la idea de una red descentralizada. En 1983 la adopción de TCP/IP creó Internet como red de redes. La web, inventada en 1989-1990, es solo un servicio sobre Internet, no Internet misma. En

México, Internet llega a tu casa así: red troncal de fibra, tu ISP (Telmex, Totalplay, Izzi, entre otros), la última milla (fibra, coaxial, cobre o inalámbrico), el módem u ONT en tu domicilio, y tu router que crea tu LAN/WLAN y reparte la conexión por DHCP.

Con `ipconfig/ip addr` ves tu configuración, con `ping` pruebas conectividad por partes (router, Internet por IP, Internet por nombre para probar DNS) y con `tracert/traceroute` ves la ruta salto por salto. La regla de oro del diagnóstico: separa siempre tu red local de la red del proveedor antes de culpar a nadie.

Llévate también estas ideas que aparecieron a lo largo de la unidad y que vas a usar todos los días: la topología estrella es el estándar para LANs porque aísla las fallas; el ancho de banda se mide en bits por segundo y el throughput real siempre es un poco menor; la latencia depende de la distancia y no se arregla contratando más megas; las direcciones IP privadas (10.x, 172.16.x, 192.168.x) viven solo dentro de tu LAN y tu router las traduce a tu IP pública para salir a Internet; y WiFi no es sinónimo de Internet: el WiFi es solo el tramo inalámbrico hasta tu router.

Si dominas esta unidad, tienes el mapa completo del territorio: qué es una red, de qué está hecha, qué tamaños existen, cómo se organizan, de dónde vienen y cómo llegan a tu casa. En la siguiente unidad aprenderás el lenguaje con el que hablan las redes por dentro: el modelo OSI y TCP/IP, capa por capa, para qué entiendas exactamente qué pasa cuando haces clic en un enlace.

UNIDAD 2: El modelo OSI y TCP/IP

En la unidad 1 aprendiste qué es una red, sus componentes y cómo llega Internet a tu casa. Ahora viene la pregunta del millón: cuando haces clic en un enlace, qué pasa exactamente dentro de la red? La respuesta es un viaje ordenado a través de capas, y los dos modelos que describen ese viaje (OSI y TCP/IP) son el tema de esta unidad. Si la unidad 1 era el mapa del territorio, esta unidad es el idioma que hablan sus habitantes.

En esta unidad vas a ver tres bloques. Primero, el modelo OSI: sus 7 capas, que hace cada una, y trucos de memoria (mnemotecnias) para recordarlas en el orden correcto, porque te las van a preguntar en entrevistas de trabajo y exámenes de certificación. Segundo, el modelo TCP/IP: sus 4 capas, cómo se relaciona con OSI y cuáles son los protocolos principales de cada capa (HTTP, TCP, UDP, IP, Ethernet, entre otros). Tercero, el encapsulamiento: como un dato baja por las capas agregando encabezados en el emisor y cómo sube quitándolos en el receptor, y los nombres que recibe en cada nivel (segmento, paquete, trama, bits).

Por qué importa en la vida real y en el trabajo? Por qué el diagnóstico profesional de redes se hace por capas. Cuando un usuario dice "no abre la página", el técnico novato reinicia todo a ver si suena la flauta; el técnico que domina este modelo piensa: capa 1 (hay enlace físico?), capa 2 (hay conexión al switch?), capa 3 (tengo IP y ruta?), capa 4 (el puerto responde?), capa 7 (el servicio web está arriba?). Cada pregunta descarta una capa y en minutos llegas a la causa. Esa forma de pensar es literalmente lo que separa a un técnico de un adivinador, y es lo que los empleadores pagan.

En México lo ves todos los días. El técnico de Telmex que llega a tu casa y primero revisa los focos del módem (capa física), luego si tu computadora tiene IP (capa de red) y al final si abre el navegador (capa de aplicación), está aplicando el modelo OSI sin decirlo. Cuando en un cyber un juego en línea va lento pero la descarga va rápida, la explicación está en la capa de transporte (UDP vs TCP). Cuando configuras un servidor en una oficina y "no se ve desde fuera", el problema casi siempre es de capa 3 (ruteo) o capa 4 (puertos). Todo el troubleshooting serio es troubleshooting por capas.

Un consejo de estudio: no intentes memorizar las 7 capas como una lista telefónica. Entiende la lógica: cada capa le presta un servicio a la de arriba y usa los servicios de la de abajo. La capa física mueve bits; el enlace los agrupa en tramas dentro de la red local; la red los lleva entre redes distintas; el transporte se asegura de que lleguen completos (o rápido, según el caso); la sesión administra la conversación; la presentación traduce formatos; y la aplicación es lo que el usuario ve. De abajo hacia arriba, cada capa agrega inteligencia. Cuando esa idea "hace clic", las capas se memorizan solas.

Explicación detallada

Por qué un modelo por capas

Imagina que quieres mandar una carta a otro país. No piensas en todo el proceso como una sola cosa: escribes la carta (contenido), la metes en un sobre con dirección (empaquete), la llevas al correo (transporte local), el correo la sube a un avión (transporte internacional), y en el destino se hace el proceso al revés. Cada etapa tiene sus reglas y sus responsables, y tu solo te preocupas por tu etapa.

Las redes funcionan igual. En los años 70 cada fabricante tenía su propio sistema cerrado: las computadoras IBM solo hablaban bien con IBM, las de DEC con DEC. La organización ISO (International Organization for Standardization) propuso en 1984 un modelo abierto por capas, el modelo OSI, para qué equipos de distintos fabricantes pudieran interoperar: si todos respetan las capas, una capa de un fabricante puede hablar con la misma capa de otro.

Las ventajas del diseño por capas son prácticas, no solo teóricas:

- División del trabajo: cada capa resuelve un problema específico. Cambiar el medio físico (de cobre a fibra) no obliga a reescribir las aplicaciones.
- Estandarización: varios fabricantes pueden implementar la misma capa y sus productos son compatibles (tu laptop y tu router son de marcas distintas y funcionan juntos).
- Diagnóstico: puedes probar cada capa por separado, como verás en los ejemplos.
- Aprendizaje: en lugar de estudiar "las redes" como una masa informe, estudias siete problemas pequeños y manejables.

El modelo OSI tiene 7 capas y es sobre todo una herramienta de referencia y enseñanza: casi nadie implementa OSI puro en productos reales. El modelo TCP/IP tiene 4 capas y es el que realmente corre en Internet. Necesitas los dos: OSI para pensar y diagnosticar, TCP/IP para lo que vas a configurar y programar todos los días. La relación exacta entre ambos la verás más adelante en esta unidad.

Las 7 capas del modelo OSI

El orden oficial se numera de abajo hacia arriba: la capa 1 es la más cercana al cable (física) y la capa 7 es la más cercana al usuario (aplicación). Vamos una por una, con su función, ejemplos de protocolos y dispositivos, y una analogía con el envío de un paquete por paquetería (DHL, Estafeta, la que uses).

Capa 1: Física

Función: transmite bits (unos y ceros) por el medio físico. Define voltajes, frecuencias, pulsos de luz, conectores, cuantos pines tiene un cable y a que velocidad se envían los bits. No sabe nada de direcciones ni de significado: solo mueve bits.

Ejemplos: cables UTP, fibra óptica, conectores RJ45, las ondas de radio del WiFi, hubs (que repiten la señal a todos los puertos sin pensar). Dispositivos de capa 1: repetidores y hubs.

Analogía de la paquetería: es el camión y la carretera. Al camión no le importa que lleva la caja; solo la mueve de un punto a otro.

Fallas típicas de capa 1: cable roto o mal ponchado, conector flojo, interferencia, distancia mayor a la permitida (más de 100 m en UTP), un puerto del switch dañado, el WiFi sin cobertura. Síntoma clásico: el foco del puerto no enciende o la interfaz aparece como DOWN. Primera regla del diagnóstico: siempre verifica la capa 1 primero, porque es la más barata de revisar (mira los focos, mueve el cable) y porque ninguna capa superior funciona sin ella.

Capa 2: Enlace de datos

Función: agrupa los bits en tramas (frames), detecta errores de transmisión y controla el acceso al medio. Además introduce el direccionamiento físico: la dirección MAC, un identificador único de fábrica que trae cada tarjeta de red (algo como 4c:72:b9:8a:1f:3e). La capa 2 solo sabe moverse dentro de la red local: no sabe salir a otras redes.

Se divide conceptualmente en dos subcapas: LLC (control del enlace lógico, la interfaz hacia la capa 3) y MAC (control de acceso al medio, quién puede transmitir y cuándo, para que no choquen las señales).

Ejemplos: protocolo Ethernet (el rey de las LANs cableadas), WiFi (estándares 802.11), switches (que leen direcciones MAC y reenvían tramas solo al puerto correcto). Dispositivos de capa 2: switches y puntos de acceso.

Analogía: es el repartidor local que conoce todas las calles de la colonia y entrega según el número de casa (la MAC). Pero no sabe salir de la colonia: para eso necesita a la capa 3.

Fallas típicas de capa 2: dirección MAC duplicada (raro, pero pasa con tarjetas clonadas), tormentas de broadcast por loops (cables conectados formando un círculo entre switches), dúplex mal negociado (un lado en full y otro en half: la red funciona pero lentísima). En WiFi: interferencia y saturación del canal.

Capa 3: Red

Función: lleva los paquetes entre redes distintas. Aquí vive el direccionamiento lógico: las direcciones IP. Mientras la MAC dice "quién eres físicamente", la IP dice "dónde estás

lógicamente" y puede cambiar si te mueves de red. La capa 3 decide la mejor ruta (ruteo) cuando hay varios caminos.

Ejemplos: protocolo IP (IPv4 e IPv6), protocolos de ruteo como OSPF y BGP (los usan los routers de los proveedores para ponerse de acuerdo en las rutas), ICMP (el protocolo de ping). Dispositivos de capa 3: routers.

Analogía: es el sistema de carreteras nacionales y la SEPOMEX decidiendo por qué ciudades pasa tu paquete para llegar a otro estado. La dirección IP es como el código postal: jerárquica y ruteable.

Fallas típicas de capa 3: IP mal configurada o duplicada, máscara de subred incorrecta, puerta de enlace equivocada, tabla de rutas incompleta, NAT mal configurado. Síntoma clásico: "me conectó al WiFi pero no tengo Internet" con IP 169.254.x.x (el DHCP no asignó dirección). El ping es la herramienta de diagnóstico de esta capa.

Diferencia clave MAC vs IP (pregunta clásica de entrevista): la MAC es física, única de fábrica y no cambia; sirve para entregar dentro de la LAN. La IP es lógica, asignada por configuración y cambia según la red; sirve para llegar entre redes. Una carta necesita el nombre del destinatario (MAC) y su dirección completa con código postal (IP).

Capa 4: Transporte

Función: entrega los datos de extremo a extremo (de tu computadora al servidor, sin importar cuantas redes crucen en medio) y con la calidad de servicio adecuada. Sus dos protocolos estrella ofrecen dos filosofías opuestas:

TCP (Transmission Control Protocol): entrega confiable. Establece conexión antes de enviar (el famoso saludo de tres pasos: SYN, SYN-ACK, ACK), numera los segmentos, confirma recepción y retransmite lo que se pierda. Garantiza que los datos lleguen completos y en orden. Precio: más overhead y un poco más de latencia. Se usa cuando no se puede perder ni un byte: páginas web, correo, transferencia de archivos, banca en línea.

UDP (User Datagram Protocol): entrega rápida sin garantías. Manda los datagramas y no espera confirmación; si algo se pierde, nadie lo retransmite. Precio: simplicidad y velocidad. Se usa cuando importa más la velocidad que la perfección: videollamadas, juegos en línea, streaming en vivo, DNS. En una llamada, prefieres perder una sílaba a que se pause todo esperando el pedazo perdido.

La capa 4 también introduce los puertos: números que identifican a qué aplicación va cada dato dentro de un equipo. Tu computadora puede navegar, recibir correo y jugar al mismo tiempo porque cada aplicación usa puertos distintos (la web usa el 80/443, el correo el

25/110/143, etc.). La combinación IP + puerto se llama socket y es la "dirección completa" de una conversación.

Analogía: TCP es paquetería con guía rastreable, firma de recibido y seguro: si se pierde, te lo reponen. UDP es aventar papeles por la ventana esperando que lleguen: rapidísimo, pero sin garantías.

Fallas típicas de capa 4: un firewall bloqueando un puerto (la página no abre pero el ping si responde: la red llega, la aplicación no), un servicio caído en el servidor, puertos mal redirigidos en el router (el famoso port forwarding para cámaras o servidores de juegos).

Capa 5: Sesión

Función: administra las sesiones, es decir, las conversaciones entre aplicaciones: quién habla cuando, cómo se inicia, cómo se mantiene y cómo se termina ordenadamente. También maneja la sincronización con puntos de control: si una transferencia grande se interrumpe, se puede retomar desde el último punto en vez de empezar de cero.

Ejemplos: el inicio de sesión en un servidor, las sesiones de una videollamada, el protocolo NetBIOS en redes Windows antiguas, las APIs de sockets que usan los programadores.

Analogía: es el moderador de un debate: da la palabra, lleva el orden del día y cierra la sesión. No le importa el contenido del debate (eso es de capas superiores).

En la práctica moderna, la capa 5 casi no tiene protocolos famosos propios: muchas de sus funciones las absorben las aplicaciones o la capa 4. Pero el concepto sigue siendo útil: cuando una página te saca por "sesión expirada", estás viendo la capa 5 en acción.

Capa 6: Presentación

Función: traduce, cifra y comprime los datos para que la aplicación los entienda. Es la traductora: convierte entre formatos (por ejemplo, de JPEG a píxeles en pantalla), comprime para ahorrar ancho de banda y cifra para seguridad.

Ejemplos: cifrado SSL/TLS (el candadito del navegador, la S de HTTPS), compresión, codificaciones de texto y formatos de imagen/video (JPEG, MP4). Cuando entras a tú banca en línea y ves HTTPS, la capa 6 está cifrando todo.

Analogía: es el traductor e intérprete en una reunión internacional: no decide que se dice (aplicación), pero se asegura de que todos lo entiendan en su idioma y de que nadie ajeno escuche (cifrado).

Capa 7: Aplicación

Función: es la capa más cercana al usuario: los servicios y protocolos que las aplicaciones usan para comunicarse por la red. Ojo: no son las aplicaciones mismas (Chrome no es la capa 7), sino los protocolos que usan (HTTP es capa 7, Chrome solo lo habla).

Ejemplos: HTTP/HTTPS (web), FTP (transferencia de archivos), SMTP/IMAP/POP3 (correo), DNS (nombres a IPs), DHCP (asignación automática de IPs), SSH (administración remota segura), Telnet (remoto inseguro, obsoleto).

Analogía: es el idioma final en qué hablan las personas: "quiero ver esta página", "manda este correo". Todo lo de abajo existe para que esta conversación ocurra.

Fallas típicas de capa 7: el servicio está caído, URL mal escrita, credenciales incorrectas, certificado SSL vencido (el navegador marca error aunque la red funcione perfecto). Síntoma: todo lo demás (ping, DNS) funciona pero la aplicación no.

Mnemotecnias para recordar las 7 capas

El orden importa y te lo van a preguntar. De arriba hacia abajo (7 a 1): Aplicación, Presentación, Sesión, Transporte, Red, Enlace, Física. De abajo hacia arriba (1 a 7): Física, Enlace, Red, Transporte, Sesión, Presentación, Aplicación.

Mnemotecnia en español (7 a 1): "Ana Pide Sopa, Toma Refresco En Familia". Ana=Aplicación, Pide=Presentación, Sopa=Sesión, Toma=Transporte, Refresco=Red, En=Enlace, Familia=Física. Inventa la tuya si quieres; lo importante es que las iniciales A-P-S-T-R-E-F queden fijas.

Mnemotecnia en inglés (7 a 1), por si lees documentación: "All People Seem To Need Data Processing" (Application, Presentation, Session, Transport, Network, Data link, Processing=Physical). La vas a ver en muchos cursos.

Para el diagnóstico se usa de abajo hacia arriba (1 a 7): "Fernando Envía Rosas Todos los Sábados Por Avión"? Mejor una directa: Física, Enlace, Red, Transporte, Sesión, Presentación, Aplicación = "Felipe Está Raro, Toma Sopa Para Almorzar". El chiste es practicarla hasta que salga sin pensar, por qué en una falla real no tienes tiempo de dudar.

Truco profesional: asocia cada capa con su pregunta de diagnóstico y su herramienta. 1 Física: hay luz/enlace? (reviso focos y cables). 2 Enlace: veo la red local? (arp, estado del switch). 3 Red: tengo IP y ruta? (ipconfig, ping, tracert). 4 Transporte: el puerto responde? (telnet al puerto, netstat). 7 Aplicación: el servicio funciona? (navegador, nslookup para DNS). Con esa tabla mental, cualquier reporte de falla se convierte en un recorrido ordenado.

El modelo TCP/IP: 4 capas

El modelo TCP/IP nació antes que OSI (viene de ARPANET y de los RFC) y es el que realmente implementan todos los sistemas operativos y dispositivos. Tiene 4 capas, más prácticas y menos teóricas:

Capa 1: Acceso a la red (Network Access)

Combina la física y el enlace de OSI: como conectar el equipo al medio y mover tramas dentro de la red local. Protocolos: Ethernet, WiFi (802.11), PPP. Aquí viven las direcciones MAC, los switches y los controladores de las tarjetas de red.

Capa 2: Internet

Equivale a la capa de red de OSI: direccionamiento IP y ruteo entre redes. Protocolos: IP (IPv4/IPv6), ICMP, ARP (traduce IPs a MACs dentro de la LAN), IGMP. Aquí viven los routers.

Capa 3: Transporte

Igual que en OSI: TCP y UDP, puertos, conexiones de extremo a extremo.

Capa 4: Aplicación

Combina las capas 5, 6 y 7 de OSI (sesión, presentación y aplicación): todo lo que usan directamente los programas. Protocolos: HTTP/HTTPS, FTP, SMTP, DNS, DHCP, SSH, Telnet.

Relación entre OSI y TCP/IP

Ponlos lado a lado y la correspondencia es clara:

OSI (7 capas)		TCP/IP (4 capas)
7. Aplicacion	\	
6. Presentacion	>---	4. Aplicacion
5. Sesion	/	
4. Transporte	-----	3. Transporte
3. Red	-----	2. Internet
2. Enlace de datos	\	
1. Fisica	>---	1. Acceso a la red

Por qué dos modelos? Historia pura: TCP/IP se creó primero, funcionando, para ARPANET; OSI llegó después como estándar internacional más completo y pedagógico. La industria adoptó TCP/IP (por qué ya funcionaba en todo) y las escuelas adoptaron OSI (por qué explica mejor). Tú necesitas ambos: piensa en OSI, configura en TCP/IP.

En el trabajo diario casi siempre hablarás en términos TCP/IP ("es un problema de la capa de Internet", "revisa la capa de aplicación"), pero cuando algo se complica, abrir el mapa de 7 capas te da más precisión para ubicar la falla. Los exámenes de certificación (como el CCNA) te exigen moverte entre los dos sin titubear.

Protocolos principales por capa (modelo TCP/IP)

Vamos a presentar a los protagonistas que vas a ver en cada diagnóstico. No memorices definiciones de diccionario: entiende que problema resuelve cada uno.

Capa de acceso a la red:

- Ethernet (IEEE 802.3): el estándar de las redes cableadas. Define tramas, direcciones MAC y cómo se accede al cable. Velocidades típicas hoy: 1 Gbps en oficinas, 10 Gbps en centros de datos. Si conectas un cable de red, estás usando Ethernet.
- WiFi (IEEE 802.11): la familia de estándares inalámbricos (a/b/g/n/ac/ax, este último comercializado como WiFi 6). Define cómo los dispositivos comparten el aire por radio sin interferirse (o interfiriéndose lo menos posible).
- ARP (Address Resolution Protocol): el traductor dentro de la LAN. Cuando tu computadora quiere hablar con 192.168.1.1 pero solo conoce la IP, ARP pregunta "¿quién tiene esa IP?" y el router responde con su MAC. Sin ARP, la capa de Internet no podría bajar a la capa de acceso. Lo verás en acción con el comando `arp -a`.

Capa de Internet:

- IP (Internet Protocol): el corazón del modelo. Define el formato de los paquetes y las direcciones. IPv4 usa direcciones de 32 bits (192.168.1.1); IPv6 usa 128 bits para no quedarse sin direcciones. IP es "mejor esfuerzo": no garantiza entrega, no confirma nada; de la confiabilidad se encarga TCP arriba.
- ICMP (Internet Control Message Protocol): el mensajero de control. Lo usa ping (echo request/reply) y tracert (mensajes de tiempo excedido) para diagnosticar. Cuando un router no puede entregar un paquete, te avisa con ICMP.
- NAT (traductor, más una técnica que un protocolo): permite que toda tu LAN salga a Internet con una sola IP pública, traduciendo direcciones privadas a la pública y viceversa. Es lo que hace tu router casero.

Capa de transporte:

- TCP: confiable, orientado a conexión, con control de flujo y de congestión. Puertos conocidos: 80 (HTTP), 443 (HTTPS), 25 (SMTP), 110 (POP3), 143 (IMAP), 22 (SSH), 21 (FTP), 53 (DNS, también usa UDP).
- UDP: rápido, sin conexión, sin garantías. Puertos conocidos: 53 (DNS), 67/68 (DHCP), 69 (TFTP), 123 (NTP, sincronización de hora), y los que usan juegos y videollamadas.

Capa de aplicación:

- HTTP/HTTPS: el protocolo de la web. HTTPS agrega TLS (cifrado) sobre HTTP: misma función, con privacidad. Puerto 80 y 443.
- DNS: el directorio telefónico de Internet; traduce nombres (www.ejemplo.com) a IPs. Puerto 53. Sin DNS tendrías que memorizar números.
- DHCP: asigna automáticamente IP, máscara, puerta de enlace y DNS a los dispositivos que se conectan. Puertos 67/68. Es lo que hace tu router cuando tu teléfono "agarra WiFi solo".
- FTP/SFTP: transferencia de archivos; SSH: terminal remota segura; SMTP/IMAP/POP3: envío y recepción de correo; Telnet: terminal remota insegura (no la uses, solo conócela para el examen).

Buena práctica: cuando estudies un protocolo nuevo, pregúntate siempre: en qué capa vive? Qué problema resuelve? Qué pasa si falla? Con esas tres respuestas lo tienes dominado para efectos prácticos.

Encapsulamiento y desencapsulamiento

Este es el concepto más elegante de la unidad y el que más impresiona cuando lo entiendes: cómo viaja un dato por las capas.

Encapsulamiento: en el equipo emisor, los datos bajan por las capas y cada capa les agrega su propio encabezado (header) con información de control, como meter una carta en sobres cada vez más grandes. El proceso, de arriba hacia abajo:

1. La aplicación genera los datos (por ejemplo, la petición HTTP "dame la página").
2. La capa de transporte los corta en pedazos manejables y a cada uno le pone su encabezado TCP (puertos origen y destino, número de secuencia): ahora se llama segmento.
3. La capa de Internet le agrega el encabezado IP (IP origen y destino): ahora se llama paquete.

4. La capa de acceso a la red le agrega el encabezado Ethernet (MAC origen y destino) y al final un verificador de errores (tráiler): ahora se llama trama.
5. La capa física convierte la trama en bits y la manda por el cable o el aire.

Desencapsulamiento: en el equipo receptor ocurre lo inverso. Los bits suben: la capa de acceso verifica la trama y le quita el encabezado Ethernet, la capa de Internet revisa el paquete y le quita el encabezado IP, la capa de transporte rearma los segmentos en orden y le quita el encabezado TCP, y la aplicación recibe los datos originales. Cada capa solo lee su propio encabezado e ignora el resto: por eso un switch (capa 2) no necesita entender IPs y un router (capa 3) no necesita entender puertos TCP.

Analogía completa de la paquetería: escribes la carta (datos), la metes en un sobre con el nombre del destinatario dentro de la empresa (encabezado TCP: puerto), metes ese sobre en una caja con la dirección y código postal (encabezado IP), le pegas la guía de la paquetería local (encabezado Ethernet), y el camión la lleva (bits). En el destino, cada nivel abre solo su propio empaque.

Por qué importa? Tres razones prácticas. Una: el overhead. Cada encabezado agrega bytes; un paquete pequeño lleva proporcionalmente más encabezado que datos útiles, por eso mandar un millón de pings de 1 byte es ineficiente. Dos: la seguridad. Un firewall puede decidir mirando solo ciertos encabezados (bloquear por IP en capa 3 o por puerto en capa 4) sin abrir el contenido. Tres: el diagnóstico. Si capturas tráfico con Wireshark, ves literalmente los encabezados apilados y puedes leer que está pasando capa por capa.

PDU: los nombres del dato en cada capa

PDU (Protocol Data Unit, unidad de datos de protocolo) es el nombre elegante para "cómo se llama el dato en cada capa". Memorízalos porque son vocabulario de todos los días:

- Capa 7-5 (aplicación): datos (data).
- Capa 4 (transporte): segmento (si es TCP) o datagrama (si es UDP).
- Capa 3 (red/Internet): paquete (packet).
- Capa 2 (enlace/acceso): trama (frame).
- Capa 1 (física): bits.

Mnemotecnia: "Si Pintas Tu Bodega" (Segmento, Paquete, Trama, Bits) de la capa 4 a la 1. O en inglés, muy usada: "Some People Think Big" (Segments, Packets, Trames=Frames, Bits).

Error común de principiante: decir "paquete" para todo. En una conversación técnica, "el switch reenvía tramas" y "el router rutea paquetes" no son intercambiables: cada dispositivo trabaja a

su nivel. Usar el término correcto te hace sonar profesional y, más importante, te obliga a pensar en la capa correcta cuando diagnosticas.

Ejemplo mental completo: abrir una página web

Vamos a juntar todo con lo que haces cien veces al día: escribir `www.ejemplo.com` en el navegador.

1. DNS (capa de aplicación): el navegador necesita la IP de `www.ejemplo.com`. Manda una consulta DNS (UDP, puerto 53) al servidor DNS configurado. Respuesta: `93.184.216.34`.
2. TCP (capa de transporte): el navegador abre una conexión TCP al puerto 443 de esa IP con el saludo de tres pasos (SYN, SYN-ACK, ACK). Si es HTTPS, aquí también se negocia el cifrado TLS (capa de presentación en OSI).
3. HTTP (capa de aplicación): por esa conexión viaja la petición: "GET / HTTP/1.1, host: `www.ejemplo.com`".
4. Encapsulamiento: la petición se vuelve segmento TCP (encabezado con puertos), luego paquete IP (encabezado con tu IP y la del servidor), luego trama Ethernet (encabezado con tu MAC y la del router), luego bits al aire o al cable.
5. Tu router (capa 3) lee la IP destino, decide que sale a Internet, hace NAT (cambia tu IP privada por su pública) y la reenvía a tu ISP.
6. Los routers del camino (capa 3) la pasan de red en red según sus tablas de ruteo hasta el servidor.
7. El servidor desencapsula: quita Ethernet, quita IP, rearma TCP, le entrega la petición HTTP a su aplicación web.
8. La respuesta (la página) hace el viaje inverso: se encapsula en el servidor, viaja por las redes, tu router la recibe, deshace el NAT, y tu navegador la desencapsula hasta mostrarte la página.

Todo eso, decenas de capas y dispositivos, en menos de un segundo. Cuando algo falla en esa cadena, tu trabajo es averiguar en qué paso se rompió: y ahora tienes el mapa para hacerlo.

Errores comunes y buenas prácticas

Errores que veo en principiantes (y como evitarlos):

- Confundir el modelo con la realidad: OSI es un modelo de referencia, no una ley física. Un switch moderno puede hacer funciones de capa 3; eso no "rompe" el modelo, solo

significa que el aparato implementa varias capas. Usa el modelo para pensar, no como camisa de fuerza.

- Diagnosticar desde arriba: empezar por reinstalar el navegador cuando no hay ni enlace físico. Siempre de abajo hacia arriba: físico, enlace, red, transporte, aplicación.
- Culpar a la capa equivocada: "el Internet no sirve" cuando lo que no sirve es el DNS (las IPs responden pero los nombres no). Aprende a probar cada capa por separado y tus diagnósticos se volverán quirúrgicos.
- Memorizar puertos sin contexto: no memorices listas infinitas; aprende los 10 más comunes (80, 443, 25, 53, 22, 21, 110, 143, 67/68, 3389) y consulta el resto cuando lo necesites.

Buenas prácticas de la industria:

- Documenta por capas: en el diagrama de tu red, anota que hace cada equipo en cada capa (este switch es capa 2, este router hace NAT en capa 3, este firewall filtra por puerto en capa 4). Cuando llegue una falla, el diagrama te dice dónde mirar.
- Nombra tus diagnósticos por capa en los reportes: "falla de capa 3: sin ruta al segmento" se entiende mejor que "no jala la red" y te hace ver profesional ante clientes y jefes.
- Para programadores: entender TCP vs UDP te evita diseñar mal una app. Si tu app necesita que todo llegue perfecto, usa TCP; si necesita velocidad en tiempo real, UDP. Esa decisión se toma en la capa 4 y afecta todo el producto.

TCP a detalle: el saludo de tres pasos

El establecimiento de una conexión TCP es tan importante que merece su propio espacio: aparece en entrevistas, en exámenes y en capturas de Wireshark reales. Se llama three-way handshake (saludo de tres pasos) y funciona así entre tu computadora (cliente) y un servidor web:

Paso 1 - SYN: el cliente manda un segmento con la bandera SYN activada y un número de secuencia inicial, digamos 1000. Es como decir: "quiero hablar contigo, empiezo a contar desde 1000".

Paso 2 - SYN-ACK: el servidor responde con SYN activado (acepta la conversación) y ACK activado (confirma lo recibido), con su propio número de secuencia, digamos 5000, y un acuse de recibo 1001 ("recibí hasta el 1000, espero él 1001"). Es como decir: "acepto, yo cuento desde 5000, y te escuche hasta el 1000".

Paso 3 - ACK: el cliente confirma con ACK y acusa 5001 ("te escuche hasta el 5000"). La conexión queda establecida y empiezan a viajar los datos.

Para terminar hay un proceso similar de 4 pasos con la bandera FIN. Por qué te importa? Por qué con una captura de paquetes puedes ver exactamente dónde muere una conexión: si ves SYN sin respuesta, el servidor no está escuchando o un firewall bloquea; si ves SYN-ACK pero no el ACK final, hay un problema de ruteo de regreso. Tres paquetes te cuentan toda la historia.

TCP además hace control de flujo (no ahogar al receptor: le pregunta cuanto puede recibir con la "ventana") y control de congestión (si la red se satura, baja el ritmo). UDP no hace nada de esto: por eso una descarga por TCP se adapta sola a la red y un stream por UDP puede saturarla si se descuida.

El encapsulamiento con números reales

Vamos a ponerle números al encapsulamiento para que deje de ser abstracto. Tu navegador quiere pedir una página; la petición HTTP mide, digamos, 400 bytes de datos.

1. Capa de transporte: TCP corta (si fuera grande) y agrega su encabezado típico de 20 bytes. Ahora el segmento mide 420 bytes. El encabezado TCP incluye: puerto origen (ej. 49152), puerto destino (443), número de secuencia, banderas.
2. Capa de Internet: IP agrega su encabezado típico de 20 bytes. Ahora el paquete mide 440 bytes. El encabezado IP incluye: IP origen (192.168.1.45), IP destino (93.184.216.34), tiempo de vida (TTL), protocolo (6 = TCP).
3. Capa de acceso: Ethernet agrega encabezado de 14 bytes (MAC destino, MAC origen, tipo) y un tráiler de 4 bytes (FCS, verificación de errores). La trama mide 458 bytes. Incluye: MAC destino (la del router, ej. aa:bb:cc:11:22:33), MAC origen (la de tu laptop).
4. Capa física: esos 458 bytes se convierten en 3664 bits que viajan por el cable o el aire.

Fijate en algo clave: la MAC destino es la del router, no la del servidor final. La capa 2 solo llega hasta el siguiente salto; es la IP destino (capa 3) la que se mantiene de extremo a extremo. Por eso en cada salto del camino la trama Ethernet se destruye y se reconstruye con nuevas MACs, pero el paquete IP viaja intacto (salvo el TTL, que cada router decrementa en 1; cuándo llega a 0 el paquete se descarta: así se evitan paquetes dando vueltas eternas).

MTU y fragmentación

MTU (Maximum Transmission Unit) es el tamaño máximo del paquete que un medio puede llevar. En Ethernet es típicamente 1500 bytes. Qué pasa si tu paquete mide más? La capa 3 lo fragmenta: lo corta en pedazos que sí quepan, cada uno con su encabezado IP, y el receptor los rearma. Funciona, pero es ineficiente y frágil (si se pierde un fragmento, se retransmite todo el paquete original).

En la práctica, TCP negocia el tamaño máximo de segmento (MSS) durante el saludo de tres pasos para evitar fragmentar. Pero hay casos famosos de problemas de MTU: conexiones VPN o túneles que agregan encabezados extra y hacen que paquetes de 1500 bytes ya no quepan, causando páginas que "cargan a medias". El diagnóstico clásico es probar ping con paquetes grandes y la bandera "no fragmentar": si los grandes no pasan y los chicos sí, hay un problema de MTU en el camino. Lo verás en los ejemplos.

Switch vs router vs hub: cada uno en su capa

Esta comparación resume la unidad en tres aparatos:

- Hub (capa 1): repite todo lo que recibe a todos los puertos. No entiende direcciones. Barato, pero ineficiente e inseguro (todos ven el tráfico de todos). Obsoleto; si encuentras uno, sugiere reemplazarlo.
- Switch (capa 2): aprende que MAC está en cada puerto y reenvía cada trama solo al puerto destino. Eficiente y es el estándar en LANs. Un switch administrable puede hacer VLANs (redes virtuales, tema de otra unidad).
- Router (capa 3): conecta redes distintas, lee IPs, decide rutas, hace NAT. Es la frontera entre tu LAN y el mundo.

Y el firewall? Normalmente trabaja en capas 3 y 4 (filtra por IP y puerto) y los modernos inspeccionan hasta capa 7. El punto de acceso WiFi es capa 2 (un puente inalámbrico). Cuando alguien te pregunte "qué hace este aparato?", responde con su capa y ya sonaste como profesional.

Comunicación de par a par: cada capa habla con su igual

Hay un detalle elegante que redondea tu comprensión: aunque físicamente los datos bajan por las capas del emisor, viajan por el cable y suben por las capas del receptor, lógicamente cada capa "habla" con su capa gemela del otro lado. La capa de transporte de tu PC establece su conexión con la capa de transporte del servidor (el saludo SYN, SYN-ACK, ACK es una conversación entre capas 4); la capa de red de tu PC direcciona hacia la capa de red del

servidor; la aplicación HTTP de tu navegador habla con la aplicación HTTP del servidor web. Los dispositivos intermedios solo participan hasta su capa: el switch solo sube hasta capa 2, el router hasta capa 3. Por eso se dice que el switch "no ve" las IPs y el router "no ve" los puertos: no es que sean tontos, es que su trabajo termina en su capa y dejan el resto intacto.

Servicios orientados y no orientados a conexión

Ya viste que TCP es orientado a conexión y UDP no. Esta distinción aparece en todas las capas, así que vale la pena generalizarla:

- Orientado a conexión: primero se establece la comunicación, luego se transfieren datos, al final se cierra ordenadamente. Ventaja: confiabilidad y control. Desventaja: overhead y latencia inicial. Ejemplos: TCP en capa 4, una llamada telefónica tradicional.
- No orientado a conexión (sin conexión): cada unidad de datos se manda por su cuenta, sin aviso previo. Ventaja: velocidad y simplicidad. Desventaja: sin garantías. Ejemplos: UDP en capa 4, IP en capa 3, mandar cartas por correo.

Fijate que IP (capa 3) es no orientada a conexión aunque TCP (capa 4) si lo sea: TCP construye su confiabilidad encima de un servicio no confiable, como mandar cartas certificadas usando el correo normal. Esa es la belleza del diseño por capas: cada capa puede ofrecer garantías que la de abajo no tiene, agregando su propia lógica en su encabezado.

Los puertos que todo técnico memoriza

No memorices cientos de puertos; con estos diez resuelves el 95% de los casos reales:

Puerto	Protocolo	Servicio
20/21	TCP	FTP (transferencia de archivos)
22	TCP	SSH (terminal remota segura)
25	TCP	SMTP (envio de correo)
53	TCP/UDP	DNS (nombres a IPs)
67/68	UDP	DHCP (IP automática)
80	TCP	HTTP (web sin cifrar)
110	TCP	POP3 (recepción de correo)
143	TCP	IMAP (recepción de correo)
443	TCP	HTTPS (web cifrada)
3389	TCP	RDP (escritorio remoto de Windows)

Cómo usarlos en la práctica: si un cliente dice "no me llega el correo", preguntas cuál usa y pruebas su puerto (25 para enviar, 110/143 para recibir). Si "la página no abre", pruebas el 80/443 con Test-NetConnection. Si "no agarra IP", el problema es el 67/68 (DHCP). Los

puertos son el vocabulario con el que la capa 4 identifica aplicaciones: dominarlos es hablar el idioma del diagnóstico.

Cuándo el modelo se estira: VPN, VLAN y túneles

Hay tecnologías que "doblan" el modelo y conviene conocerlas desde ahora para no confundirte después:

- VPN (red privada virtual): toma paquetes completos (con sus encabezados), los cifra y los mete dentro de otros paquetes para cruzar Internet de forma segura. Es encapsulamiento dentro del encapsulamiento: por eso las VPN a veces tienen problemas de MTU (el paquete doble ya no cabe en 1500 bytes).
- VLAN (red de área local virtual): un switch de capa 2 finge ser varios switches, separando grupos de puertos como si fuerán redes distintas. Lógicamente son LANs separadas aunque físicamente compartan el aparato.
- Túneles en general: cualquier técnica que mete un protocolo dentro de otro para cruzar una red que no lo entiende.

Ninguna "rompe" el modelo OSI: todas se explican cómo capas agregando encabezados. Cuando las estudies a fondo en otras unidades, vuelve a esta idea y verás que ya las entiendes por anticipado.

Ejemplos paso a paso

Ejemplo 1: ver el saludo TCP con netstat (Windows y Linux)

El comando netstat muestra las conexiones activas de tu equipo: literalmente puedes ver la capa 4 trabajando.

```
C:\Users\esteban> netstat -an | findstr ESTABLISHED
```

Salida típica (simplificada):

TCP	192.168.1.45:51234	142.250.0.4:443	ESTABLISHED
TCP	192.168.1.45:51235	93.184.216.34:443	ESTABLISHED

Línea por línea:

- "TCP": el protocolo de transporte de esta conexión (capa 4).

- "192.168.1.45:51234": tu IP privada y un puerto origen alto y efímero (51234), asignado automáticamente a tu navegador. Cada conexión usa uno distinto.
- "142.250.0.4:443": la IP del servidor y el puerto 443 (HTTPS). Ahí ves la capa 3 (IPs) y la capa 4 (puertos) juntas en un socket.
- "ESTABLISHED": la conexión completo el saludo de tres pasos y está transfiriendo datos.

En Linux es casi igual:

```
esteban@laptop:~$ netstat -tun | head -5
```

Las opciones -t (TCP), -u (UDP), -n (numérico, sin resolver nombres) te dan la misma vista. Prueba también `netstat -an | findstr LISTENING` (Windows) para ver que puertos tiene abiertos tu propia máquina: cada línea LISTENING es un servicio esperando conexiones (capa 4 y 7 trabajando juntas).

Ejemplo 2: DNS en acción con nslookup

DNS es el protocolo de capa de aplicación que traduce nombres a IPs. Vamos a verlo trabajar:

```
C:\Users\esteban> nslookup www.ejemplo.com
```

Salida típica:

```
Servidor:  router.lan
Address:  192.168.1.1

Respuesta no autoritativa:
Nombre:  www.ejemplo.com
Address:  93.184.216.34
```

Línea por línea:

- "Servidor: router.lan / 192.168.1.1": tu computadora le preguntó al DNS configurado, que es tu router (te lo asignó por DHCP). La consulta viajó por UDP al puerto 53 (capa 4) dentro de un paquete IP (capa 3) en una trama Ethernet (capa 2).
- "Respuesta no autoritativa": la respuesta vino de la cache (del router o del proveedor), no del servidor dueño del dominio. Es normal y es lo que hace rápido a DNS.
- "Address: 93.184.216.34": la IP que tu navegador usará para abrir la conexión TCP. Sin este paso, no hay web.

Prueba de diagnóstico: si ``ping 8.8.8.8`` funciona pero ``nslookup www.google.com`` falla, tu problema es 100% DNS (capa de aplicación), no de conectividad. La solución típica: cambiar los DNS a unos públicos (8.8.8.8 de Google o 1.1.1.1 de Cloudflare) en tu configuración de red o en el router.

En Linux el equivalente moderno es ``dig``:

```
esteban@laptop:~$ dig www.ejemplo.com +short
93.184.216.34
```

Ejemplo 3: la tabla ARP, el puente entre capa 3 y capa 2

Recuerda: para enviar un paquete IP dentro de tu LAN, tu equipo necesita la MAC del destino. La tabla ARP guarda esas traducciones:

```
C:\Users\esteban> arp -a
```

Salida típica (simplificada):

```
Interfaz: 192.168.1.45 --- 0xa
  Direccion de Internet      Direccion fisica      Tipo
  192.168.1.1                aa-bb-cc-11-22-33     dinamico
  192.168.1.50                4c-72-b9-8a-1f-3e     dinamico
```

Línea por línea:

- "192.168.1.1 -> aa-bb-cc-11-22-33": tu router. Cuando mandas un paquete a Internet, la trama Ethernet lleva como destino esta MAC (capa 2: solo hasta el siguiente salto), aunque el paquete IP lleve como destino la IP del servidor final (capa 3: de extremo a extremo). Esta línea es el encapsulamiento en vivo.
- "dinámico": la entrada la aprendió sola por protocolo ARP y caduca con el tiempo. Si fuera "estático", alguien la configuró a mano.

En Linux: ``ip neigh`` muestra lo mismo. Utilidad práctica: si cambias un router y "no hay Internet" aunque todo se ve bien, una entrada ARP vieja (la IP del router asociada a la MAC del aparato anterior) puede ser la culpable; borrar la tabla ARP (``arp -d *`` en Windows) lo resuelve.

Ejemplo 4: leer una captura conceptual capa por capa

No necesitas instalar nada para este ejemplo: vamos a "leer" como lo haría Wireshark un ping entre tu PC (192.168.1.45, MAC 4c:72:b9:8a:1f:3e) y tu router (192.168.1.1, MAC aa:bb:cc:11:22:33):

```
Trama Ethernet (capa 2):
  MAC destino: aa:bb:cc:11:22:33 (el router, siguiente salto)
  MAC origen: 4c:72:b9:8a:1f:3e (tu PC)
Paquete IP (capa 3):
  IP origen: 192.168.1.45
  IP destino: 192.168.1.1
  TTL: 128
  Protocolo: 1 (ICMP)
Mensaje ICMP (carga util):
  Tipo: 8 (echo request / ping)
```

Observa el encapsulamiento: el mensaje ICMP va dentro del paquete IP, que va dentro de la trama Ethernet. Cada capa agrega su encabezado. La respuesta del router sería idéntica pero con origen y destino intercambiados y tipo ICMP 0 (echo reply). Si abres Wireshark algún día y capturas un ping, verás exactamente estas líneas: ahora ya sabes leerlas.

Ejemplo 5: detectar un problema de MTU con ping

Cuándo una página carga a medias o una VPN se conecta pero no pasa tráfico, sospecha MTU. La prueba: mandar pings cada vez más grandes con prohibición de fragmentar.

En Windows:

```
C:\Users\esteban> ping -f -l 1472 8.8.8.8
```

- "-f": no fragmentar. "-l 1472": 1472 bytes de datos (más 28 de encabezados IP+ICMP = 1500, el MTU de Ethernet).

Si responde, el camino soporta 1500. Si dice "es necesario fragmentar el paquete pero se estableció DF", el camino tiene un MTU menor (típico en VPNs o túneles PPPoE). Vas bajando el tamaño (1400, 1300...) hasta que responda: ese es tu MTU real. En Linux:

```
esteban@laptop:~$ ping -M do -s 1472 -c 4 8.8.8.8
```

"-M do" equivale a no fragmentar. Este ejemplo usa capas 3 (IP, fragmentación, MTU) y muestra cómo un concepto teórico se convierte en un comando de diagnóstico real.

Ejemplo 6: ver tú ruta por defecto (la capa 3 de tu PC)

Tu computadora decide a dónde mandar cada paquete con su tabla de rutas:

```
C:\Users\esteban> route print -4
```

Salida simplificada (la línea que importa):

Destino de red	Mascara de red	Puerta de enlace	Interfaz
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.45

Esa línea 0.0.0.0 es la ruta por defecto: "todo lo que no sea mi red local, mandalo al router 192.168.1.1". Es la configuración de capa 3 más importante de tu equipo, y normalmente la pone el DHCP automáticamente. Si alguien la borra o la pone mal, tendrás red local pero no Internet: síntoma clásico de "todo se ve bien pero no sale". En Linux: `ip route` muestra lo mismo en una línea (`default via 192.168.1.1 dev wlan0`).

Ejemplo 7: probar si un puerto está abierto (diagnóstico de capa 4)

El ping te dice si hay red (capa 3), pero no si el servicio escucha. Para eso pruebas el puerto directamente con telnet o PowerShell:

```
C:\Users\esteban> telnet 192.168.1.10 80
```

Si la pantalla se queda en negro (o dice "conectado"), el puerto 80 de ese servidor responde: la capa 4 está bien y hay un servicio web escuchando. Si dice "no se puede abrir la conexión", el puerto está cerrado o un firewall lo bloquea. En Windows modernas telnet no viene instalado; la alternativa con PowerShell:

```
PS C:\Users\esteban> Test-NetConnection 192.168.1.10 -Port 80
```

Salida:

```
TcpTestSucceeded : True
```

"True" significa que el saludo TCP se completó: hay conectividad de extremo a extremo hasta ese servicio. Este es el paso que sigue al ping en todo diagnóstico serio: ping OK + puerto cerrado = "la red llega, la aplicación no". En Linux puedes usar `nc -zv 192.168.1.10 80` con el mismo propósito.

Ejemplo 8: ver el HTTP crudo con curl (capa de aplicación al desnudo)

El comando curl te muestra la conversación HTTP sin el maquillaje del navegador:

```
esteban@laptop:~$ curl -v http://www.ejemplo.com/ 2>&1 | head -20
```

Salida típica (simplificada):

```
* Trying 93.184.216.34:80...
* Connected to www.ejemplo.com (93.184.216.34) port 80
> GET / HTTP/1.1
> Host: www.ejemplo.com
< HTTP/1.1 200 OK
< Content-Type: text/html
```

Línea por línea:

- "Trying 93.184.216.34:80": curl ya resolvió el DNS y va a abrir TCP al puerto 80 (capas 3 y 4 en acción, invisibles pero presentes).
- "Connected": el saludo de tres pasos se completó.
- "> GET / HTTP/1.1": la petición HTTP cruda, lo que tu navegador manda en cada clic (él ">" indica datos que salen).
- "< HTTP/1.1 200 OK": la respuesta del servidor (él "<" indica datos que llegan); 200 significa éxito.

Con este ejemplo ves la capa 7 sin intermediarios y entiendes que el navegador no es magia: solo es un programa que habla HTTP por ti. En Windows, curl viene incluido en versiones recientes y funciona igual desde cmd o PowerShell.

Ejemplo 9: ipconfig /all, tu configuración vista por capas

El comando que ya conoces tiene una versión detallada que muestra protocolos de capa de aplicación funcionando:

```
C:\Users\esteban> ipconfig /all
```

Salida típica (simplificada):

Adaptador de LAN inalámbrica Wi-Fi:

```
Direccion IPv4. . . . . : 192.168.1.45
Mascara de subred . . . . . : 255.255.255.0
Puerta de enlace . . . . . : 192.168.1.1
Servidores DNS. . . . . : 192.168.1.1
DHCP habilitado . . . . . : si
Concesion obtenida. . . . . : sabado, 19 de septiembre de 2026 08:12:33
```

Lectura por capas: la IPv4, la máscara y la puerta de enlace son tu configuración de capa 3; "Servidores DNS" te dice a quién le preguntas los nombres (capa de aplicación, protocolo DNS); "DHCP habilitado: si" y la fecha de concesión te muestran que el protocolo DHCP (capa de aplicación, puertos UDP 67/68) te asignó todo automáticamente y cuando. Si el DNS apuntará a una IP que no responde, ya sabes por qué las páginas no abren aunque el ping a IPs funcione. Este comando es el parte médico completo de tu conexión: ante cualquier falla, es lo primero que un técnico experimentado pide ver.

Práctica

1. Ordeña las 7 capas del modelo OSI de la 1 a la 7 con su función en una frase, y escribe una mnemotecnia propia para recordarlas.

SOLUCIÓN: 1 Física: transmite bits por el medio. 2 Enlace: tramas dentro de la red local con direcciones MAC. 3 Red: paquetes entre redes con direcciones IP y ruteo. 4 Transporte: entrega de extremo a extremo, TCP confiable o UDP rápido, con puertos. 5 Sesión: administra inicio, mantenimiento y cierre de las conversaciones. 6 Presentación: traduce formatos, comprime y cifra. 7 Aplicación: protocolos que usan los programas (HTTP, DNS, correo). Tu mnemotecnia puede ser cualquiera mientras fije las iniciales F-E-R-T-S-P-A (de abajo hacia arriba) o A-P-S-T-R-E-F (de arriba hacia abajo); por ejemplo "Felipe Está Raro, Toma Sopa Para Almorzar". Lo importante no es la frase bonita sino que salga automática cuando diagnostiques: en una falla real no hay tiempo de dudar.

2. Para cada dispositivo o concepto indica en qué capa OSI trabaja principalmente: switch, router, hub, dirección MAC, dirección IP, puerto TCP 443, cable UTP, protocolo HTTP, punto de acceso WiFi, firewall que filtra por IP.

SOLUCIÓN: Switch: capa 2 (reenvía tramas por MAC). Router: capa 3 (rutea paquetes por IP). Hub: capa 1 (repite bits sin entender nada). Dirección MAC: capa 2. Dirección IP: capa 3. Puerto TCP 443: capa 4 (los puertos viven en transporte). Cable UTP: capa 1.

HTTP: capa 7. Punto de acceso WiFi: capa 2 (puentea tramas entre aire y cable). Firewall que filtra por IP: capas 3 y 4 (mira IPs y puertos). Si dudaste en alguna, vuelve a la regla: pregunta que dirección o decisión usa el aparato; si usa MAC es capa 2, si usa IP es capa 3, si usa puertos es capa 4. Este ejercicio es literalmente una pregunta típica de entrevista de soporte.

3. Explica la diferencia entre TCP y UDP y dí cuál usarías (y por qué) para: a) una transferencia de un archivo importante, b) una videollamada, c) consultar el DNS, d) tú banca en línea.

SOLUCIÓN: TCP es orientado a conexión, confirma recepción y retransmite: llega todo, en orden, más lento. UDP manda sin confirmar: rapidísimo, sin garantías. a) Archivo importante: TCP, porque no se puede perder ni un byte; la velocidad extra no compensa un archivo corrupto. b) Videollamada: UDP, porque importa la fluidez en tiempo real; mejor perder un fragmento de imagen que pausar todo esperando retransmisión. c) DNS: UDP, porque son consultas minúsculas de pregunta-respuesta donde montar una conexión TCP sería más costoso que el dato mismo. d) Banca en línea: TCP (con HTTPS/TLS encima), porque cada dato debe llegar íntegro y el cifrado necesita una base confiable.

4. Dibuja el proceso de encapsulamiento cuando tu PC (IP 192.168.1.45, MAC 4c:72:b9:8a:1f:3e) pide una página al servidor 93.184.216.34 a través de tu router (IP 192.168.1.1, MAC aa:bb:cc:11:22:33). Indica que encabezado agrega cada capa y que PDU resulta.

SOLUCIÓN: Datos HTTP ("GET / ...") -> capa 4 agrega encabezado TCP (puerto origen efímero, puerto destino 443, secuencia): resulta un segmento. -> capa 3 agrega encabezado IP (origen 192.168.1.45, destino 93.184.216.34, TTL): resulta un paquete. -> capa 2 agrega encabezado Ethernet (MAC origen 4c:72:b9:8a:1f:3e, MAC destino aa:bb:cc:11:22:33 que es el router, el siguiente salto) más tráiler de verificación: resulta una trama. -> capa 1 convierte a bits y transmite. Puntos que califican: el orden de los encabezados, que la MAC destino es la del router (no la del servidor) mientras la IP destino si es la del servidor final, y los nombres correctos de PDU (segmento, paquete, trama, bits).

5. Un usuario reporta: "el WiFi se conecta pero no abre ninguna página; el ping a 8.8.8.8 si responde". Aplica el diagnóstico por capas y dí dónde está probablemente el problema y como lo confirmarías.

SOLUCIÓN: Recorre de abajo hacia arriba. Capa 1 y 2: el WiFi se conecta, hay enlace. Capa 3: el ping a 8.8.8.8 (una IP numérica) responde, así que hay IP, ruta y salida a

Internet: la capa 3 funciona. El fallo aparece al usar nombres (páginas), así que el problema está en la capa de aplicación: el DNS no resuelve. Confirmación: ejecuta `nslookup www.google.com`; si falla o tarda, confirmado. Solución: revisar los DNS configurados (`ipconfig /all`) y probar con DNS públicos (8.8.8.8) en la PC o en el router. Nota profesional: este caso demuestra por qué se prueba con IP numérica y con nombre por separado; quien solo prueba "abrir Google" no puede distinguir una falla de red de una falla de DNS.

6. Completa la tabla de correspondencia OSI vs TCP/IP y explica con tus palabras por qué existen dos modelos.

SOLUCIÓN: OSI 7 Aplicación + 6 Presentación + 5 Sesión corresponden a TCP/IP 4 Aplicación. OSI 4 Transporte = TCP/IP 3 Transporte. OSI 3 Red = TCP/IP 2 Internet. OSI 2 Enlace + 1 Física = TCP/IP 1 Acceso a la red. Existen dos porque nacieron en momentos distintos con propósitos distintos: TCP/IP se desarrolló primero, funcionando, para ARPANET/Internet, y es lo que implementan los sistemas reales; OSI llegó después como estándar internacional más detallado y pedagógico. La industria se quedó con TCP/IP por inercia de lo que ya funcionaba, y la enseñanza usa OSI porque sus 7 capas explican mejor cada función. Tú usas OSI para pensar y diagnosticar, y TCP/IP para configurar.

7. Explica qué es la PDU y nombra la PDU de cada capa con un ejemplo de protocolo que la genere.

SOLUCIÓN: PDU (unidad de datos de protocolo) es el nombre que recibe el dato en cada capa. Capa 4: segmento (TCP) o datagrama (UDP); ejemplo: un segmento TCP hacia el puerto 443. Capa 3: paquete; ejemplo: un paquete IP con destino 8.8.8.8. Capa 2: trama; ejemplo: una trama Ethernet con MAC destino del router. Capa 1: bits; ejemplo: los pulsos eléctricos en el cable UTP. En capas 5 a 7 se habla simplemente de datos. Usar el término correcto importa porque cada dispositivo procesa su PDU: el switch mira tramas, el router mira paquetes; decir "paquete" para todo es el error típico de principiante.

8. En una captura ves que tu PC manda SYN al puerto 80 de un servidor y nunca llega respuesta. En otra captura ves SYN, luego SYN-ACK, pero tu PC nunca manda el ACK final. Qué significa cada caso y dónde buscarías la falla?

SOLUCIÓN: Caso 1 (SYN sin respuesta): el servidor no está escuchando en el puerto 80, está apagado, o un firewall en el camino bloquea. Buscar: si el servicio web está arriba en el servidor, reglas del firewall, y si la IP destino es correcta. Caso 2 (falta el ACK final): el servidor sí respondió, así que el camino de ida funciona, pero tu respuesta no

regresa o no se procesa: posible problema de ruteo de retorno, NAT mal configurado, o firewall que deja salir pero no entrar la respuesta. La diferencia es diagnóstica: el caso 1 apunta al destino o al camino de ida; el caso 2 apunta al camino de regreso. Así se lee una captura como profesional: cada paquete ausente tiene significado.

9. Tu jefe te dice: "monta un servidor web en la oficina para que se vea desde Internet". Lista que configurarías en cada capa (1 a 4 y 7) para que funcione.

SOLUCIÓN: Capa 1: cable UTP del servidor al switch, focos de enlace encendidos, nada de WiFi para un servidor (cable siempre). Capa 2: el switch aprende la MAC del servidor; verifica que el puerto negocie bien (1 Gbps full dúplex). Capa 3: IP fija al servidor (no DHCP, para que no cambie), puerta de enlace correcta, y en el router una redirección de puertos (port forwarding) del puerto 80/443 público hacia la IP privada del servidor, más la regla del firewall permitiendo ese tráfico entrante. Capa 4: el servicio web escuchando en los puertos 80 y 443 (verificable con netstat -an en el servidor). Capa 7: el servidor HTTP instalado y sirviendo la página, y si quieres nombre en vez de IP, un registro DNS apuntando a tu IP pública. Si algo falla, ya sabes en qué capa buscar: la mayoría de los "no se ve desde fuera" son capa 3 (falta el port forwarding) o capa 4 (firewall bloqueando el puerto).

10. Compara una videollamada que usa UDP con una descarga que usa TCP cuando la red se congestiona. Que le pasa a cada una y por qué?

SOLUCIÓN: Con congestión hay pérdida de paquetes y más latencia. La descarga TCP: detecta la pérdida, retransmite lo perdido y baja su ritmo (control de congestión); la descarga tarda más pero el archivo llega íntegro. La videollamada UDP: no retransmite ni baja el ritmo por sí sola; los paquetes perdidos se notan como imagen congelada o voz robótica, pero la llamada sigue en tiempo real sin pausas largas. Por eso en una red saturada "el Netflix se traba pero sigue" (usa TCP con buffer) y "la llamada se oye mal pero no se corta" (UDP). La moraleja de diseño: TCP sacrifica velocidad por integridad; UDP sacrifica integridad por tiempo real. Elegir bien entre ellos es una decisión de capa 4 que define la experiencia del usuario.

11. Explica por qué el switch no necesita entender direcciones IP y por qué el router sí necesita entender direcciones MAC, usando el concepto de encapsulamiento.

SOLUCIÓN: El switch trabaja en capa 2: su trabajo es leer la MAC destino de la trama y reenviarla al puerto correcto; nunca necesita abrir el paquete IP porque la decisión de reenvío se toma con el encabezado Ethernet. El router trabaja en capa 3: para mandar el paquete al siguiente salto necesita construir una trama Ethernet nueva, y para eso debe conocer la MAC del siguiente router o destino final, que obtiene por ARP. En resumen:

cada dispositivo opera hasta su capa; el switch se detiene en la trama, el router abre hasta el paquete pero igual necesita la capa 2 para transmitir físicamente. Esto demuestra el encapsulamiento en acción: las capas inferiores son el "servicio de mensajería" que usan las superiores sin que estas sepan los detalles.

12. Un técnico dice "voy a revisar la capa 8". Sabiendo que el modelo OSI tiene 7 capas, a que se refiere en broma y por qué ese chiste existe en la industria?

SOLUCIÓN: La "capa 8" es el usuario: el chiste significa que el problema no está en la red sino en quién la usa (cable desconectado por accidente, WiFi apagado en la laptop, contraseña mal escrita, el monitor apagado). Existe porque una parte real de los reportes se resuelve verificando lo obvio del lado humano antes de tocar configuraciones. La lección profesional detrás del chiste: en tu diagnóstico por capas, incluye siempre una "capa 0 humana": verifica que el equipo este encendido, el cable conectado, el WiFi activado y las credenciales correctas antes de diagnosticar protocolos. Te ahorrará más tiempo del que imaginas y te evitará la vergüenza de reinstalar drivers cuando solo había que prender el switch.

Resumen de la unidad

13. Sin ver tus apuntes, escribe de memoria las 7 capas de OSI (1 a 7), las 4 de TCP/IP y la PDU de cada nivel (segmento, paquete, trama, bits). Luego verifica y marca en que te equivocaste.

SOLUCIÓN: OSI: 1 Física, 2 Enlace, 3 Red, 4 Transporte, 5 Sesión, 6 Presentación, 7 Aplicación. TCP/IP: 1 Acceso a la red, 2 Internet, 3 Transporte, 4 Aplicación. PDU: capa 4 segmento (o datagrama en UDP), capa 3 paquete, capa 2 trama, capa 1 bits. Si fallaste en el orden, usa tu mnemotecnica ("Felipe Está Raro, Toma Sopa Para Almorzar"); si fallaste en las PDU, recuerda "Si Pintas Tu Bodega". Repite este ejercicio una vez al día durante una semana y quedará grabado para siempre: es el conocimiento que más vas a usar en entrevistas y diagnósticos.

El modelo OSI describe la comunicación en 7 capas: Física (bits), Enlace (tramas, MAC), Red (paquetes, IP, ruteo), Transporte (segmentos, TCP/UDP, puertos), Sesión (conversaciones), Presentación (formatos, cifrado) y Aplicación (HTTP, DNS, correo). El modelo TCP/IP, el que realmente corre en Internet, usa 4: Acceso a la red, Internet, Transporte y Aplicación. La correspondencia es directa: las tres capas altas de OSI caben en la Aplicación de TCP/IP, y las dos bajas en Acceso a la red.

Los protocolos clave por capa TCP/IP: Ethernet, WiFi y ARP en acceso; IP, ICMP y NAT en Internet; TCP (confiable, con saludo de tres pasos SYN, SYN-ACK, ACK) y UDP (rápido, sin garantías) en transporte; HTTP/HTTPS, DNS, DHCP, FTP, SSH y correo en aplicación. Los puertos (como el 443 de HTTPS o el 53 de DNS) identifican la aplicación destino dentro de cada equipo, y el socket (IP + puerto) identifica cada conversación.

El encapsulamiento baja los datos agregando encabezados por capa (datos -> segmento -> paquete -> trama -> bits) y el desencapsulamiento los sube quitándolos; cada capa solo lee su propio encabezado. Regla de oro: la MAC destino cambia en cada salto (siempre es el siguiente equipo), pero la IP destino se mantiene de extremo a extremo. El MTU (1500 bytes en Ethernet) limita el tamaño del paquete; si algo no cabe, se fragmenta.

Diagnóstica siempre de abajo hacia arriba: físico, enlace, red, transporte, aplicación. Con ipconfig, ping (por IP y por nombre para separar red de DNS), tracert, nslookup/dig, netstat, arp y route ya puedes ubicar fallas en la capa exacta sin adivinar. Piensa en OSI, configura en TCP/IP. Diagnóstica siempre de abajo hacia arriba: físico, enlace, red, transporte, aplicación. Con ipconfig, ping (por IP y por nombre para separar red de DNS), tracert, nslookup/dig, netstat, arp y route ya puedes ubicar fallas en la capa exacta sin adivinar. Memoriza los 10 puertos esenciales (22, 25, 53, 67/68, 80, 110, 143, 443, 3389, 20/21) porque son el vocabulario diario de la capa 4.

Piensa en OSI, configura en TCP/IP: esa frase resume la relación entre los dos modelos y tu trabajo con ellos. El modelo no es un adorno académico: es el checklist que convierte reportes vagos ("no sirve el Internet") en diagnósticos precisos ("falla de DNS en capa de aplicación, la capa 3 responde"). Cada vez que resuelvas un problema recorriendo las capas en orden, estarás aplicando esta unidad sin darte cuenta.

Un último consejo para llevarte: cuando estudies las siguientes unidades (direccionamiento IP, ruteo, switching, WiFi, seguridad), ubica cada tema nuevo en su capa antes de memorizar detalles. "Esto es capa 2", "esto es capa 3": ese reflejo hace que todo el libro se organice solo en tu cabeza, en lugar de ser una pila de datos sueltos. Los técnicos que piensan por capas aprenden más rápido, diagnostican mejor y explican con claridad a clientes y jefes. Ya tienes el mapa y el idioma; lo que sigue es practicarlos todos los días.

En la siguiente unidad entrarás de lleno a la capa 3: direccionamiento IP, máscaras y subredes, donde los números se vuelven tu herramienta diaria.

UNIDAD 3: Medios físicos, cableado y topologías

Piensa en la última vez que se quedó sin internet tu casa. Llamaste a tu proveedor, te dijeron que reiniciarás el módem, nada funciona, y al final llegó el técnico. El técnico no abrió una ventana de configuración complicada ni escribió comandos raros: revisó el cable que entra a tu casa, lo movió un poco, quizá lo volvió a ponchar, y la señal regresó. Esa escena se repite todos los días en México: el técnico de Telmex o de Totalplay que instala la fibra, el ingeniero que cablea una oficina nueva en Guadalajara, el dueño del ciber que conecta veinte computadoras para que los chavos jueguen en red. Detrás de todo lo "inalámbrico" y lo "virtual" que parece magia, siempre hay algo físico: un cable, un conector, una antena.

Esta unidad trata exactamente de eso: de lo físico. De los medios por los que viajan los datos, de los cables y conectores que vas a tocar con tus manos, y de la forma en que se conectan los equipos entre sí. Son la clase 7 (medios de transmisión), la clase 8 (cables y conectores) y la clase 9 (topologías y dispositivos básicos) del curso. Puede sonar menos emocionante que configurar un router, pero te voy a decir algo que todo técnico con experiencia sabe: la mayoría de los problemas de red están en la capa física. Un cable mal ponchado, un conector flojo, una categoría de cable insuficiente o una topología mal planeada tumban redes enteras, y ningún comando del mundo los arregla. Quien domina lo físico diagnostica en minutos lo que otros tardan horas en adivinar.

En la vida real esto se traduce en trabajo. Cuando una empresa abre oficinas nuevas, alguien tiene que decidir qué cable comprar, cuántos metros, qué categoría, dónde van los puntos de red y cómo se conectan. Cuando el internet de una escuela falla cada que llueve, alguien tiene que descubrir que el cable UTP pasa junto a un tubo de luz y la interferencia lo mata. Cuando un negocio quiere conectar su bodega que está a dos cuadras, alguien tiene que saber que el cobre no llega tan lejos y que la respuesta es fibra óptica. Ese alguien puedes ser tú, y esta unidad te da las bases para serlo.

Vas a aprender los cuatro grandes medios de transmisión: el par trenzado de cobre (el cable azul que ves en todas las oficinas), el cable coaxial (el de la televisión por cable), la fibra óptica (la que usan Telmex y Totalplay para llevarte internet rapidísimo) y los medios inalámbricos (el Wi-Fi de tu casa). Vas a comparar sus ventajas y desventajas con números reales: velocidades, distancias y costos. Después vas a meter las manos: categorías de cable Cat5e, Cat6 y Cat6a, el conector RJ45, las normas de colores T568A y T568B, la diferencia entre cable directo y cruzado, las herramientas que necesitas y el procedimiento completo para ponchar un cable paso a paso, como lo hace un profesional. Y para cerrar, las topologías: las

formas en que se organizan las redes (bus, estrella, anillo, malla e híbrida), los dispositivos más básicos (hub, repetidor y punto de acceso) y la razón por la que la topología de estrella domina el mundo actual.

Una analogía te va a acompañar toda la unidad: piensa en la red como un sistema de carreteras. Los medios de transmisión son el tipo de camino (terracería, carretera de dos carriles, autopista). Los cables y conectores son la construcción misma del camino y sus señalamientos. Las topologías son el mapa: cómo se conectan las ciudades entre sí. Un buen ingeniero de redes, igual que un buen ingeniero civil, tiene que dominar las tres cosas. Empecemos por el camino.

Explicación detallada

Qué es un medio de transmisión

Un medio de transmisión es el camino físico por el que viajan las señales que llevan tus datos. Todo lo que mandas por una red (un mensaje de WhatsApp, un video de YouTube, un archivo de la oficina) se convierte en algún tipo de señal: pulsos eléctricos que corren por un cable de cobre, destellos de luz que viajan por un hilo de vidrio, u ondas de radio que cruzan el aire. El medio es lo que transporta esa señal del punto A al punto B.

Hay tres familias de señales y cada una usa su medio. Las señales eléctricas viajan por conductores metálicos, normalmente cobre: es el caso del par trenzado y del cable coaxial. Las señales luminosas viajan por fibra óptica, que es vidrio o plástico especial. Las ondas electromagnéticas viajan por el aire sin necesidad de cable: es el caso del Wi-Fi, el Bluetooth y los enlaces de microondas. No hay un medio "mejor" en absoluto: cada uno es la mejor opción para cierta distancia, cierta velocidad y cierto presupuesto.

Tres conceptos técnicos te van a perseguir en todo este tema, así que dejálos claros desde ahora. La atenuación es la pérdida de fuerza de la señal conforme avanza por el medio: como gritar en un túnel largo, entre más lejos llega, más débil se escucha. Por eso cada medio tiene una distancia máxima. La interferencia es el ruido externo que se mete a la señal y la deforma: motores eléctricos, cables de luz, hornos de microondas y hasta otros cables de red cercanos. Y el ancho de banda es la capacidad del medio, cuánta información puede pasar por él en un segundo, y se mide en bits por segundo (bps): mientras más ancho de banda, más rápido viajan tus datos. Cuando compares medios, compara siempre estos tres: que tanta distancia aguantan sin atenuarse, que tan sensibles son a la interferencia y cuánto ancho de banda ofrecen.

Un error común de principiante es pensar que "el cable es el cable" y que cualquiera sirve. No es así: poner un cable barato de categoría vieja en una instalación nueva es como construir una autopista con un solo carril. Funciona el primer día, pero cuando la empresa crece y necesita más velocidad, hay que romper paredes y volver a cablear. La buena práctica de la industria es cablear pensando en el futuro: instalar hoy cable de categoría superior a la que necesitas, porque el cable dentro de la pared o del techo se queda ahí diez o quince años, mientras que los equipos se cambian cada tres o cuatro.

El par trenzado: UTP y STP

El par trenzado es el caballo de batalla de las redes: el cable más usado del planeta para conectar computadoras en oficinas, escuelas y casas. Si has visto un cable de red azul o amarillo conectado a una computadora, eso es par trenzado. Por dentro lleva ocho hilos de cobre delgados, agrupados en cuatro pares, y cada par está trenzado como una trenza de cabello. Ese trenzado no es decoración: es la genialidad del invento.

Para entender el trenzado, imagina dos personas hablando por teléfono con mucho ruido alrededor. Si cada una grita por su cuenta, el ruido las confunde. Pero si hablan de forma coordinada, el cerebro filtra el ruido. Algo parecido pasa en el cable: cada par lleva la misma señal en dos versiones opuestas (una positiva y una negativa). La interferencia externa afecta a los dos hilos del par por igual, y al llegar al destino el equipo resta una señal de la otra: la interferencia, que llegó igual a ambos hilos, se cancela sola, mientras que la señal útil, que viaja invertida, se refuerza. A esto se le llama cancelación de interferencia, y funciona mejor mientras más vueltas tenga el trenzado. Por eso los pares dentro del cable tienen diferente número de vueltas: así evitan interferirse entre ellos.

Existen dos grandes tipos. El UTP (Unshielded Twisted Pair, par trenzado sin blindaje) no lleva ninguna protección metálica: solo los hilos, su forro de colores y la cubierta exterior. Es barato, flexible, fácil de instalar y suficiente para la mayoría de oficinas y casas. El STP (Shielded Twisted Pair, par trenzado con blindaje) lleva una malla o lámina metálica alrededor de los pares que actúa como escudo contra la interferencia electromagnética. Es más caro, más rígido, más difícil de instalar (el blindaje tiene que conectarse a tierra física para funcionar) y se usa donde hay mucha interferencia: fábricas con motores grandes, hospitales con equipos médicos, o instalaciones donde el cable pasa pegado a cables eléctricos de alta potencia. También existe el FTP, una versión intermedia con una lámina general. Regla práctica: si no hay una razón clara para blindar, usa UTP; es lo que vas a encontrar en nueve de cada diez instalaciones.

Los colores de los hilos siguen un código estricto: cada par tiene un hilo de color sólido y uno blanco con franja de ese color. Los cuatro pares son naranja, verde, azul y café. Así quedan:

blanco-naranja con naranja, blanco-verde con verde, blanco-azul con azul, blanco-café con café. Memoriza estos colores porque los vas a usar al ponchar, y un solo hilo fuera de su lugar deja el cable inservible.

Ventajas del par trenzado: es barato (el cable más económico por metro), fácil de conseguir en cualquier tienda de electrónica, flexible y fácil de pasar por muros y techos, y con las categorías modernas alcanza velocidades de hasta 10 Gbps. Desventajas: distancias cortas (máximo 100 metros por tramo, incluyendo los cables de parcheo), vulnerable a la interferencia en su versión UTP, y el cobre es atractivo para los amantes de lo ajeno en instalaciones expuestas. Para redes locales de oficina, sin embargo, no tiene rival: por eso domina el cableado estructurado en todo el mundo.

El cable coaxial

El cable coaxial es el veterano de las redes: fue el primer medio usado para conectar computadoras en red local, mucho antes de que el par trenzado lo desplazara. Hoy casi no se usa para redes de computadoras, pero lo ves todos los días: es el cable redondo, grueso, que lleva la señal de televisión por cable a tu casa y el que usan muchos proveedores para darte internet por cable (tecnología DOCSIS). Si en tu casa el internet llega por él mismo cable que la televisión, estás usando coaxial.

Su estructura es como un tubo dentro de otro tubo. Al centro va un conductor de cobre sólido o trenzado, rodeado por un aislante plástico grueso. Sobre el aislante va una malla metálica trenzada que funciona como blindaje, y todo queda cubierto por una funda exterior protectora. La gracia del diseño es geométrica: el conductor central y la malla exterior comparten el mismo eje (de ahí "co-axial"), y esa malla bloquea muy bien la interferencia externa. Por eso el coaxial aguanta bien en ambientes ruidosos y puede llevar señales a distancias mayores que el par trenzado sin tanto problema.

En redes se usaron dos tipos históricos: el Thicknet (grueso, para troncales) y el Thinnet (delgado, más manejable), con conectores BNC en forma de bayoneta. Hoy el conector más común es el tipo F, el de rosca que enroscas al módem o a la televisión. Los cables más usados son el RG-6 (para televisión e internet por cable) y el RG-59 (más delgado, para distancias cortas como cámaras de seguridad analógicas).

Ventajas del coaxial: excelente blindaje natural contra interferencia, distancias decentes (hasta 500 metros en las versiones de red antiguas, y varios cientos de metros en TV por cable), y una infraestructura ya instalada en millones de hogares. Desventajas: es grueso y poco flexible, más caro que el par trenzado, difícil de instalar en topologías modernas (un solo cable dañado tumbaba toda la red en las topologías de bus antiguas), y sus velocidades quedaron

atrás frente a la fibra. Su futuro en redes de datos es limitado, pero mientras la televisión por cable exista, el coaxial seguirá entrando a las casas.

Un error común es pensar que "cable coaxial" es sinónimo de "cable viejo e inútil". En la práctica mexicana, miles de hogares reciben su internet por coaxial con velocidades de cientos de megas, y funciona muy bien. La lección es no despreciar un medio por viejo: lo que importa es si cumple con la velocidad y distancia que necesitas.

La fibra óptica: monomodo y multimodo

La fibra óptica es la reina de las telecomunicaciones modernas. Cuando el técnico de Telmex te instala "internet de fibra", está metiendo a tu casa un hilo de vidrio purísimo, más delgado que un cabello humano, por el que viajan pulsos de luz que llevan tus datos a la velocidad de la luz. Toda la columna vertebral del internet (los cables submarinos que cruzan océanos, las conexiones entre ciudades) es fibra óptica. Nada le compite en velocidad ni en distancia.

El principio es sencillo y hermoso: la luz queda atrapada dentro del hilo de vidrio por reflexión interna total, rebotando por las paredes como una pelota en un pasillo de espejos, y así viaja kilómetros sin salirse. Como la señal es luz y no electricidad, la fibra tiene dos superpoderes: es inmune a la interferencia electromagnética (puedes pasarla junto a cables de alta tensión sin problema) y no conduce electricidad (no hay riesgo de cortos ni de descargas, ideal para exteriores y para conectar edificios).

Hay dos tipos fundamentales y confundirlos es uno de los errores más caros del oficio. La fibra monomodo tiene un núcleo delgadísimo (unos 9 micras, la micra es la milésima parte de un milímetro) por el que solo cabe un rayo de luz, un solo "modo". Usa láser como fuente de luz, alcanza distancias enormes (decenas de kilómetros) y velocidades altísimas. Es la que usan los proveedores para largas distancias. Su cubierta exterior suele ser amarilla. La fibra multimodo tiene un núcleo más grueso (50 o 62.5 micras) por el que viajan varios rayos de luz al mismo tiempo, rebotando en ángulos distintos. Usa LED (más barato que el láser), es más económica en equipos y conectores, pero los rayos llegan con ligeros retrasos entre sí (dispersión modal) y eso limita la distancia: unos 550 metros como máximo en las versiones comunes, suficiente para dentro de un edificio o un campus. Su cubierta suele ser naranja o aqua (verde agua).

Los conectores de fibra también tienes que conocerlos: el SC (cuadrado, de inserción directa, muy común en instalaciones de proveedor), el LC (pequeño, el favorito en centros de datos porque ocupa poco espacio) y el ST (de bayoneta, redondo, común en instalaciones viejas). A diferencia del cobre, los conectores de fibra exigen limpieza quirúrgica: una mota de polvo en la punta puede tumbar el enlace, y los técnicos usan toallitas y microscopios especiales. Otra

diferencia: la fibra no se "poncha" con una pinza barata; se fusiona con una fusionadora que suelda los hilos con un arco eléctrico, un equipo que cuesta miles de dólares. Por eso la instalación de fibra la hacen técnicos especializados.

Ventajas de la fibra: velocidades gigantescas (de 1 Gbps a 400 Gbps y más), distancias larguísimas, inmunidad total a la interferencia, seguridad (es muy difícil interceptar la luz sin cortar el cable, y al cortarlo se nota de inmediato), y es delgada y ligera. Desventajas: costo alto de instalación y de equipos, fragilidad (el vidrio se rompe si lo doblas demasiado; hay un radio mínimo de curvatura que se debe respetar), instalación especializada y conectores delicados.

Buena práctica de la industria: usa fibra para troncales (backbone) entre pisos de un edificio, entre edificios de un campus y para enlaces largos; usa cobre para llegar al escritorio de cada usuario. Esa combinación (fibra en el centro, cobre en los bordes) es la arquitectura típica de una red empresarial bien diseñada.

Medios inalámbricos

Los medios inalámbricos transmiten datos por ondas de radio (o infrarrojas, en casos viejos) sin ningún cable físico. El Wi-Fi de tu casa, el Bluetooth de tus audífonos y los enlaces de microondas que conectan torres en los cerros son todos medios inalámbricos. Su gran promesa es la movilidad: conectarte sin estar atado a un cable.

El Wi-Fi opera principalmente en bandas de frecuencia: 2.4 GHz (llega más lejos y atraviesa mejor las paredes, pero es una banda congestionada y con más interferencia: hornos de microondas, Bluetooth y las redes de los vecinos compiten ahí), 5 GHz (más velocidad y menos congestión, pero menor alcance) y 6 GHz (la más nueva, rapidísima y limpia, pero de corto alcance). La velocidad real que obtienes depende de la distancia al punto de acceso, los obstáculos (cada pared de concreto le roba señal), la cantidad de dispositivos conectados (el aire es un medio compartido: todos los equipos se reparten el mismo ancho de banda) y la interferencia de otras redes.

Ventajas: movilidad total, instalación rapidísima (sin romper paredes ni pasar cables), ideal para dispositivos móviles y para lugares donde cablear es imposible o carísimo (una casa antigua, una plaza, un evento temporal). Desventajas: la velocidad es compartida y variable, el alcance es limitado (decenas de metros en interiores), es vulnerable a interferencia, y la seguridad exige más cuidado (las ondas cruzan las paredes y un vecino curioso podría intentar escuchar; por eso el cifrado WPA2/WPA3 es obligatorio, nunca dejes una red abierta en una empresa).

Error común de principiante: creer que "inalámbrico" significa "sin infraestructura física". Falso: cada punto de acceso Wi-Fi necesita un cable de red que lo alimente con datos (y muchas veces con energía eléctrica mediante PoE), y detrás de toda red Wi-Fi sería hay cableado estructurado de cobre o fibra. El aire es solo el último tramo. Otro error: poner un solo punto de acceso barato para cubrir una oficina de tres pisos y quejarse de qué "el Wi-Fi no sirve". El diseño inalámbrico serio calcula cuántos puntos de acceso se necesitan y dónde van.

Comparativa de medios: cuál usar y cuando

Aquí tienes una tabla comparativa con valores típicos para que tomes decisiones como profesional. Los números son aproximados y dependen de la categoría y la tecnología exacta, pero te dan el orden de magnitud correcto.

Medio	Velocidad típica	Distancia máxima	Costo relativo	Interferencia
Par trenzado UTP	1 a 10 Gbps	100 metros	Bajo	Media (sin blindaje)
Par trenzado STP	1 a 10 Gbps	100 metros	Medio	Baja (con blindaje)
Cable coaxial	100 Mbps a 1 Gbps	500 metros	Medio	Baja
Fibra multimodo	10 a 100 Gbps	550 metros	Alto	Nula (inmune)
Fibra monomodo	100 Gbps y más	40 km y más	Muy alto	Nula (inmune)
Inalámbrico Wi-Fi	100 Mbps a 1+ Gbps	30 a 100 metros	Bajo-medio	Alta (variable)

Cómo leer esta tabla en la vida real: para conectar las computadoras de una oficina, par trenzado UTP (barato y suficiente). Para subir del cuarto de telecomunicaciones de un piso al siguiente, fibra multimodo. Para conectar dos edificios separados por dos kilómetros, fibra monomodo sin dudar. Para dar movilidad a laptops y celulares, Wi-Fi complementando el cableado, nunca sustituyendolo del todo. Y el coaxial, donde ya exista infraestructura de TV por cable.

Categorías de cable: Cat5e, Cat6 y Cat6a

No todo el par trenzado es igual: se clasifica en categorías que garantizan cierto rendimiento. La categoría es como el "modelo" del cable, y usar la categoría correcta es una de las decisiones más importantes (y más económicas a largo plazo) de una instalación.

Cat5e (la "e" es de "enhanced", mejorado): soporta 1 Gbps hasta 100 metros y frecuencias de hasta 100 MHz. Fue el estándar de oficinas durante años y todavía lo encuentras instalado por todos lados. Hoy se considera la categoría mínima aceptable; para instalaciones nuevas ya no se recomienda.

Cat6: soporta 10 Gbps hasta 55 metros (y 1 Gbps hasta 100 metros), con frecuencias de hasta 250 MHz. Su trenzado es más apretado y suele llevar un separador plástico en forma de cruz por dentro que aísla los pares entre sí. Es el estándar recomendado para instalaciones nuevas de oficina.

Cat6a (la "a" es de "augmented", aumentado): soporta 10 Gbps en los 100 metros completos, hasta 500 MHz. Es más grueso y un poco más difícil de instalar, pero es la apuesta a futuro: si cableas hoy una oficina que va a durar quince años, Cat6a es la decisión inteligente.

Existen categorías superiores (Cat7, Cat8) para centros de datos con necesidades extremas, pero para el 95 por ciento de las instalaciones, la discusión real es Cat6 contra Cat6a. Regla de oro: nunca instales categoría inferior a Cat6 en obra nueva; la diferencia de precio del cable es mínima comparada con el costo de volver a cablear en cinco años.

Ojo con un detalle práctico: la categoría la determinan el cable Y los conectores Y la instalación. Un cable Cat6a ponchado con conectores baratos sin categoría, o instalado con dobleces muy cerrados, rinde como un cable inferior. La cadena es tan fuerte como su eslabón más débil.

El conector RJ45

El RJ45 es el conector transparente de plástico que va en los extremos del cable de red, el que hace "clic" al entrar al puerto de la computadora o del switch. Técnicamente es un conector 8P8C (8 posiciones, 8 contactos): ocho láminas doradas que perforan el aislamiento de los ocho hilos y hacen contacto eléctrico. Hay conectores para cable sólido (el de instalación fija en paredes, hilos rígidos) y para cable multifilar (el de los cables de parcheo flexibles, hilos trenzados finos); usar el tipo equivocado da conexiones inestables, así que revisa el empaque.

El conector lleva una pestana de plástico (el "seguro") que lo fija al puerto. Esa pestana se rompe con mirarla feo, y un conector sin pestana se sale solo y genera fallas intermitentes que vuelven loco a cualquiera: la red "se cae a ratos". Buena práctica: usa capuchones (boots) de goma que protegen la pestana, y si un cable pierde la pestana, vuelve a poncharlo; no lo dejes así "por mientras", porque ese "mientras" dura años.

Normas de ponchado: T568A y T568B

Los ocho hilos del cable deben colocarse en un orden exacto dentro del RJ45. Existen dos normas de orden, T568A y T568B, definidas por la industria de telecomunicaciones. Las dos funcionan igual de bien; lo importante es usar la misma en toda la instalación para no volverse loco.

Orden T568B (la más usada en México y América en general), viendo el conector de frente con la pestana hacia abajo, del pin 1 al pin 8:

1. Blanco-naranja
2. Naranja
3. Blanco-verde
4. Azul
5. Blanco-azul
6. Verde
7. Blanco-café
8. Café

Orden T568A, misma posición:

1. Blanco-verde
2. Verde
3. Blanco-naranja
4. Azul
5. Blanco-azul
6. Naranja
7. Blanco-café
8. Café

Fijate que la única diferencia es que los pares naranja y verde intercambian su lugar. Un truco para memorizar la B: "naranja primero". En la A, "verde primero". Si en un examen o en campo dudas, recuerda: en México, por defecto, poncha en B a menos que el cliente o el plano pida A. Y nunca mezcles: si un extremo está en A y el otro en B sin querer, acabas de fabricar un cable cruzado por accidente.

Cable directo vs cable cruzado

Con las dos normas claras, aparecen dos tipos de cable. El cable directo (straight-through) lleva el mismo estándar en ambos extremos: B en un lado y B en el otro (o A con A). Es el cable normal, el que usas para conectar una computadora a un switch, un switch a un router, o un punto de acceso a un switch. En una instalación típica, el 99 por ciento de los cables son directos.

El cable cruzado (crossover) lleva T568A en un extremo y T568B en el otro. Al cruzar los pares verde y naranja, lo que hace es conectar el transmisor de un equipo con el receptor del otro. Se inventó para conectar dos equipos "iguales" entre sí sin un switch en medio: computadora con computadora, o switch con switch. En los equipos viejos, si conectabas dos computadoras con un cable directo, los transmisores se hablaban entre ellos y nadie escuchaba, como dos personas gritando al mismo tiempo por teléfono.

Hoy casi no necesitas cables cruzados porque los equipos modernos traen Auto-MDIX: detectan automáticamente el tipo de cable y ajustan sus pines por software. Pero en exámenes de certificación y en equipos viejos que todavía circulan en escuelas y oficinas, la pregunta sigue apareciendo. Resumen práctico: equipos diferentes (PC a switch) usan directo; equipos iguales (PC a PC, switch a switch) usaban cruzado; y con Auto-MDIX, en la práctica moderna, el directo sirve para casi todo.

Herramientas para ponchar

Ponchar un cable es una habilidad manual que todo técnico de redes debe dominar. Estas son las herramientas, de la indispensable a la recomendable:

1. Ponchadora (crimpadora) RJ45: la pinza que presiona el conector y clava los contactos dorados en los hilos. Hay sencillas y económicas que hacen bien el trabajo; no necesitas la más cara para empezar.
2. Pelacables o navaja: para retirar la cubierta exterior sin dañar los hilos internos. La navaja sirve, pero el pelacables ajustable es más seguro para no cortar los hilos.
3. Tijeras o cortador: para recortar los hilos parejos antes de insertarlos.
4. Probador de cables (tester): una cajita con dos partes que se conecta a cada extremo del cable y enciende ocho luces en secuencia (1 al 8) más la de tierra. Si las luces encienden en orden en ambos lados, el cable está bien ponchado; si alguna no enciende o enciende fuera de orden, hay un error. Es la herramienta que separa al profesional del improvisado: jamás entregues un cable sin probarlo.

5. Conectores RJ45 del tipo correcto (para cable sólido o multifilar, según el caso) y capuchones (boots) para proteger la pestana.

Consejo de quién ha punchado cientos: compra conectores de más. Al principio fallarás varios (orden mal, hilos cortos, pestana rota) y es normal; cada error te enseña. Un técnico experimentado poncha un cable en dos minutos; tu primero te tomará quince. La práctica manda.

Cómo ponchar un cable paso a paso

Vamos con el procedimiento completo para un cable directo T568B, que es el que más vas a fabricar. Sigue cada paso sin saltarte ninguno:

Paso 1: Corta el cable a la medida que necesites, dejando un poco de holgura extra (unos 30 centímetros de más). Es mejor que sobre a que falte.

Paso 2: Pela la cubierta exterior unos 2 a 3 centímetros con el pelacables, con cuidado de no cortar los hilos internos. Si cortas un hilo, empieza de nuevo: un hilo dañado es un cable muerto.

Paso 3: Destrensa los cuatro pares y estira cada hilo con los dedos para que queden lo más rectos posible. Luego ordenalos de izquierda a derecha según T568B: blanco-naranja, naranja, blanco-verde, azul, blanco-azul, verde, blanco-café, café. Repite el orden en voz alta mientras lo haces; suena tonto, pero evita errores.

Paso 4: Con los hilos ordenados y planos, recortalos parejos dejando aproximadamente 1.3 centímetros desde la cubierta. El corte debe ser recto y limpio. Este largo es crítico: si los hilos quedan muy largos, no entran bien; si quedan muy cortos, no llegan a los contactos.

Paso 5: Toma el conector RJ45 con la pestana hacia abajo y mete los ocho hilos hasta el fondo, manteniendo el orden. Empuja con firmeza: los hilos deben llegar hasta la punta del conector. Verifica el orden mirando a través del plástico transparente; este es tu último momento para corregir.

Paso 6: Mete el conector en la punchadora y aprieta con fuerza hasta qué la herramienta llegue a su tope. La punchadora clava los ocho contactos dorados en los hilos y además presiona una cuna plástica sobre la cubierta exterior para dar resistencia mecánica. Fijate que la cubierta exterior quede atrapada dentro del conector: si los hilos quedan expuestos fuera del conector, el cable se romperá con el uso.

Paso 7: Repite todo en el otro extremo con el mismo estándar (B con B para cable directo).

Paso 8: Conecta el tester a ambos extremos y verifica que las ocho luces enciendan en secuencia del 1 al 8 en las dos unidades. Si todo enciende en orden, felicidades: acabas de fabricar un cable de red profesional. Si alguna luz falla, corta los conectores y vuelve a empezar; no intentes "arreglar" un conector ya ponchado.

Errores típicos de principiante: no destrenzar lo suficiente (los hilos no entran parejos), dejar los hilos de distinto largo (alguno no hace contacto), invertir el orden en un extremo (cable cruzado accidental), y no meter la cubierta dentro del conector (cable frágil). Todos se detectan con el tester en diez segundos.

Topologías físicas y lógicas

La topología es la forma en que se organizan los equipos de una red. Hay dos conceptos que no debes confundir. La topología física describe cómo están conectados físicamente los cables: el mapa real de quién se conecta con quién. La topología lógica describe cómo viajan los datos, como si fuera el flujo del tráfico: por ejemplo, una red puede estar cableada en estrella física pero funcionar como un bus lógico (eso pasaba con los hubs viejos, como verás más adelante). En exámenes siempre preguntan la diferencia, así que grabatela: física es cables, lógica es flujo de datos.

Topología de bus

En el bus, todos los equipos comparten un solo cable troncal al que se conectan en serie, como focos conectados a un mismo cable de luz. Fue la topología de las primeras redes con cable coaxial. Es barata y fácil de instalar porque usa poco cable. Pero tiene defectos mortales: si el cable troncal se rompe en cualquier punto, toda la red se cae; diagnosticar dónde está la falla es una pesadilla; y como todos comparten el mismo cable, solo un equipo puede transmitir a la vez (si dos hablan al mismo tiempo, chocan). Hoy esta topología está muerta en redes locales, pero sobrevive como concepto y como topología lógica en algunas tecnologías.

Topología de estrella

En la estrella, cada equipo se conecta con su propio cable a un dispositivo central (un switch). Es como una rueda de bicicleta: el switch es el eje y cada computadora es un rayo. Es la topología dominante hoy y la que vas a instalar toda tu vida profesional. Sus ventajas lo explican todo: si un cable falla, solo se cae ese equipo y el resto sigue trabajando; es facilísima de diagnosticar (el puerto del switch te dice que equipo tiene problema); y es escalable (para agregar equipos, solo conectas más cables al switch o agregas otro switch). Su única debilidad

real es el punto central: si el switch se descompone, se cae todo lo conectado a él. Por eso en instalaciones críticas se usan switches de respaldo o se conectan switches entre sí de forma redundante.

Topología de anillo

En el anillo, cada equipo se conecta con sus dos vecinos formando un círculo cerrado, y los datos viajan en una dirección (o en ambas, en las versiones modernas) pasando de equipo en equipo hasta llegar a su destino. Fue famosa con la tecnología Token Ring de IBM. Su ventaja es el orden: no hay choques porque un "testigo" (token) autoriza a transmitir. Su desventaja es frágil: si un equipo falla o un cable se rompe, el anillo se interrumpe (aunque las versiones modernas usan doble anillo para recuperarse). Hoy casi no se usa en redes locales, pero el concepto de anillo vive en las redes de fibra de los proveedores, que conectan sus nodos en anillos para tener rutas de respaldo.

Topología de malla

En la malla, cada equipo se conecta con varios otros (en la malla completa, con todos). Es la topología de la máxima redundancia: si un camino falla, los datos toman otro. Suena perfecta hasta qué ves el costo: conectar todo con todo necesita muchísimo cable y muchos puertos. Por eso la malla completa solo se usa en el núcleo de redes críticas (entre los switches principales de un centro de datos, por ejemplo). Existe también la malla parcial, donde solo los equipos importantes tienen conexiones redundantes: es el equilibrio práctico entre confiabilidad y costo. El internet mismo, a gran escala, funciona como una malla parcial gigante.

Topología híbrida

En la vida real, las redes grandes no usan una sola topología pura: las combinan. Una empresa típica tiene estrella en cada oficina (cada PC a su switch), los switches conectados en una especie de bus o anillo parcial entre pisos, y enlaces de malla parcial entre sus sucursales. Eso es una topología híbrida: la mezcla pragmática que resulta de diseñar para el mundo real. Cuando te pidan "diseñar la red de una empresa", casi siempre la respuesta correcta es una híbrida con estrella en el acceso.

Dispositivos básicos: hub, repetidor y punto de acceso

Tres dispositivos pertenecen a esta unidad porque trabajan en la capa física o muy cerca de ella.

El repetidor es el más simple: recibe una señal débil, la amplifica y la reenvía. Sirve para extender la distancia de un cable más allá de su límite (por ejemplo, unir dos tramos de 100 metros). No entiende nada de datos: repite todo lo que escucha, incluyendo el ruido. Hoy casi no se usan como equipos independientes, pero el concepto vive dentro de otros dispositivos.

El hub (concentrador) fue el dispositivo central de las redes en estrella de los años noventa. Recibe datos por un puerto y los repite por TODOS los demás puertos, como un megáfono: todos escuchan todo. Eso lo hace barato pero ineficiente e inseguro: el ancho de banda se comparte entre todos los equipos (diez equipos en un hub de 100 Mbps se reparten esos 100 Mbps) y cualquier equipo puede espiar el tráfico de los demás. El hub está obsoleto y fue reemplazado por el switch, que es inteligente y manda los datos solo al puerto del destinatario. Si ves un hub en un examen, recuerda: repite todo, un solo dominio de colisión, tecnología muerta pero concepto importante para entender la evolución.

El punto de acceso (Access Point, AP) es el dispositivo que crea la red Wi-Fi: se conecta por cable a la red y emite la señal inalámbrica a la que se conectan laptops y celulares. Es el puente entre el mundo cableado y el inalámbrico. En una casa, tu módem-router trae el punto de acceso integrado; en una empresa, se instalan varios APs en techos y pasillos, todos cableados al switch, para cubrir el edificio. Los APs empresariales se administran de forma centralizada con un controlador que coordina canales y potencia para evitar interferencias entre ellos.

Por qué la estrella domina hoy

La estrella gana por razones prácticas, no teóricas. Primera: tolerancia a fallas. En una oficina de cincuenta personas, que se dane un cable significa que una persona se queda sin red, no cincuenta. Segunda: diagnóstico sencillo. Cada puerto del switch tiene luces indicadoras: si el puerto 12 no enciende, el problema está en el cable o el equipo del puerto 12, punto. Tercera: administración centralizada. Todo el tráfico pasa por el switch, así que ahí puedes medir, filtrar y priorizar. Cuarta: escalabilidad barata. Crecer es agregar switches y cables, sin rediseñar nada.

El bus murió porque un solo corte tumbaba todo. El anillo murió en redes locales porque era caro y frágil frente a la simpleza de la estrella con switches baratos. La malla completa es demasiado cara para el acceso. Así que el diseño moderno es: estrella para conectar usuarios (con switches inteligentes), con toques de malla parcial en el núcleo para redundancia y fibra para las distancias largas. Cuando disenes o revises una red, busca la estrella: si la encuentras, vas por buen camino.

Cableado estructurado: el sistema detrás del desorden

Hasta ahora hablamos de cables sueltos, pero en una empresa real los cables no andan tirados por el piso: forman un sistema planeado que se llama cableado estructurado. Es el conjunto de reglas y componentes para instalar el cableado de un edificio de forma ordenada, documentada y duradera. Si alguna vez entras al "cuartito de sistemas" de una oficina y ves un rack metálico con cables perfectamente peinados y etiquetados, estás viendo cableado estructurado bien hecho. Si ves una maraña de cables enredados sin etiquetas, estás viendo lo que pasa cuando no se planea.

Los componentes principales son: el cable horizontal, que va desde el cuarto de telecomunicaciones hasta cada punto de red (roseta) en las oficinas, con un máximo de 90 metros; el patch panel, que es una regleta metálica en el rack donde terminan todos esos cables, cada uno en su puerto numerado; los patch cords (cables de parcheo), que son cables cortos y flexibles que conectan el patch panel con el switch; y el cuarto de telecomunicaciones, el espacio dedicado donde viven el rack, el patch panel, los switches y el UPS. La idea es simple: el cableado fijo dentro de paredes y techos nunca se mueve (ahí va cable sólido, más rígido pero de mejor rendimiento), y todos los cambios se hacen con patch cords en el rack, sin tocar la instalación fija.

Las buenas prácticas de la industria en cableado estructurado son directas: etiqueta TODO (cada cable, cada puerto del patch panel y cada roseta debe tener un código único; dentro de un año nadie recordará que cable es cuál); respeta el radio mínimo de curvatura (no dobles el cable en ángulos cerrados, sobre todo la fibra); no excedas los 90 metros de cable horizontal más 10 metros de patch cords (el límite total de 100 metros incluye todo); separa el cable de red de los cables eléctricos por al menos 30 centímetros, y si deben cruzarse, que sea en ángulo de 90 grados para minimizar la interferencia; deja holgura de servicio (un poco de cable extra enrollado en el rack) para futuros movimientos; y documenta todo en un plano: que puntó de red llega a que puerto del patch panel. Un técnico que hereda una instalación bien etiquetada y documentada te lo agradecerá toda la vida; uno que hereda una maraña sin etiquetas maldice al instalador anterior.

Errores caros que debes evitar

Cierro la explicación con los errores que más dinero y tiempo cuestan en instalaciones reales, para que no los cometas:

Primero, comprar cable sin categoría certificada o de dudosa procedencia. El cable "barato" del mercado informal muchas veces es de aluminio bañado en cobre (CCA) en lugar de cobre puro, y no cumple ninguna categoría aunque la etiqueta diga Cat6. Resultado: velocidades

bajas, fallas intermitentes y una instalación que hay que repetir. Compra cable de cobre 100 por ciento y de marca reconocida.

Segundo, exceder los 100 metros "porque casi llega". La atenuación no perdona: un tramo de 120 metros puede funcionar a ratos y fallar cuando hay más tráfico o más calor. Si la distancia no alcanza, la solución profesional es poner un switch intermedio o usar fibra, no estirar el cobre más allá de su límite.

Tercero, pasar el cable UTP junto a cables eléctricos, balastras de lámparas fluorescentes o motores. La interferencia electromagnética se come la señal y el síntoma es lentitud y pérdida de paquetes que aparece y desaparece sin lógica aparente. La separación física es la solución más barata.

Cuarto, no probar ni etiquetar. Entregar una instalación sin probar cada punto con el tester (o mejor, con un certificador) es como entregar un examen sin revisar: los errores aparecen cuando ya es tarde y cuestan el triple. Y no etiquetar convierte cualquier reparación futura en una cacería.

Quinto, olvidar la puesta a tierra en instalaciones con STP o en exteriores. El blindaje sin tierra no protege; peor aún, puede actuar como antena y captar más interferencia. Si usas blindado, conecta la tierra cómo manda la norma.

PoE: cuando el cable lleva energía además de datos

Hay un truco moderno del par trenzado que vale la pena conocer: PoE (Power over Ethernet, energía sobre Ethernet). Es una tecnología que permite que el mismo cable de red lleve datos y energía eléctrica al dispositivo. Gracias a PoE, un punto de acceso Wi-Fi colgado del techo, una cámara de seguridad o un teléfono IP funcionan con un solo cable, sin necesidad de un contacto eléctrico cercano. Cuando veas un AP en el techo de un centro comercial sin ningún cable de luz a la vista, ahí hay PoE trabajando.

Funciona así: el switch (o un inyector PoE intermedio) mete voltaje de corriente directa (unos 48 volts, seguros) por los pares del cable, y el dispositivo al otro extremo lo separa de los datos y se alimenta. Existen tres estándares principales: 802.3af (PoE clásico, hasta 15.4 watts por puerto, suficiente para teléfonos IP y APs sencillos), 802.3at (PoE+, hasta 30 watts, para APs potentes y cámaras con movimiento) y 802.3bt (hasta 60 o 90 watts, para pantallas, iluminación LED e incluso laptops delgadas). El switch y el dispositivo negocian automáticamente cuanta energía necesita cada uno, así que no hay riesgo de "quemar" un equipo que no soporta PoE: si el equipo no lo pide, el switch no manda energía.

PoE tiene implicaciones directas para el cableado. Primera: la energía genera calor en el cable, y el calor aumenta la atenuación; por eso para instalaciones con mucho PoE se recomienda Cat6a, que disipa mejor el calor por ser más grueso. Segunda: evita los cables de aluminio bañado (CCA) que mencionamos antes, porque su mayor resistencia eléctrica los calienta más y pueden ser un riesgo. Tercera: no juntes demasiados cables PoE en un manojo apretado sin ventilación. Con estas precauciones, PoE es seguro y es una de las razones por las que el par trenzado seguirá vivo por muchos años: ningún otro medio lleva datos y energía juntos de forma tan sencilla.

Ejemplos paso a paso

La teoría de cables y topologías se vuelve real cuando la verificas con comandos. Estos ejemplos simulan lo que harías después de ponchar un cable o instalar un punto de red: comprobar que el enlace físico funciona y que los datos fluyen. Cada bloque muestra el comando y su salida de ejemplo, explicados línea por línea.

Ejemplo 1: verificar el enlace físico en Linux con ethtool

Acabas de conectar un cable entre tu computadora y el switch. Antes de configurar nada, verifica que el enlace físico (la capa 1) este activo:

```
$ sudo ethtool eth0
Settings for eth0:
    Supported ports: [ TP ]
    Supported link modes:   10baseT/Half 10baseT/Full
                           100baseT/Half 100baseT/Full
                           1000baseT/Full

    Speed: 1000Mb/s
    Duplex: Full
    Link detected: yes
```

Explicación línea por línea: "Supported ports: [TP]" indica que el puerto usa par trenzado (Twisted Pair). "Supported link modes" lista las velocidades que la tarjeta soporta: 10, 100 y 1000 Mbps. "Speed: 1000Mb/s" es la velocidad negociada con el switch: un gigabit, excelente. "Dúplex: Full" significa full-dúplex, es decir, puede transmitir y recibir al mismo tiempo (el modo correcto en redes modernas con switch). "Link detected: yes" es la línea más importante: confirma que hay enlace físico, o sea, que el cable está bien conectado en ambos extremos y conduce señal. Si dijera "no", tu problema es físico: cable mal ponchado, conector sin pestana, puerto apagado o cable desconectado. Ninguna configuración de IP arregla un "Link detected: no".

Ejemplo 2: ver tu configuración de red en Windows con ipconfig

En Windows, el comando básico para ver el estado de tus adaptadores de red es:

```
C:\> ipconfig /all
```

Adaptador de Ethernet Ethernet:

```
Descripcion . . . . . : Realtek PCIe GbE Family Controller
Direccion fisica . . . . . : 4C-72-B9-8A-3D-21
DHCP habilitado . . . . . : sí
Direccion IPv4. . . . . : 192.168.1.25
Mascara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . : 192.168.1.1
```

Explicación: "Descripción" te dice que tarjeta de red tienes. "Dirección física" es la MAC, el identificador único de tu tarjeta (la verás a fondo en la siguiente unidad). "DHCP habilitado: sí" indica que tu IP la asignó automáticamente el router. "Dirección IPv4" es tu dirección lógica actual. Si en lugar de una IP válida ves "169.254.x.x", significa que no hubo comunicación con el DHCP y Windows se autoasignó una dirección APIPA: casi siempre es síntoma de un problema físico (cable desconectado o dañado). Si ves "Medios desconectados", el cable no está haciendo contacto: revisa el ponchado antes de tocar cualquier configuración.

Ejemplo 3: probar un cable recién ponchado con ping

La prueba definitiva de un cable es mandar tráfico real por él. El comando ping envía paquetes de prueba y mide cuantos regresan:

```
C:\> ping 192.168.1.1 -n 10
```

Haciendo ping a 192.168.1.1 con 32 bytes de datos:

Respuesta desde 192.168.1.1: bytes=32 tiempo<1ms TTL=64

Respuesta desde 192.168.1.1: bytes=32 tiempo<1ms TTL=64

Respuesta desde 192.168.1.1: bytes=32 tiempo<1ms TTL=64

[... se repiten las 10 respuestas ...]

Estadísticas de ping para 192.168.1.1:

Paquetes: enviados = 10, recibidos = 10, perdidos = 0 (0% perdidos),

Tiempos aproximados de ida y vuelta en milisegundos:

Minimo = 0ms, Maximo = 0ms, Media = 0ms

Explicación: "-n 10" pide diez paquetes en Windows (en Linux sería "-c 10"). Cada "Respuesta desde" confirma que el paquete llegó al router (192.168.1.1) y regreso: el cable conduce en ambas direcciones. "tiempo<1ms" indica latencia mínima, normal en red local. Las estadísticas finales son el veredicto: 10 enviados, 10 recibidos, 0 perdidos (0 por ciento). Un cable sano en red local debe dar 0 por ciento de pérdida. Si ves pérdida de paquetes (por ejemplo, 25 por ciento perdidos) o tiempos muy variables, sospecha del cable: un par mal ponchado o un cable dañado produce exactamente ese síntoma. Así de directo es el diagnóstico: ping con pérdida en red local casi siempre es capa física.

Ejemplo 4: interpretar un probador (tester) de cables

El tester tiene dos módulos: el principal (MÁSTER) y el remoto (REMOTE). Conectas un extremo del cable a cada uno y lo enciendes. Una salida típica se representa así:

```
MASTER:  1 2 3 4 5 6 7 8 G   (todas las luces encienden en orden)
```

```
REMOTE:  1 2 3 4 5 6 7 8 G   (todas las luces encienden en orden)
```

```
RESULTADO: CABLE CORRECTO (directo T568B en ambos extremos)
```

Explicación: cada número es un hilo. Si las ocho luces encienden en secuencia en ambos módulos, los ocho hilos están continuos y en el orden correcto. La "G" es la tierra del blindaje (solo aplica en STP). Casos de falla comunes: si la luz 3 no enciende en el remoto, el hilo 3 está cortado o no hace contacto (vuelve a ponchar ese extremo); si en el remoto encienden en orden 1 2 4 3 5 6 7 8, los hilos 3 y 4 están cruzados (error de orden); si encienden 3 6 1 4 5 2 7 8, fabricaste un cruzado sin querer. El tester no miente: úsalo siempre antes de instalar un cable en un lugar difícil de alcanzar.

Ejemplo 5: revisar la señal Wi-Fi en Windows

Para el medio inalámbrico, el equivalente a revisar el cable es revisar la calidad de la señal:

```
C:\> netsh wlan show interfaces
```

```
Nombre                : Wi-Fi
Estado                : conectado
SSID                  : Oficina_Piso2
Señal                 : 82%
Tipo de radio         : 802.11ac
Velocidad de recepcion : 866.7 Mbps
Velocidad de transmision : 866.7 Mbps
```

Explicación: "Estado: conectado" confirma la asociación con el punto de acceso. "SSID" es el nombre de la red. "Señal: 82%" es la calidad de recepción: arriba de 70 por ciento es buena; debajo de 50 por ciento tendrás cortés y lentitud, y la solución es física (acercarte al AP, quitar obstáculos o agregar otro punto de acceso). Las velocidades de recepción y transmisión son la tasa negociada con el AP, no la velocidad real de internet, pero te dicen el techo de tu conexión inalámbrica. Si la señal es baja y la velocidad negociada también, no llames al proveedor de internet: tu problema está entre tu equipo y el punto de acceso, es decir, en el medio inalámbrico.

Práctica

1. Una empresa quiere conectar su oficina principal con su bodega, que está a 1.5 kilómetros de distancia en línea recta. Necesitan al menos 1 Gbps de velocidad y el presupuesto es medio. Que medio de transmisión recomiendas y por qué? Descarta las demás opciones con argumentos.

SOLUCIÓN: La respuesta correcta es fibra óptica monomodo. Paso a paso: primero revisa la distancia. El par trenzado UTP llega a 100 metros, así que queda descartado de inmediato: 1.5 kilómetros es quince veces su límite. El cable coaxial de red llegaba a 500 metros, también descartado. El Wi-Fi en exteriores con antenas direccionales podría cubrir la distancia, pero no garantiza 1 Gbps estables y sufre con la lluvia y la interferencia; para un enlace crítico entre edificios no es profesional. Queda la fibra. Entre monomodo y multimodo: la multimodo llega a unos 550 metros, insuficiente para 1.5 kilómetros, así que debe ser monomodo, que cubre decenas de kilómetros sin problema y da velocidades de 1 Gbps y mucho más. El costo de instalación es mayor que el cobre, pero es la única opción técnicamente viable; además, una vez instalada,

esa fibra servirá por décadas. Conclusión: fibra monomodo, instalada por personal especializado, con convertidores de medios o switches con puertos SFP en cada extremo.

2. Vas a cablear una oficina nueva que debe durar al menos diez años. El cliente quiere estar preparado para 10 Gbps en cada escritorio dentro de unos años, y la distancia más larga desde el cuarto de telecomunicaciones hasta un punto de red es de 80 metros. ¿qué categoría de cable instalas: Cat5e, Cat6 o Cat6a? Justifica con números.

SOLUCIÓN: Debes instalar Cat6a. Analicemos cada opción. Cat5e soporta 1 Gbps hasta 100 metros: hoy funcionaría, pero no da 10 Gbps, así que no cumple el requisito futuro; descartada. Cat6 soporta 10 Gbps, pero solo hasta 55 metros; como la distancia máxima de esta instalación es de 80 metros, en los puntos lejanos no garantizaría los 10 Gbps; descartada para este caso. Cat6a soporta 10 Gbps en los 100 metros completos, así que cubre los 80 metros con holgura y cumple el requisito futuro. El cable Cat6a es un poco más caro y más grueso (cuesta más trabajo pasarlo por ductos), pero la diferencia de precio del material es mínima comparada con romper paredes y recablear dentro de cinco años. Buena práctica aplicada: cablear pensando en el futuro, cómo dice la unidad.

3. Escribe de memoria el orden de colores de la norma T568B del pin 1 al pin 8, y explica qué pasaría si por error ponchas un extremo en T568B y el otro en T568A.

SOLUCIÓN: El orden T568B es: 1. blanco-naranja, 2. naranja, 3. blanco-verde, 4. azul, 5. blanco-azul, 6. verde, 7. blanco-café, 8. café. Si un extremo queda en B y el otro en A, fabricaste sin querer un cable cruzado, porque los pares naranja y verde quedan intercambiados entre extremos (los pines 1, 2, 3 y 6 se cruzan). En equipos modernos con Auto-MDIX, ese cable probablemente funcionará igual para conectar una PC a un switch, y quizá nunca notes el error. Pero es una mala práctica: si alguien usa ese cable para diagnosticar o lo conecta entre equipos que no tienen Auto-MDIX, dará fallas confusas. La lección: usa el tester siempre; si las luces encienden en orden 3 6 1 4 5 2 7 8 en el remoto, ya sabes que cruzaste los pares por accidente. Corta los conectores y vuelve a ponchar.

4. Conectas dos computadoras viejas directamente entre sí con un cable de red para pasar archivos, pero no se comunican. El cable es directo (T568B en ambos extremos) y el tester dice que está bien ponchado. ¿Cuál es el problema y cómo lo resuelves?

SOLUCIÓN: El problema es el tipo de cable. Dos computadoras son equipos "iguales": ambas transmiten por los mismos pines y reciben por los mismos pines. Con un cable directo, el transmisor de una queda conectado al transmisor de la otra, y nadie escucha

a nadie; es como dos personas hablando al mismo tiempo por teléfono. La solución clásica es usar un cable cruzado (T568A en un extremo y T568B en el otro), que cruza los pares de transmisión y recepción para que el transmisor de una llegue al receptor de la otra. Paso a paso: corta un conector del cable directo, vuelve a poncharlo en T568A, verifica con el tester que el remoto encienda en el orden cruzado, y conecta de nuevo. Nota moderna: si las computadoras tienen Auto-MDIX (casi todas las fabricadas después del 2005), el cable directo debería funcionar; si no funciona ni con cruzado, el problema ya no es el cable sino la configuración IP, que verás en la siguiente unidad.

5. Eres el técnico de una escuela. Varias computadoras del laboratorio pierden conexión a ratos: el ping al router muestra 20 por ciento de paquetes perdidos y a veces la red se cae por completo unos minutos. El switch está bien y los equipos tienen IP correcta. Describe tu diagnóstico paso a paso empezando por la capa física.

SOLUCIÓN: Los síntomas (pérdida de paquetes intermitente en red local, caídas temporales) apuntan a la capa física, así que el diagnóstico empieza ahí, del más simple al más complejo. Paso 1: revisa físicamente los cables de las computadoras afectadas; busca conectores sin pestana, cables aplastados por muebles o dobleces muy cerrados. Paso 2: corre "ethtool" o revisa las luces del switch; si un puerto parpadea de forma irregular o el enlace se cae y regresa, ese cable es sospechoso. Paso 3: prueba cada cable sospechoso con el tester; un hilo con falso contacto da exactamente este síntoma. Paso 4: pregunta que cambió recientemente: si movieron muebles o pasaron un cable nuevo junto a un tubo de luz o un motor, la interferencia es la culpable (recuerda: el UTP sin blindaje sufre cerca de cables eléctricos). Paso 5: si el cableado pasa por el techo, verifica que ningún tramo exceda los 100 metros y que no haya empalmes improvisados con cinta aislante (un clásico en escuelas). La regla de oro: en red local, la pérdida de paquetes casi siempre es cable, conector o interferencia; no reinstales sistemas operativos ni cambies configuraciones hasta descartar lo físico.

6. Dibuja con palabras (o en papel) la topología física de esta red casera: un módem-router en la sala, una computadora de escritorio conectada por cable al router, una laptop y dos celulares conectados por Wi-Fi al mismo router, y una smart TV conectada por cable. ¿Qué topología es y por qué? ¿qué pasaría si se dana el cable de la computadora de escritorio?

SOLUCIÓN: Es una topología de estrella (híbrida cableada-inalámbrica, pero físicamente en estrella). Cada dispositivo se conecta de forma independiente al dispositivo central, que es el módem-router: la PC y la TV con su propio cable cada una (rayos de la estrella por cobre), y la laptop y los celulares por Wi-Fi al punto de acceso integrado en el router (rayos de la estrella por aire). Todos dependen del centro, ninguno depende de otro dispositivo. Si se dana el cable de la computadora de escritorio, solo esa computadora

pierde la conexión; la TV, la laptop y los celulares siguen funcionando normalmente. Esa es exactamente la gran ventaja de la estrella que estudiaste: las fallas están contenidas y el diagnóstico es trivial (si solo un equipo falla, el problema está en su cable o en su conexión al centro). Si en cambio se apaga el router, se cae todo: esa es la debilidad del punto central.

7. Te contratan para instalar 12 puntos de red en una oficina pequeña. El cuarto de sistemas está en un extremo del local y el punto más lejano queda a 65 metros de cable. El cliente quiere conectar 4 puntos de acceso Wi-Fi en el techo (con PoE), 6 computadoras de escritorio y 2 impresoras. El presupuesto es ajustado pero la instalación debe durar diez años. Elabora tu plan: qué categoría de cable usas, que norma de ponchado, que componentes de cableado estructurado incluyes y que precauciones tomas con el PoE.

SOLUCIÓN: El plan profesional sería este. Categoría: Cat6a, porque la instalación debe durar diez años y los 4 APs usarán PoE (el Cat6a disipa mejor el calor que genera la energía); además, a 65 metros el Cat6a garantiza 10 Gbps futuros sin problema. Norma de ponchado: T568B en todos los extremos, el estándar de facto en México, y cable directo en todos los tramos (todos los equipos se conectan al switch). Componentes de cableado estructurado: un rack pequeño en el cuarto de sistemas con un patch panel de 24 puertos (12 usados más holgura para crecer), cable sólido Cat6a para los tramos fijos dentro de muros y techo (máximo 90 metros por norma; aquí el más largo es 65, perfecto), rosetas con jacks en cada punto de red, y patch cords multifilares cortos para conectar el patch panel al switch. El switch debe ser PoE+ (802.3at) con al menos 4 puertos PoE para los APs, o un switch normal más un inyector PoE si el presupuesto no alcanza para un switch PoE completo. Precauciones: etiquetar cada cable y cada puerto del patch panel desde el día uno; no pasar el cable junto a los tubos de luz del techo; comprar cable de cobre 100 por ciento (nada de CCA) por el PoE; probar los 12 puntos con el tester antes de entregar; y documentar en un plano que puntó llega a que puerto. Con esto, la instalación queda lista para diez años y para crecer sin romper nada.

Resumen de la unidad

En esta unidad bajaste al nivel más físico de las redes y descubriste que todo lo digital viaja por algo material. Aprendiste que un medio de transmisión es el camino de las señales y que hay cuatro grandes: el par trenzado de cobre (UTP barato y flexible para oficinas, STP blindado para ambientes con interferencia), el cable coaxial (el veterano de la TV por cable, con gran blindaje pero poco futuro en datos), la fibra óptica (monomodo para kilómetros con láser, multimodo para cientos de metros con LED, inmune a la interferencia y reina de la velocidad) y los medios inalámbricos (movilidad total a cambio de velocidad compartida y

variable). Compararlos por velocidad, distancia, costo e interferencia es la habilidad que te permite elegir el medio correcto para cada escenario, desde una casa hasta dos edificios separados por kilómetros.

Después metiste las manos en el cableado: las categorías Cat5e, Cat6 y Cat6a y por qué Cat6a es la apuesta a futuro; el conector RJ45 de 8 pines y el cuidado de su pestana; las normas de colores T568A y T568B (con la B como estándar en México); la diferencia entre cable directo (mismo estándar en ambos extremos, para equipos diferentes) y cable cruzado (A en un extremo y B en el otro, para equipos iguales, aunque Auto-MDIX lo ha vuelto casi innecesario); las herramientas del oficio (ponchadora, pelacables, tijeras y el infaltable tester); y el procedimiento completo de ponchado en ocho pasos, con sus errores típicos. Ponchar bien es una habilidad manual que ningún curso teórico sustituye: práctica hasta hacerlo en minutos y prueba cada cable antes de instalarlo.

Cerraste con las topologías: la diferencia entre física (cables) y lógica (flujo de datos), y las cinco formas de organizar una red (bus, estrella, anillo, malla e híbrida). Viste que la estrella domina porque contiene las fallas, se diagnostica fácil y escala barato; que el bus y el anillo son historia en redes locales; y que la malla (parcial) se reserva para núcleos críticos que necesitan redundancia. Conociste al repetidor, al hub obsoleto que repetía todo como megáfono, y al punto de acceso que une el mundo cableado con el inalámbrico.

La idea que debes llevarte grabada: la mayoría de los problemas de red viven en la capa física, y quien sabe diagnosticarlos (con `ethtool`, `ipconfig`, `ping` y un tester en la mano) resuelve en minutos lo que otros persiguen por horas. En la siguiente unidad subirás un nivel: dejarás los cables y entrarás al mundo lógico del direccionamiento IPv4, donde cada equipo recibe su "dirección postal" y aprenderás a leerla, clasificarla y calcularla.

UNIDAD 4: Direccionamiento IPv4

Imagina que quieres mandar una carta a un amigo que vive en otra ciudad. Escribes su nombre, su calle, su número, su colonia, su ciudad y su código postal en el sobre, la echas al buzón y el sistema postal hace el resto. Ahora imagina que quieres mandar un mensaje de WhatsApp. No escribes ninguna dirección: solo eliges el contacto y listo. Pero detrás de esa facilidad, tu teléfono y los servidores están haciendo algo muy parecido al correo postal: cada equipo conectado a una red tiene una "dirección postal" numérica que lo identifica, y cada paquete de datos lleva escrita la dirección del destinatario. Esa dirección se llama dirección IP, y en esta unidad vas a dominarla por completo.

La dirección IP versión 4 (IPv4) es el sistema de direcciones más usado del planeta. Lleva funcionando desde principios de los años ochenta y, aunque ya existe su sucesora (IPv6, que verás más adelante en el curso), IPv4 sigue siendo la que vas a configurar, diagnosticar y reparar todos los días en redes locales y empresariales. Cuando el internet "no funciona" en una oficina, las primeras preguntas del técnico son sobre direcciones IP: tiene IP el equipo? Es la correcta? Cuál es su máscara? Cuál es su puerta de enlace? Sin entender IPv4 a fondo, es imposible trabajar en redes.

Esta unidad cubre las clases 10, 11 y 12 del curso. En la clase 10 entenderás qué es una dirección IPv4: sus 32 bits, la notación decimal con puntos que la hace legible para humanos, y sus dos partes (red y host), con la analogía de las direcciones postales que te acompañará todo el capítulo. En la clase 11 aprenderás el sistema de clases A, B, C, D y E con sus rangos exactos, las direcciones privadas de la RFC 1918 (esos 192.168.x.x que ves en tu casa), y las direcciones especiales: loopback, APIPA, broadcast y multicast. En la clase 12 entrarás a la parte más práctica: la máscara de subred, la notación CIDR, la puerta de enlace predeterminada y el procedimiento exacto que usa un equipo para saber si su destino está en su misma red o hay que mandarlo al router.

Por qué importa en la vida real y en el trabajo? Por qué configurar mal una IP es uno de los errores más comunes y más paralizantes en una red. Un equipo con la IP equivocada simplemente no se comunica, y el síntoma ("no tengo internet") es idéntico al de un cable dañado o un router caído. El técnico que entiende direccionamiento diagnostica en segundos con un ipconfig: ve la IP, ve la máscara, ve la puerta de enlace y sabe exactamente dónde está el problema. El que no lo entiende, reinicia equipos a ciegas esperando un milagro. Además, diseñar una red (decidir que rangos de IP usa cada departamento de una empresa, por ejemplo) es una tarea típica de un administrador de red junior, y se basa por completo en lo que verás aquí.

Una advertencia honesta: esta unidad tiene matemáticas. Vas a convertir números entre binario y decimal, vas a hacer operaciones lógicas con bits y vas a calcular direcciones de red. No te asustes: es aritmética de primaria con números pequeños (del 0 al 255) y te voy a llevar de la mano paso a paso, desde cero, sin asumir que sabes nada de binario. Los técnicos que hoy configuran redes en todo México aprendieron esto mismo sentado frente a una hoja de papel. Tú puedes hacerlo igual. Empecemos por lo más básico: qué es realmente una dirección IP.

Explicación detallada

Qué es una dirección IPv4

Una dirección IPv4 es un número de 32 bits que identifica de forma única a un equipo (o, más precisamente, a una interfaz de red) dentro de una red. Esos 32 bits son 32 dígitos binarios, es decir, 32 unos y ceros. Por ejemplo, la dirección de tu computadora podría verse así en binario puro:

```
110000001010100000000000100001010
```

Impronunciable, verdad? Por eso los humanos usamos la notación decimal con puntos (dotted decimal): dividimos los 32 bits en cuatro grupos de 8 bits (cada grupo se llama octeto, por qué tiene ocho bits), convertimos cada octeto a decimal y separamos los cuatro números con puntos. El ejemplo de arriba queda así:

```
192.168.1.10
```

Mucho más manejable. Cada octeto en decimal va del 0 al 255 (porque 8 bits pueden representar 256 valores distintos, del 0 al 255). Así que una dirección IPv4 siempre tiene la forma a.b.c.d donde cada letra es un número entre 0 y 255. Ejemplos validos: 10.0.0.1, 172.16.5.20, 8.8.8.8 (los famosos servidores DNS de Google). Ejemplos inválidos: 192.168.1.256 (un octeto no puede pasar de 255), 10.0.0 (faltan octetos), 192.168.1.1.5 (sobran octetos).

La dirección IP cumple dos funciones al mismo tiempo, y entender esta dualidad es la clave de toda la unidad. Primera función: identificar la RED a la que pertenece el equipo (como el código postal o la ciudad en una dirección postal). Segunda función: identificar al EQUIPO específico dentro de esa red (como la calle y el número de tu casa). Toda dirección IPv4 se divide en dos partes: la porción de red y la porción de host. La porción de red es igual para todos los equipos de la misma red; la porción de host es única para cada equipo dentro de esa red. Dónde termina una y empieza la otra lo define la máscara de subred, que estudiarás en la clase 12. Por ahora quedate con la idea: IP = dirección de red + identificador de equipo.

La analogía postal funciona así: piensa en la dirección "Av. Juárez 123, Col. Centro, Guadalajara, Jalisco, CP 44100". El país, el estado, la ciudad y el código postal identifican la zona (la "red"): todas las cartas que van a esa zona comparten esos datos. La calle y el número identifican el destino exacto dentro de la zona (el "host"): solo esa casa tiene ese número. En una IP como 192.168.1.10 con máscara 255.255.255.0, la porción de red es 192.168.1 (la "colonia", compartida por todos) y la porción de host es 10 (el "número de casa", único). Dos equipos con la misma porción de red están en la misma red local y pueden hablar directamente; si la porción de red difiere, necesitan un router que les haga de "oficina postal" entre zonas.

Un error común de principiante es creer que la IP identifica a la computadora como aparato físico. No exactamente: identifica a su conexión de red. Una laptop con cable Ethernet y Wi-Fi activos tiene dos direcciones IP (una por interfaz), y si mañana la conectas a otra red, tendrá direcciones distintas. La identidad permanente del hardware es la dirección MAC, que verás en otra unidad. La IP es lógica y puede cambiar; la MAC es física y normalmente no cambia.

Los 32 bits: anatomía de una dirección

Vamos a diseccionar una dirección para que los 32 bits dejen de ser un misterio. Toma la dirección 192.168.1.10 y su máscara 255.255.255.0. En binario se ven así:

IP: 11000000.10101000.00000001.00001010 Máscara: 11111111.11111111.11111111.00000000

Cuenta los bits: $8 + 8 + 8 + 8 = 32$ en la IP, y 32 en la máscara. La máscara es una secuencia de unos seguidos de ceros: los unos marcan la porción de red (24 unos = los primeros 24 bits son red) y los ceros marcan la porción de host (8 ceros = los últimos 8 bits son host). Por eso esta máscara se escribe también como /24: indica que 24 bits son de red. Esta es la notación CIDR, que dominarás más adelante.

Con 8 bits de host, cuántos equipos puede tener esta red? Cada bit duplica las combinaciones: 2 elevado a la 8 = 256 direcciones posibles, de la 192.168.1.0 a la 192.168.1.255. Pero ojo: no

todas se pueden asignar a equipos. La primera (192.168.1.0, todos los bits de host en cero) es la dirección de red: identifica a la red misma, no a un equipo. La última (192.168.1.255, todos los bits de host en uno) es la dirección de broadcast: sirve para hablarle a todos los equipos de la red a la vez. Así que los equipos usables van de 192.168.1.1 a 192.168.1.254: 254 equipos. Esta resta de dos (red y broadcast) aparece en todos los cálculos de redes; grabatela desde ahora.

Memoriza también los valores de cada posición de bit dentro de un octeto, porque los usarás para convertir binario a decimal mentalmente. De izquierda a derecha, cada bit vale el doble que el anterior:

128 64 32 16 8 4 2 1

Así, el binario 11000000 vale $128 + 64 = 192$. El binario 10101000 vale $128 + 32 + 8 = 168$. El binario 00001010 vale $8 + 2 = 10$. Con esta tabla, convertir cualquier octeto es una suma sencilla. En la sección de ejemplos lo practicaremos hasta qué salga natural.

Conversión entre binario y decimal, desde cero

Si el binario te suena a chino, esta sección es para ti. Vamos desde cero absoluto, sin prisa.

El sistema decimal que usas todos los días tiene diez dígitos (0 al 9) y cada posición vale diez veces más que la anterior: unidades, decenas, centenas. El número 192 significa 1 centena + 9 decenas + 2 unidades. El sistema binario es lo mismo pero con solo dos dígitos (0 y 1) y cada posición vale el doble que la anterior. En un octeto hay ocho posiciones, y sus valores son:

Posición: 1 2 3 4 5 6 7 8 Valor: 128 64 32 16 8 4 2 1

Para convertir de binario a decimal, sumas los valores de las posiciones donde hay un 1 e ignoras donde hay un 0. Ejemplo con 11000000: hay unos en las posiciones de 128 y 64, así que $128 + 64 = 192$. Ejempló con 10101000: unos en 128, 32 y 8, así que $128 + 32 + 8 = 168$. Ejempló con 00001010: unos en 8 y 2, así que $8 + 2 = 10$. Fácil, verdad? Es solo sumar.

Para convertir de decimal a binario, haces lo inverso: restas sucesivas de mayor a menor. Toma el número 192. El valor más grande que cabe es 128: lo restas ($192 - 128 = 64$) y pones un 1 en esa posición. Ahora con el 64 restante: el siguiente valor es 64, cabe exacto ($64 - 64 = 0$), pones un 1. Ya no queda nada, así que todas las demás posiciones llevan 0. Resultado: 11000000. Otro ejemplo, el 168: 128 cabe ($168 - 128 = 40$), pones 1. 64 no cabe en 40, pones 0. 32 cabe ($40 - 32 = 8$), pones 1. 16 no cabe en 8, pones 0. 8 cabe ($8 - 8 = 0$), pones 1. El resto ceros. Resultado: 10101000. Un ejemplo más, el 10: 128 no cabe, 0; 64 no cabe, 0; 32 no cabe, 0; 16 no cabe, 0; 8 cabe ($10 - 8 = 2$), 1; 4 no cabe en 2, 0; 2 cabe ($2 - 2 = 0$), 1; 1 no

cabe, 0. Resultado: 00001010. Práctica con estos números hasta qué el método salga solo: 255, 0, 128, 64, 191, 223.

Hay valores que conviene memorizar porque aparecen todo el tiempo en máscaras y direcciones:

Decimal	Binario 0	00000000 (todos ceros)	128	10000000	192	11000000	224			
	11100000	240	11110000	248	11111000	252	11111100	254	11111110	255
	11111111	(todos unos)								

Fijate en el patrón: son unos acumulandose desde la izquierda. Estos ocho valores son los únicos que pueden aparecer en una máscara de subred válida (más los intermedios como 160 o 96 en casos raros de clase), así que memorizarlos te ahorra mucho tiempo. Un truco: 255 menos el valor te dice cuantos ceros... mejor dicho, cada valor es 256 menos una potencia de dos: $255 = 256 - 1$, $254 = 256 - 2$, $252 = 256 - 4$, $248 = 256 - 8$, $240 = 256 - 16$, $224 = 256 - 32$, $192 = 256 - 64$, $128 = 256 - 128$. Este truco te servirá para calcular rangos de subred más adelante.

Error común: intentar convertir el número completo de 32 bits de un jalón. No lo hagas: trabaja siempre octeto por octeto, son cuatro conversiones pequeñas e independientes. Otro error: olvidar los ceros a la izquierda. El decimal 10 en un octeto es 00001010, no 1010: los ceros de la izquierda cuentan para completar los 8 bits, y sin ellos la dirección queda mal escrita.

Las clases de direcciones: A, B, C, D y E

En los primeros años del internet, cuando las direcciones IP se repartían a empresas y universidades, se inventó un sistema simple para organizarlas: las clases. La idea era repartir el espacio de direcciones según el tamaño de cada organización: las redes gigantes recibían clase A (pocas redes, pero cada una con millones de direcciones), las medianas clase B y las pequeñas clase C. Las clases D y E se reservaron para propósitos especiales. Aunque hoy el reparto por clases está obsoleto (fue reemplazado por CIDR, que verás en la clase 12), las clases siguen vivas en exámenes, en certificaciones y en la forma en qué hablamos de redes. Tienes que dominarlas.

Cómo sabes a qué clase pertenece una dirección? Por su primer octeto. Originalmente la distinción era por los primeros bits, pero en la práctica memorizas los rangos del primer octeto:

Clase	Primer octeto	Rango completo	Máscara por defecto	Redes posibles
Hosts por red A	1 a 126	1.0.0.0 a 126.255.255.255	255.0.0.0 (/8)	126
~16.7 millones B	128 a 191	128.0.0.0 a 191.255.255.255	255.255.0.0 (/16)	
~16,000 65,534 C	192 a 223	192.0.0.0 a 223.255.255.255	255.255.255.0 (/24)	
~2 millones 254 D	224 a 239	224.0.0.0 a 239.255.255.255	(multicast)	-
- E 240 a 255	240.0.0.0 a 255.255.255.255	(experimental)	-	-

Vamos clase por clase. La clase A (primer octeto del 1 al 126) usa 8 bits para red y 24 para hosts: poquitas redes (126), pero cada una con casi 17 millones de direcciones. Se las dieron a gigantes históricos: IBM, General Electric y algunas universidades tienen redes clase A completas. Suena a desperdicio, y lo fue: por eso se cambió el sistema. Nota el hueco: el 0 y el 127 no están en la tabla. El 0.0.0.0 significa "esta red" o "todas las direcciones" según el contexto, y el 127.0.0.0/8 está reservado para loopback (lo verás en direcciones especiales).

La clase B (128 a 191) usa 16 bits para red y 16 para hosts: unas 16,000 redes con 65,534 equipos cada una. Era el tamaño ideal para universidades medianas y empresas grandes. La clase C (192 a 223) usa 24 bits para red y 8 para hosts: más de 2 millones de redes pequeñas de 254 equipos. Es la clase de las redes caseras y de las pymes: tu casa casi seguro usa una red clase C privada (192.168.1.x).

La clase D (224 a 239) no es para equipos normales: son direcciones multicast, para mandar un paquete a un grupo de equipos interesados al mismo tiempo (videoconferencias, streaming interno, protocolos de enrutamiento). No tienen porción de red/host en el sentido tradicional y nunca se asignan a una computadora. La clase E (240 a 255) está reservada para experimentación futura; no la uses nunca en una red real.

Los primeros bits de cada clase (por si te los preguntan en un examen): la clase A empieza con 0, la B con 10, la C con 110, la D con 1110 y la E con 1111. Es el patrón binario original del que salen los rangos decimales. Por ejemplo, un primer octeto que empieza con 110 está entre 192 (11000000) y 223 (11011111): clase C.

De dónde salen los números de "hosts por red"? De los bits de host menos las dos direcciones reservadas (red y broadcast). Clase A: 24 bits de host = $2^{24} = 16,777,216$ direcciones, menos 2 = 16,777,214 hosts. Clase B: $2^{16} = 65,536$ menos 2 = 65,534. Clase C: $2^8 = 256$ menos 2 = 254. Y las "redes posibles": clase A tiene 7 bits útiles de red (el primer bit es 0 fijo) = $2^7 = 128$, menos las redes 0 y 127 = 126. Clase B: 14 bits útiles = 16,384 redes. Clase C: 21 bits útiles = 2,097,152 redes.

Buena práctica: cuando veas una IP, clasifícala automáticamente por su primer octeto antes de hacer cualquier cálculo. Es un reflejo que te ahorra errores: 10.5.3.1 es A, 172.20.8.4 es B, 200.100.50.25 es C, 230.1.1.1 es D (multicast, no es un equipo normal).

Direcciones privadas: la RFC 1918

Aquí viene una de las ideas más prácticas de todo el networking. Las direcciones IP públicas (las que te identifican en internet) son un recurso limitado: solo hay unos 4,300 millones de direcciones IPv4 y los equipos conectados ya son muchos más. La solución fue genial y sencilla: reservar bloques de direcciones para uso privado dentro de redes locales, bloques que nunca se usan en internet público y que por tanto se pueden repetir en millones de redes distintas. Tu casa usa 192.168.1.x, la oficina de al lado también usa 192.168.1.x, y no hay conflicto porque esas direcciones nunca salen tal cuál a internet: el router las traduce mediante NAT (traducción de direcciones, tema de otra unidad).

La RFC 1918 (una RFC es un documento oficial que define estándares de internet; no inventes números de RFC, este es el correcto para direcciones privadas) reserva tres bloques:

Bloque privado	Rango	Clase	Redes tipo 10.0.0.0/8
10.0.0.0 a 10.255.255.255		A	Una red gigante (16.7 millones de hosts)
172.16.0.0/12	172.16.0.0 a 172.31.255.255	B	16 redes medianas (65,534 hosts cada una)
192.168.0.0/16	192.168.0.0 a 192.168.255.255	C	256 redes pequeñas (254 hosts cada una)

Fijate en los detalles porque los exámenes los adoran. El bloque 10.x usa toda la clase A privada: cualquier dirección que empiece con 10 es privada (10.0.0.5, 10.200.100.3, todas). El bloque 172.16.x NO es todo el rango 172.x: solo del 172.16.0.0 al 172.31.255.255. La dirección 172.15.8.8 es pública y la 172.32.1.1 también; solo el segundo octeto entre 16 y 31 es privado. Este es el error más común con las privadas, así que repítelo: 172.16 a 172.31, ni uno más ni uno menos. El bloque 192.168.x usa todo el tercer octeto: 192.168.0.1, 192.168.100.50, 192.168.255.254, todas privadas.

Cuándo usar cada bloque? El 192.168.0.0/16 es el favorito para casas y pymes: los routers caseros vienen configurados con 192.168.0.x o 192.168.1.x por defecto. El 172.16.0.0/12 es popular en empresas medianas: con sus 16 subredes clase B puedes asignar una a cada departamento o sucursal. El 10.0.0.0/8 es para empresas grandes y proveedores: un solo bloque con millones de direcciones para repartir internamente. En la práctica mexicana, si entras a dar soporte a una empresa y ves direcciones 10.x, sabes que su red interna es grande y probablemente bien planeada; si ves 192.168.x, es una red pequeña o un router casero haciendo de todo.

Regla de oro: las direcciones privadas nunca deben aparecer en internet público. Si configuras un servidor con una IP privada y esperas que alguien lo vea desde fuera sin NAT ni redirección de puertos, no funcionará jamás. Y al revés: si en un diagnóstico ves que tu equipo tiene una IP pública directamente (no 10.x, ni 172.16-31.x, ni 192.168.x), estás conectado directo al

proveedor sin router intermedio, algo raro en una casa pero normal en algunos enlaces empresariales.

Direcciones especiales que debes conocer

Además de las privadas, hay direcciones con propósitos reservados que aparecen constantemente en el trabajo diario. Conocelas todas:

La dirección de loopback: 127.0.0.1. Es la dirección que apunta a tu propia máquina, un "espejo" interno. Todo el bloque 127.0.0.0/8 está reservado para loopback, pero en la práctica siempre se usa 127.0.0.1 (localhost). Para qué sirve? Para probar que tu pila de red funciona sin necesidad de cables ni de nadie más: si haces ping a 127.0.0.1 y responde, tu tarjeta de red lógica y tu sistema operativo están bien; el problema (si lo hay) está afuera. Es la primera prueba de diagnóstico cuando nada funciona: ping a 127.0.0.1, luego ping a tu propia IP, luego ping a la puerta de enlace, luego ping a internet. Ese orden, de adentro hacia afuera, es el método profesional de diagnóstico.

APIPA: 169.254.0.0/16. Cuando un equipo configurado para obtener IP automática (DHCP) no encuentra ningún servidor DHCP, Windows (y otros sistemas) se autoasigna una dirección de este rango, como 169.254.23.45. Es una señal de auxilio: te dice "no pude hablar con nadie". Si ves una 169.254.x.x en un ipconfig, no pierdas tiempo revisando configuraciones lógicas: tu problema es que el equipo no llega al servidor DHCP, y en nueve de cada diez casos la causa es física (cable desconectado, switch apagado) o el servicio DHCP caído. APIPA permite que los equipos se comuniquen entre sí en una red pequeña sin servidor, pero no da puerta de enlace, así que no hay salida a internet.

La dirección de broadcast: sirve para hablarle a todos los equipos de la red al mismo tiempo. Hay dos tipos. El broadcast dirigido usa la última dirección de la red: en 192.168.1.0/24 es 192.168.1.255. Un paquete enviado ahí lo reciben todos los equipos de esa red. El broadcast limitado es 255.255.255.255: significa "todos los de MI red local" y los routers nunca lo dejan pasar a otras redes. Los broadcasts son necesarios (así se descubren servicios y se resuelven direcciones), pero en exceso saturan la red; por eso los routers los bloquean entre redes y las redes muy grandes se dividen en subredes (tema avanzado que verás después).

Multicast: las direcciones de clase D (224.0.0.0 a 239.255.255.255) identifican grupos de equipos interesados en recibir cierto tráfico, como una estación de radio: quién se suscribe al grupo, recibe. Se usa en videoconferencias, distribución de video y en protocolos de enrutamiento. Como técnico junior rara vez las configurarás, pero debes reconocerlas: si ves una 230.5.5.5 asignada a una interfaz de equipo, algo anda mal, porque las multicast no van en interfaces normales.

La dirección 0.0.0.0 tiene dos significados según el contexto: "esta red" cuando un equipo aún no tiene IP (la verás en las peticiones DHCP), y "todas las direcciones" en tablas de enrutamiento (la ruta por defecto 0.0.0.0/0 significa "todo lo que no sepa a dónde va, mandalo por aquí"). La irás conociendo en su momento; por ahora basta con no confundirla con una IP asignable.

Tabla resumen de direcciones especiales para consulta rápida:

Dirección / bloque	Nombre	Para qué sirve	127.0.0.1 (127.0.0.0/8)	Loopback
Probar tu propia pila de red (localhost)	169.254.0.0/16	APIPA		Autoasignación
cuando no hay DHCP (síntoma de falla)	192.168.1.255 (ejemplo)	Broadcast dirigido		Hablarle a todos los de una red específica
255.255.255.255		Broadcast limitado		Hablarle a todos los de tu red local
224.0.0.0 a 239.255.255.255		Multicast		Grupos de suscripción (clase D)
0.0.0.0	Sin especificar	"Esta red" o "todas las rutas" según contexto	10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16	Privadas RFC 1918
				Redes internas (nunca en internet público)

La máscara de subred: qué es y para qué sirve

Ya sabes que toda dirección IP se divide en porción de red y porción de host. La pregunta es: cómo sabe el equipo dónde termina una y empieza la otra? La respuesta es la máscara de subred, el compañero inseparable de toda dirección IP. Una IP sin máscara es como una dirección postal sin código postal: incompleta y ambigua.

La máscara es un número de 32 bits con una forma muy específica: una secuencia de unos seguida de ceros, sin mezclas. Los unos marcan los bits de la porción de red; los ceros, los de host. Ejemplos que ya conoces:

255.0.0.0 = 11111111.00000000.00000000.00000000 (8 unos: /8, clase A por defecto)
 255.255.0.0 = 11111111.11111111.00000000.00000000 (16 unos: /16, clase B por defecto)
 255.255.255.0 = 11111111.11111111.11111111.00000000 (24 unos: /24, clase C por defecto)

Para qué sirve en la práctica? Para dos cálculos fundamentales que el equipo hace con cada paquete que quieré enviar. Primero: cuál es MI red (se calcula una vez, al configurarse). Segundo: está el destino en MÍ red o en OTRA red (se calcula con cada paquete). Si el destino está en mí red, el equipo le habla directamente. Si está en otra red, se lo manda a la puerta de enlace (el router) para que lo encamine. Todo este proceso usa una operación lógica llamada AND, que verás paso a paso en la siguiente sección.

Una máscara no válida sería algo como 255.0.255.0: los unos no son consecutivos (hay ceros en medio). Las máscaras siempre son unos corridos desde la izquierda y luego ceros. Si ves una máscara "rara" en un examen, ese es el primer filtro: unos consecutivos o no es máscara.

Las máscaras también permiten el subneteo: tomar prestados bits de la porción de host para crear subredes más pequeñas dentro de una red grande. Por ejemplo, una empresa con la red 192.168.1.0/24 (254 hosts) puede dividirla en dos subredes de 126 hosts usando la máscara 255.255.255.128 (/25). El subneteo completo es un tema de otra unidad, pero la idea nace aquí: la máscara es la herramienta que parte y reparte el espacio de direcciones.

Error común: configurar la IP bien pero la máscara mal. Si dos equipos tienen IP 192.168.1.10 y 192.168.1.20 pero uno tiene máscara 255.255.255.0 y el otro 255.255.0.0, pueden tener problemas sutiles de comunicación con otras subredes, porque cada uno calcula "su" red de forma distinta. La máscara debe ser la misma en todos los equipos de la red. Otro error: pensar que la máscara "se adivina" por la clase. En redes modernas con CIDR, la máscara la define el diseño, no la clase: una red 10.x puede usar /24 perfectamente.

Notación CIDR: la forma corta de escribir la máscara

Escribir 255.255.255.0 es largo y propenso a errores de dedo. La notación CIDR (Classless Inter-Domain Routing) lo abrevia con un número después de una diagonal: /24 significa "24 bits de red". Así, 192.168.1.10/24 es lo mismo que IP 192.168.1.10 con máscara 255.255.255.0. Los administradores modernos hablan en CIDR: "la red de ventas es la 10.5.0.0/16", "el enlace punto a punto es un /30". Tienes que leer CIDR con fluidez.

Tabla de equivalencias CIDR a máscara decimal (las más usadas; memoriza al menos /8, /16, /24 y /30):

CIDR	Máscara decimal	Bits de host	Direcciones totales	Hosts útiles /8	255.0.0.0	
24	16,777,216	16,777,214	/16	255.255.0.0	16	65,536
65,534 /24	255.255.255.0	8	256	254 /25	255.255.255.128	7
128	126 /26	255.255.255.192	6	64	62 /27	255.255.255.224
5	32	30 /28	255.255.255.240	4	16	14 /29
255.255.255.248	3	8	6 /30	255.255.255.252	2	4
2 /31	255.255.255.254	1	2	2 (caso especial punto a punto) /32		
255.255.255.255	0	1	1 (un solo equipo)			

Cómo se lee la tabla? El número después de la diagonal dice cuantos bits son de red; el resto (32 menos ese número) son bits de host. Las direcciones totales son 2 elevado a los bits de host: /24 tiene 8 bits de host, $2^8 = 256$. Los hosts útiles restan 2 (dirección de red y broadcast), excepto en /31 y /32 que son casos especiales. Él /30 merece atención: con solo 2

hosts útiles, es el tamaño perfecto para un enlace punto a punto entre dos routers (cada router usa una IP y no se desperdicia nada). Lo verás muchísimo en diseños reales.

Para convertir CIDR a máscara decimal, cuenta los unos por octeto. Ejemplo /26: 26 unos = 8 + 8 + 8 + 2. Los primeros tres octetos llenos son 255.255.255. El cuarto octeto tiene 2 unos: 11000000 = 128 + 64 = 192. Resultado: 255.255.255.192. Otro ejemplo, /20: 8 + 8 + 4. Tercer octeto con 4 unos: 11110000 = 128 + 64 + 32 + 16 = 240. Resultado: 255.255.240.0. Con la tabla de valores memorizada (128, 192, 224, 240, 248, 252, 254, 255), esta conversión te toma segundos.

La puerta de enlace predeterminada

La puerta de enlace predeterminada (default gateway) es la dirección IP del router que le da salida a tu red hacia otras redes. Es, siguiendo la analogía postal, la oficina de correos de tu colonia: todo lo que va fuera de tu zona pasa por ahí. En tu casa, la puerta de enlace suele ser 192.168.1.1 o 192.168.0.1: la IP del módem-router. En una empresa, es la IP de la interfaz del router que mira hacia tu subred.

Su configuración es crítica: un equipo con IP y máscara correctas pero sin puerta de enlace (o con la puerta mal escrita) podrá hablar con sus vecinos de red local, pero nada de lo que vaya a otra red saldrá jamás. El síntoma clásico: "puedo hacer ping a mis compañeros pero no tengo internet". Antes de culpar al proveedor, revisa la puerta de enlace con ipconfig: si está vacía o mal, ahí está tu culpable. La puerta de enlace debe pertenecer a tu misma red (tener la misma porción de red que tu IP); una puerta 192.168.2.1 no le sirve a un equipo en 192.168.1.10/24, porque está en otra red y el equipo ni siquiera podría hablarle directamente.

En redes con DHCP, la puerta de enlace llega automáticamente junto con la IP y la máscara. En configuración manual (servidores, impresoras, equipos de red), la tienes que escribir tu, y un dedazo aquí deja al equipo aislado del mundo. Verifica siempre los tres datos juntos: IP, máscara y puerta de enlace. Son el trio inseparable de la configuración IPv4.

Cómo sabe un equipo si el destino está en su red: la operación AND

Llegamos al corazón lógico de la unidad: el procedimiento exacto que sigue tu computadora cada vez que envía un paquete. Es un algoritmo de tres pasos que usa la operación AND bit a bit.

La operación AND compara dos bits y da 1 solo si ambos son 1; en cualquier otro caso da 0. Tabla completa:

1 AND 1 = 1 1 AND 0 = 0 0 AND 1 = 0 0 AND 0 = 0

Truco para recordarla: AND es estricto, solo el 1 con 1 pasa.

El procedimiento: paso 1, el equipo calcula SU dirección de red haciendo AND entre su IP y su máscara. Paso 2, calcula la dirección de red DEL DESTINO haciendo AND entre la IP destino y SU PROPIA máscara (usa su máscara, no la del destino, porque no la conoce). Paso 3, compara: si ambas direcciones de red son iguales, el destino está en su red local y le habla directamente; si son distintas, le manda el paquete a la puerta de enlace.

Vamos con un ejemplo completo, bit a bit. Tu equipo: IP 192.168.1.10, máscara 255.255.255.0. Quiero hablar con 192.168.1.50.

Paso 1: tu red = 192.168.1.10 AND 255.255.255.0. Los primeros tres octetos: cualquier número AND 255 da el mismo número (porque 255 es 11111111 y AND con unos deja todo igual). El cuarto octeto: 10 AND 0 = 0. Resultado: 192.168.1.0. Esa es tu red.

Paso 2: red del destino = 192.168.1.50 AND 255.255.255.0 = 192.168.1.0.

Paso 3: 192.168.1.0 es igual a 192.168.1.0. Conclusión: el destino está en tu red. Tu equipo averigua la MAC del destino (con ARP, tema de otra unidad) y le habla directamente, sin router.

Segundo ejemplo: mismo equipo, destino 192.168.2.50.

Paso 1: tu red = 192.168.1.0 (ya calculada). Paso 2: red del destino = 192.168.2.50 AND 255.255.255.0 = 192.168.2.0. Paso 3: 192.168.1.0 es distinto de 192.168.2.0. Conclusión: el destino está en OTRA red. Tu equipo manda el paquete a su puerta de enlace (por ejemplo 192.168.1.1) y el router se encarga de llevarlo.

Tercer ejemplo con máscara distinta para que veas el poder de la máscara. Equipo: 10.10.5.20 con máscara 255.255.0.0 (/16). Destino: 10.10.8.40.

Paso 1: 10.10.5.20 AND 255.255.0.0. Primeros dos octetos igual (10.10), últimos dos AND 0 = 0.0. Tu red: 10.10.0.0. Paso 2: 10.10.8.40 AND 255.255.0.0 = 10.10.0.0. Paso 3: iguales. El destino está en tu red local aunque el tercer octeto difiera (5 contra 8), porque con máscara /16 el tercer octeto es porción de host. Si la máscara fuera /24, serían redes distintas. La máscara manda: ella define que significa "mi red".

Este procedimiento lo ejecuta tu equipo miles de veces por segundo sin que lo notes. Entenderlo te da superpoderes de diagnóstico: cuando alguien dice "no veo al servidor", tú calculas las redes de ambos extremos y en segundos sabes si el problema es que están en redes distintas sin ruta, o si están en la misma red y el problema es otro.

Subneteo básico: partir una red en pedazos

Ya sabes usar la máscara para identificar redes; ahora aprende su superpoder: el subneteo (subnetting), qué es tomar una red grande y partirla en subredes más pequeñas. Por qué querrías partir una red? Por tres razones: para aislar tráfico (que el departamento de contabilidad no vea el tráfico de ventas), para reducir los broadcasts (cada subred es su propio dominio de broadcast, y menos equipos por dominio significa menos ruido) y para organizar (una subred por piso, por departamento o por sucursal). Es una de las tareas clásicas del administrador de red, así que vamos a hacerla completa con un ejemplo.

Escenario: tu empresa tiene la red 192.168.10.0/24 (254 hosts útiles) y quieré dividirla en 4 subredes iguales, una por departamento. Procedimiento paso a paso:

Paso 1: cuantos bits necesito robarle a la porción de host? Necesito 4 subredes, y $2^2 = 4$, así que robo 2 bits. La máscara pasa de /24 a /26 ($24 + 2$). Nueva máscara: 255.255.255.192.

Paso 2: cuál es el tamaño de cada subred? Me quedan 6 bits de host: $2^6 = 64$ direcciones por subred, 62 útiles.

Paso 3: cuáles son las 4 subredes? El cuarto octeto se divide en bloques de 64:

Subred 1: 192.168.10.0/26 (red .0, broadcast .63, útiles .1 a .62) Subred 2: 192.168.10.64/26 (red .64, broadcast .127, útiles .65 a .126) Subred 3: 192.168.10.128/26 (red .128, broadcast .191, útiles .129 a .190) Subred 4: 192.168.10.192/26 (red .192, broadcast .255, útiles .193 a .254)

Verificación: 4 subredes por 64 direcciones = 256, que es la red original completa. Nada se pierde, nada se traslapa. Cada departamento recibe su subred con 62 equipos útiles, y para comunicarlás entre si se usa un router (o un switch de capa 3) como puerta de enlace de cada una.

La fórmula general que debes memorizar: si necesitas N subredes, buscas el número de bits prestados (b) tal que 2^b sea mayor o igual a N; la nueva máscara es la original más b bits; cada subred tendrá $2^{(\text{bits de host restantes})}$ direcciones. Ejemplo rápido: red 10.0.0.0/8 dividida en 8 subredes: $2^3 = 8$, robo 3 bits, nueva máscara /11, cada subred con $2^{21} = 2,097,152$ direcciones. El método es él mismo sin importar el tamaño.

Errores típicos al subnetear: olvidar restar las 2 direcciones reservadas por subred (no por red original: cada subred tiene su propia red y su propio broadcast); traslapar rangos por no verificar que los bloques sumen el total; y elegir un número de bits prestados que no sea potencia útil (si necesitas 6 subredes, debes robar 3 bits y te salen 8: las 2 sobrantes se reservan para crecer, no se regalan a otra red).

Configuración manual vs DHCP: dónde viven estos datos

La IP, la máscara y la puerta de enlace tienen que llegar al equipo de alguna forma. Hay dos: configuración manual (estática) y configuración automática por DHCP.

En la configuración manual, tú escribes los tres datos (más los DNS) en las propiedades del adaptador de red. Se usa en equipos que nunca deben cambiar de dirección: servidores, impresoras de red, routers, puntos de acceso y cámaras. Ventaja: control total y direcciones predecibles (el servidor de archivos siempre es el .10, por ejemplo). Desventaja: no escala; configurar a mano 200 computadoras es una tortura y un dedazo deja un equipo fuera de la red. Buena práctica: documenta cada IP estática en una hoja de cálculo (equipo, IP, MAC, ubicación) para no asignar la misma dos veces; una IP duplicada produce fallas intermitentes misteriosas en ambos equipos.

DHCP (Dynamic Host Configuration Protocol, protocolo de configuración dinámica) es el método automático: un servidor DHCP (normalmente tu router en casa, o un servidor dedicado en empresas) reparte IPs de un rango definido, junto con la máscara, la puerta de enlace y los DNS. El equipo al encenderse pide ("¿quién me da IP?"), el servidor le ofrece una libre, el equipo la acepta y listo, en segundos y sin intervención humana. Es lo que hace que conectar tu celular al Wi-Fi de un café funcione mágicamente.

El DHCP reparte direcciones en "préstamo" (lease): cada IP se asigna por un tiempo (horas o días) y se renueva automáticamente. El servidor lleva la cuenta de cuáles están ocupadas para no repetirlas. Puedes configurar reservas: decirle al DHCP "a esta MAC siempre dale esta IP", combinando lo mejor de ambos mundos (automaticidad + predictibilidad), ideal para impresoras.

Cuándo falla el DHCP, ya sabes el síntoma: APIPA 169.254.x.x. Las causas, en orden de probabilidad: el equipo no llega físicamente al servidor (revisa cable y switch primero, cómo aprendiste en la unidad 3), el servidor DHCP está apagado o sin direcciones libres en su rango, o alguien puso un segundo servidor DHCP pirata en la red (un router casero conectado al revés, clásico en oficinas) que reparte datos incorrectos. El comando para renovar la configuración en Windows es "ipconfig /renew", y para liberarla "ipconfig /release": son tu primer auxilio lógico después de revisar lo físico.

Errores comunes al configurar IPv4 (y cómo detectarlos)

Cierro la explicación con la galería de errores que verás en el campo, con su síntoma y su diagnóstico:

IP duplicada: dos equipos con la misma IP. Síntoma: ambos se conectan y desconectan de forma intermitente; Windows muestra un aviso de conflicto. Diagnóstico: revisa tu documentación de IPs estáticas o el registro del DHCP; cambia una de las dos.

Máscara incorrecta: el equipo calcula mal su red. Síntoma: ve a algunos vecinos pero no a otros, de forma aparentemente aleatoria. Diagnóstico: compara la máscara del equipo con la del resto de la red; debe ser idéntica.

Puerta de enlace incorrecta o ausente: síntoma ya estudiado, red local si, internet no. Diagnóstico: ipconfig y compara con un equipo que sí navegue.

IP de otra red: alguien configuro 192.168.5.10 en una red 192.168.1.0/24. Síntoma: el equipo no ve a nadie. Diagnóstico: el AND revela que su red calculada no coincide con la de los demás.

DNS mal configurado: cuidado, este se disfraza de problema de IP. Síntoma: el ping a 8.8.8.8 funciona pero las páginas no abren ("no tengo internet" cuando en realidad si hay conectividad). Diagnóstico: si los pings a IPs funcionan pero los nombres no resuelven, el problema es DNS, no IP. Lo verás a fondo en su unidad, pero desde ahora separa en tú mente "llegar a la IP" de "resolver el nombre".

El método profesional de diagnóstico, en orden, es: 1) físico (cable, enlace, luces), 2) IP propia (tengo IP válida o APIPA?), 3) ping a mí puerta de enlace, 4) ping a una IP de internet (8.8.8.8), 5) ping a un nombre (google.com). El paso donde se rompa la cadena te dice exactamente la capa del problema. Este método, de adentro hacia afuera, te convierte de "reiniciador de módems" en técnico de verdad.

IPv4 en la vida real: tu casa por dentro

Vamos a aplicar todo lo aprendido a la red que mejor conoces: la de tu casa. Entender tu propia red con ojos de técnico es el mejor laboratorio gratuito que existe.

Un hogar típico mexicano con internet de Telmex o Totalplay funciona así. El módem-router que te instaló el técnico tiene dos "caras". Hacia afuera (hacia internet) tiene una IP pública que le asigna el proveedor, por ejemplo 187.45.120.33: esa es la dirección con la que tu casa se presenta al mundo, y es la única que "existe" en internet. Hacia adentro (hacia tus equipos) el router crea una red privada, casi siempre 192.168.1.0/24, y él mismo router ocupa la 192.168.1.1 como puerta de enlace. Es decir: tu casa entera comparte una sola IP pública hacia afuera (gracias al NAT del router), mientras adentro cada equipo tiene su IP privada.

El servidor DHCP del router reparte direcciones de un rango como 192.168.1.100 a 192.168.1.200 para los equipos que se conectan (tu celular, tu laptop, la smart TV, la tablet de

tu hermano). Las primeras direcciones (.2 a .99) suelen quedar libres para asignaciones manuales: ahí pondrías la impresora de red (.50) o tu servidor casero (.10) si quieres que nunca cambien. La máscara en todos es 255.255.255.0, la puerta es 192.168.1.1 y los DNS los del proveedor o públicos como 8.8.8.8.

Haz este ejercicio mental de técnico: tu celular tiene la 192.168.1.105 y quieré ver un video en un servidor con IP pública 142.250.0.10. Tu celular calcula con AND: su red es 192.168.1.0, la red del destino (con su máscara) es 142.250.0.0; distintas, así que manda el paquete a su puerta 192.168.1.1. El router recibe el paquete, lo traduce con NAT (cambia la IP privada origen por su IP pública 187.45.120.33 y anota la conversación), lo manda a internet, recibe la respuesta y se la devuelve a tu celular. Todo esto pasa en milisegundos, cientos de veces por segundo, por cada equipo de la casa. Cuando entiendes este flujo completo (tu IP privada, tu red, tu puerta, el NAT del router, la IP pública), ya piensas como un profesional de redes.

Y cuando algo falla en casa, aplica el método de diagnóstico: tu laptop dice "sin internet". Paso 1: el Wi-Fi está conectado? (físico/inalámbrico). Paso 2: ipconfig, tengo 192.168.1.x o una 169.254.x.x? Si es APIPA, el DHCP del router no responde: reinicia el router. Paso 3: ping a 192.168.1.1, responde? Si no, el problema está entre tu equipo y el router. Paso 4: ping a 8.8.8.8, responde? Si la puerta responde pero internet no, el problema está en el proveedor o en el NAT. Paso 5: si 8.8.8.8 responde pero google.com no abre, es DNS. Con este método ya no dependes de "apagar y prender a ver si se arregla": sabes exactamente dónde está el problema antes de llamar al técnico.

Ejemplos paso a paso

Aquí practicamos los cálculos que un técnico hace en papel o mentalmente. Sigue cada ejemplo con tu propia hoja y verifica los resultados antes de leer la explicación.

Ejemplo 1: convertir 192.168.10.25 a binario, octeto por octeto

Usamos el método de restas con la tabla de valores 128 64 32 16 8 4 2 1.

Octeto 1: 192

192 - 128 = 64 -> 1

64 - 64 = 0 -> 1

resto 0 -> 0 0 0 0 0 0

Resultado: 11000000

Octeto 2: 168

168 - 128 = 40 -> 1

64 no cabe -> 0

40 - 32 = 8 -> 1

16 no cabe -> 0

8 - 8 = 0 -> 1

resto 0 -> 0 0 0

Resultado: 10101000

Octeto 3: 10

128, 64, 32, 16 no caben -> 0 0 0 0

10 - 8 = 2 -> 1

4 no cabe -> 0

2 - 2 = 0 -> 1

1 no cabe -> 0

Resultado: 00001010

Octeto 4: 25

128, 64, 32 no caben -> 0 0 0

25 - 16 = 9 -> 1

9 - 8 = 1 -> 1

4, 2 no caben -> 0 0

1 - 1 = 0 -> 1

Resultado: 00011001

Dirección completa: 11000000.10101000.00001010.00011001

Explicación: cada octeto se resuelve por separado restando de mayor a menor. El error típico es saltarse una posición y escribir 7 bits en lugar de 8: cuenta siempre ocho dígitos por octeto antes de pasar al siguiente.

Ejemplo 2: convertir 11000000.10101000.00001010.00011001 a decimal

Ahora el camino inverso, sumando los valores de las posiciones con 1:

```
11000000 -> 128 + 64 = 192
10101000 -> 128 + 32 + 8 = 168
00001010 -> 8 + 2 = 10
00011001 -> 16 + 8 + 1 = 25
```

Dirección completa: 192.168.10.25

Explicación: es el mismo ejemplo anterior al revés, y el resultado coincide, lo que confirma que ambas conversiones están bien. En la práctica memorizarás los valores comunes (192, 168, 10, 172, 255) y solo calcularás los raros.

Ejemplo 3: diseccionar una red completa 172.16.45.100/20

Este es el ejercicio completo que te pedirán en exámenes y en el trabajo: dada una IP con CIDR, obtener todos los datos de su red.

Datos: IP 172.16.45.100, CIDR /20

Paso 1: mascara decimal.

/20 = 20 unos = 8 + 8 + 4

Tercer octeto con 4 unos: 11110000 = 128+64+32+16 = 240

Mascara: 255.255.240.0

Paso 2: direccion de red (IP AND mascara, octeto por octeto).

172 AND 255 = 172

16 AND 255 = 16

45 AND 240 = ?

45 = 00101101

240 = 11110000

AND = 00100000 = 32

100 AND 0 = 0

Direccion de red: 172.16.32.0

Paso 3: direccion de broadcast (red con todos los bits de host en 1).

Bits de host = 32 - 20 = 12

Los ultimos 12 bits en 1: tercer octeto 00101111 = 47, cuarto 255

Broadcast: 172.16.47.255

Paso 4: rango de hosts utiles.

Desde la red + 1 hasta el broadcast - 1:

172.16.32.1 a 172.16.47.254

Paso 5: numero de hosts utiles.

$2^{12} = 4096$ direcciones, menos 2 = 4094 hosts utiles.

Resumen de la red 172.16.32.0/20:

Red: 172.16.32.0 | Broadcast: 172.16.47.255

Utiles: 172.16.32.1 - 172.16.47.254 (4094 equipos)

Explicación: el paso clave es el AND del tercer octeto (45 AND 240 = 32), porque ahí la máscara "corta" en medio del octeto. Observa que la red no es 172.16.45.0 como parecería a simple vista: con /20, el tercer octeto se agrupa de 16 en 16 (0-15, 16-31, 32-47, 48-63...), y él 45 cae en el bloque 32-47. Este es el tipo de detalle que separa a quién memoriza de quién calcula.

Ejemplo 4: están en la misma red? 10.0.3.15/24 y 10.0.4.20/24

Equipo A: 10.0.3.15, mascara 255.255.255.0

Equipo B: 10.0.4.20, mascara 255.255.255.0

Red de A: 10.0.3.15 AND 255.255.255.0 = 10.0.3.0

Red de B: 10.0.4.20 AND 255.255.255.0 = 10.0.4.0

10.0.3.0 es distinto de 10.0.4.0 -> REDES DISTINTAS

Conclusion: A y B necesitan un router (puerta de enlace) para hablar.

Explicación: aunque las IP "se parecen", el tercer octeto difiere y con /24 ese octeto es porción de red. Si la máscara fuera /16, ambas estarían en 10.0.0.0 y hablarían directo. Moraleja: nunca juzgues por apariencia; calcula.

Ejemplo 5: tabla de potencias de 2 para cálculos rápidos

Guarda esta tabla; es tu calculadora mental para hosts y subredes:

```
2^1  = 2
2^2  = 4
2^3  = 8
2^4  = 16
2^5  = 32
2^6  = 64
2^7  = 128
2^8  = 256
2^9  = 512
2^10 = 1024
2^11 = 2048
2^12 = 4096
2^16 = 65536
2^24 = 16777216
```

Explicación: los bits de host (n) te dan 2^n direcciones. Con /26 hay 6 bits de host: $2^6 = 64$ direcciones, 62 útiles. Con /12 hay 20 bits de host: $2^{20} = 1,048,576$ direcciones. Memoriza del 2^1 al 2^8 y los hitos 2^{10} , 2^{16} y 2^{24} ; lo demás lo interpolas.

Ejemplo 6: leer la configuración real con ipconfig

```
C:\> ipconfig
```

```
Adaptador de Ethernet Ethernet:
```

```
Direccion IPv4. . . . . : 192.168.1.25
Mascara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . : 192.168.1.1
```

Explicación línea por línea aplicada a lo aprendido: la IP 192.168.1.25 es privada (bloque 192.168.0.0/16 de la RFC 1918) y de clase C. La máscara /24 indica red 192.168.1.0, broadcast 192.168.1.255 y 254 hosts útiles (del .1 al .254); tu equipo es el host 25. La puerta 192.168.1.1 pertenece a tu misma red (pasa la prueba del AND), así que es válida. Todo paquete hacia otra red saldrá por 192.168.1.1. En diez segundos de lectura ya sabes la clase, la red, el broadcast, tu número de host y tu salida: eso es leer una IP como profesional.

Práctica

1. Convierte la dirección 172.20.8.75 a binario, octeto por octeto, mostrando las restas.

SOLUCIÓN: Trabajamos cada octeto con la tabla 128 64 32 16 8 4 2 1. Octeto 172: 172 - 128 = 44, pongo 1; 64 no cabe, 0; 44 - 32 = 12, pongo 1; 16 no cabe, 0; 12 - 8 = 4, pongo 1; 4 - 4 = 0, pongo 1; resto ceros: 0, 0. Resultado: 10101100. Verificación: 128 + 32 + 8 + 4 = 172, correcto. Octeto 20: 128, 64, 32 no caben: 0, 0, 0; 20 - 16 = 4, pongo 1; 8 no cabe, 0; 4 - 4 = 0, pongo 1; resto 0, 0. Resultado: 00010100. Verificación: 16 + 4 = 20, correcto. Octeto 8: solo cabe el 8: 00001000. Octeto 75: 75 - 64 = 11, pongo 1; 32 no cabe, 0; 16 no cabe, 0; 11 - 8 = 3, pongo 1; 4 no cabe, 0; 3 - 2 = 1, pongo 1; 1 - 1 = 0, pongo 1. Resultado: 01001011. Verificación: 64 + 8 + 2 + 1 = 75, correcto. Dirección completa: 10101100.00010100.00001000.01001011. Cada octeto tiene exactamente 8 dígitos: si alguno te quedó de 7, te faltó un cero a la izquierda.

2. Convierte 11000000.10101000.01100100.00000111 a decimal. Que clase es? Es privada o pública?

SOLUCIÓN: Sumamos por octeto. 11000000: $128 + 64 = 192$. 10101000: $128 + 32 + 8 = 168$. 01100100: $64 + 32 + 4 = 100$. 00000111: $4 + 2 + 1 = 7$. Dirección: 192.168.100.7. Clase: el primer octeto 192 está en el rango 192-223, así que es clase C. Es privada: pertenece al bloque 192.168.0.0/16 de la RFC 1918. Conclusión: es la típica IP de un equipo en una red local pequeña, probablemente asignada por el DHCP de un router casero o de una pyme.

3. Clasifica cada dirección: indica su clase y si es privada, pública o especial. a) 10.15.2.8 b) 172.32.5.1 c) 192.168.200.7 d) 224.0.0.251 e) 127.0.0.1 f) 169.254.10.20

SOLUCIÓN: a) 10.15.2.8: primer octeto 10, clase A; privada (bloque 10.0.0.0/8 de la RFC 1918). b) 172.32.5.1: primer octeto 172, parecería privada, pero el segundo octeto es 32 y el rango privado es 172.16 a 172.31; por tanto es PÚBLICA de clase B. Este es el caso trampa clásico: memoriza 16 a 31. c) 192.168.200.7: clase C, privada (bloque 192.168.0.0/16). d) 224.0.0.251: primer octeto 224, clase D, multicast; especial, nunca se asigna a un equipo. e) 127.0.0.1: clase A por rango, pero reservada como loopback; especial, apunta a tu propia máquina. f) 169.254.10.20: APIPA; especial, significa que el equipo no encontró servidor DHCP y se autoasigna. Si la ves en un diagnóstico, busca el problema en la capa física o en el DHCP.

4. Para la red 192.168.50.130/26 calcula: máscara decimal, dirección de red, dirección de broadcast, rango de hosts útiles y número de hosts útiles.

SOLUCIÓN: Paso 1, máscara: /26 son 26 unos, o sea $8 + 8 + 8 + 2$; el cuarto octeto con 2 unos es 11000000 = 192. Máscara: 255.255.255.192. Paso 2, red: hago AND octeto por octeto; los tres primeros quedan 192.168.50; el cuarto: $130 \text{ AND } 192$. En binario, $130 = 10000010$ y $192 = 11000000$; AND = $10000000 = 128$. Red: 192.168.50.128. (Truco alternativo: con /26 los bloques del cuarto octeto van de 64 en 64: 0-63, 64-127, 128-191, 192-255; él 130 cae en el bloque 128-191, así que la red es .128.) Paso 3, broadcast: bits de host = $32 - 26 = 6$; el bloque termina en $128 + 64 - 1 = 191$. Broadcast: 192.168.50.191. Paso 4, rango útil: de la red + 1 al broadcast - 1, es decir, 192.168.50.129 a 192.168.50.190. Paso 5, hosts útiles: $2^6 = 64$ direcciones menos 2 = 62 hosts. Resumen: red 192.168.50.128, broadcast 192.168.50.191, útiles del .129 al .190, 62 equipos.

5. Dos equipos en una oficina: la PC-A tiene IP 192.168.10.5, máscara 255.255.255.0 y puerta 192.168.10.1; la PC-B tiene IP 192.168.10.200, máscara 255.255.255.0 y no tiene puerta de enlace configurada. La PC-B puede hacer ping a la PC-A pero no puede abrir ninguna página de internet. La PC-A navega sin problema. Cuál es el diagnóstico y la solución?

SOLUCIÓN: El diagnóstico es que a la PC-B le falta la puerta de enlace. Analicemos: ambas están en la red 192.168.10.0/24 (el AND lo confirma), por eso el ping entre ellas funciona: el tráfico local no necesita router. Pero todo lo que va a internet está en otra red, y sin puerta de enlace la PC-B no sabe a quién entregarle esos paquetes; los descarta. La PC-A si tiene puerta (192.168.10.1) y por eso navega. La solución es configurar en la PC-B la puerta de enlace 192.168.10.1, la misma que la PC-A. Paso a paso: abrir la configuración del adaptador, agregar la puerta de enlace predeterminada 192.168.10.1, y probar con ping a la puerta primero y luego a una dirección de internet. Moraleja del ejercicio: "veo mi red local pero no tengo internet" casi siempre es puerta de enlace ausente o incorrecta; es de los primeros tres datos que se revisan en un diagnóstico.

6. Una sucursal nueva tendrá 60 equipos conectados. El administrador propone usar 192.168.20.0/24 para esa sucursal. Otro técnico propone 192.168.20.0/26. Evalúa ambas propuestas: cuántos hosts útiles da cada una, alcanza para los 60 equipos, y cuántas direcciones se desperdician en cada caso?

SOLUCIÓN: Evaluemos. Propuesta /24: 8 bits de host = 256 direcciones, 254 útiles. Alcanza de sobra para 60 equipos, pero desperdicia $254 - 60 = 194$ direcciones. Propuesta /26: 6 bits de host = 64 direcciones, 62 útiles. Alcanza justo para 60 equipos (quedan 2 libres), desperdiciando solo $62 - 60 = 2$ direcciones. Técnicamente la /26 es más eficiente y sería la respuesta "de libro". Pero el criterio profesional matiza: con /26 quedan solo 2 direcciones libres, así que sí la sucursal crece a 63 equipos habrá que cambiar toda la máscara; con /24 hay margen para crecer sin tocar nada. En direcciones privadas el desperdicio no cuesta dinero (no se agotan), así que muchos administradores prefieren /24 por simplicidad y margen de crecimiento, reservando el subneteo ajustado para cuándo el espacio si es limitado. Conclusión: /26 es la eficiente, /24 es la cómoda; con IPs privadas, la recomendación práctica es /24 a menos que haya una razón para ajustar. Lo importante es que sepas calcular ambas y justificar tu decisión.

7. Una empresa tiene la red 192.168.44.0/24 y necesita dividirla en 8 subredes iguales para sus 8 departamentos. Calcula: cuántos bits debes robar, cuál es la nueva máscara en decimal y CIDR, cuántas direcciones útiles tiene cada subred, y escribe la dirección de red y el rango útil de la tercera subred.

SOLUCIÓN: Paso 1, bits a robar: necesito 8 subredes y $2^3 = 8$, así que robo 3 bits. Nueva máscara: $/24 + 3 = /27$, que en decimal es 255.255.255.224 (terceros tres octetos llenos y cuarto octeto con 3 unos: $11100000 = 128 + 64 + 32 = 224$). Paso 2, tamaño de cada subred: me quedan 5 bits de host, $2^5 = 32$ direcciones por subred, 30 útiles.

Verificación: 8 subredes por 32 = 256, la red original completa. Paso 3, bloques: el cuarto octeto se divide de 32 en 32: subred 1: 192.168.44.0/27 (útiles .1 a .30), subred 2: 192.168.44.32/27 (útiles .33 a .62), subred 3: 192.168.44.64/27 (útiles .65 a .94), subred 4: .96/27, subred 5: .128/27, subred 6: .160/27, subred 7: .192/27, subred 8: .224/27. **Respuesta pedida:** la tercera subred es 192.168.44.64/27, su broadcast es 192.168.44.95 y su rango útil es 192.168.44.65 a 192.168.44.94 (30 equipos). Cada departamento conectaría su switch a un router con 8 interfaces (o un switch de capa 3) que haría de puerta de enlace de cada subred, por ejemplo .65 para la tercera. Si un departamento crece más de 30 equipos, habría que replanear: por eso se estima el crecimiento antes de subnetear.

Resumen de la unidad

En esta unidad convertiste las direcciones IP de un misterio en una herramienta de trabajo. Aprendiste que una dirección IPv4 son 32 bits divididos en cuatro octetos, que los humanos leemos en notación decimal con puntos (192.168.1.10), y que toda dirección se parte en porción de red (la "colonia", común a todos) y porción de host (el "número de casa", único por equipo). Dominaste la conversión entre binario y decimal desde cero con la tabla de valores 128 a 1 y los métodos de restas y sumas, incluyendo los valores de máscara que debes memorizar.

Estudiaste el sistema de clases: A (1-126, redes gigantes), B (128-191, redes medianas), C (192-223, redes pequeñas como tu casa), D (224-239, multicast) y E (240-255, experimental), con sus rangos, sus máscaras por defecto y el cálculo de hosts (2 elevado a los bits de host, menos la red y el broadcast). Conociste las direcciones privadas de la RFC 1918 (10.0.0.0/8, 172.16.0.0/12 con el truco del 16 al 31, y 192.168.0.0/16) y por qué se pueden repetir en millones de redes. Y memorizaste las especiales: loopback 127.0.0.1 para probarte a ti mismo, APIPA 169.254.x.x como síntoma de falla de DHCP, broadcast dirigido y limitado para hablarle a todos, multicast de clase D y el 0.0.0.0 de doble significado.

La parte más práctica fue la clase 12: la máscara de subred como divisoria entre red y host, la notación CIDR (/24, /30 y su tabla de equivalencias) como el idioma moderno de los administradores, la puerta de enlace como la "oficina postal" hacia otras redes, y el algoritmo del AND que ejecuta tu equipo con cada paquete: calcula su red, calcula la red del destino con su propia máscara, compara, y decide si habla directo o manda al router. Practicaste diseccionar redes completas (red, broadcast, rango útil, número de hosts) y a diagnosticar con lógica en lugar de adivinar.

También aprendiste a partir redes con el subneteo básico: robar bits de host para crear subredes iguales (como dividir 192.168.10.0/24 en cuatro /26), con la fórmula de 2 elevado a los bits prestados y la verificación de que los bloques sumen la red original. Viste dónde viven los datos de configuración: la asignación manual para servidores e impresoras (con su documentación obligatoria) y el DHCP automático para el resto, con sus síntomas de falla (APIPA) y sus comandos de auxilio (ipconfig /release y /renew). Repasaste la galería de errores típicos (IP duplicada, máscara mal, puerta ausente, IP de otra red y el DNS disfrazado de problema de IP) y el método de diagnóstico de adentro hacia afuera en cinco pasos. Y cerraste aplicando todo a tu propia casa: la doble cara del módem-router, el NAT compartiendo una IP pública, el rango DHCP y el flujo completo de un paquete desde tu celular hasta internet.

La idea que debes llevarte: una IP sin su máscara y sin su puerta de enlace no dice nada; los tres datos juntos cuentan la historia completa de un equipo en la red. Con lo físico de la unidad 3 (cables, señal, enlace) y lo lógico de esta unidad 4 (direcciones, máscaras, puertas), ya tienes las dos primeras capas del modelo OSI en tus manos. Antes de pasar a la siguiente unidad, verifica que puedes hacer estas siete cosas sin mirar tus apuntes: convertir cualquier octeto entre binario y decimal en menos de un minuto; decir la clase de cualquier IP por su primer octeto; identificar si una dirección es privada, pública o especial; escribir la máscara decimal de /8, /16, /24, /26 y /30; calcular red, broadcast y rango útil de una /24 y una /26; aplicar el AND para decidir si dos equipos están en la misma red; y explicar con tus palabras que hace la puerta de enlace. Si alguna te cuesta, regresa a su sección y practícala con otros números: la fluidez con estos cálculos es lo que distingue al técnico que diagnostica del que adivina. Nos vemos en la siguiente unidad, donde las direcciones IP cobrarán vida en el tráfico real de la red.

En la siguiente unidad subirás otro nivel: el protocolo ARP que traduce IPs a direcciones físicas, y el ICMP con el que el ping y el diagnóstico se vuelven tú segunda naturaleza.

UNIDAD 5: Subneteo, CIDR y VLSM

Hay un momento en la vida de todo estudiante de redes en el que las direcciones IP dejan de ser números sueltos y se convierten en un rompecabezas que se resuelve con lápiz, papel y un poco de lógica. Ese momento es el subneteo, y esta unidad es tu guía completa para dominarlo desde cero hasta un nivel que te permita resolver ejercicios de certificación sin temblar.

En esta unidad vas a ver tres clases encadenadas. La clase 13 te enseña el subneteo clásico: por qué se divide una red, cómo se prestan bits de la porción de host, la famosa fórmula 2^n , y como calcular para cada subred su dirección de red, su dirección de broadcast y su rango de direcciones útiles, con ejemplos completos usando la red 192.168.1.0/24. La clase 14 te presenta CIDR y la notación de barra: que significa ese "/24", "/26" o "/30" que ves después de las direcciones, la tabla completa de máscaras, como convertir una máscara a prefijo y viceversa, y el supernetting, que es la operación contraria al subneteo y sirve para agregar rutas. La clase 15 cierra con VLSM, las máscaras de longitud variable: como diseñar subredes de tamaños distintos según lo que cada departamento necesite, con el método del bloque más grande primero y un ejemplo completo de una empresa real.

Por qué importa tanto este tema. Imagina que trabajas en el área de sistemas de una empresa mediana. Tienen 200 computadoras repartidas en ventas, contabilidad, soporte técnico y gerencia, más una red para invitados y un par de enlaces hacia sucursales. Si pones a las 200 máquinas en una sola red plana, pasan tres cosas malas. Primera: cada vez que una computadora grita un broadcast buscando a otra, las 200 lo escuchan, y ese ruido constante frena la red. Segunda: cualquiera ve a cualquiera, así que el becario de ventas podría curiosear los servidores de contabilidad donde están las nóminas. Tercera: si la empresa crece y necesitas más redes, ya no tienes de dónde sacarlas porque desperdiciaste todo el espacio en una sola. El subneteo resuelve las tres: divide la red grande en pedazos lógicos, cada departamento en su subred, los broadcasts se quedan encerrados en su pedazo, pones un router entre subredes para controlar quien habla con quién, y aprovechas cada dirección.

El segundo motivo es más personal: si algún día presentas un examen de certificación como el CCNA, el subneteo aparece en una cantidad enorme de preguntas. No es exageración decir que dominar estos cálculos puede ser la diferencia entre aprobar y reprobar. Y lo mejor es que, una vez que entiendes el método, cada ejercicio se vuelve mecánico: sigues los pasos, haces las cuentas y llegas al resultado. No hay magia, solo práctica.

Al terminar esta unidad sabrás leer una dirección como 192.168.1.0/24 y decir al instante cuantas direcciones tiene, cuál es su máscara, cuál es su broadcast y cuantas máquinas

caben. Sabrás dividirla en 2, 4, 8 o 64 subredes iguales, convertir máscaras a prefijos de memoria, resumir varias redes en una sola ruta y diseñar un plan VLSM completo para una empresa sin desperdiciar direcciones. Vamos paso a paso, sin prisa y con muchos números resueltos.

Explicación detallada

Repaso rápido: el binario sin lágrimas

Todo el subneteo vive en el sistema binario, así que antes de prestar bits y calcular saltos necesitas sentirte cómodo convirtiendo entre decimal y binario. La buena noticia es que solo necesitas manejar números del 0 al 255, que son exactamente los valores que caben en un octeto, es decir, en 8 bits.

Cada posición de un número binario de 8 bits vale el doble que la anterior, de derecha a izquierda: 1, 2, 4, 8, 16, 32, 64 y 128. Para convertir un decimal a binario, simplemente preguntas: cuál es el valor más grande de la lista que cabe en mi número. Lo restas, pones un 1 en esa posición, y repites con lo que sobra. Las posiciones que no usaste llevan 0.

Mira el 192, que aparece en casi todos los ejemplos de redes privadas. El valor más grande que cabe en 192 es 128. Lo restas: $192 - 128 = 64$. Él 64 cabe exacto en 64: $64 - 64 = 0$. Entonces él 192 es $128 + 64$, y en binario queda 11000000. Él 168 es $128 + 32 + 8$, así que en binario es 10101000. Él 1 es 00000001 y él 0 es 00000000. Con esto ya puedes escribir 192.168.1.0 en binario:

```
11000000.10101000.00000001.00000000
```

Para convertir al revés, de binario a decimal, sumas los valores de las posiciones donde hay un 1. Por ejemplo 11100000 es $128 + 64 + 32 = 224$. Y 11110000 es $128 + 64 + 32 + 16 = 240$. Estos dos números, 224 y 240, te van a perseguir durante toda la unidad porque son valores típicos de máscaras de subred. Memoriza de una vez la tabla de los octetos "fronterizos", los que aparecen en las máscaras:

```
10000000 = 128
11000000 = 192
11100000 = 224
11110000 = 240
11111000 = 248
11111100 = 252
11111110 = 254
11111111 = 255
```

Fijate en el patrón: cada valor agrega un 1 más a la izquierda. Si sabes que 128 es un 1 seguido de ceros, y que cada paso suma el siguiente valor de la lista 64, 32, 16, 8, 4, 2, 1, puedes reconstruir la tabla en cualquier momento. En un examen, escribir esta tablita en una hoja antes de empezar te ahorra minutos valiosos.

Un truco útil: si ves un octeto de máscara y quieres saber cuantos unos tiene en binario sin convertirlo todo, cuenta cuantos valores de la lista 128, 64, 32, 16, 8, 4, 2, 1 necesitas sumar para llegar a él. Él 240 necesita 128 + 64 + 32 + 16, o sea 4 unos. Él 248 necesita 5 unos. Él 192 necesita 2 unos. Este conteo de unos es exactamente lo que significa el número después de la diagonal en la notación CIDR, como verás en la clase 14.

Por qué dividir una red: el problema que resuelve el subneteo

Una dirección IPv4 tiene 32 bits. En el esquema clásico, esos bits se reparten entre la porción de red, que identifica a la red, y la porción de host, que identifica a cada equipo dentro de esa red. Una red /24, por ejemplo, usa 24 bits para red y deja 8 bits para hosts, lo que da 256 direcciones en total. Hasta aquí todo bien cuando tu red es pequeña.

El problema aparece cuando la red crece o cuando necesitas orden. Piensa en una escuela: no metes a todos los alumnos de todos los grados en un solo salón gigante. Los separas por grupos, cada grupo con su maestro y su salón, porque así se controla mejor el ruido, se mantiene el orden y cada grupo avanza a su ritmo. Una red sin subnetear es ese salón gigante: todos los equipos comparten el mismo espacio, los mensajes de broadcast llegan a todos, y no hay forma de aplicar reglas distintas a grupos distintos.

Dividir una red en subredes te da tres beneficios concretos. Primero, reduces el tráfico de broadcast. Un broadcast es un mensaje que una máquina envía a todas las demás de su red, por ejemplo cuando pregunta "¿quién tiene esta dirección IP?". En una red de 500 equipos, cada broadcast interrumpe a 499. Si divides esos 500 equipos en 5 subredes de 100, cada broadcast solo molesta a 99. Los routers no reenvían broadcasts, así que cada subred queda con su propio dominio de broadcast, pequeño y manejable.

Segundo, mejoras la seguridad y el control. Entre subredes tiene que haber un router, y en ese router puedes poner reglas: la subred de invitados puede salir a internet pero no puede entrar a la subred de contabilidad; la subred de servidores solo acepta conexiones de la subred de administradores. Sin subredes, todo ese control es imposible porque todos están en el mismo segmento.

Tercero, aprovechas mejor las direcciones. Supon que tu proveedor te asigna la red 192.168.1.0/24, con 256 direcciones, pero en realidad necesitas tres redes separadas: una de 100 equipos, una de 50 y una de 20. Sin subneteo tendrías que pedir tres redes /24 distintas y desperdiciarías cientos de direcciones. Con subneteo, partes tu /24 en pedazos del tamaño justo para cada necesidad y no desperdicias casi nada.

Hay un cuarto beneficio que solo se aprecia con el tiempo: el orden administrativo. Cuando cada departamento, cada piso del edificio o cada sucursal tiene su propia subred con un rango conocido, diagnosticar fallas es mucho más fácil. Si alguien reporta que no tiene internet y su IP es 192.168.1.130, tú ya sabes que está en la segunda subred y puedes ir directo a revisar el switch o el cableado de ese segmento.

El préstamo de bits: la idea central del subneteo

Aquí está la idea que lo explica todo: subnetear es tomar prestados bits de la porción de host y usarlos como bits extra de red. Esos bits prestados sirven para numerar las subredes, y los bits de host que quedan sirven para numerar los equipos dentro de cada subred.

Imagina la red 192.168.1.0/24. En binario, los primeros 24 bits son la porción de red y los últimos 8 son la porción de host:

```
Red (24 bits):  11000000.10101000.00000001.  
Host (8 bits):                                00000000
```

Si tomas prestados 2 bits de la porción de host, la división queda así: 26 bits de red y 6 bits de host. La notación cambia de /24 a /26, y la máscara cambia de 255.255.255.0 a 255.255.255.192. Esos 2 bits prestados pueden valer 00, 01, 10 u 11, o sea 4 combinaciones, o sea 4 subredes. Los 6 bits de host que quedan pueden numerar 64 direcciones por subred.

```
Bits prestados (2):    00 | 01 | 10 | 11  -> 4 subredes  
Bits de host (6):     000000 a 111111  -> 64 direcciones por subred
```

Cada bit que prestas duplica la cantidad de subredes y reduce a la mitad el tamaño de cada una. Es un trueque directo: más subredes significa subredes más pequeñas. Por eso el primer

paso de cualquier diseño es preguntarte que necesitas más: muchas subredes o subredes grandes. La respuesta depende de tu caso, y las fórmulas que siguen te permiten calcular las dos cosas.

Un error común de principiantes es pensar que al subnetear "se crean direcciones nuevas". No es así. El total de direcciones sigue siendo el mismo: 256 en nuestro ejemplo. Lo único que cambia es como las agrupas. Es como cortar una pizza en 4 rebanadas en vez de 8: la pizza sigue siendo la misma, solo cambia el tamaño de cada pedazo.

La fórmula 2^n y la tabla de potencias de 2

Todo el subneteo se reduce a dos fórmulas y una tabla que debes saberte de memoria. La primera fórmula calcula cuantas subredes obtienes:

```
Numero de subredes =  $2^n$   
donde n = numero de bits prestados
```

La segunda calcula cuantos hosts caben en cada subred:

```
Hosts por subred =  $2^h - 2$   
donde h = numero de bits de host que quedan
```

Se restan 2 porque en cada subred hay dos direcciones reservadas que ningún equipo puede usar: la dirección de red, que identifica a la subred misma, y la dirección de broadcast, que sirve para hablarle a todos los equipos de la subred a la vez. En un momento verás exactamente cuáles son.

La tabla de potencias de 2 es tu mejor amiga en esta unidad. Memorízala completa, del 2^1 al 2^{16} como mínimo:

$2^1 = 2$	$2^9 = 512$
$2^2 = 4$	$2^{10} = 1024$
$2^3 = 8$	$2^{11} = 2048$
$2^4 = 16$	$2^{12} = 4096$
$2^5 = 32$	$2^{13} = 8192$
$2^6 = 64$	$2^{14} = 16384$
$2^7 = 128$	$2^{15} = 32768$
$2^8 = 256$	$2^{16} = 65536$

Con la tabla a la mano, los cálculos son inmediatos. Ejemplo: prestas 3 bits. Subredes = $2^3 = 8$. Si partiste de un /24, te quedan 5 bits de host. Hosts por subred = $2^5 - 2 = 32 - 2 = 30$. Así de rápido.

Otro ejemplo al revés, que es como suelen preguntarlo en exámenes: necesitas al menos 12 subredes. Cuantos bits debes prestar. Buscas en la tabla la potencia de 2 qué sea igual o mayor que 12: $2^3 = 8$ no alcanza, $2^4 = 16$ si alcanza. Respuesta: 4 bits prestados, que te dan 16 subredes, de las cuales usarás 12 y te sobran 4 para crecer. Fijate que siempre redondeas hacia arriba: nunca puedes tener "un pedazo de bit", así que tomas la potencia que cubra tu necesidad aunque sobre un poco.

Y un tercer ejemplo: necesitas subredes con al menos 50 hosts cada una. Cuantos bits de host necesitas. Buscas $2^h - 2 \geq 50$, o sea $2^h \geq 52$. En la tabla: $2^5 = 32$ no alcanza, $2^6 = 64$ si alcanza. Necesitas 6 bits de host, que te dan 62 hosts útiles por subred. Si partiste de un /24, los bits prestados son $8 - 6 = 2$, así que tu prefijo será /26 y obtendrás 4 subredes de 62 hosts.

Estos tres tipos de pregunta, bits para N subredes, hosts que caben con H bits, y bits necesarios para N hosts, son el 80 por ciento de los ejercicios de subneteo. Domina la tabla y dominas los ejercicios.

Dirección de red, broadcast y rango útil: las tres direcciones clave

Cada subred tiene tres direcciones que debes saber identificar con los ojos cerrados: la dirección de red, la dirección de broadcast y el rango útil. Vamos a definirlas con precisión porque confundirlas es el error número uno en los exámenes.

La dirección de red es la primera dirección de la subred: todos los bits de host en 0. No se le asigna a ningún equipo; sirve para identificar a la subred completa. Es como el nombre de la calle: no es la dirección de ninguna casa, es cómo se llama la calle entera. Cuando un router tiene que decidir a dónde mandar un paquete, compara la dirección destino con las direcciones de red de su tabla de ruteo.

La dirección de broadcast es la última dirección de la subred: todos los bits de host en 1. Tampoco se asigna a ningún equipo; sirve para enviar un mensaje a todos los equipos de la subred al mismo tiempo. Es el equivalente a gritar en el pasillo para que todos los salones te escuchen. Los protocolos la usan para descubrir vecinos, pedir direcciones y anunciar servicios.

El rango útil son todas las direcciones entre la dirección de red y la de broadcast. Estas si se pueden asignar a computadoras, impresoras, teléfonos y a la interfaz del router que sirve como puerta de enlace. La primera dirección útil suele reservarse para el router, aunque no es una regla obligatoria: es una convención muy extendida que facilita la administración.

Vamos a calcularlo con un ejemplo concreto: la red 192.168.1.0/24 sin dividir. Tiene 8 bits de host, o sea 256 direcciones, de la 192.168.1.0 a la 192.168.1.255.

```
Direccion de red: 192.168.1.0    (todos los bits de host en 0)
Direccion de broadcast: 192.168.1.255 (todos los bits de host en 1)
Rango util:      192.168.1.1 a 192.168.1.254
Hosts utiles:    256 - 2 = 254
```

Ahora dividela en 4 subredes prestando 2 bits, quedando un prefijo /26. Cada subred tiene 6 bits de host, o sea 64 direcciones y 62 útiles. La primera subred usa los bits prestados en 00:

```
Subred 1: bits prestados = 00
  Direccion de red: 192.168.1.0    (00000000 en el ultimo octeto)
  Direccion de broadcast: 192.168.1.63 (00111111 en el ultimo octeto)
  Rango util:      192.168.1.1 a 192.168.1.62
```

Fijate en el último octeto en binario: los dos primeros bits son los prestados (00) y los seis restantes son los de host. La dirección de red pone los seis en 0: 00000000 = 0. El broadcast los pone en 1: 00111111 = 63. El rango útil va del 1 al 62. La segunda subred usa los bits prestados en 01, así que su último octeto va de 01000000 (64) a 01111111 (127). Y así con las cuatro.

Un truco para no equivocarte: la dirección de broadcast de una subred siempre es la dirección de red de la siguiente subred menos uno. Si la segunda subred empieza en 192.168.1.64, el broadcast de la primera es 192.168.1.63. Y el rango útil siempre empieza en red + 1 y termina en broadcast - 1. Con estas dos reglas puedes reconstruir todo aunque solo recuerdes las direcciones de red.

La máscara de subred: el mapa que separa red de host

La máscara de subred es un número de 32 bits que le dice a cualquier equipo cuáles bits de una dirección IP pertenecen a la red y cuales al host. Donde la máscara tiene un 1, ese bit es de red; donde tiene un 0, ese bit es de host. Los unos siempre van juntos al principio y los ceros al final, sin mezclarse.

Para la red 192.168.1.0/24, la máscara tiene 24 unos seguidos de 8 ceros:

```
Mascara /24 en binario: 11111111.11111111.11111111.00000000
Mascara /24 en decimal: 255.255.255.0
```

Cuándo prestas 2 bits y pasas a /26, la máscara gana dos unos:

```
Mascara /26 en binario: 11111111.11111111.11111111.11000000
Mascara /26 en decimal: 255.255.255.192
```

Para qué sirve en la práctica. Cuando tu computadora quiere saber si otra IP está en su misma red o en una red distinta, hace una operación AND lógico entre su propia IP y la máscara, y hace lo mismo con la IP destino. Si los dos resultados son iguales, el destino está en la misma red y la computadora le habla directamente. Si son distintos, el destino está en otra red y la computadora manda el paquete a su puerta de enlace, el router, para que él lo encamine. Todo ese proceso ocurre en milisegundos cada vez que abres una página.

Hagamos el AND a mano una vez para que veas que no es magia. Tu IP es 192.168.1.70 con máscara 255.255.255.192 (/26), y quieres hablar con 192.168.1.100. Tomas el último octeto de cada una en binario: 70 es 01000110, 100 es 01100100, y la máscara es 11000000. El AND compara bit por bit y pone 1 solo donde ambos son 1:

```
01000110 (70)
AND 11000000 (mascara 192)
= 01000000 (64)
```

```
01100100 (100)
AND 11000000 (mascara 192)
= 01000000 (64)
```

Ambos resultados son 64, así que las dos direcciones pertenecen a la subred 192.168.1.64/26 y pueden hablarse directamente. Si el destino fuera 192.168.1.200 (11001000), el AND daría 11000000 = 192, o sea la subred 192.168.1.192/26, distinta, y el paquete iría al router. Así de simple y así de poderoso es el AND con la máscara.

El cálculo del salto: el atajo que usan los profesionales

Calcular subredes en binario funciona, pero es lento. Los profesionales usan un atajo llamado salto, también conocido como tamaño de bloque o "magic number". El salto te dice de cuanto en cuanto avanzan las direcciones de red de las subredes, y se calcula así:

Salto = 256 - valor del octeto interesante de la mascara

El octeto interesante es aquel donde la máscara no es ni 255 ni 0, es decir, dónde ocurre la división entre unos y ceros. En 255.255.255.192, el octeto interesante es el cuarto y vale 192, así que el salto es $256 - 192 = 64$. Eso significa que las subredes empiezan en 0, 64, 128 y 192. Exactamente lo que calculamos antes con binario, pero en dos segundos.

Práctica el salto con varias máscaras típicas sobre un /24:

```
Mascara 255.255.255.128 (/25): salto = 256 - 128 = 128 -> subredes en 0, 128
Mascara 255.255.255.192 (/26): salto = 256 - 192 = 64 -> subredes en 0, 64, 128, 192
Mascara 255.255.255.224 (/27): salto = 256 - 224 = 32 -> subredes en 0, 32, 64, 96, 128, 160, 192, 224
Mascara 255.255.255.240 (/28): salto = 256 - 240 = 16 -> subredes en 0, 16, 32, ... , 240
Mascara 255.255.255.248 (/29): salto = 256 - 248 = 8 -> subredes en 0, 8, 16, ... , 248
Mascara 255.255.255.252 (/30): salto = 256 - 252 = 4 -> subredes en 0, 4, 8, ... , 252
```

Memoriza esta lista. Con ella puedes resolver casi cualquier ejercicio de subneteo sobre redes /24 sin tocar el binario: el salto te da las direcciones de red, el broadcast es la siguiente red menos uno, y el rango útil es lo de en medio.

El método completo y rápido para resolver un ejercicio, suponiendo que te dan red y máscara o prefijo, es este: primero identifica el octeto interesante y calcula el salto; segundo, escribe las direcciones de red sumando el salto; tercero, para la subred que te pidan, el broadcast es la siguiente dirección de red menos uno; cuarto, el rango útil va de red + 1 a broadcast - 1; quinto, si te piden la cantidad de hosts, usa $2^h - 2$ con los bits de host que queden. Cinco pasos, siempre los mismos, sin importar el ejercicio.

Un detalle importante: el salto también funciona cuando el octeto interesante no es el cuarto. Si subnetas 10.0.0.0/8 con máscara 255.255.0.0, no hay préstamo y no hay cálculo. Pero si usas 255.255.128.0 (/17), el octeto interesante es el tercero con valor 128, el salto es 128, y las subredes son 10.0.0.0/17 y 10.0.128.0/17. El salto se aplica al octeto donde esté, y los octetos a su derecha se quedan en cero para las direcciones de red.

Ejemplo completo guiado: 192.168.1.0/24 dividida en 4 subredes

Vamos a juntar todo en un ejemplo resuelto de principio a fin, como los que te pondrán en un examen. Enunciado: divide la red 192.168.1.0/24 en 4 subredes iguales. Para cada subred indica la dirección de red, la dirección de broadcast, el rango útil y la máscara.

Paso 1: cuantos bits hay que prestar. Necesitas 4 subredes, y $2^2 = 4$, así que prestas 2 bits. El prefijo pasa de /24 a /26.

Paso 2: la máscara. Un /26 tiene 26 unos: 255.255.255.192. En binario el último octeto es 11000000.

Paso 3: el salto. $256 - 192 = 64$. Las direcciones de red son 192.168.1.0, 192.168.1.64, 192.168.1.128 y 192.168.1.192.

Paso 4: hosts por subred. Quedan 6 bits de host: $2^6 - 2 = 62$ hosts útiles por subred.

Paso 5: la tabla completa.

Subred 1:

Dirección de red: 192.168.1.0
Dirección de broadcast: 192.168.1.63
Rango útil: 192.168.1.1 - 192.168.1.62
Máscara: 255.255.255.0 -> 255.255.255.192 (/26)

Subred 2:

Dirección de red: 192.168.1.64
Dirección de broadcast: 192.168.1.127
Rango útil: 192.168.1.65 - 192.168.1.126
Máscara: 255.255.255.192 (/26)

Subred 3:

Dirección de red: 192.168.1.128
Dirección de broadcast: 192.168.1.191
Rango útil: 192.168.1.129 - 192.168.1.190
Máscara: 255.255.255.192 (/26)

Subred 4:

Dirección de red: 192.168.1.192
Dirección de broadcast: 192.168.1.255
Rango útil: 192.168.1.193 - 192.168.1.254
Máscara: 255.255.255.192 (/26)

Verificación rápida, que siempre debes hacer: 4 subredes por 64 direcciones = 256 direcciones totales, que es justo lo que tenía la /24 original. Nada se creó ni se perdió. Y 4 por 62 hosts

útiles = 248 direcciones asignables. Si tu verificación no cuadra, revisa el salto: el 90 por ciento de los errores están ahí.

Fíjate además en un patrón útil: la última subred siempre termina en .255 cuándo partes de una /24, y su broadcast es la dirección final de la red original. Esto te sirve para detectar errores: si tú última subred no llega a .255, algo calculaste mal.

Vamos a hacer un segundo ejemplo rápido con otros números para que veas que el método no cambia: divide 192.168.1.0/24 en 8 subredes. Bits prestados: $2^3 = 8$, prestas 3 bits, prefijo /27, máscara 255.255.255.224, salto $256 - 224 = 32$, hosts por subred $2^5 - 2 = 30$. Las redes van de 32 en 32: .0, .32, .64, .96, .128, .160, .192, .224. Toma la tercera como muestra: red 192.168.1.64, broadcast 192.168.1.95, rango útil 192.168.1.65 a 192.168.1.94. Mismo método, distintos números, mismo resultado correcto.

CIDR y la notación de barra: adiós a las clases

Hasta ahora hemos usado la notación de barra, como /24 o /26, de forma natural. Es momento de entenderla a fondo, porque CIDR, que significa enrutamiento entre dominios sin clases, cambio para siempre la forma de repartir direcciones IP.

Antes de CIDR, a principios de los años 90, las direcciones se repartían por clases rígidas: las redes clase A usaban /8, las clase B usaban /16 y las clase C usaban /24, sin punto medio. Si tu empresa necesitaba 300 direcciones, la clase C con 254 útiles no te alcanzaba y tenías que pedir una clase B completa con más de 65 mil direcciones, desperdiciando casi todo. Era como si en una tienda solo vendieran zapatos en talla chica, mediana y enorme, sin intermedios.

CIDR eliminó esas tallas fijas y permitió cualquier longitud de prefijo: /19, /22, /25, /27, la que necesites. El número después de la diagonal indica exactamente cuantos bits, contando desde la izquierda, pertenecen a la porción de red. Eso es todo lo que significa: /26 quiere decir "los primeros 26 bits son de red y los 6 restantes son de host". La máscara es simplemente esa misma información escrita en decimal punteado: 26 unos seguidos de ceros, o sea 255.255.255.192.

Gracias a CIDR, un proveedor de internet puede asignarte exactamente el tamaño que necesitas. Si pides espacio para 1000 hosts, te puede dar un /22 con 1022 útiles en vez de obligarte a tomar una clase B entera. Y los routers de internet, en vez de guardar millones de rutas /24 individuales, guardan rutas agregadas más cortas, lo que mantiene manejable la tabla de ruteo global. Sin CIDR, el crecimiento de internet habría colapsado los routers hace décadas.

Un punto que confunde a muchos: CIDR no es lo mismo que subneteo, aunque usan las mismas herramientas. El subneteo divide una red que ya tienes en pedazos más pequeños, prestando bits hacia la derecha, haciendo el prefijo más largo. CIDR es el sistema general de notación y asignación que permite prefijos de cualquier longitud, y además permite la operación contraria: el supernetting, que agrupa redes pequeñas en una más grande acortando el prefijo. Piensa en el subneteo como cortar la pizza en rebanadas y en el supernetting como juntar rebanadas para describir la pizza entera con una sola frase.

Tabla completa de máscaras y prefijos

Esta tabla es oro puro. Copiala a mano un par de veces y quedará grabada en tu memoria. Incluye los prefijos más usados, del /8 al /30, con su máscara en decimal, su máscara en binario resumida y cuantas direcciones y hosts útiles representa cada uno.

Prefijo	Mascara decimal	Unos en binario	Direcciones	Hosts utiles
/8	255.0.0.0	8 unos + 24 ceros	16,777,216	16,777,214
/9	255.128.0.0	9 unos + 23 ceros	8,388,608	8,388,606
/10	255.192.0.0	10 unos + 22 ceros	4,194,304	4,194,302
/11	255.224.0.0	11 unos + 21 ceros	2,097,152	2,097,150
/12	255.240.0.0	12 unos + 20 ceros	1,048,576	1,048,574
/13	255.248.0.0	13 unos + 19 ceros	524,288	524,286
/14	255.252.0.0	14 unos + 18 ceros	262,144	262,142
/15	255.254.0.0	15 unos + 17 ceros	131,072	131,070
/16	255.255.0.0	16 unos + 16 ceros	65,536	65,534
/17	255.255.128.0	17 unos + 15 ceros	32,768	32,766
/18	255.255.192.0	18 unos + 14 ceros	16,384	16,382
/19	255.255.224.0	19 unos + 13 ceros	8,192	8,190
/20	255.255.240.0	20 unos + 12 ceros	4,096	4,094
/21	255.255.248.0	21 unos + 11 ceros	2,048	2,046
/22	255.255.252.0	22 unos + 10 ceros	1,024	1,022
/23	255.255.254.0	23 unos + 9 ceros	512	511
/24	255.255.255.0	24 unos + 8 ceros	256	254
/25	255.255.255.128	25 unos + 7 ceros	128	126
/26	255.255.255.192	26 unos + 6 ceros	64	62
/27	255.255.255.224	27 unos + 5 ceros	32	30
/28	255.255.255.240	28 unos + 4 ceros	16	14
/29	255.255.255.248	29 unos + 3 ceros	8	6
/30	255.255.255.252	30 unos + 2 ceros	4	2

Observa los patrones. Cada vez que el prefijo aumenta en 1, las direcciones se reducen a la mitad: es la misma lógica del préstamo de bits. Los prefijos /30 son especiales: con solo 2 bits de host dan 4 direcciones y 2 útiles, y se usan casi exclusivamente para enlaces punto a punto

entre dos routers, donde solo se necesitan dos direcciones, una para cada extremo del cable. Existe también el /31, con 2 direcciones y ninguna reservada, que algunos equipos modernos aceptan para esos mismos enlaces, pero en exámenes y en la práctica común el /30 es el estándar para punto a punto.

Otro patrón útil: los hosts útiles siempre son una potencia de 2 menos 2. Si memorizas las potencias, ya tienes la columna de hosts sin memorizar nada más: /26 tiene 6 bits de host, $2^6 = 64$, menos 2 = 62. Así de directo.

Cómo convertir máscara a prefijo y viceversa

Convertir en ambas direcciones es una habilidad básica que te pedirán de muchas formas. Hay dos métodos: el rápido, usando la tabla de arriba, y el manual, contando unos en binario. Aprende el manual primero y usa la tabla para verificar.

De máscara a prefijo, método manual: convierte a binario el octeto u octetos que no sean 255 ni 0, y cuenta los unos. Ejemplo: 255.255.255.224. Los tres primeros octetos aportan $8 + 8 + 8 = 24$ unos. El 224 es 11100000, que tiene 3 unos. Total: 27. La máscara es un /27. Otro ejemplo: 255.255.240.0. Primeros dos octetos: 16 unos. El 240 es 11110000: 4 unos. Total: 20. Es un /20.

De prefijo a máscara, método manual: escribe tantos unos como indique el prefijo, completa con ceros hasta 32 bits, y convierte cada octeto a decimal. Ejemplo: /26. Son 26 unos: los primeros tres octetos quedan en 8 unos cada uno, o sea 255.255.255, y el cuarto octeto tiene 2 unos y 6 ceros: 11000000 = 192. Resultado: 255.255.255.192. Otro ejemplo: /19. Primeros dos octetos: 255.255. El tercer octeto tiene 3 unos: 11100000 = 224. El cuarto: 0. Resultado: 255.255.224.0.

Con práctica harás estas conversiones en segundos. Un ejercicio mental para el camión o la fila del banco: toma un prefijo al azar entre /16 y /30, convierte a máscara, y luego convierte de regreso. Cuando puedas hacerlo sin dudar, esta habilidad está dominada.

Supernetting y agregación de rutas: juntar en vez de dividir

El supernetting, también llamado agregación de rutas o resumen de rutas, es la operación inversa del subneteo: en vez de dividir una red grande en pedazos, tomas varias redes pequeñas contiguas y las describes con una sola ruta más corta. Su gran utilidad está en los routers: menos rutas en la tabla significa menos memoria usada y decisiones más rápidas.

Ejemplo clásico: tienes cuatro redes /24 consecutivas: 192.168.0.0/24, 192.168.1.0/24, 192.168.2.0/24 y 192.168.3.0/24. En vez de anunciar las cuatro por separado, puedes

anunciar una sola ruta: 192.168.0.0/22. Cómo se llega a ese /22. Escribes el tercer octeto de la primera y la última red en binario: 0 es 00000000 y 3 es 00000011. Los bits que son iguales en ambas, contando desde la izquierda, son los primeros 6: 000000. Esos 6 bits, sumados a los 16 del /24 original en los dos primeros octetos, dan 22 bits de red común. La ruta agregada es 192.168.0.0/22 con máscara 255.255.252.0, y cubre exactamente de 192.168.0.0 a 192.168.3.255.

La regla de oro para agregar es que las redes deben ser contiguas y su cantidad debe ser una potencia de 2: 2, 4, 8, 16 redes. Además deben estar alineadas al límite del bloque: cuatro redes /24 se pueden agregar en un /22 solo si empiezan en un múltiplo de 4 en el tercer octeto, como 0, 4 u 8. Las redes 192.168.1.0/24 a 192.168.4.0/24 no se pueden resumir en un solo /22 porque no están alineadas; el resumen correcto tendría que ser más largo o en dos rutas.

Otro ejemplo: ocho redes /24 de 10.1.0.0/24 a 10.1.7.0/24. Ocho es 2^3 , así que el prefijo se acorta 3 bits: de /24 a /21. La ruta agregada es 10.1.0.0/21, máscara 255.255.248.0, que cubre de 10.1.0.0 a 10.1.7.255. Verificalo con el salto: el tercer octeto de la máscara es 248, salto = $256 - 248 = 8$, así que el bloque /21 avanza de 8 en 8 en el tercer octeto: 0 a 7 es el primer bloque. Cuadra perfecto.

En la práctica, la agregación se usa muchísimo en redes grandes y en internet: un proveedor que tiene asignado un bloque /19 no anuncia miles de /24 a sus vecinos, anuncia su /19 y listo. Menos rutas, internet más rápido para todos.

VLSM: máscaras de longitud variable

El subneteo clásico que vimos en la clase 13 tiene una limitación: todas las subredes resultantes son del mismo tamaño. Si divides un /24 en 4 subredes, las 4 son /26 con 62 hosts cada una. Pero en la vida real los departamentos no son iguales: ventas necesita 100 equipos, contabilidad 25, y los enlaces entre routers solo 2. Si usas subredes iguales, o te quedas corto en ventas o desperdicias direcciones en los enlaces.

VLSM, que significa máscara de subred de longitud variable, resuelve esto permitiendo que cada subred tenga su propio tamaño, su propia longitud de máscara. Sobre la misma red original puedes crear una subred /25 para ventas, una /27 para contabilidad y varias /30 para los enlaces. Cada pedazo se ajusta a su necesidad, como un sastre que corta cada traje a la medida en vez de vender solo talla mediana.

La única regla que no puedes romper con VLSM es que las subredes no deben traslaparse: cada dirección de la red original puede pertenecer a una sola subred. Por eso existe un método ordenado para diseñar, que evita errores y desperdicio: el método del bloque más grande primero.

El método del bloque más grande primero

El método tiene cuatro pasos y funciona siempre:

Paso 1: ordeña tus necesidades de mayor a menor cantidad de hosts. Siempre empieza por la más grande.

Paso 2: para la necesidad más grande, calcula el prefijo más pequeño que la cubra usando $2^h - 2$. Asigna el primer bloque libre de la red a esa subred.

Paso 3: pasa a la siguiente necesidad, calcula su prefijo, y asignale el siguiente bloque libre, justo donde terminó la anterior.

Paso 4: repite hasta cubrir todas las necesidades. Lo que sobre al final queda como espacio libre para crecer.

Por qué el orden importa. Si asignas primero los bloques pequeños, dejas huecos fragmentados entre ellos y después el bloque grande ya no cabe en ningún espacio continuo. Es como guardar maletas en la cajuela: primero las grandes y luego rellenas los huecos con las chicas. Al revés no funciona.

Vamos a aplicarlo a un caso de empresa completo, con todos los cálculos a la vista.

Ejemplo completo VLSM: la empresa con cuatro departamentos

Enunciado: la empresa tiene asignada la red 192.168.5.0/24. Necesita subredes para: ventas con 100 hosts, soporte con 50 hosts, contabilidad con 25 hosts, gerencia con 10 hosts, y dos enlaces punto a punto entre routers, cada uno con 2 hosts. Diseña el plan VLSM.

Paso 1: ordenar de mayor a menor: ventas 100, soporte 50, contabilidad 25, gerencia 10, enlace 1 con 2, enlace 2 con 2.

Paso 2: ventas, 100 hosts. Necesito $2^h - 2 \geq 100$, o sea $2^h \geq 102$. En la tabla: $2^6 = 64$ no alcanza, $2^7 = 128$ si alcanza. Hago 7 bits de host, prefijo /25, máscara 255.255.255.128, salto 128. Primer bloque libre: empieza en 0.

Ventas: 192.168.5.0/25

Direccion de red: 192.168.5.0

Direccion de broadcast: 192.168.5.127

Rango util: 192.168.5.1 - 192.168.5.126 (126 utiles, cubre los 100)

Paso 3: soporte, 50 hosts. Necesito $2^h \geq 52$: $2^5 = 32$ no alcanza, $2^6 = 64$ si alcanza. Prefijo /26, máscara 255.255.255.192, salto 64. Siguiendo bloque libre: empieza en 128.

Soporte: 192.168.5.128/26

Direccion de red: 192.168.5.128

Direccion de broadcast: 192.168.5.191

Rango util: 192.168.5.129 - 192.168.5.190 (62 utiles, cubre los 50)

Contabilidad, 25 hosts. Necesito $2^h \geq 27$: $2^4 = 16$ no alcanza, $2^5 = 32$ si alcanza. Prefijo /27, máscara 255.255.255.224, salto 32. Siguiendo bloque libre: empieza en 192.

Contabilidad: 192.168.5.192/27

Direccion de red: 192.168.5.192

Direccion de broadcast: 192.168.5.223

Rango util: 192.168.5.193 - 192.168.5.222 (30 utiles, cubre los 25)

Gerencia, 10 hosts. Necesito $2^h \geq 12$: $2^3 = 8$ no alcanza, $2^4 = 16$ si alcanza. Prefijo /28, máscara 255.255.255.240, salto 16. Siguiendo bloque libre: empieza en 224.

Gerencia: 192.168.5.224/28

Direccion de red: 192.168.5.224

Direccion de broadcast: 192.168.5.239

Rango util: 192.168.5.225 - 192.168.5.238 (14 utiles, cubre los 10)

Enlace 1, 2 hosts. Necesito $2^h \geq 4$: $2^2 = 4$ exacto. Prefijo /30, máscara 255.255.255.252, salto 4. Siguiendo bloque libre: empieza en 240.

Enlace WAN 1: 192.168.5.240/30

Direccion de red: 192.168.5.240

Direccion de broadcast: 192.168.5.243

Rango util: 192.168.5.241 - 192.168.5.242 (2 utiles, justo lo necesario)

Enlace 2, igual: siguiente bloque libre en 244.

```
Enlace WAN 2: 192.168.5.244/30
  Direccion de red:      192.168.5.244
  Direccion de broadcast: 192.168.5.247
  Rango util:           192.168.5.245 - 192.168.5.246
```

Paso 4: verificación. Direcciones usadas: $128 + 64 + 32 + 16 + 4 + 4 = 248$. La red /24 tiene 256, así que quedan libres 8 direcciones: de 192.168.5.248 a 192.168.5.255, qué forman un bloque /29 disponible para crecer. Ninguna subred se traslapa con otra y cada departamento quedo con un pequeño colchón para crecer. Diseño limpio y profesional.

Compara con lo que habría pasado usando subredes iguales: para cubrir a ventas con 100 hosts necesitarías subredes /25, y un /24 solo se divide en dos /25. Te faltarían subredes para los demás departamentos. Con VLSM, una sola /24 alcanzo para todo y sobro espacio. Esa es la magia de las máscaras de longitud variable.

Errores comunes de principiantes

Primero: olvidar restar las 2 direcciones reservadas. Si calculas $2^5 = 32$ y dices que caben 32 hosts, está mal: caben 30. La dirección de red y el broadcast no se asignan. Este error aparece en casi todos los exámenes como opción trampa.

Segundo: confundir bits prestados con bits de host en las fórmulas. Recuerda: 2^n para subredes usa los bits prestados, $2^h - 2$ para hosts usa los bits de host que quedan. Si mezclas las letras, los resultados salen al revés.

Tercero: calcular mal el salto por usar el octeto equivocado de la máscara. El salto se calcula con el octeto interesante, el que no es 255 ni 0. En 255.255.255.192 el interesante es el cuarto. En 255.255.240.0 el interesante es el tercero. Si aplicas el salto al octeto equivocado, todas las subredes salen mal.

Cuarto: en VLSM, asignar los bloques en desorden y provocar traslapos. Siempre del bloque más grande al más chico, y cada bloque nuevo empieza donde terminó el anterior. Dibuja una línea de números del 0 al 255 y ve tachando: es el método visual que nunca falla.

Quinto: pensar que la primera dirección útil "tiene" que ser el router y la última "tiene" que ser otra cosa. Son convenciones útiles, no reglas del protocolo. Lo que sí es regla es no usar la dirección de red ni el broadcast en ningún equipo.

Sexto: en supernetting, intentar agregar redes que no están alineadas al límite del bloque. Cuatro /24 solo forman un /22 si empiezan en múltiplo de 4. Verifica la alineación antes de anunciar el resumen.

Buenas prácticas

Documenta tu plan de direccionamiento antes de configurar nada. Una tabla con subred, prefijo, red, broadcast, rango útil y propósito te salva de dolores de cabeza cuando la red crezca o cuando otro técnico tenga que entenderla.

Deja siempre espacio libre para crecer. En el ejemplo VLSM sobre un /29 completo. En diseños reales se suele dejar al menos un 20 por ciento del espacio sin asignar. Las empresas crecen, llegan departamentos nuevos, y re-subnetear una red en producción es un dolor que quieres evitar.

Usa bloques /30 para enlaces punto a punto entre routers. Es el estándar, desperdicia solo 2 direcciones por enlace y deja claro en la documentación que ese segmento es un enlace, no una LAN.

Reserva la primera dirección útil de cada subred para la puerta de enlace. No es obligatorio, pero cuando todos tus routers están en la .1 de su subred, diagnosticar es rapidísimo.

Y por último: verifica siempre tus cálculos con las dos reglas de oro. Regla uno: la suma de las direcciones de todas las subredes debe dar el total de la red original. Regla dos: el broadcast de cada subred es la siguiente dirección de red menos uno. Si ambas se cumplen, tu diseño está bien.

Subneteo más allá del cuarto octeto: prefijos menores a /24

Hasta ahora todos los ejemplos partieron de un /24 y prestaron bits en el cuarto octeto. Pero el mismo método funciona con cualquier prefijo inicial, y en redes grandes es común subnetear un /16 o un /8. La única diferencia es donde cae el octeto interesante.

Toma la red 172.16.0.0/16 y prestale 4 bits: el prefijo pasa a /20 y la máscara a 255.255.240.0. El octeto interesante es el tercero, con valor 240, así que el salto es $256 - 240 = 16$ y se aplica al tercer octeto. Las subredes son 172.16.0.0/20, 172.16.16.0/20, 172.16.32.0/20, y así hasta 172.16.240.0/20. Son $2^4 = 16$ subredes. Los bits de host que quedan son $32 - 20 = 12$, así que cada subred tiene $2^{12} - 2 = 4094$ hosts útiles. Fijate que el cuarto octeto de cada dirección de red queda en cero: cuando el salto vive en el tercer octeto, el cuarto siempre es cero en las direcciones de red.

Otro ejemplo: 10.0.0.0/8 con 8 bits prestados, prefijo /16, máscara 255.255.0.0. Aquí no hay octeto interesante con valor intermedio: el salto se calcula igual, $256 - 255 = 1$ no aplica porque el tercer octeto es 0 completo. En realidad cuando la máscara tiene octetos completos en 255, el salto es 1 en el siguiente octeto: las subredes son 10.0.0.0/16, 10.1.0.0/16, 10.2.0.0/16, hasta 10.255.0.0/16. Son 256 subredes de 65534 hosts cada una. La regla general: el salto siempre

es 256 menos el valor del octeto interesante, y si el octeto interesante vale 0 porque la división cae justo en el límite del octeto, el salto es 1 aplicado al octeto siguiente.

Un caso que vale la pena conocer es el prefijo /31, con máscara 255.255.255.254. Tiene un solo bit de host: 2 direcciones, y en este caso especial ninguna se reserva, así que las 2 son útiles. Se usa únicamente en enlaces punto a punto entre dos routers con equipos modernos que lo soportan. En exámenes clásicos casi no aparece, pero en redes reales lo verás cada vez más. Y el /32, con máscara 255.255.255.255, identifica a un solo host: se usa en tablas de ruteo para rutas específicas a un equipo, como la ruta por defecto invertida o las direcciones loopback.

La moraleja es que el método de los cinco pasos no cambia nunca: identifica el octeto interesante, calcula el salto, escribe las redes, deriva broadcasts y rangos, y verifica. Solo cambia en qué octeto aplicas el salto. Si dominas eso, puedes subnetear cualquier red que te pongan enfrente.

Ejemplos paso a paso

Aquí van cuatro cálculos resueltos de principio a fin con el método de los cinco pasos: identificar el salto, escribir las redes, calcular broadcast, obtener el rango útil y verificar. Leelos con lápiz en mano y repite cada operación antes de ver el resultado.

Ejemplo 1: dividir 192.168.1.0/24 en 4 subredes /26

Enunciado: divide 192.168.1.0/24 en 4 subredes iguales y entrega la tabla completa de cada una.

Paso 1: bits prestados

Necesito 4 subredes $\rightarrow 2^2 = 4 \rightarrow$ presto 2 bits

Prefijo nuevo: $/24 + 2 = /26$

Mascara: 255.255.255.192

Paso 2: salto

Octeto interesante: el cuarto, vale 192

Salto = $256 - 192 = 64$

Direcciones de red: .0, .64, .128, .192

Paso 3: hosts por subred

Bits de host que quedan: $32 - 26 = 6$

Hosts utiles = $2^6 - 2 = 64 - 2 = 62$

Paso 4: tabla completa

Subred 1: red 192.168.1.0 broadcast 192.168.1.63 rango .1 - .62

Subred 2: red 192.168.1.64 broadcast 192.168.1.127 rango .65 - .126

Subred 3: red 192.168.1.128 broadcast 192.168.1.191 rango .129 - .190

Subred 4: red 192.168.1.192 broadcast 192.168.1.255 rango .193 - .254

Paso 5: verificacion

4 subredes x 64 direcciones = 256 = total de la /24. Correcto.

Cada broadcast = siguiente red - 1. Correcto.

Ejemplo 2: cuantas subredes y hosts salen de un /24 con prefijo /27

Enunciado: sobre la red 10.20.30.0/24 aplicas máscara 255.255.255.224. Cuantas subredes obtienes, cuantos hosts por subred, y a que subred pertenece la IP 10.20.30.100.

Paso 1: prefijo de la mascara

255.255.255.224 -> el 224 es 11100000, tiene 3 unos

Prefijo: $24 + 3 = /27$. Bits prestados: 3.

Paso 2: numero de subredes y hosts

Subredes = $2^3 = 8$

Bits de host = $32 - 27 = 5$

Hosts utiles = $2^5 - 2 = 32 - 2 = 30$

Paso 3: salto y redes

Salto = $256 - 224 = 32$

Redes: 10.20.30.0, .32, .64, .96, .128, .160, .192, .224

Paso 4: ubicar la IP 10.20.30.100

100 esta entre 96 y 128 -> pertenece a la subred 10.20.30.96/27

Broadcast de esa subred: $128 - 1 = 10.20.30.127$

Rango util: 10.20.30.97 - 10.20.30.126

La .100 esta dentro del rango util. Es una direccion asignable.

Paso 5: verificacion

$8 \times 32 = 256$. Correcto.

Fijate en la técnica del paso 4: para ubicar una IP dentro de sus subredes no necesitas listarlas todas. Tomas el último octeto, 100, y buscas entre que múltiplos del salto cae: los múltiplos de 32 son 0, 32, 64, 96, 128. El 100 cae entre 96 y 128, así que su red es la .96. Esta técnica de "múltiplos del salto" es la más rápida para responder "a que subred pertenece esta IP".

Ejemplo 3: conversión de máscara a prefijo y de prefijo a máscara

Enunciado A: convierte la máscara 255.255.240.0 a notación de barra.

Los dos primeros octetos aportan $8 + 8 = 16$ unos.

El tercer octeto es 240 = 11110000 -> 4 unos.

El cuarto octeto es 0 -> 0 unos.

Total: $16 + 4 = 20$.

Respuesta: 255.255.240.0 es un /20.

Comprobacion con la tabla: un /20 tiene 4096 direcciones. $256 - 240 = 16$ de salto en el tercer octeto, y $16 \times 256 = 4096$. Cuadra.

Enunciado B: convierte el prefijo /28 a máscara decimal.

28 unos: tres octetos completos = 255.255.255.
Cuarto octeto: 4 unos -> 11110000 = 128 + 64 + 32 + 16 = 240.
Respuesta: /28 = 255.255.255.240.
Comprobacion: salto = 256 - 240 = 16, hosts = $2^4 - 2 = 14$.
Coincide con la tabla de mascararas.

Ejemplo 4: supernetting de cuatro redes /24

Enunciado: resume en una sola ruta las redes 192.168.0.0/24, 192.168.1.0/24, 192.168.2.0/24 y 192.168.3.0/24.

Paso 1: verificar que se puede agregar
Son 4 redes = 2^2 , cantidad valida (potencia de 2).
Son contiguas: tercer octeto 0, 1, 2, 3.
Estan alineadas: empiezan en multiplo de 4 (el 0).
Si se puede agregar.

Paso 2: encontrar los bits comunes
Tercer octeto de la primera: 0 = 00000000
Tercer octeto de la ultima: 3 = 00000011
Bits iguales desde la izquierda: 0, 0, 0, 0, 0, 0 -> 6 bits comunes.

Paso 3: construir el prefijo agregado
16 bits de los dos primeros octetos + 6 bits comunes = /22.
Ruta agregada: 192.168.0.0/22
Mascara: 255.255.252.0

Paso 4: verificar el rango cubierto
Salto en el tercer octeto: 256 - 252 = 4.
El bloque /22 cubre del tercer octeto 0 al 3:
de 192.168.0.0 a 192.168.3.255.
Incluye exactamente las 4 redes originales, ni mas ni menos.

Si las redes hubieran sido de la .1 a la .4, el resumen /22 no serviría porque el bloque tendría que empezar en múltiplo de 4. Ese detalle de la alineación es lo que más se pregunta en exámenes sobre agregación.

Ejemplo 5: subneteo de 172.16.0.0/16 en subredes /20

Enunciado: divide la red 172.16.0.0/16 en subredes /20. Indica cuantas subredes salen, cuantos hosts por subred y las primeras tres subredes completas.

Paso 1: bits prestados

De /16 a /20 se prestan 4 bits.

Subredes = $2^4 = 16$.

Mascara: 255.255.240.0.

Paso 2: salto

Octeto interesante: el tercero, vale 240.

Salto = $256 - 240 = 16$, aplicado al tercer octeto.

Primeras redes: 172.16.0.0, 172.16.16.0, 172.16.32.0.

Paso 3: hosts por subred

Bits de host: $32 - 20 = 12$.

Hosts utiles = $2^{12} - 2 = 4096 - 2 = 4094$.

Paso 4: primeras tres subredes completas

Subred 1: red 172.16.0.0

broadcast 172.16.15.255

rango util 172.16.0.1 - 172.16.15.254

Subred 2: red 172.16.16.0

broadcast 172.16.31.255

rango util 172.16.16.1 - 172.16.31.254

Subred 3: red 172.16.32.0

broadcast 172.16.47.255

rango util 172.16.32.1 - 172.16.47.254

Paso 5: verificacion

16 subredes x 4096 direcciones = 65536 = total de la /16. Correcto.

Cada broadcast = siguiente red - 1 en el tercer octeto. Correcto.

Observa como el broadcast de la primera subred es 172.16.15.255: el tercer octeto llega a 15 porque la siguiente red empieza en 16, y el cuarto octeto llega a 255 porque todos sus bits son de host. Este es el patrón general cuando el salto vive en el tercer octeto.

Práctica

Resuelve cada ejercicio en papel antes de leer la solución. El subneteo se aprende haciendo, no mirando.

1. Divide la red 192.168.20.0/24 en 8 subredes iguales. Indica la máscara nueva en decimal y en notación de barra, la cantidad de hosts útiles por subred y la tabla completa con dirección de red, broadcast y rango útil de cada subred.

SOLUCIÓN:

Para 8 subredes necesitas $2^3 = 8$, así que prestas 3 bits. El prefijo pasa de /24 a /27 y la máscara queda en 255.255.255.224. El salto es $256 - 224 = 32$, así que las direcciones de red son 192.168.20.0, .32, .64, .96, .128, .160, .192 y .224. Te quedan 5 bits de host, así que cada subred tiene $2^5 - 2 = 30$ hosts útiles. La tabla completa queda así:

Subred 1:	red 192.168.20.0	broadcast 192.168.20.31	rango .1 - .30
Subred 2:	red 192.168.20.32	broadcast 192.168.20.63	rango .33 - .62
Subred 3:	red 192.168.20.64	broadcast 192.168.20.95	rango .65 - .94
Subred 4:	red 192.168.20.96	broadcast 192.168.20.127	rango .97 - .126
Subred 5:	red 192.168.20.128	broadcast 192.168.20.159	rango .129 - .158
Subred 6:	red 192.168.20.160	broadcast 192.168.20.191	rango .161 - .190
Subred 7:	red 192.168.20.192	broadcast 192.168.20.223	rango .193 - .222
Subred 8:	red 192.168.20.224	broadcast 192.168.20.255	rango .225 - .254

Verificación: 8 por 32 = 256 direcciones totales, y cada broadcast es la siguiente red menos uno. Si tú tabla coincide con esta, el método ya está en tus manos.

2. Tienes la red 172.16.0.0/16 y necesitas crear al menos 200 subredes, cada una con capacidad para al menos 200 hosts. Que prefijó debes usar. Cuantas subredes obtienes en realidad y cuantos hosts útiles caben en cada una.

SOLUCIÓN:

Primero los bits para las subredes: necesitas $2^n \geq 200$. En la tabla de potencias, $2^7 = 128$ no alcanza y $2^8 = 256$ si alcanza, así que prestas 8 bits. El prefijo pasa de /16 a /24. Ahora verifica los hosts: con prefijo /24 te quedan 8 bits de host, o sea $2^8 - 2 = 254$ hosts útiles por subred, que sí cubre los 200 requeridos. Respuesta: usa /24, obtienes 256 subredes reales con 254 hosts útiles cada una. Fijate que el requisito de hosts también se cumple de sobra; si no se cumpliera, tendrías que prestar menos bits y aceptar menos subredes, buscando el equilibrio entre ambas necesidades.

3. Convierte a notación de barra las máscaras 255.255.255.240 y 255.255.254.0. Luego convierte a decimal puntuado los prefijos /27 y /21. Explica cada conversión contando unos en binario.

SOLUCIÓN:

Máscara 255.255.255.240: los tres primeros octetos dan 24 unos. El 240 es 11110000, que tiene 4 unos. Total 28: es un /28. Máscara 255.255.254.0: los dos primeros octetos dan 16 unos. El 254 es 11111110, con 7 unos. Total 23: es un /23. Prefijo /27: 27 unos son tres octetos completos más 3 unos en el cuarto: 11100000 = 224, así que la máscara es 255.255.255.224. Prefijo /21: 21 unos son dos octetos completos más 5 unos en el tercero:

11111000 = 248, así que la máscara es 255.255.248.0. Comprueba cada resultado con el salto: para el /28 el salto es 16 y los hosts son 14; para el /23 el salto en el tercer octeto es 2 y las direcciones son 512. Todo cuadra con la tabla de máscaras.

4. Diseño VLSM: te asignan la red 10.10.0.0/24 para una sucursal que necesita: laboratorio con 60 hosts, oficinas con 28 hosts, red de invitados con 12 hosts y dos enlaces punto a punto entre routers. Ordeña las necesidades, calcula el prefijo de cada subred y entrega la tabla con red, broadcast y rango útil de cada una, más el espacio que queda libre.

SOLUCIÓN:

Ordeño de mayor a menor: laboratorio 60, oficinas 28, invitados 12, enlace 1 con 2, enlace 2 con 2. Laboratorio: necesito $2^h \geq 62$, así que $h = 6$ porque $2^5 = 32$ no alcanza y $2^6 = 64$ si alcanza. Prefijo /26, máscara 255.255.255.192, salto 64. Primer bloque libre en 0: red 10.10.0.0/26, broadcast 10.10.0.63, rango útil 10.10.0.1 a 10.10.0.62, con 62 útiles que cubren los 60. Oficinas: necesito $2^h \geq 30$, $h = 5$ porque $2^4 = 16$ no alcanza y $2^5 = 32$ si alcanza. Prefijo /27, máscara 255.255.255.224, salto 32. Siguiendo bloque en 64: red 10.10.0.64/27, broadcast 10.10.0.95, rango útil 10.10.0.65 a 10.10.0.94, con 30 útiles que cubren los 28. Invitados: necesito $2^h \geq 14$, $h = 4$ porque $2^3 = 8$ no alcanza y $2^4 = 16$ si alcanza. Prefijo /28, máscara 255.255.255.240, salto 16. Siguiendo bloque en 96: red 10.10.0.96/28, broadcast 10.10.0.111, rango útil 10.10.0.97 a 10.10.0.110, con 14 útiles que cubren los 12. Enlace 1: necesito $2^h \geq 4$, $h = 2$ exacto. Prefijo /30, máscara 255.255.255.252, salto 4. Siguiendo bloque en 112: red 10.10.0.112/30, broadcast 10.10.0.115, rango útil 10.10.0.113 a 10.10.0.114. Enlace 2: siguiente bloque en 116: red 10.10.0.116/30, broadcast 10.10.0.119, rango útil 10.10.0.117 a 10.10.0.118. Verificación: $64 + 32 + 16 + 4 + 4 = 120$ direcciones usadas de 256, así que quedan libres 136 direcciones, de 10.10.0.120 a 10.10.0.255, disponibles para crecer. Ningún bloque se traslapa y cada necesidad quedo cubierta con su colchón.

5. Agregación de rutas: resume en una sola ruta las ocho redes 192.168.16.0/24, 192.168.17.0/24, 192.168.18.0/24, 192.168.19.0/24, 192.168.20.0/24, 192.168.21.0/24, 192.168.22.0/24 y 192.168.23.0/24. Indica el prefijo agregado, la máscara y el rango total cubierto. Explica por qué estas redes si se pueden agregar.

SOLUCIÓN:

Son 8 redes, qué es 2^3 , una potencia de 2 válida. Son contiguas, del tercer octeto 16 al 23. Están alineadas: el primer bloque de 8 en el tercer octeto empieza en múltiplo de 8, y 16 es múltiplo de 8. Verifico con bits comunes: 16 es 00010000 y 23 es 00010111; los bits iguales desde la izquierda son 0, 0, 0, 1, 0, o sea 5 bits comunes. Sumados a los 16 de los dos primeros octetos dan un prefijo /21. La ruta agregada es 192.168.16.0/21 con máscara

255.255.248.0. El rango cubierto: salto = $256 - 248 = 8$ en el tercer octeto, así que el bloque va de 192.168.16.0 a 192.168.23.255, exactamente las ocho redes originales, ni una más ni una menos. Se pueden agregar porque cumplen las tres condiciones: cantidad potencia de 2, contigüidad y alineación al límite del bloque. Si las redes hubieran sido de la 17 a la 24, por ejemplo, no estarían alineadas y el resumen /21 no serviría.

6. Te dan la IP 192.168.100.75 con máscara 255.255.255.224. Determina: a que subred pertenece, cuál es su dirección de red, su broadcast, su rango útil y cuantos hosts útiles tiene esa subred. Usa la técnica de los múltiplos del salto.

SOLUCIÓN:

Primero el prefijo: 224 es 11100000 con 3 unos, así que es un /27 con 3 bits prestados y 5 bits de host. El salto es $256 - 224 = 32$, así que las subredes empiezan en múltiplos de 32: 0, 32, 64, 96, 128 y así. El último octeto de la IP es 75, que cae entre 64 y 96, así que pertenece a la subred 192.168.100.64/27. Su dirección de red es 192.168.100.64, su broadcast es la siguiente red menos uno: 192.168.100.95, y su rango útil va de 192.168.100.65 a 192.168.100.94. La .75 está dentro del rango útil, así que es una dirección asignable a un equipo. Hosts útiles de la subred: $2^5 - 2 = 30$. Número de subredes totales en la /24 original: $2^3 = 8$. Todo verificado y consistente.

Resumen de la unidad

En esta unidad aprendiste el arte del subneteo, una de las habilidades más valiosas y mejor pagadas en el mundo de las redes. Empezaste repasando el binario y la tabla de potencias de 2, tus dos herramientas inseparables: con ellas conviertes direcciones, cuentas unos en las máscaras y resuelves cualquier cálculo sin depender de calculadoras.

Entendiste por qué se dividen las redes: para reducir el tráfico de broadcast, para aislar departamentos y aplicar seguridad entre ellos, para aprovechar las direcciones y para mantener un orden administrativo que facilita el diagnóstico de fallas. Viste que subnetear es prestar bits de la porción de host para crear subredes, y que cada bit prestado duplica las subredes y reduce a la mitad su tamaño, un trueque que se resume en las dos fórmulas de oro: 2^n para el número de subredes y $2^h - 2$ para los hosts útiles por subred.

Dominaste las tres direcciones clave de cada subred: la dirección de red con todos los bits de host en cero, la dirección de broadcast con todos en uno, y el rango útil entre ambas, que es lo único asignable a equipos. Aprendiste el papel de la máscara de subred y la operación AND que usan los equipos para saber si un destino está en su red o hay que mandarlo al router. Y adoptaste el atajo profesional del salto, 256 menos el octeto interesante, que te da las direcciones de red en segundos.

Con CIDR dejaste atrás las clases rígidas y entendiste la notación de barra: el número después de la diagonal cuenta los bits de red. Memorizaste la tabla de máscaras del /8 al /30, aprendiste a convertir máscaras a prefijos y viceversa contando unos en binario, y descubriste el supernetting, la operación inversa que agrega redes contiguas y alineadas en una sola ruta para aligerar las tablas de los routers.

Cerraste con VLSM, las máscaras de longitud variable que permiten subredes de tamaños distintos sobre la misma red original, usando el método del bloque más grande primero para no desperdiciar ni traslapar direcciones. El ejemplo completo de la empresa te mostró como un solo /24 alcanza para cuatro departamentos y dos enlaces WAN cuando cada pedazo se corta a la medida.

Si algo debes llevarte grabado, es el método de los cinco pasos: calcula el salto, escribe las redes, saca cada broadcast como la siguiente red menos uno, define el rango útil entre red más uno y broadcast menos uno, y verifica que todo sumé el total original. Práctica ese método hasta hacerlo dormido, evita los errores típicos como olvidar restar las dos direcciones reservadas, y estarás listo para cualquier ejercicio de subneteo que te pongan enfrente, en un examen o en una red real.

Y recuerda la lección más grande de esta unidad: las direcciones IP no son números mágicos, son un sistema lógico que premia a quién hace las cuentas con calma. Cada vez que dudes, vuelve al binario, vuelve a la tabla de potencias de 2 y vuelve al salto. Esas tres herramientas, bien dominadas, resuelven el cien por ciento de los problemas de subneteo, CIDR y VLSM que encontrarás en tu camino como profesional de redes.

UNIDAD 6: Switches, routers y ruteo

Si la unidad anterior te enseñó a dividir el mapa en territorios, esta unidad te presenta a los dos personajes que hacen que los datos viajen por ese mapa: el switch y el router. Son las dos cajas más importantes de cualquier red, y entender que hace cada una, cómo piensan y cómo se configuran es lo que separa a quién "conecta cables" de quién "diseña redes".

En esta unidad vas a ver tres clases encadenadas. La clase 16 se enfoca en los switches: que hacen, cómo conmutan tramas, cómo aprenden direcciones en su tabla MAC, la diferencia entre dominios de colisión y dominios de broadcast, y las VLANs, esas redes virtuales que permiten dividir un switch físico en varias redes lógicas, con sus puertos de acceso y trunk. La clase 17 presenta a los routers: que hacen, cómo reenvían paquetes, cómo está formada su tabla de ruteo con red destino, máscara, siguiente salto e interfaz, que es la puerta de enlace y cómo decide un router, paso a paso, a dónde enviar cada paquete. La clase 18 cierra con el ruteo estático contra el dinámico: rutas estáticas, la ruta por defecto, y los protocolos dinámicos más famosos, RIP, OSPF, EIGRP y BGP, con sus métricas y distancias administrativas, más un ejemplo de configuración básica de un router con comandos reales.

Por qué importa este tema en la vida real. Imagina que entras a trabajar al área de sistemas de una empresa y te dicen: "el departamento de contabilidad no puede entrar a internet, pero sí puede ver sus servidores; además vamos a abrir una sucursal nueva y hay que conectarla". Para resolver eso necesitas saber que el switch de contabilidad probablemente tiene una VLAN separada, que el router tiene una ruta hacia la sucursal o le falta, y que la puerta de enlace de esas máquinas apunta al router correcto. Sin entender switches, routers y ruteo, cada falla es un misterio; entendiéndolos, cada falla es un procedimiento: revisas la tabla MAC, revisas la tabla de ruteo, revisas la puerta de enlace, y encuentras el problema.

El segundo motivo es el examen de certificación. Las preguntas sobre cómo un switch aprende direcciones, qué es una VLAN, cómo un router elige una ruta y qué protocolo usar en cada caso aparecen una y otra vez. Son preguntas que regalan puntos si entiendes los conceptos, y que quitan puntos si solo memorizaste definiciones sin haberlas razonado.

Al terminar esta unidad sabrás explicar con tus palabras que hace un switch y que hace un router, leer una tabla de ruteo cómo quien lee un mapa, decidir cuándo un puerto debe ser de acceso y cuando trunk, comparar RIP, OSPF, EIGRP y BGP sin confundirlos, y escribir la configuración básica de un router con rutas estáticas. Vamos por partes, como siempre: primero los conceptos, luego los ejemplos, luego la práctica.

Explicación detallada

El switch: el cartero inteligente de la red local

Un switch es el dispositivo que conecta los equipos dentro de una misma red local y se encarga de llevar cada trama a su destino. Opera en la capa 2 del modelo OSI, la capa de enlace de datos, y toma sus decisiones mirando direcciones MAC, esas direcciones físicas únicas que trae cada tarjeta de red de fábrica.

Para entender al switch, compáralo con el dispositivo que reemplazó: el hub. Un hub era un repetidor tonto: todo lo que entraba por un puerto salía por todos los demás, como gritar en un cuarto para que todos escuchen. Eso generaba colisiones constantes y desperdiciaba el ancho de banda. El switch, en cambio, es inteligente: aprende que equipo está conectado en cada puerto y envía cada trama solo por el puerto donde está el destinatario. Es la diferencia entre gritar en un cuarto y entregar cartas puerta por puerta.

La unidad mínima de datos que maneja el switch se llama trama. Una trama lleva, entre otras cosas, la dirección MAC de origen, la dirección MAC de destino y los datos. Cuando el switch recibe una trama por un puerto, hace dos cosas: primero anota en su memoria la MAC de origen junto con el puerto por dónde llegó, porque así aprende dónde vive ese equipo; segundo, busca la MAC de destino en su memoria y, si la encuentra, reenvía la trama solo por el puerto correspondiente. Ese proceso de recibir por un puerto y enviar por otro se llama conmutación, y de ahí viene el nombre del aparato.

Piensa en un ejemplo cotidiano: en tu casa, el switch es como el conserje de un edificio que conoce a todos los vecinos. Cuando llega un paquete para el departamento 302, no lo grita por el altavoz para todo el edificio; lo lleva directo a la puerta del 302 porque sabe dónde vive cada quien. Y cada vez que un vecino nuevo se presenta, el conserje anota su nombre y su departamento en su libreta. Esa libreta es la tabla MAC.

La tabla MAC: la libreta de direcciones del switch

La tabla MAC, también llamada tabla CAM por el tipo de memoria rápida donde se guarda, es el corazón del switch. Cada entrada relaciona una dirección MAC con el número de puerto donde se vio por última vez a ese equipo, y a veces con la VLAN a la que pertenece. Un ejemplo simplificado de cómo se ve:

Dirección MAC	Puerto	VLAN
00:1A:2B:3C:4D:5E	1	10
00:1A:2B:3C:4D:5F	2	10
00:1A:2B:3C:4D:60	3	20
00:1A:2B:3C:4D:61	8	10

El proceso de aprendizaje funciona así. Supon un switch recién encendido con la tabla vacía. La computadora A, conectada al puerto 1, envía una trama a la computadora B. El switch recibe la trama por el puerto 1, lee la MAC de origen, que es la de A, y anota: "la MAC de A vive en el puerto 1". Luego busca la MAC de destino, la de B, en su tabla. Como la tabla está vacía, no la encuentra, así que hace flooding: envía la trama por todos los puertos menos por el que llegó. Todas las computadoras la reciben, pero solo B la acepta porque reconoce su MAC destino; las demás la ignoran. Cuando B responde a A, el switch aprende que la MAC de B vive en el puerto 2, y a partir de ese momento el tráfico entre A y B va solo por los puertos 1 y 2, sin molestar a nadie más.

Las entradas de la tabla no son eternas: tienen un temporizador, típicamente de unos 5 minutos. Si un equipo deja de hablar, su entrada envejece y se borra, para que la tabla no se llene de direcciones de equipos que ya no están. Si el equipo se mueve de puerto, el switch simplemente actualiza la entrada cuando lo ve aparecer por el nuevo puerto. Este aprendizaje automático es lo que hace al switch un dispositivo "conecta y funciona": no hay que configurarle a mano quién está dónde.

Un detalle fino pero importante para exámenes: el switch aprende con la dirección de origen y decide con la dirección de destino. Aprender con origen, reenviar según destino. Si te preguntan "que dirección usa el switch para aprender", la respuesta es la MAC de origen. Si te preguntan "que dirección usa para decidir por dónde reenviar", la respuesta es la MAC de destino.

Flooding, broadcast y multicast: cuando el switch habla con todos

Hay tres situaciones en las que el switch envía una trama por varios puertos en vez de por uno solo, y conviene distinguirlas bien.

La primera es el flooding por destino desconocido, que ya viste: si la MAC destino no está en la tabla, el switch inunda todos los puertos menos el de llegada. Es un mecanismo de seguridad para no perder tramas, y ocurre sobre todo cuando el switch acaba de encenderse o cuando aparece un equipo nuevo.

La segunda es el broadcast: tramas dirigidas a la dirección MAC de broadcast, que es FF:FF:FF:FF:FF:FF, todos los bits en uno. Un broadcast significa "esto es para todos", y el switch lo reenvía por todos los puertos menos el de origen. Los equipos usan broadcasts para preguntar cosas como "quien tiene tal dirección IP", y son normales en pequeñas cantidades.

La tercera es el multicast: tramas dirigidas a un grupo de equipos interesados, no a todos. El switch básico las trata como broadcasts y las inunda, aunque los switches más avanzados pueden aprender que puertos tienen miembros del grupo y limitar el envío.

La lección importante es que el switch, por si solo, no contiene los broadcasts: todo lo que entra a un switch sale hacia todos los puertos en forma de broadcast. Por eso se dice que un switch no separa dominios de broadcast. Para separar dominios de broadcast necesitas VLANs o routers, como verás en seguida.

Dominios de colisión contra dominios de broadcast

Estos dos conceptos se confunden muchísimo, así que vamos a dejarlos cristalinos con una definición simple para cada uno.

Un dominio de colisión es un conjunto de equipos donde solo uno puede hablar a la vez sin que sus mensajes choquen. En los tiempos del hub y del cable coaxial, todos los equipos compartían el mismo dominio de colisión: si dos hablaban al mismo tiempo, había una colisión y ambos tenían que reintentar. Cada puerto de un switch moderno, trabajando en full dúplex, es su propio dominio de colisión: puede enviar y recibir al mismo tiempo sin chocar con nadie. Así que en un switch de 24 puertos con 24 equipos conectados hay 24 dominios de colisión, uno por puerto. Las colisiones, en la práctica, son historia.

Un dominio de broadcast es un conjunto de equipos donde un broadcast llega a todos. Como el switch reenvía los broadcasts por todos sus puertos, todos los equipos conectados a un switch sin VLANs forman un solo dominio de broadcast. Si conectas dos switches entre si con un cable, siguen siendo un solo dominio de broadcast, porque el broadcast cruza de un switch al otro. El único dispositivo que detiene los broadcasts es el router: cada interfaz de un router marca el límite de un dominio de broadcast.

Memoriza la frase para el examen: el switch separa dominios de colisión pero no de broadcast; el router separa ambos. Y la consecuencia práctica: si tu red tiene cientos de equipos en un solo dominio de broadcast, los broadcasts empiezan a robar ancho de banda notable. La solución es dividir en dominios más pequeños con VLANs o con routers.

Para fijar ideas, un ejercicio mental: tienes un router con 2 interfaces, cada una conectada a un switch de 8 puertos, y cada switch tiene 6 computadoras. Cuantos dominios de colisión hay.

Cada puerto de switch con equipo es un dominio: $6 + 6 = 12$, más los 2 enlaces switch-router, que también son puertos: total 14 dominios de colisión. Cuantos dominios de broadcast. Cada interfaz del router separa: hay 2 dominios de broadcast, uno por segmento. Si mañana agregas una VLAN en cada switch, los dominios de broadcast se multiplican según las VLANs, como verás ahora.

VLANs: varias redes lógicas dentro de un switch físico

Una VLAN, sigla de red de área local virtual, es una forma de dividir un switch físico en varios switches lógicos independientes. Cada VLAN es su propio dominio de broadcast: los equipos de la VLAN 10 pueden hablar entre si, los de la VLAN 20 entre si, pero un broadcast de la VLAN 10 nunca llega a la VLAN 20, aunque compartan él mismo aparato físico.

La analogía clásica es un edificio de oficinas con un solo conserje pero con pisos incomunicados: el conserje atiende a todos, pero los inquilinos del piso 2 no pueden entrar al piso 5 ni escuchar lo que se habla allá. El switch es el edificio, las VLANs son los pisos, y el conserje reparte la correspondencia solo dentro de cada piso.

Para qué sirven en la práctica. Primero, segmentación sin comprar más fierros: con un solo switch de 24 puertos puedes crear la VLAN 10 para ventas, la VLAN 20 para contabilidad y la VLAN 30 para invitados, cada una aislada de las demás. Segundo, seguridad: el tráfico de contabilidad no llega físicamente a los puertos de ventas, así que un curioso no puede husmear con un sniffer. Tercero, orden: cada VLAN suele corresponder a una subred IP distinta, así que tu plan de VLANs y tu plan de subneteo van de la mano, por ejemplo VLAN 10 con 192.168.10.0/24 y VLAN 20 con 192.168.20.0/24.

Cómo se identifica cada VLAN. Cada una lleva un número, el ID de VLAN, que va del 1 al 4094. La VLAN 1 existe por defecto en todos los puertos y se usa para administración; por seguridad se recomienda no usarla para datos de usuarios. Los rangos se reparten así: del 1 al 1005 es el rango normal, usable en cualquier switch, y del 1006 al 4094 es el rango extendido. En la práctica verás mucho las VLANs 10, 20 y 30 para departamentos, y números como 100 o 200 para usos especiales.

Un punto clave: por defecto, equipos en VLANs distintas no pueden comunicarse entre si, aunque esten en él mismo switch. Para que hablen necesitan un router que enrute entre las VLANs, lo que se llama enrutamiento entre VLANs. Esto es una ventaja de seguridad, no una limitación: tú decides en el router que tráfico entre VLANs permites y cuál bloqueas.

Puertos de acceso y puertos trunk

Los puertos de un switch se configuran en dos modos, y elegir el correcto es una de las decisiones más comunes del día a día.

Un puerto de acceso pertenece a una sola VLAN y se usa para conectar dispositivos finales: computadoras, impresoras, teléfonos IP, puntos de acceso. Cuando una trama entra por un puerto de acceso, el switch la marca internamente como perteneciente a esa VLAN, y cuando sale hacia el dispositivo final, sale sin marca, porque el dispositivo final no sabe nada de VLANs. Ejemplo: configuras el puerto 5 en modo acceso para la VLAN 20 y conectas la PC de contabilidad; esa PC queda automáticamente en la VLAN 20 sin que su tarjeta de red se entere.

Un puerto trunk transporta tráfico de múltiples VLANs por un solo enlace y se usa para conectar switches entre sí o un switch con un router. Como por él mismo cable viajan tramas de varias VLANs, cada trama lleva una etiqueta que dice a qué VLAN pertenece. Esa etiqueta la define el estándar 802.1Q: son 4 bytes extra que se insertan en la trama e incluyen el ID de VLAN. Cuando el switch del otro extremo recibe la trama etiquetada, lee la etiqueta y la entrega solo a los puertos de esa VLAN.

Hay un detalle importante en los trunks: la VLAN nativa. Es la única VLAN cuyas tramas viajan sin etiqueta por el trunk, por compatibilidad con equipos viejos que no entienden etiquetas. Por defecto es la VLAN 1, y por seguridad se recomienda cambiarla a una VLAN sin usar, para evitar ciertos ataques que abusan de la VLAN nativa.

La regla de oro para no equivocarte: dispositivo final va en puerto de acceso; conexión entre switches o hacia el router va en puerto trunk. Si conectas dos switches con un puerto de acceso, solo pasará una VLAN y las demás quedarán incomunicadas entre switches, un error típico que deja a medio edificio sin red. Si conectas una PC a un trunk, la PC recibirá tramas etiquetadas que no entiende y la conexión fallará de formas extrañas.

Un ejemplo completo: dos switches, SW1 y SW2, con VLAN 10 y VLAN 20 en ambos. Los puertos de las PCs van en modo acceso, cada uno en su VLAN. El cable que une SW1 con SW2 va en modo trunk en ambos extremos, permitiendo VLANs 10 y 20. Resultado: una PC de la VLAN 10 en SW1 puede hablar con una PC de la VLAN 10 en SW2, porque el trunk transporta esa VLAN entre switches; pero no puede hablar con la VLAN 20, porque son dominios de broadcast separados. Así se construyen redes grandes con muchos switches sin perder la segmentación.

Errores típicos con VLANs y como evitarlos

El error más común es olvidar configurar el trunk entre switches, dejando puertos en modo acceso por defecto. Síntoma: las PCs de la misma VLAN en switches distintos no se ven. Solución: revisar que el enlace entre switches este en modo trunk y que permita las VLANs necesarias.

El segundo error es la VLAN nativa distinta en cada extremo del trunk. Si SW1 tiene nativa 99 y SW2 tiene nativa 1, el tráfico sin etiquetar se mezcla mal y aparecen fallas intermitentes difíciles de rastrear. Solución: usar la misma VLAN nativa en ambos extremos, y que sea una VLAN sin equipos de usuario.

El tercer error es asignar el puerto de acceso a la VLAN equivocada. Síntoma: la PC obtiene dirección IP de la subred incorrecta o no obtiene ninguna. Solución: verificar en que VLAN quedo cada puerto y que corresponda con el plan de direccionamiento.

Enrutamiento entre VLANs: el router ón a stick

Ya sabes que equipos en VLANs distintas no pueden hablarse directamente porque cada VLAN es un dominio de broadcast separado. Pero en la vida real, la PC de ventas a veces necesita llegar al servidor de contabilidad. La solución es el enrutamiento entre VLANs: un router con una pata en cada VLAN que reenvía el tráfico permitido entre ellas.

Hay dos formas de hacerlo. La clásica usa una interfaz física del router por cada VLAN: si tienes 4 VLANs, usas 4 interfaces del router, cada una conectada a un puerto de acceso de su VLAN. Funciona, pero desperdicia puertos del router y no escala: con 20 VLANs necesitarías 20 interfaces.

La forma moderna es el router ón a stick: una sola interfaz física del router conectada a un puerto trunk del switch, dividida lógicamente en subinterfaces, una por cada VLAN. Cada subinterfaz lleva la etiqueta 802.1Q de su VLAN y tiene su propia IP, que sirve como puerta de enlace de esa VLAN. Gráficamente parece un palo con varias ramas, de ahí el nombre.

Así se configura en un router Cisco. Supon el trunk en G0/0 y dos VLANs: la 10 con red 192.168.10.0/24 y la 20 con red 192.168.20.0/24:

```
R1(config)# interface GigabitEthernet0/0
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface GigabitEthernet0/0.10
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# ip address 192.168.10.1 255.255.255.0
R1(config-subif)# exit
R1(config)# interface GigabitEthernet0/0.20
R1(config-subif)# encapsulation dot1Q 20
R1(config-subif)# ip address 192.168.20.1 255.255.255.0
```

La interfaz física no lleva IP propia: solo se enciende. Cada subinterfaz se identifica con el número después del punto, declara su encapsulamiento 802.1Q con el ID de VLAN y recibe la IP que será la puerta de enlace de esa VLAN. Del lado del switch, el puerto hacia el router va en modo trunk permitiendo las VLANs 10 y 20. Con esto, una PC de la VLAN 10 puede llegar a la VLAN 20 pasando por el router, y en el router puedes poner listas de acceso para permitir solo lo necesario, por ejemplo que ventas vea el servidor pero no las PCs de contabilidad.

Este diseño conecta las tres clases de la unidad en un solo escenario: las VLANs de la clase 16, el reenvío del router de la clase 17 y las rutas de la clase 18. Si entiendes el router ón a stick, entiendes cómo se arma una red empresarial real.

El router: él guía que conecta redes distintas

Si el switch es el conserje del edificio, el router es el sistema de carreteras entre ciudades. Un router conecta redes distintas y decide, para cada paquete que recibe, cuál es el mejor camino hacia su destino. Opera en la capa 3 del modelo OSI, la capa de red, y toma sus decisiones mirando direcciones IP, no MAC.

La diferencia fundamental con el switch está en la unidad de datos y en la decisión. El switch maneja tramas y decide por MAC dentro de la misma red; el router maneja paquetes y decide por IP entre redes distintas. Cada interfaz de un router pertenece a una red diferente: por ejemplo, la interfaz 1 en 192.168.10.1/24 y la interfaz 2 en 192.168.20.1/24. Un paquete que llega por la interfaz 1 con destino a la red 192.168.20.0/24 sale por la interfaz 2, y en el camino el router quita la trama vieja y construye una nueva con las MACs correspondientes al siguiente tramo. Por eso se dice que el router "termina" los dominios de broadcast y también los de colisión: nada de la capa 2 cruza de un lado al otro.

En una red casera, el aparatito que te da tu proveedor de internet es un router: tiene una interfaz hacia internet con tu IP pública y otra hacia tu casa con la red privada, y se encarga de qué tus paquetes salgan y de qué las respuestas regresen al equipo correcto. En una

empresa, los routers conectan sucursales, departamentos y salidas a internet, y sus tablas de ruteo pueden tener cientos de entradas.

La tabla de ruteo: el mapa del router

La tabla de ruteo es la estructura donde el router guarda todo lo que sabe sobre como llegar a cada destino. Cada entrada, cada ruta, tiene estos campos esenciales:

```
Red destino:    la red a la que lleva esta ruta, por ejemplo 192.168.20.0
Mascara:        el prefijo que delimita esa red, por ejemplo /24
Siguiendo salto: la IP del proximo router en el camino, por ejemplo 10.0.0.2
Interfaz de salida: el puerto fisico por donde sale el paquete, por ejemplo G0/1
Metrica:         el costo de usar esta ruta, segun el protocolo
Distancia administrativa: que tan confiable es la fuente de esta ruta
```

Una tabla real simplificada se ve así:

Codigo	Red destino	Mascara	Siguiendo salto	Interfaz
C	192.168.10.0	255.255.255.0	directamente	G0/0
C	192.168.20.0	255.255.255.0	directamente	G0/1
S	192.168.30.0	255.255.255.0	10.0.0.2	G0/2
S	0.0.0.0	0.0.0.0	200.10.10.1	G0/3

La letra del código indica el origen: C significa conectada directamente, el router tiene una interfaz en esa red y no necesita que nadie se lo diga; S significa estática, la configuró a mano un administrador. Más adelante verás códigos de protocolos dinámicos como R de RIP, O de OSPF y D de EIGRP.

Lee la tabla como un mapa: "para llegar a 192.168.30.0/24, sal por G0/2 y entregale el paquete a 10.0.0.2, que sabrá que hacer con él". El siguiente salto siempre es la IP de un router vecino alcanzable directamente por la interfaz de salida. El router no necesita saber la ruta completa hasta el destino final; le basta saber a quién pasarle el paquete para que se acerque, igual que cuando preguntas una dirección en la calle y te dicen "avanza dos cuadras y pregunta de nuevo".

La puerta de enlace: la salida de tu red

La puerta de enlace, o gateway, es la dirección IP del router que le da salida a tu red local. Es el primer router que verá tus paquetes cuando quierán ir a otra red. En la configuración de red de tu computadora aparece como "puerta de enlace predeterminada", y típicamente es la primera dirección útil de tu subred: si tu red es 192.168.10.0/24, tu gateway probablemente sea 192.168.10.1, que es la interfaz del router en tu segmento.

El flujo es este: tu PC quiere hablar con un servidor en otra red. Primero hace el AND con la máscara y descubre que el destino no está en su red local. Entonces, en vez de buscar al servidor directamente, arma el paquete con la IP del servidor como destino final, pero lo mete en una trama dirigida a la MAC de su puerta de enlace. El router recibe la trama, saca el paquete, consulta su tabla de ruteo y lo reenvía hacia el destino. Cuando la respuesta vuelve, el router la entrega a tu PC. Todo internet funciona con este mecanismo repetido salto tras salto.

Si la puerta de enlace está mal configurada, el síntoma es clásico y fácil de reconocer: puedes hablar con los equipos de tu misma red, pero nada de afuera responde, ni siquiera un ping al router vecino. En el soporte técnico diario, "revisa la puerta de enlace" es uno de los primeros pasos del diagnóstico, junto con "revisa que tengas IP" y "revisa el cable".

Cómo decide un router: la coincidencia más larga manda

Cuando un paquete llega al router, este sigue un procedimiento fijo para decidir por dónde enviarlo. Entender este procedimiento te permite predecir el comportamiento de cualquier red con solo leer su tabla de ruteo.

Paso 1: el router extrae la IP destino del paquete. Paso 2: compara esa IP con cada entrada de su tabla de ruteo, de la más específica a la menos específica. Paso 3: usa la coincidencia más larga, es decir, la ruta cuyo prefijo coincida con más bits de la IP destino. Paso 4: reenvía el paquete por la interfaz de salida indicada, hacia el siguiente salto. Paso 5: si ninguna ruta coincide, descarta el paquete.

La regla de la coincidencia más larga merece un ejemplo. Supon esta tabla:

```
192.168.0.0/16  -> salir por G0/1
192.168.10.0/24 -> salir por G0/2
0.0.0.0/0       -> salir por G0/3
```

Llega un paquete destinado a 192.168.10.50. Coincide con las tres rutas: con la /16 porque los primeros 16 bits coinciden, con la /24 porque los primeros 24 bits coinciden, y con la /0 porque todo coincide con nada. La coincidencia más larga es la /24, así que el paquete sale por G0/2. Si el destino fuera 192.168.99.50, solo coincidiría con la /16 y la /0; ganaría la /16 y saldría por

G0/1. Y si el destino fuera 8.8.8.8, solo coincidiría la /0 y saldría por G0/3. La lógica es impecable: ante la duda, el router prefiere la descripción más precisa del destino.

Este mecanismo explica por qué el orden de las rutas en la tabla no importa: el router no usa la primera que coincide, usa la más específica. Y también explica la importancia de la ruta por defecto 0.0.0.0/0: como su prefijo es de longitud cero, coincide con todo y funciona como red de seguridad. Si no existiera y llegaría un paquete sin ruta específica, el router lo descartaría.

Un detalle de examen: si hay dos rutas con él mismo prefijo hacia él mismo destino, por ejemplo dos rutas /24 aprendidas por él mismo protocolo con distinta métrica, el router elige la de menor métrica. Y si las métricas también empatan, muchos routers reparten el tráfico entre ambas, lo que se llama balanceo de carga.

Ruteo estático contra ruteo dinámico

Hay dos formas de llenar la tabla de ruteo: a mano o automáticamente. Las rutas estáticas las escribe el administrador comando por comando; las rutas dinámicas las aprenden los routers conversando entre si con protocolos de enrutamiento. Cada enfoque tiene su lugar.

El ruteo estático es simple, predecible y no consume ancho de banda en conversaciones entre routers. Es ideal para redes pequeñas, para enlaces estables que no cambian, y para la ruta por defecto hacia internet. Su gran debilidad es que no se adapta: si un enlace se cae, la ruta estática sigue apuntando al vacío hasta que un humano la corrija. En una red con 5 routers y rutas que nunca cambian, lo estático es perfecto. En una red con 200 routers y enlaces que suben y bajan, lo estático es una pesadilla administrativa.

El ruteo dinámico usa protocolos para que los routers se avisen entre si que redes conocen y por dónde se llega. Si un enlace se cae, los routers lo detectan, recalculan y encuentran caminos alternos sin intervención humana. Su costo es complejidad de configuración, consumo de recursos en los routers y un tiempo de convergencia, que es lo que tardan todos los routers en ponerse de acuerdo después de un cambio. Para redes medianas y grandes, el dinámico es obligatorio.

La analogía: el ruteo estático es como memorizar de memoria el camino a tu trabajo; rápido y eficiente mientras nada cambie, inútil el día que cierran tu calle. El ruteo dinámico es como usar una app de navegación con tráfico en tiempo real: gasta datos y batería, pero te desvía sola cuando hay un accidente.

Rutas estáticas y la ruta por defecto

Configurar una ruta estática es decirle al router: "para llegar a esta red, sal por esta interfaz o entregale el paquete a este vecino". En sintaxis de Cisco, que es la que verás en exámenes y en la mayoría de los equipos, el comando es:

```
ip route <red-destino> < mascara> <siguiente-salto o interfaz>
```

Ejemplo: tu router necesita llegar a la red 192.168.30.0/24 y sabe que el router vecino 10.0.0.2 está en el camino. El comando es "ip route 192.168.30.0 255.255.255.0 10.0.0.2". También puedes indicar la interfaz de salida en vez del siguiente salto: "ip route 192.168.30.0 255.255.255.0 GigabitEthernet0/2". La primera forma es la más común en redes Ethernet.

La ruta por defecto es una ruta estática especial que coincide con todo: "ip route 0.0.0.0 0.0.0.0 200.10.10.1". Significa "todo lo que no sepas a dónde mandar, mandalo a 200.10.10.1". Es la ruta que apunta hacia internet en la mayoría de las redes, porque ningún router pequeño puede tener una ruta para cada red del planeta: para lo desconocido, a la salida.

Las rutas estáticas flotantes son un truco elegante: es una ruta estática con distancia administrativa mayor a la normal, que solo entra en acción si la ruta dinámica principal desaparece. Sirve como respaldo barato: mientras el protocolo dinámico funciona, la flotante duerme; si el enlace principal cae, la flotante despierta y mantiene la conectividad por el camino alternativo.

Protocolos de enrutamiento dinámico: RIP, OSPF, EIGRP y BGP

Cada protocolo dinámico tiene su personalidad, su métrica y su territorio natural. Vamos a conocer a los cuatro grandes.

RIP, protocolo de información de enrutamiento, es el abuelo de todos: simple, viejo y limitado. Funciona por vector distancia: cada router le dice a sus vecinos a qué distancia cree que están las redes, midiendo la distancia en saltos, o sea en cantidad de routers intermedios. Su métrica es el número de saltos y su límite es 15: una red a 16 saltos se considera inalcanzable. RIP envía su tabla completa a sus vecinos cada 30 segundos, lo que lo hace lento para converger y gastan en redes grandes. Hoy solo se usa en redes muy pequeñas o en laboratorios de práctica, pero en exámenes aparece siempre como ejemplo de vector distancia. Su versión moderna es RIPv2, que al menos soporta máscaras variables y autenticación.

OSPF, primero la ruta libre más corta, es el protocolo estándar para redes medianas y grandes de un solo fabricante o mixtas. Funciona por estado de enlace: cada router construye un mapa

completo de la red y calcula con el algoritmo de Dijkstra el camino más corto hacia cada destino. Su métrica es el costo, que se deriva del ancho de banda: a más ancho de banda, menor costo, así que OSPF prefiere los enlaces rápidos. Converge rápido ante cambios, soporta VLSM y CIDR sin problemas, y organiza las redes grandes en áreas para no sobrecargar a los routers. Si te preguntan qué protocolo usar en una red empresarial multivendedor, la respuesta casi siempre es OSPF.

EIGRP, protocolo de enrutamiento de puerta interior mejorado, es el protocolo avanzado de Cisco. Se le describe como un vector distancia mejorado o híbrido, porque combina lo mejor de ambos mundos: la simplicidad del vector distancia con una convergencia rapidísima gracias a su algoritmo DUAL, que mantiene rutas de respaldo precalculadas. Su métrica es compuesta y usa principalmente el ancho de banda y el retardo del camino. Solo funciona entre equipos Cisco, así que su territorio natural son las redes donde todo es de ese fabricante. En exámenes lo reconoces por DUAL y por la métrica de ancho de banda más retardo.

BGP, protocolo de puerta de enlace de frontera, juega en otra liga: es el protocolo que mantiene unido a internet. Mientras los anteriores enrutan dentro de una organización, BGP enruta entre organizaciones, entre sistemas autónomos como proveedores de internet, universidades y grandes empresas. Funciona por vector de ruta: no solo dice la distancia, sino la lista completa de sistemas autónomos que hay que cruzar, lo que evita ciclos a escala planetaria. Su métrica no es un número simple sino un conjunto de atributos, donde el más conocido es la longitud de la ruta de sistemas autónomos. BGP es lento para converger comparado con OSPF, pero a cambio es extremadamente estable y controlable con políticas: un proveedor puede decidir "mi tráfico hacia tal red sale por este enlace por contrato comercial", algo que ningún protocolo interior permite con ese nivel de control.

Para compararlos de un vistazo:

Protocolo	Tipo	Métrica	Uso típico
RIP	Vector distancia	Salto (max 15)	Redes pequeñas, práctica
OSPF	Estado de enlace de banda	Costo por ancho	Empresas multivendedor
EIGRP	Vector distancia mejorado (DUAL)	Ancho de banda + retardo	Redes solo Cisco
BGP	Vector de ruta	Atributos, ruta de sistemas autónomos	Internet, entre proveedores

Métrica y distancia administrativa: quién gana cuando hay empate

Cuándo un router aprende dos caminos al mismo destino desde fuentes distintas, necesita dos criterios para desempatar, uno dentro de cada protocolo y otro entre protocolos.

La métrica es el costo dentro de un mismo protocolo: cada protocolo define que significa "mejor camino" a su manera. En RIP la mejor métrica es menos saltos; en OSPF es menor costo acumulado; en EIGRP es menor valor compuesto. La métrica solo sirve para comparar rutas del mismo protocolo: no puedes comparar "3 saltos RIP" contra "costo 50 OSPF" porque son unidades distintas, como comparar kilos con litros.

La distancia administrativa resuelve el empate entre protocolos distintos: es un número que indica que tan confiable considera el router a cada fuente de rutas. Menor número significa más confiable, y la fuente más confiable gana y entra a la tabla de ruteo. Los valores clásicos en Cisco son:

Fuente de la ruta	Distancia administrativa
Red conectada directamente	0
Ruta estatica	1
EIGRP (interno)	90
OSPF	110
RIP	120
EIGRP (externo)	170
iBGP	200
Desconocida	255

Ejemplo práctico: tu router aprende la red 10.5.0.0/16 por OSPF y también por RIP. La de OSPF tiene distancia 110 y la de RIP 120. Gana OSPF por ser más confiable, y es la que entra a la tabla de ruteo; la de RIP queda como respaldo silencioso. Si mañana OSPF deja de anunciar esa red, el router instalará la de RIP automáticamente. Otro ejemplo: configuras una ruta estática hacia una red que OSPF también anuncia. La estática tiene distancia 1 contra 110 de OSPF, así que la estática gana siempre. Por eso las estáticas flotantes se configuran con distancia alta a propósito, para que solo ganen cuando el protocolo dinámico falla.

La frase para el examen: la métrica desempata dentro del protocolo, la distancia administrativa desempata entre protocolos. Menor valor gana en ambos casos.

Configuración básica de un router: los comandos esenciales

Vamos a configurar un router sencillo desde cero, con los comandos que todo técnico debe saber. Imagina un router con dos interfaces: G0/0 hacia la LAN 192.168.10.0/24 y G0/1 hacia el router vecino por el enlace 10.0.0.0/30. Además necesita una ruta estática hacia la red remota 192.168.20.0/24 vía el vecino 10.0.0.2, y una ruta por defecto hacia internet vía 200.10.10.1.

Primero entras al modo privilegiado y luego al modo de configuración global. Le pones nombre al equipo para identificarlo, configuras cada interfaz con su IP y su máscara, las enciendes con el comando no shutdown, y agregas las rutas. Así se ve la sesión completa:

```
Router> enable
Router# configure terminal
Router(config)# hostname R1
R1(config)# interface GigabitEthernet0/0
R1(config-if)# description LAN de ventas
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface GigabitEthernet0/1
R1(config-if)# description Enlace al router R2
R1(config-if)# ip address 10.0.0.1 255.255.255.252
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# ip route 192.168.20.0 255.255.255.0 10.0.0.2
R1(config)# ip route 0.0.0.0 0.0.0.0 200.10.10.1
R1(config)# end
R1# copy running-config startup-config
```

Cada línea tiene su razón. "enable" te da permisos de administrador. "configure terminal" entra al modo donde se cambian cosas. "hostname" le pone nombre para qué el prompt te diga en qué equipo estas, vital cuando administras varios. "interface" selecciona el puerto a configurar. "description" es una etiqueta de texto que no afecta nada pero salva vidas cuando otro técnico lee la configuración. "ip address" asigna la IP y la máscara a la interfaz. "no shutdown" enciende la interfaz, porque por defecto vienen apagadas: olvidar este comando es el error número uno de los principiantes y deja la interfaz caída aunque todo lo demás este bien. "ip route" agrega las rutas estáticas. "end" sale al modo privilegiado. Y "copy running-config startup-config" guarda la configuración en la memoria permanente: sin este paso, todo lo que configuraste se pierde al reiniciar el equipo, una lección que todos aprenden una sola vez.

Para verificar que todo quedo bien, estos son los comandos de consulta más usados:

```
R1# show ip interface brief
R1# show ip route
R1# show running-config
R1# ping 192.168.20.1
```

"show ip interface brief" muestra en una tabla compacta cada interfaz, su IP y si está arriba o abajo: es tu primera parada ante cualquier falla. "show ip route" muestra la tabla de ruteo con los códigos de origen, y ahí confirmas que tus rutas estáticas aparecen marcadas con S. "show running-config" muestra toda la configuración actual por si necesitas auditarla. Y "ping" comprueba conectividad real de extremo a extremo.

Armando el rompecabezas: el viaje completo de un paquete

Vamos a juntar todo lo de esta unidad en un solo recorrido. Imagina esta red: una PC en la VLAN 10 del switch SW1 quiere abrir una página en un servidor que está en la VLAN 20 del switch SW2. Los switches están unidos por un trunk, y un router ón a stick conectado a SW1 enruta entre las VLANs.

Paso 1: la PC arma el paquete con la IP del servidor como destino y, como el servidor está en otra red, lo mete en una trama dirigida a la MAC de su puerta de enlace, que es la subinterfaz del router para la VLAN 10. La trama sale por el puerto de acceso de la PC.

Paso 2: SW1 recibe la trama, aprende la MAC de la PC si no la conocía, y como el destino es la MAC del router, la reenvía por el puerto trunk hacia el router, etiquetada con la VLAN 10 según 802.1Q.

Paso 3: el router recibe la trama en su subinterfaz de la VLAN 10, quita la etiqueta, saca el paquete y consulta su tabla de ruteo. La red de la VLAN 20 aparece como conectada directamente en su otra subinterfaz, así que decide reenviar por ahí.

Paso 4: el router arma una trama nueva etiquetada con la VLAN 20 y la envía de vuelta por el trunk a SW1. Fijate: la trama original murio en el router y nació una nueva. Las direcciones MAC se reescriben en cada salto, pero las IPs de origen y destino final no cambian nunca.

Paso 5: SW1 recibe la trama de la VLAN 20 y la envía por su trunk hacia SW2, porque la tabla MAC le dice que el servidor vive del otro lado. SW2 la recibe, lee la etiqueta de la VLAN 20 y la entrega por el puerto de acceso donde está el servidor.

Paso 6: el servidor responde invirtiendo el camino: trama al router por su puerta de enlace, decisión de ruteo, trama nueva hacia la VLAN 10, trunks y puertos de acceso hasta la PC.

En ese viaje de ida y vuelta se usaron todos los conceptos de la unidad: la tabla MAC del switch, el flooding inicial si las MACs eran desconocidas, las VLANs separando dominios de broadcast, los puertos de acceso y trunk con 802.1Q, la puerta de enlace, la tabla de ruteo con sus redes conectadas y la coincidencia más larga. Cuando puedas narrar este viaje sin mirar apuntes, la unidad está dominada.

Errores comunes de principiantes

Primero: olvidar "no shutdown" en las interfaces. El router muestra la interfaz como "administratively down" y nada funciona. Acostumbrate a escribirlo siempre después de "ip address".

Segundo: no guardar la configuración con "copy running-config startup-config". Todo funciona perfecto hasta que se va la luz, y al volver el router amanece de fábrica. Guarda siempre antes de cerrar la sesión.

Tercero: configurar mal la puerta de enlace en las PCs. Síntoma inconfundible: la red local funciona pero no hay salida a nada más. Verifica la puerta de enlace antes de culpar al router.

Cuarto: confundir dominio de colisión con dominio de broadcast en exámenes. Repite la frase: el switch separa colisiones, el router separa broadcasts. Cada puerto del switch es un dominio de colisión; cada VLAN y cada interfaz de router es un dominio de broadcast.

Quinto: poner puertos de acceso donde van trunks y viceversa. Dispositivo final en acceso, enlace entre switches o al router en trunk. Un trunk mal configurado deja VLANs incomunicadas entre switches.

Sexto: en ruteo, olvidar la ruta de regreso. Configuras la ruta de ida hacia la red remota pero el router remoto no tiene ruta de vuelta hacia ti, y el ping falla a la mitad del camino. El ruteo siempre se configura en ambos sentidos.

Buenas prácticas

Etiqueta todo: usa "description" en cada interfaz del router y documenta que VLAN va en cada puerto del switch. La red que documentas hoy es la red que diagnosticas rápido mañana.

Estandariza tus esquemas: primera dirección útil para la puerta de enlace, VLAN 10 para tal departamento, mismo rango de IDs en todos los switches. La consistencia reduce errores cuando la red crece o cuando entra personal nuevo.

Prefiere OSPF como protocolo dinámico en redes multivendedor y documenta tus rutas estáticas con comentarios sobre por qué existen. Cada ruta estática misteriosa es una trampa para el técnico del futuro.

Cambia la VLAN nativa de los trunks a una VLAN sin uso y no uses la VLAN 1 para datos de usuarios. Son dos ajustes pequeños que cierran huecos de seguridad conocidos.

Y ante cualquier falla, sigue el orden lógico: capa física primero con "show ip interface brief", luego capa 2 revisando VLANs y trunks, luego capa 3 leyendo la tabla de ruteo y probando la puerta de enlace. Ese orden, de abajo hacia arriba, resuelve el 90 por ciento de los casos sin adivinanzas.

Ejemplos paso a paso

Ejemplo 1: cómo elige un router la ruta para tres paquetes distintos

Enunciado: un router tiene esta tabla de ruteo. Determina por qué interfaz sale cada uno de estos paquetes: destino 192.168.10.50, destino 192.168.99.50 y destino 8.8.8.8.

Tabla de ruteo del router R1:

```
C 192.168.10.0/24 -> G0/0 (red conectada directamente)
S 192.168.0.0/16  -> G0/1 via 10.0.0.2 (ruta estatica)
S 0.0.0.0/0      -> G0/2 via 200.10.10.1 (ruta por defecto)
```

Paquete 1: destino 192.168.10.50

Coincide con 192.168.10.0/24 (24 bits iguales).
Coincide con 192.168.0.0/16 (16 bits iguales).
Coincide con 0.0.0.0/0 (0 bits, coincide con todo).
Coincidencia mas larga: /24. Sale por G0/0.
Nota: es red conectada, el router entrega directo al equipo.

Paquete 2: destino 192.168.99.50

NO coincide con 192.168.10.0/24 (el tercer octeto 99 != 10).
Coincide con 192.168.0.0/16 (primeros 16 bits iguales).
Coincide con 0.0.0.0/0.
Coincidencia mas larga: /16. Sale por G0/1 hacia 10.0.0.2.

Paquete 3: destino 8.8.8.8

No coincide con ninguna ruta especifica.
Solo coincide con 0.0.0.0/0.
Sale por G0/2 hacia 200.10.10.1, la salida a internet.

Conclusion: el router siempre prefiere la descripcion mas especifica del destino, sin importar el orden de la tabla.

Este es exactamente el tipo de ejercicio que aparece en exámenes: te dan una tabla y varias IPs, y debes aplicar la coincidencia más larga. Práctica el procedimiento mecánico: lista las coincidencias, quedate con el prefijo más largo, y esa es la salida.

Ejemplo 2: configuración completa de dos routers con ruta estática

Enunciado: conecta dos routers en serie. R1 tiene la LAN 192.168.10.0/24 en G0/0 y se conecta a R2 por el enlace 10.0.0.0/30 en G0/1. R2 tiene la LAN 192.168.20.0/24 en G0/0 y se conecta a R1 por el mismo enlace en G0/1. Configura ambos para que las dos LANs se hablen, sin olvidar la ruta de regreso.

Configuracion de R1:

```
R1> enable
R1# configure terminal
R1(config)# hostname R1
R1(config)# interface GigabitEthernet0/0
R1(config-if)# description LAN ventas
```

```
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface GigabitEthernet0/1
R1(config-if)# description Enlace a R2
R1(config-if)# ip address 10.0.0.1 255.255.255.252
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# ip route 192.168.20.0 255.255.255.0 10.0.0.2
R1(config)# end
R1# copy running-config startup-config
```

Configuracion de R2 (la ruta de regreso):

```
R2> enable
R2# configure terminal
R2(config)# hostname R2
R2(config)# interface GigabitEthernet0/0
R2(config-if)# description LAN contabilidad
R2(config-if)# ip address 192.168.20.1 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)# exit
R2(config)# interface GigabitEthernet0/1
R2(config-if)# description Enlace a R1
R2(config-if)# ip address 10.0.0.2 255.255.255.252
R2(config-if)# no shutdown
R2(config-if)# exit
R2(config)# ip route 192.168.10.0 255.255.255.0 10.0.0.1
R2(config)# end
R2# copy running-config startup-config
```

Verificacion en R1:

```
R1# show ip interface brief
(confirma que G0/0 y G0/1 estan up/up)
R1# show ip route
(debe mostrar C para 192.168.10.0/24 y 10.0.0.0/30,
 y S para 192.168.20.0/24 via 10.0.0.2)
R1# ping 192.168.20.1
(debe responder: la ruta de ida existe en R1 y la de
 regreso existe en R2)
```

El punto didáctico central: sin la ruta estática en R2, el ping de ida llegaría pero la respuesta se perdería. El ruteo siempre se piensa en ambos sentidos.

Ejemplo 3: diagnóstico de una falla típica con VLANs

Enunciado: en un edificio hay dos switches conectados entre si. Las PCs de la VLAN 10 en el switch 1 no pueden hablar con las PCs de la VLAN 10 en el switch 2, pero dentro de cada switch las PCs de la misma VLAN si se comunican. Diagnóstica paso a paso.

Paso 1: verificar capa fisica

Revisar que el cable entre switches este conectado y los LEDs de los puertos encendidos. Si hay luz, el problema es logico.

Paso 2: revisar el modo de los puertos del enlace

En ambos switches, el puerto que conecta con el otro switch debe estar en modo trunk y permitir la VLAN 10.

Sintoma tipico: los puertos quedaron en modo acceso por defecto, asi que solo pasa la VLAN 1 entre switches.

Paso 3: corregir la configuracion

```
SW1(config)# interface GigabitEthernet0/24
SW1(config-if)# switchport mode trunk
SW1(config-if)# switchport trunk allowed vlan 10,20
(repetir en SW2 en su puerto de enlace)
```

Paso 4: verificar

Probar ping entre una PC de la VLAN 10 en SW1 y otra en SW2.

Si responde, el trunk era el problema.

Si no responde, revisar que la VLAN 10 exista en ambos switches y que los puertos de las PCs esten en modo acceso en la VLAN 10.

Este ejemplo muestra la metodología de diagnóstico de abajo hacia arriba: físico, luego capa 2, luego capa 3. El 90 por ciento de las fallas de VLAN caen en el paso 2.

Ejemplo 4: configurar trunks y puertos de acceso en un switch

Enunciado: en un switch con VLAN 10 (ventas) y VLAN 20 (contabilidad), configura los puertos 1 al 10 como acceso para la VLAN 10, los puertos 11 al 20 como acceso para la VLAN 20, y el puerto 24 como trunk hacia el segundo switch permitiendo ambas VLANs. Verifica la configuración.

```

SW1> enable
SW1# configure terminal
SW1(config)# vlan 10
SW1(config-vlan)# name ventas
SW1(config-vlan)# exit
SW1(config)# vlan 20
SW1(config-vlan)# name contabilidad
SW1(config-vlan)# exit
SW1(config)# interface range GigabitEthernet0/1-10
SW1(config-if-range)# switchport mode access
SW1(config-if-range)# switchport access vlan 10
SW1(config-if-range)# exit
SW1(config)# interface range GigabitEthernet0/11-20
SW1(config-if-range)# switchport mode access
SW1(config-if-range)# switchport access vlan 20
SW1(config-if-range)# exit
SW1(config)# interface GigabitEthernet0/24
SW1(config-if)# switchport mode trunk
SW1(config-if)# switchport trunk allowed vlan 10,20
SW1(config-if)# end
SW1# copy running-config startup-config

```

Verificacion:

```

SW1# show vlan brief
(muestra que puertos quedaron en cada VLAN)
SW1# show interfaces trunk
(muestra el puerto 24 en modo trunk con las VLANs 10 y 20)

```

Observa el comando "interface range": configura varios puertos a la vez y ahorra muchísimo tiempo en switches de 24 o 48 puertos. Y nota que primero se crean las VLANs con "vlan 10" antes de asignar puertos a ellas: si asignas un puerto a una VLAN que no existe, el switch la crea solo en algunos modelos, pero hacerlo explícito evita sorpresas.

Práctica

Resuelve cada ejercicio antes de leer la solución. Aquí no hay cálculos largos, hay razonamiento: lee con calma y decide como un técnico.

1. Tienes un switch de 24 puertos con 20 computadoras conectadas, un router con una interfaz conectada a ese switch, y todo en una sola VLAN. Cuantos dominios de colisión hay y cuantos dominios de broadcast. Si divides el switch en 4 VLANs iguales, cómo cambian los números.

SOLUCIÓN:

Dominios de colisión: cada puerto del switch con un equipo es su propio dominio de colisión en full dúplex. Hay 20 puertos con computadoras más 1 puerto con el enlace al router, así que hay 21 dominios de colisión. Dominios de broadcast: el switch no los separa y hay una sola VLAN, así que todo el segmento es un único dominio de broadcast: 1. Si divides en 4 VLANs, los dominios de colisión no cambian, siguen siendo 21, porque las VLANs no afectan las colisiones. Los dominios de broadcast pasan a ser 4, uno por VLAN, porque cada VLAN es un dominio de broadcast separado. Para qué las 4 VLANs hablen entre si necesitarían un router con enrutamiento entre VLANs.

2. Tienes que conectar dos switches entre si y necesitas que tres VLANs, la 10, la 20 y la 30, pasen de un switch al otro. Que modo de puerto usas en cada extremo del enlace y por qué. qué pasaría si dejarás esos puertos en modo acceso.

SOLUCIÓN:

Usas modo trunk en ambos extremos, porque el trunk transporta multiples VLANs por un solo enlace etiquetando cada trama con su ID de VLAN según el estándar 802.1Q. Además debes permitir explícitamente las VLANs 10, 20 y 30 en el trunk y usar la misma VLAN nativa en ambos extremos. Si dejarás los puertos en modo acceso, solo pasaría una VLAN, la configurada en esos puertos, y las otras dos quedarían incomunicadas entre switches: las PCs de la VLAN 20 en el switch 1 no verían a las de la VLAN 20 en el switch 2. Ese es uno de los errores más comunes en redes con VLANs y el síntoma es conectividad parcial que confunde mucho.

3. Un router tiene esta tabla de ruteo. Un paquete con destino 10.5.5.5 llega al router. Que ruta se elige y por qué. qué pasaría si el destino fuera 10.5.0.1.

```
O  10.5.0.0/16    -> G0/1
S  10.5.5.0/24    -> G0/2 via 172.16.0.2
S  0.0.0.0/0      -> G0/3 via 200.10.10.1
```

SOLUCIÓN:

Para el destino 10.5.5.5: coincide con 10.5.0.0/16, con 10.5.5.0/24 y con la ruta por defecto. La coincidencia más larga es la /24, así que el paquete sale por G0/2 hacia 172.16.0.2, aunque la ruta /16 también lo cubriría. La regla de oro: ante varias coincidencias, gana el prefijo más largo, sin importar que la /24 sea estática y la /16 sea OSPF. Para el destino 10.5.0.1: coincide con la /16 y con la /0, pero no con la /24 porque el tercer octeto es 0 y no 5. Gana la /16 y sale por G0/1. Este ejercicio demuestra que el router no usa el orden de la tabla ni el protocolo para esté desempate, solo la longitud del prefijo.

4. Escribe la secuencia de comandos para agregar en un router Cisco una ruta estática hacia la red 192.168.20.0/24 con siguiente salto 10.0.0.2, y una ruta por defecto con siguiente salto 200.10.10.1. Incluye como guardar la configuración y que comandos usarías para verificar que las rutas quedaron instaladas.

SOLUCIÓN:

La secuencia completa, suponiendo que ya estás en modo privilegiado, es:

```
Router> enable
Router# configure terminal
Router(config)# ip route 192.168.20.0 255.255.255.0 10.0.0.2
Router(config)# ip route 0.0.0.0 0.0.0.0 200.10.10.1
Router(config)# end
Router# copy running-config startup-config
```

El primer comando ip route dice: para llegar a la red 192.168.20.0 con máscara 255.255.255.0, entregue los paquetes al vecino 10.0.0.2. El segundo dice: para todo lo demás, la ruta 0.0.0.0 con máscara 0.0.0.0, entregue los paquetes a 200.10.10.1. El copy guarda todo en la memoria permanente para que sobreviva a un reinicio. Para verificar usas "show ip route" y buscas las líneas marcadas con S: debes ver "S 192.168.20.0/24 vía 10.0.0.2" y "S 0.0.0.0/0 vía 200.10.10.1". También puedes probar con "ping 192.168.20.1" para confirmar conectividad real, recordando que el router remoto necesita su propia ruta de regreso hacia tus redes.

5. Un router aprende la red 172.20.0.0/16 por dos caminos: OSPF la anuncia con métrica de costo 50 y RIP la anuncia con métrica de 3 saltos. Cuál de las dos rutas entra a la tabla de ruteo y por qué. Que cambiaría si además configurarás una ruta estática hacia esa misma red.

SOLUCIÓN:

Entra la ruta de OSPF. La métrica no sirve para comparar porque cada protocolo mide con unidades distintas: 3 saltos de RIP contra costo 50 de OSPF no son comparables, como kilos contra litros. El desempate entre protocolos lo hace la distancia administrativa: OSPF tiene 110 y RIP tiene 120, y gana el valor menor por ser más confiable. Así que la tabla instala la ruta OSPF y la de RIP queda como respaldo silencioso. Si además configuras una ruta estática hacia 172.20.0.0/16, la estática tiene distancia administrativa 1, menor que 110, así que la estática desbanca a OSPF y entra a la tabla. La moraleja: una ruta estática mal pensada puede imponerse sobre un diseño dinámico bien hecho, por eso las estáticas se usan con criterio y las flotantes llevan distancia alta a propósito.

6. Te piden diseñar el enrutamiento para tres casos: una red empresarial de 500 routers con equipos de varios fabricantes que necesita converger rápido ante fallas; la conexión de tu empresa con dos proveedores de internet distintos; y una red pequeña de 4 routers en una sola oficina. Que protocolo o método usarías en cada caso y por qué.

SOLUCIÓN:

Para la red de 500 routers multivendedor usas OSPF. Es un estándar abierto que funciona entre fabricantes, su convergencia es rápida gracias al algoritmo de estado de enlace, su métrica por costo prefiere los enlaces de mayor ancho de banda y soporta áreas para organizar una red de ese tamaño sin saturar a los routers. RIP queda descartado porque su límite de 15 saltos y su convergencia lenta lo hacen inviable a esa escala, y EIGRP queda descartado porque solo funciona entre equipos Cisco y aquí hay varios fabricantes. Para la conexión con dos proveedores de internet usas BGP, porque es el protocolo diseñado para enrutar entre sistemas autónomos: te permite recibir rutas de ambos proveedores, aplicar políticas como preferir un proveedor para cierto tráfico, y es el idioma común de internet. Ningún protocolo interior sirve para eso. Para la red pequeña de 4 routers lo más sensato es ruteo estático con una ruta por defecto: 4 routers no justifican la complejidad de un protocolo dinámico, las rutas estáticas son predecibles, no consumen recursos conversando entre si, y con una ruta por defecto bien puesta tienes salida a internet. Si esa oficina creciera a 30 routers, ahí si migrarías a OSPF. La lección: no hay un protocolo ganador absoluto, hay un protocolo adecuado para cada tamaño y cada contexto.

Resumen de la unidad

En esta unidad conociste a los dos grandes protagonistas de las redes: el switch y el router, y aprendiste a pensar como cada uno. El switch trabaja en la capa 2 con tramas y direcciones MAC: aprende con la dirección de origen, decide con la dirección de destino, guarda todo en su tabla MAC y solo molesta a todos con flooding cuando no conoce al destinatario o con broadcasts dirigidos a FF:FF:FF:FF:FF:FF. Grabaste la frase clave: el switch separa dominios de colisión, uno por puerto en full dúplex, pero no separa dominios de broadcast. Esa distinción, que al principio parece un juego de palabras, es la base para entender VLANs, trunks y todo el diseño de redes locales modernas.

Con las VLANs aprendiste a dividir un switch físico en varias redes lógicas, cada una su propio dominio de broadcast, identificadas por un ID del 1 al 4094. Distinguiste los puertos de acceso, para dispositivos finales en una sola VLAN, de los puertos trunk, que transportan multiples VLANs etiquetadas con 802.1Q entre switches y hacia el router. Y viste los errores típicos: trunks olvidados, VLAN nativa distinta en cada extremo y puertos en la VLAN equivocada.

El router, en cambio, trabaja en la capa 3 con paquetes y direcciones IP: conecta redes distintas, termina los dominios de broadcast y decide cada envío consultando su tabla de ruteo. Aprendiste a leer esa tabla como un mapa: red destino, máscara, siguiente salto e interfaz de salida, con los códigos que indican el origen de cada ruta. Entendiste la puerta de enlace como la salida de tu red local y el procedimiento de decisión del router, donde ante varias coincidencias siempre gana el prefijo más largo.

Comparaste el ruteo estático, simple y predecible pero rígido, con el ruteo dinámico, adaptable pero más complejo. Conociste a los cuatro protocolos: RIP con su métrica de saltos para redes pequeñas, OSPF con su costo por ancho de banda para empresas multivendedor, EIGRP con DUAL y métrica compuesta para mundos Cisco, y BGP con su vector de ruta para mantener unido a internet entre sistemas autónomos. Y aprendiste las dos reglas del desempate: la métrica decide dentro del protocolo, la distancia administrativa decide entre protocolos, y en ambas gana el valor menor.

Cerraste configurando un router de verdad con comandos Cisco: hostname, interfaces con ip address y no shutdown, rutas estáticas con ip route, la ruta por defecto 0.0.0.0/0, y el guardado con copy running-config startup-config que nunca debes olvidar. Si dominas leer una tabla de ruteo, elegir acceso contra trunk y escribir esos comandos básicos, ya piensas como un técnico de redes, no como un simple conectacables. La próxima unidad pondrá todo esto a trabajar en escenarios completos.

Guarda esta imagen mental para siempre: el switch reparte cartas dentro del edificio mirando apellidos MAC, el router decide entre ciudades mirando direcciones IP, y tu, con la tabla de ruteo en una mano y la tabla MAC en la otra, eres quien mantiene el correo funcionando. Cada falla que encuentres de aquí en adelante, preguntate primero: es problema de carta o es problema de carretera. Esa sola pregunta te pone en el camino correcto nueve de cada diez veces.

Antes de cerrar, verifica que puedes hacer estas diez cosas sin mirar apuntes: explicar que hace un switch y que hace un router con tus propias palabras; describir cómo aprende la tabla MAC y la diferencia entre aprender con origen y decidir con destino; contar cuantos dominios de colisión y de broadcast hay en un escenario dado; explicar qué es una VLAN y para qué sirve; decidir si un puerto va en modo acceso o trunk; leer una tabla de ruteo y predecir por dónde sale un paquete aplicando la coincidencia más larga; explicar qué es la puerta de enlace y que falla cuando está mal; comparar RIP, OSPF, EIGRP y BGP diciendo tipo, métrica y uso típico de cada uno; explicar la diferencia entre métrica y distancia administrativa con sus valores clásicos; y escribir la configuración básica de un router con interfaces, rutas estáticas, ruta por defecto y guardado. Si las diez te salen fluidas, esta unidad está dominada y puedes seguir con confianza a la siguiente. Y cuando en tu trabajo diario te toque explicar a alguien

por qué su computadora no llega al servidor, ya tienes el guion: revisa la tabla MAC, revisa las VLANs y los trunks, revisa la puerta de enlace y lee la tabla de ruteo. Ese guion, repetido con disciplina, resuelve casi todo.

UNIDAD 7: DHCP, DNS y NAT

Bienvenido a la Unidad 7 del Curso Completo de Redes de Lucas EGA Academy. En esta unidad vas a conocer a los tres trabajadores invisibles que hacen que tu experiencia en Internet se sienta sencilla y sin esfuerzo: DHCP, DNS y NAT. Son tres servicios que casi nunca ves, que casi nadie menciona en una conversación normal, y sin los cuales nada de lo que haces en línea funcionaría como lo conoces.

Piensa en lo que pasa todos los días en tu casa. Llegas, sacas tu teléfono del bolsillo y, sin tocar nada, ya estás conectado al Wi-Fi. Abres el navegador, escribes google.com y la página aparece en un segundo. Tu hermano está viendo videos, tú mamá hace una videollamada y tú estás jugando en línea, todo al mismo tiempo, y nadie tuvo que configurar nada en ningún aparato. Detrás de esa sencillez hay tres mecanismos trabajando en equipo, y en esta unidad los vas a desarmar pieza por pieza para entenderlos de verdad.

El primero es DHCP, el protocolo que reparte direcciones IP de forma automática. Cada vez que tu teléfono se conecta al Wi-Fi de tu casa y obtiene una dirección IP sin que tú muevas un dedo, ahí está DHCP trabajando. Sin el, tendrías que escribir a mano la dirección IP, la máscara de subred, la puerta de enlace y los servidores DNS en cada teléfono, cada tableta, cada computadora y cada foco inteligente de tu casa. Imagina hacerlo en una oficina con quinientas computadoras, o en un aeropuerto donde miles de personas se conectan y desconectan cada hora. Sería imposible de administrar. DHCP convierte esa pesadilla en un proceso automático que tarda segundos.

El segundo es DNS, el sistema de nombres de dominio. Es la razón por la que escribes google.com, facebook.com o lucasegaacademy.com en vez de memorizar secuencias de números como 142.250.0.1. Los humanos somos malos recordando números pero muy buenos recordando nombres, así que DNS funciona como el directorio telefónico de Internet: traduce los nombres que tú escribes a las direcciones IP que las máquinas entienden. Cada vez que abres una página web, mandas un correo o abres una aplicación, hay una consulta DNS ocurriendo en fracciones de segundo antes de que cualquier otra cosa pase.

El tercero es NAT, la traducción de direcciones de red. Es la razón por la que toda tu casa puede salir a Internet usando una sola dirección IP pública, aunque tengas diez, veinte o cincuenta dispositivos conectados. Las direcciones IPv4 se acabaron hace años porque el mundo tiene muchos más dispositivos que direcciones disponibles, y NAT es el truco ingenioso que permite que millones de redes privadas compartan unas cuantas direcciones públicas. Sin NAT, el Internet que conoces hoy simplemente no podría existir con IPv4.

En esta unidad vas a ver las clases 19, 20 y 21. En la clase 19 dominarás DHCP: para qué sirve, el famoso proceso DORÁ con sus cuatro mensajes (Discover, Offer, Request y Acknowledge), qué es una concesión o lease y cómo se renueva, qué son las reservas de direcciones, cómo funciona el servidor DHCP que vive dentro de tu router casero, y qué pasa cuando no hay ningún servidor DHCP disponible, que es cuando aparece la misteriosa dirección APIPA que empieza con 169.254. En la clase 20 te sumergirás en DNS: la jerarquía completa desde los servidores raíz hasta los subdominios, los tipos de registros (A, AAAA, CNAME, MX, TXT y NS), cómo ocurre una resolución paso a paso, la diferencia entre consultas recursivas e iterativas, para qué sirve la cache, cuales son los servidores DNS públicos más usados como 8.8.8.8 y 1.1.1.1, y como usar los comandos nslookup y dig para interrogar al sistema DNS como un profesional. En la clase 21 conquistarás NAT y PAT: por qué existen, cómo funcionan el NAT estático, el NAT dinámico y el PAT con sobrecarga de puertos, la diferencia entre una IP pública y una privada, el ejemplo clásico de toda tu casa saliendo con una sola IP, y cómo funciona el reenvío de puertos o port forwarding.

Al terminar esta unidad serás capaz de explicar con tus propias palabras qué pasa en la red desde el momento en qué enciendes tu computadora hasta que se carga tú página favorita, pasando por la obtención automática de la IP, la traducción del nombre de dominio y la salida a Internet a través de NAT. Ese conocimiento es exactamente lo que distingue a alguien que "usa Internet" de alguien que "entiende redes", y es la base que todo técnico, administrador y especialista en seguridad necesita dominar.

Explicación detallada

1. DHCP: el repartidor automático de direcciones IP

DHCP son las siglas de Dynamic Host Configuration Protocol, o protocolo de configuración dinámica de equipos. Su trabajo es sencillo de describir pero enorme en impacto: entregar automáticamente todos los parámetros de red que un dispositivo necesita para comunicarse. Cuando hablamos de "parámetros de red" nos referimos principalmente a cuatro datos: la dirección IP del dispositivo, la máscara de subred, la puerta de enlace predeterminada y la dirección de al menos un servidor DNS. Sin esos cuatro datos, un dispositivo está sordo y mudo en la red: no sabe quién es, no sabe quién es su vecino y no sabe por dónde salir hacia otras redes.

Para entender por qué DHCP es tan importante, imagina el mundo antes de qué existiera, cuando todo se configuraba a mano. El administrador de red tenía que ir computadora por computadora escribiendo la dirección IP, la máscara, la puerta de enlace y el DNS. En una red

pequeña de diez equipos era tedioso pero posible. En una empresa de quinientos equipos era una pesadilla administrativa. Y lo peor no era el trabajo inicial, sino los errores humanos: dos computadoras con la misma dirección IP se pelean y ninguna de las dos navega bien, una máscara mal escrita deja a un equipo aislado de su propia red, una puerta de enlace incorrecta impide salir a Internet. Cada error significaba ir físicamente hasta la máquina a corregirlo. DHCP elimina todo eso centralizando la repartición: un solo servidor guarda un rango de direcciones disponibles y las presta a quién las pida, llevando un registro de a quién le dio que y por cuanto tiempo.

Es importante entender la palabra "dinámica" en su nombre. DHCP no regala direcciones para siempre: las presta por un tiempo limitado que se llama concesión o lease. Cuando el tiempo se acaba, el dispositivo debe renovar el préstamo o devolver la dirección. Esto permite reutilizar direcciones: en un café con cien direcciones disponibles pueden pasar mil clientes al día, porque cada cliente usa su dirección solo mientras está ahí. Si las direcciones fueran permanentes, el café se quedaría sin direcciones al llegar el cliente número ciento uno.

DHCP funciona con el modelo cliente-servidor y usa los puertos UDP 67 y 68. El servidor escucha en el puerto 67 y el cliente usa el puerto 68. Recuerda qué es UDP y no TCP, porque al inicio de la conversación el cliente ni siquiera tiene una dirección IP, así que no podría establecer una conexión TCP formal. Los mensajes iniciales se envían por broadcast a toda la red local, gritando básicamente "hay algún servidor DHCP por ahí", y eso solo funciona con UDP.

Una analogía que ayuda mucho: piensa en DHCP como la recepción de un hotel. Tú llegas sin habitación asignada (sin dirección IP), te acercas al mostrador y pides una habitación (Discover). La recepcionista revisa su sistema y te ofrece la habitación 204 (Offer). Tú confirmas que la quieres (Request) y ella te entrega la llave con las reglas del hotel: la hora de salida y donde está todo (Acknowledge, que incluye la puerta de enlace y el DNS). Si te quedas más días, renuevas tu estancia antes de que venza (renovación). Y si el hotel está lleno o no hay recepcionista, no hay habitación para ti (APIPA, que veremos más adelante).

2. El proceso DORÁ: los cuatro mensajes que lo hacen todo

Todo dispositivo que quiere una dirección por DHCP pasa por una conversación de cuatro mensajes conocida como DORA, por las iniciales de cada paso en inglés: Discover, Offer, Request y Acknowledge. Memoriza este proceso porque es una de las preguntas más clásicas en exámenes y entrevistas de redes. Vamos a seguirlo con un ejemplo concreto: tu laptop recién encendida conectándose al Wi-Fi de tu casa.

Paso 1: DHCP Discover. Tu laptop acaba de encenderse y no tiene dirección IP. Su dirección es literalmente 0.0.0.0, que significa "no tengo dirección". Como no sabe dónde está el servidor DHCP, envía un mensaje de descubrimiento por broadcast a la dirección 255.255.255.255, usando como destino de capa 2 la dirección MAC de broadcast ff:ff:ff:ff:ff:ff. Ese mensaje llega a todos los dispositivos de la red local. Su contenido es básicamente: "Hola, soy una laptop con esta dirección MAC, necesito que alguien me de una dirección IP". El mensaje sale del puerto UDP 68 del cliente hacia el puerto UDP 67 del servidor.

Paso 2: DHCP Offer. El servidor DHCP de tu router recibe el Discover, revisa su lista de direcciones disponibles y elige una, por ejemplo 192.168.1.25. Entonces responde con un mensaje de oferta. La oferta incluye la dirección IP propuesta, la máscara de subred, el tiempo de concesión ofrecido y la propia dirección IP del servidor. Técnicamente el Offer puede enviarse por unicast directamente a la MAC del cliente, aunque en algunas implementaciones también usa broadcast. El mensaje dice: "Te ofrezco la 192.168.1.25 con máscara 255.255.255.0 por 24 horas, mi dirección es 192.168.1.1".

Un detalle interesante: si hubiera dos servidores DHCP en la misma red, el cliente podría recibir dos ofertas distintas. En ese caso el cliente normalmente se queda con la primera que llegue. Por eso tener dos servidores DHCP activos sin coordinación en la misma red es una mala idea: repartirían direcciones traslapadas y causarían conflictos.

Paso 3: DHCP Request. La laptop recibe la oferta y responde con un mensaje de solicitud. Ojo con este detalle que muchos pasan por alto: el Request también se envía por broadcast, no solo al servidor que hizo la oferta. La razón es cortesía de protocolo: así los demás servidores que hayan hecho ofertas se enteran de qué el cliente eligió otra y pueden liberar la dirección que habían apartado. El mensaje dice: "Acepto la oferta de la 192.168.1.25 del servidor 192.168.1.1, por favor confirmala".

Paso 4: DHCP Acknowledge. El servidor elegido recibe el Request y responde con la confirmación final. Este mensaje incluye todos los parámetros de red completos: la dirección IP asignada (192.168.1.25), la máscara de subred (255.255.255.0), la puerta de enlace (192.168.1.1), las direcciones de los servidores DNS, el tiempo de concesión y posiblemente opciones extra como el nombre de dominio local. A partir de este momento, la laptop ya puede comunicarse normalmente en la red. Si el servidor no pudiera cumplir lo pedido, enviaría un DHCP NAK (negación) en vez de un ACK, y el cliente tendría que empezar de nuevo con otro Discover.

Fijate en algo hermoso de este diseño: en ningún momento el cliente necesito saber la dirección del servidor de antemano. Todo se resolvió con broadcasts locales y el servidor se identificó solo. Esa es la magia que permite que llegues a un hotel, te conectes al Wi-Fi y en segundos ya estes navegando.

3. La concesión (lease): un alquiler con fecha de vencimiento

La concesión o lease es el tiempo durante el cual un cliente tiene derecho a usar la dirección IP que le prestó el servidor DHCP. No es una propiedad, es un alquiler. Los tiempos típicos varían según el entorno: en un router casero lo normal son 24 horas, en redes empresariales con equipos fijos puede ser de varios días, y en lugares con mucha rotación como aeropuertos o cafés puede ser de apenas una o dos horas para reciclar rápido las direcciones.

El ciclo de vida de una concesión tiene momentos clave marcados por dos temporizadores. Cuando el cliente obtiene su dirección, arranca un conteo. Al llegar al 50 por ciento del tiempo de concesión, el cliente entra en estado de renovación e intenta contactar directamente al servidor DHCP original con un mensaje DHCP Request enviado por unicast (ya no por broadcast, porque ahora si conoce la dirección del servidor). Si el servidor responde con un ACK, la concesión se renueva por un período completo nuevo y el conteo vuelve a empezar. Esto pasa en silencio, sin que tú notes nada: tu teléfono renueva su dirección IP todos los días sin interrumpir tus videos ni tus mensajes.

Si el servidor original no responde al llegar al 50 por ciento, el cliente sigue usando su dirección normalmente y espera hasta el 87.5 por ciento del tiempo. En ese punto entra en estado de reasociación y envía un DHCP Request por broadcast, preguntándole a cualquier servidor DHCP disponible que le renueve o le de una dirección nueva. Si algún servidor responde, el cliente sigue trabajando, posiblemente con una dirección distinta. Solo si llega al 100 por ciento sin respuesta el cliente debe dejar de usar la dirección y volver a empezar todo el proceso con un DHCP Discover. En la práctica, esto significa que si tu router se apaga unas horas, tus dispositivos siguen funcionando con su última dirección hasta que la concesión expire.

El cliente también puede liberar su dirección voluntariamente con un mensaje DHCP Release, por ejemplo cuando apagas tu laptop de forma ordenada. Así el servidor recupera la dirección de inmediato sin esperar a que venza la concesión. Es un detalle de buena ciudadanía en la red.

Un error común de principiantes es pensar que la dirección que te da DHCP es "tuya para siempre". No lo es. Si apagas tu computadora una semana y la vuelves a encender, es perfectamente normal que recibas una dirección distinta a la que tenías. Para los dispositivos

normales esto no importa en absoluto, pero para equipos que otros necesitan encontrar siempre en el mismo lugar, como una impresora de red o un servidor, se usan las reservas, que veremos en la siguiente sección.

4. Reservas DHCP y rangos de exclusión: control sin perder la automatización

Hay casos en los que quieres lo mejor de los dos mundos: la comodidad de DHCP y la estabilidad de una dirección fija. Para eso existen las reservas DHCP, también llamadas asignaciones estáticas por DHCP. Una reserva es una regla en el servidor que dice: "cada vez que el dispositivo con esta dirección MAC pida una dirección, dale siempre esta IP específica". El dispositivo sigue usando DHCP y sigue pasando por el proceso DORÁ, pero el resultado es predecible: siempre termina con la misma dirección.

El ejemplo clásico es la impresora de red de una oficina. Si la impresora obtuviera cada semana una IP distinta, todos los usuarios tendrían que reconfigurar el controlador de impresión cada vez. Con una reserva, la impresora siempre recibe por ejemplo 192.168.1.50, y la configuración de todos queda fija para siempre. Otros candidatos típicos para reservas son los servidores internos, las cámaras de seguridad, los puntos de acceso Wi-Fi y cualquier equipo al que le hagas reenvío de puertos (port forwarding), porque el reenvío apunta a una IP interna específica y se rompería si esa IP cambiará.

No confundas una reserva con una IP estática configurada a mano en el dispositivo. El resultado es parecido (el equipo siempre tiene la misma IP), pero la administración es muy distinta: con reservas, toda la información vive centralizada en el servidor DHCP. Si algún día cambias la puerta de enlace o los servidores DNS de tu red, con reservas no tienes que tocar ningún dispositivo: el servidor entrega los parámetros nuevos automáticamente en la siguiente renovación. Con IPs estáticas manuales tendrías que ir equipo por equipo.

El concepto hermano de la reserva es el rango de exclusión. Cuando configuras un servidor DHCP defines un ámbito o pool, que es el rango total de direcciones que puede repartir, por ejemplo de 192.168.1.100 a 192.168.1.200. Pero quizás ya tienes algunos equipos con IP fija manual entre la 192.168.1.10 y la 192.168.1.30. Si no excluyes ese rango, el servidor podría prestarle a alguien la 192.168.1.20 y provocar un conflicto con el equipo que ya la usa manualmente. La buena práctica es excluir del pool todas las direcciones que uses de forma estática, y usar reservas para los equipos que quieres fijos pero administrados por DHCP.

5. El servidor DHCP dentro de tu router casero

Casi todos los routers caseros traen un servidor DHCP integrado y activado por defecto, y es el responsable de que conectar un dispositivo nuevo a tu Wi-Fi sea tan fácil. Cuando entras a

la página de administración de tu router (normalmente en 192.168.1.1 o 192.168.0.1) encuentras una sección de DHCP o de "servidor DHCP" con opciones como: activar o desactivar el servicio, la dirección IP inicial y final del rango a repartir, el tiempo de concesión, y la lista de reservas.

Un detalle que vale oro para diagnosticar problemas: esa página también muestra la tabla de clientes DHCP, es decir, la lista de todos los dispositivos que tienen una concesión activa, con su nombre, su dirección MAC y la IP asignada. Cuando en tu casa alguien dice "el internet no me funciona", una de las primeras cosas que puedes revisar es si su dispositivo aparece en esa tabla. Si no aparece, el problema puede estar en el Wi-Fi o en qué el dispositivo no está completando el proceso DORÁ.

En redes más grandes, el servidor DHCP suele ser un equipo dedicado o un servicio corriendo en un servidor Windows o Linux, capaz de manejar múltiples ámbitos para distintas subredes. Un problema interesante aparece ahí: los mensajes DHCP Discover son broadcast y los broadcasts no cruzan routers, así que un servidor DHCP central no escucharía los Discover de otras subredes. La solución es el agente de retransmisión DHCP, conocido como DHCP relay o ip helper-address en equipos Cisco: el router de cada subred escucha los broadcast locales y los reenvía por unicast al servidor central, que responde de vuelta por él mismo camino. Así una empresa puede tener un solo servidor DHCP administrando decenas de sucursales.

6. Cuándo no hay DHCP: APIPA y la dirección 169.254

Qué pasa si enciendes tu computadora, pide una dirección por DHCP y nadie responde. Quizás el router se descompuso, el cable de red está dañado, el servicio DHCP se apagó por error o estás conectado a un switch sin servidor. Después de varios intentos sin respuesta, el sistema operativo no se queda sin dirección: se autoasigna una del rango especial 169.254.0.1 a 169.254.255.254, con máscara 255.255.0.0. Este mecanismo se llama APIPA, por Automatic Private IP Addressing, y es la forma que tiene el equipo de decir "no encontré quién me diera una dirección, así que me invente una para al menos poder hablar con mis vecinos".

Es fundamental que entiendas lo que una dirección APIPA significa y lo que no significa. Si ves una 169.254.x.x en tu equipo, eso es un síntoma clarísimo de que DHCP falló. Con esa dirección tu equipo puede comunicarse con otros equipos que también tengan direcciones APIPA en la misma red local, porque están en el mismo rango, pero no tendrá puerta de enlace ni servidores DNS válidos, así que no podrás salir a Internet ni llegar a otras subredes. Muchos principiantes ven que "tengo una dirección IP" y asumen que la red está bien, cuando en realidad esa dirección es la prueba de qué algo anda mal.

El procedimiento de diagnóstico cuando encuentras una APIPA es metódico. Primero revisa lo físico: el cable bien conectado, el Wi-Fi realmente asociado a tu red y no a la del vecino. Segundo, verifica que el servidor DHCP este encendido y funcionando: reinicia el router casero, que resuelve una cantidad sorprendente de casos. Tercero, en el equipo ejecuta la liberación y renovación manual de la concesión para forzar un DORÁ nuevo. Cuarto, revisa que no haya un segundo servidor DHCP peleando o un switch mal configurado. Y quinto, considera que el problema puede ser el propio equipo: un controlador de red dañado también impide completar el proceso.

Un error común es intentar "arreglar" una APIPA configurando una IP estática cualquiera sin entender el problema de fondo. Eso puede funcionar como parche temporal, pero si la causa era que el router estaba apagado, tu IP estática tampoco tendrá puerta de enlace útil. La APIPA es un síntoma, no la enfermedad: siempre busca la causa del fallo de DHCP.

Errores comunes de principiantes con DHCP

El primer error es configurar dos servidores DHCP en la misma red sin coordinarlos, por ejemplo conectar un segundo router casero sin desactivar su DHCP. Ambos reparten direcciones del mismo rango, se generan duplicados y los equipos se conectan y desconectan de forma intermitente. La solución es tener un único servidor DHCP por segmento de red, o coordinar rangos que no se traslapen.

El segundo error es olvidar las exclusiones: poner IPs fijas manuales dentro del rango que reparte el DHCP. Tarde o temprano el servidor le presta esa dirección a otro equipo y aparece el temido conflicto de IP duplicada, con mensajes de error en ambos equipos y conectividad intermitente.

El tercer error es elegir tiempos de concesión inadecuados. Un lease de una semana en la red Wi-Fi de un estadio con miles de visitantes rotando garantiza quedarse sin direcciones a mitad del partido. Un lease de treinta minutos en una oficina con equipos fijos genera tráfico de renovación innecesario. Ajusta el tiempo al ritmo de rotación de tus clientes.

El cuarto error es no documentar las reservas. Con el tiempo nadie recuerda por qué la impresora tiene la .50 ni que MAC corresponde a cada reserva, y cuando hay que migrar de router se vuelve un rompecabezas. Guarda una tabla sencilla con dispositivo, MAC, IP reservada y motivo.

7. DNS: el directorio telefónico de Internet

DNS son las siglas de Domain Name System, el sistema de nombres de dominio. Su misión es traducir los nombres que los humanos escribimos, como google.com o lucasegaacademy.com, a las direcciones IP que las máquinas necesitan para comunicarse, cómo 142.250.0.1. Funciona exactamente como el directorio telefónico de antes: tú buscas el nombre de una persona y obtienes su número de teléfono; aquí buscas un nombre de dominio y obtienes su número IP.

Para dimensionar su importancia, haz este experimento mental: cada página que abres, cada video que reproduces, cada mensaje que envías por una aplicación que usa un nombre de servidor, genera al menos una consulta DNS antes de qué empiece la comunicación real. Sin DNS tendrías que memorizar cientos de direcciones IP, algo imposible en la práctica. DNS es lo que hace que Internet sea usable para seres humanos.

Técnicamente DNS es un sistema distribuido y jerárquico, no una base de datos central. Nadie tiene "la lista completa" de todos los dominios del mundo; en cambio, miles de servidores se reparten la responsabilidad por zonas, y las consultas van saltando de servidor en servidor hasta encontrar la respuesta. Esa distribución es lo que lo hace escalable a miles de millones de nombres y resistente a fallos: no hay un único punto que pueda tumbarlo todo.

DNS trabaja principalmente sobre el puerto 53, usando UDP para las consultas normales (rápidas y ligeras) y TCP cuando la respuesta es muy grande o para transferencias de zona entre servidores. Un detalle que te servirá toda la vida: cuando configuras la red manualmente o revisas lo que te entregó DHCP, los "servidores DNS" son simplemente las direcciones IP a las que tu equipo les pregunta "oye, que IP tiene este nombre".

La analogía del directorio telefónico se queda corta en un aspecto: el DNS también guarda otros tipos de información además de la IP de un nombre. Puede decirte que servidor recibe el correo de un dominio, que servidores tienen autoridad sobre una zona, o incluir textos de verificación para servicios. Esos son los tipos de registros, que veremos en detalle más adelante. Por ahora quedate con la idea central: DNS traduce nombres a números, y sin el no hay Internet usable.

8. La jerarquía del DNS: raíz, TLD, dominio y subdominio

Los nombres de dominio están organizados como un árbol invertido, con la raíz arriba y las ramas extendiéndose hacia abajo. Entender esta jerarquía es entender cómo se delega la autoridad en DNS: cada nivel es responsable de su parte y delega lo de abajo. Vamos de arriba hacia abajo con el ejemplo www.lucasegaacademy.com.

En la cima están los servidores raíz. Son trece identidades lógicas nombradas de la a a la m (a.root-servers.net hasta m.root-servers.net), aunque físicamente existen cientos de copias distribuidas por el mundo usando una técnica llamada anycast. Los servidores raíz no saben la IP de www.lucasegaacademy.com; su trabajo es mucho más limitado y por eso pueden ser tan pocos: solo saben dónde están los servidores responsables de cada TLD. Son como la recepción del edificio que no conoce a cada inquilino pero sabe en que piso está cada departamento administrativo.

El siguiente nivel es el TLD, Top Level Domain o dominio de nivel superior. Son las terminaciones como .com, .org, .net, .edu, .mx, .es o .io. Cada TLD tiene sus propios servidores autoritativos. Los servidores del TLD .com saben que servidores tienen autoridad sobre cada dominio .com registrado, pero no saben nada de los .org ni de los .mx. Existen TLD genéricos (.com, .org, .net), TLD de código de país (.mx para México, .es para España, .ar para Argentina) y TLD patrocinados o nuevos (.edu, .gov, .tech, entre cientos de opciones modernas).

Después viene el dominio registrado, también llamado dominio de segundo nivel: lucasegaacademy.com, google.com, wikipedia.org. Cuando alguien registra un dominio, el TLD delega en los servidores de nombres que el dueño elija toda la autoridad sobre ese dominio y lo que cuelgue de él. Esos servidores autoritativos son los que guardan los registros reales: que IP tiene www, a dónde llega el correo, etc.

Finalmente están los subdominios, que son divisiones del dominio principal: www.lucasegaacademy.com, blog.lucasegaacademy.com, tienda.lucasegaacademy.com. El dueño del dominio puede crear todos los subdominios que quiera sin pedir permiso a nadie, porque la autoridad ya fue delegada en él. Cada subdominio puede apuntar a una IP distinta, a un servidor distinto o incluso delegarse a otros servidores de nombres.

Un detalle elegante del sistema: un nombre completo y bien escrito termina con un punto, como www.lucasegaacademy.com. con el punto final. Ese punto representa la raíz, y el nombre completo se llama FQDN (Fully Qualified Domain Name). Tu navegador lo agrega por ti si lo omites, así que casi nunca lo ves, pero saberlo te ayuda a leer la jerarquía de derecha a izquierda: punto (raíz), com (TLD), [lucasegaacademy](http://lucasegaacademy.com) (dominio), www (subdominio).

Esta delegación jerárquica es lo que permite que el sistema escale. El servidor raíz no necesita saber nada de tu pequeño dominio, el TLD solo necesita saber a quién le delegó cada dominio, y cada dueño administra lo suyo. Si mañana registras midominio.com, nadie en la raíz ni en el TLD tiene que configurar nada especial: solo se registra la delegación hacia tus servidores de nombres y listo.

9. Tipos de registros DNS: más que nombres e IPs

Cuándo consultas al DNS no siempre preguntas "cuál es la IP de este nombre". El sistema maneja varios tipos de registros, cada uno con un propósito distinto. Conocerlos es esencial porque cuando administres un dominio o diagnostiques problemas de correo o de web, vas a trabajar directamente con ellos. Estos son los seis que debes dominar:

Registro A (Address): es el más básico y el más usado. Asocia un nombre de dominio o subdominio con una dirección IPv4. Por ejemplo, un registro A puede decir que `www.lucasegaacademy.com` apunta a `192.0.2.10`. Cuándo escribes una dirección web en el navegador, el registro A es casi siempre lo primero que se consulta.

Registro AAAA (quad-A): exactamente lo mismo que el A, pero para direcciones IPv6. Se llama AAAA porque una dirección IPv6 mide 128 bits, cuatro veces los 32 bits de IPv4. Un dominio moderno suele tener ambos: un A con su IPv4 y un AAAA con su IPv6, para atender a clientes de los dos mundos.

Registro CNAME (Canonical Name): crea un aliás, es decir, dice "este nombre es en realidad este otro nombre". Por ejemplo, puedes crear un CNAME que diga que `blog.lucasegaacademy.com` es un aliás de `servidor-hosting.example.net`. Cuando alguien consulta el alias, el DNS resuelve el nombre canónico y devuelve su IP. Es muy útil para apuntar varios subdominios al mismo destino sin duplicar IPs: si la IP cambia, solo actualizas el registro A del nombre canónico. Regla de oro que causa muchos dolores de cabeza: un nombre con CNAME no puede tener ningún otro registro al mismo tiempo, y por eso un CNAME no puede usarse en la raíz desnuda del dominio (el llamado dominio ápex).

Registro MX (Mail Exchange): indica que servidores reciben el correo electrónico de un dominio. Cada registro MX lleva un número de prioridad: el servidor con el número más bajo es el preferido, y los de número más alto son respaldos. Por ejemplo, `lucasegaacademy.com` podría tener un MX con prioridad 10 apuntando a `mail1.proveedor.com` y otro con prioridad 20 a `mail2.proveedor.com`. Si el primero no responde, el correo intenta con el segundo. Sin registros MX, nadie podría enviarte correo a tu dominio.

Registro TXT (Text): guarda texto libre asociado a un nombre. Su uso más común hoy es la seguridad del correo: registros SPF que dicen que servidores tienen permiso de enviar correo en nombre del dominio, y registros DKIM y DMARC relacionados. También se usan para verificaciones de propiedad, como cuando Google te pide agregar un TXT para demostrar que el dominio es tuyo. Aunque suene simple, un TXT mal escrito puede hacer que todo tu correo legítimo termine en spam.

Registro NS (Name Server): indica que servidores tienen autoridad sobre una zona o dominio. Son los que hacen posible la delegación de la que hablamos en la jerarquía: el TLD .com tiene registros NS que dicen "para lucasegaacademy.com preguntale a estos servidores". Si los NS están mal configurados, tu dominio simplemente deja de resolverse en todo el mundo, así que son de los registros más delicados.

10. Resolución paso a paso: recursivo contra iterativo, y la cache

Ahora juntemos las piezas y sigamos una consulta real de principio a fin. Escribes `www.ejemplo.com` en tu navegador por primera vez en el día. Esto es lo que ocurre en milisegundos:

Primero tu equipo revisa su propia cache DNS local: quizás ya resolvió ese nombre hace poco y todavía guarda la respuesta. Si la encuentra y no ha expirado, la usa y ahí termina todo. Si no, tu equipo (que actúa como resolvidor stub, un cliente sencillo) le pregunta a su servidor DNS recursivo configurado, normalmente el de tu proveedor de Internet o uno público como 8.8.8.8. Esta pregunta es recursiva: tu equipo le dice "resuélveme esto completo y no me devuelvas hasta tener la respuesta final".

El servidor recursivo revisa su propia cache. Si otro cliente preguntó lo mismo hace poco, responde de inmediato. Si no, empieza el recorrido iterativo por la jerarquía. Le pregunta a un servidor raíz: "cuál es la IP de `www.ejemplo.com`". El raíz no lo sabe, pero responde con una referencia: "no sé, pero aquí están los servidores del TLD .com, preguntales a ellos". Eso es una consulta iterativa: el servidor no resuelve por ti, te dice a quién preguntar después.

El recursivo entonces le pregunta a un servidor del TLD .com, que responde de forma similar: "no sé la IP, pero `ejemplo.com` está delegado a estos servidores NS, ve con ellos". Finalmente el recursivo le pregunta al servidor autoritativo de `ejemplo.com`, que sí tiene el registro A y responde con la IP final, por ejemplo 192.0.2.50.

El servidor recursivo le entrega esa respuesta a tu equipo y, muy importante, la guarda en su cache durante el tiempo indicado por el TTL (Time To Live) del registro. La próxima vez que alguien pregunte lo mismo, responderá desde la cache sin repetir todo el viaje. Tu equipo también guarda la respuesta en su cache local por el mismo TTL.

La diferencia clave quedó clara: tu equipo hizo una consulta recursiva (exigió la respuesta completa) y el servidor recursivo hizo consultas iterativas (fue escalando la jerarquía por referencias). La cache en cada nivel es lo que hace que DNS sea rápido en la práctica: la primera consulta de un nombre popular puede tardar decenas de milisegundos por el recorrido completo, pero las siguientes se responden en uno o dos milisegundos desde la cache.

El TTL merece atención especial porque es una de las fuentes más comunes de confusión. Si cambias la IP de tu página web pero el registro anterior tenía un TTL de 24 horas, muchos usuarios seguirán llegando a la IP vieja hasta por un día completo, porque los servidores recursivos del mundo tienen la respuesta vieja en cache. Por eso, antes de una migración planeada, los administradores bajan el TTL a unos minutos con anticipación, hacen el cambio, y luego lo vuelven a subir. Es un truco profesional que te ahorra llamadas de "la página no se ve".

11. DNS públicos y los comandos nslookup y dig

Por defecto tus dispositivos usan los servidores DNS de tu proveedor de Internet, que reciben automáticamente por DHCP. Pero nada te obliga a usarlos: puedes configurar manualmente servidores DNS públicos, operados por empresas que los ofrecen gratis. Los más conocidos son los de Google (8.8.8.8 y 8.8.4.4) y los de Cloudflare (1.1.1.1 y 1.0.0.1), este último famoso por su enfoque en privacidad y velocidad. Cambiar tus DNS puede ayudarte si los de tu proveedor son lentos, si censuran o redirigen páginas, o si están caídos.

Para interrogar al DNS como profesional tienes dos herramientas clásicas. En Windows el caballito de batalla es nslookup, y en Linux y macOS el estándar es dig (aunque nslookup también existe ahí). Con ellas puedes preguntar que IP tiene un dominio, que registros MX tiene, qué servidor DNS estás usando y hasta seguir el recorrido completo de una resolución. En la sección de ejemplos los usarás paso a paso.

Errores comunes de principiantes con DNS

El error número uno es confundir "no resuelve el nombre" con "no hay Internet". Si puedes hacer ping a 8.8.8.8 pero no abrir google.com, tu conexión está bien y tu problema es DNS: quizás los servidores DNS configurados no responden o están mal escritos. Esa distinción te ahorra reiniciar el router cuando no hace falta.

El segundo error es olvidar el TTL después de cambiar un registro. Cambias la IP de tu servidor, pruebas al minuto y "no funciona", entras en pánico y empiezas a tocar cosas, cuando lo único que pasaba es que la cache todavía servía la respuesta vieja. Paciencia y TTL bajos antes de migraciones.

El tercer error es crear un CNAME en la raíz del dominio o ponerle registros extra a un nombre que ya tiene CNAME. El DNS lo prohíbe y la configuración falla de formas confusas. Recuerda: CNAME vive solo, sin compañeros en el mismo nombre.

El cuarto error es no configurar registros MX (o configurarlos mal) y luego sorprenderse de qué el correo del dominio no llega o se va a spam. El correo depende totalmente de DNS: MX para entrega, SPF en TXT para autorización.

12. NAT: por qué existe y que problema resuelve

NAT son las siglas de Network Address Translation, traducción de direcciones de red. Nació por una razón muy concreta: las direcciones IPv4 se acabaron. IPv4 usa 32 bits, lo que da unos 4,300 millones de direcciones posibles. Suena mucho hasta que cuentas los miles de millones de teléfonos, computadoras, tabletas, televisores, focos inteligentes, relojes y cámaras del planeta. La demanda superó a la oferta hace años, y sin embargo Internet siguió creciendo. Como. Gracias en gran parte a NAT.

La idea de NAT es brillante por lo simple: permite que toda una red privada salga a Internet usando una o unas pocas direcciones IP públicas. Tu casa es el ejemplo perfecto. Tienes una sola dirección IP pública asignada por tu proveedor, pero adentro tienes el teléfono, la laptop, la tableta, la tele y quien sabe que más, cada uno con su IP privada (192.168.1.10, 192.168.1.11, etc.). Cuando cualquiera de ellos quiere hablar con Internet, el router traduce su dirección privada a la pública al salir, y cuando la respuesta regresa, la traduce de vuelta a la privada correspondiente. Desde afuera, todo el tráfico de tu casa parece venir de una sola dirección.

Para hablar de NAT con precisión se usan cuatro términos que describen las direcciones según desde dónde las mires. La dirección IP privada de tu dispositivo dentro de tu red se llama inside local (interna local). Cuando el router la traduce a la IP pública para salir, esa versión pública se llama inside global (interna global). Del otro lado, la IP real del servidor en Internet es outside global (externa global), y si hubiera alguna traducción del lado externo sería outside local. No te asustes con los nombres: en el 99 por ciento de los casos solo te importan las dos primeras, la privada de adentro y la pública con la que sales.

Un efecto lateral importante de NAT es que funciona como una barrera natural contra conexiones entrantes no solicitadas. Como las IPs privadas no son visibles ni alcanzables desde Internet directamente, nadie de afuera puede iniciar una conexión hacia tu laptop a menos que tu router tenga una regla explícita que lo permita. Ojo: esto no es un firewall de verdad ni sustituye uno, pero explica por qué los ataques directos a equipos caseros son menos comunes de lo que serían sin NAT.

13. NAT estático, NAT dinámico y PAT: los tres sabores

Existen tres formas principales de hacer NAT, de la más rígida a la más flexible.

NAT estático es un mapeo uno a uno y permanente entre una IP privada y una IP pública. Por ejemplo: la 192.168.1.10 interna siempre se traduce a la 203.0.113.10 pública, y viceversa. Se usa cuando un equipo interno debe ser alcanzable desde Internet siempre en la misma dirección pública, como un servidor web o un servidor de correo de una empresa. Su desventaja es obvia: consume una IP pública por cada equipo, así que no escala y no resuelve el problema de la escasez.

NAT dinámico usa un pool o conjunto de direcciones públicas que se asignan bajo demanda. Cuando un equipo interno quiere salir, el router le presta una IP pública libre del pool; cuando termina, la devuelve. Si tienes 10 IPs públicas y 50 equipos internos, funciona mientras no haya más de 10 equipos activos al mismo tiempo. El mapeo es uno a uno pero temporal. Mejora el aprovechamiento, pero sigue limitado por la cantidad de IPs públicas del pool.

PAT, Port Address Translation, también llamado NAT con sobrecarga (overload), es el que usa tu casa y la mayoría de las redes del mundo. Permite que cientos o miles de equipos privados compartan una sola IP pública. El truco está en los puertos: cuando dos equipos internos salen al mismo tiempo, el router les asigna números de puerto de origen distintos en la traducción, y usa la combinación de IP pública más puerto para distinguir a quién pertenece cada respuesta que regresa.

Mira un ejemplo concreto. Tu laptop (192.168.1.10) abre una página web. El router traduce el origen a su IP pública 203.0.113.5 con puerto 50001. Al mismo tiempo tu teléfono (192.168.1.11) abre otra página y el router lo traduce a 203.0.113.5 con puerto 50002. Para el servidor web, ambas conexiones vienen de 203.0.113.5, solo que de puertos distintos, y responde a cada puerto por separado. Cuando las respuestas llegan, el router consulta su tabla NAT, ve que el puerto 50001 corresponde a la laptop y el 50002 al teléfono, y entrega cada paquete a su dueño. Como hay más de 65,000 puertos disponibles por IP, una sola dirección pública puede manejar miles de conexiones simultáneas sin despeinarse.

14. IP pública contra IP privada, y el reenvío de puertos

Ya hablamos de rangos privados en unidades anteriores, pero vale repasarlos aquí porque son el corazón de NAT: 10.0.0.0/8, 172.16.0.0/12 y 192.168.0.0/16 son rangos reservados para uso interno, no se enrutan en Internet y puedes usarlos libremente en tus redes. Tu router casero casi seguro usa 192.168.1.0/24 o 192.168.0.0/24. La IP pública, en cambio, es única en todo Internet y te la asigna tu proveedor; es la que ven los servidores cuando los visitas.

Puedes ver tu IP pública buscando "cuál es mi IP" en el navegador, y ver tu IP privada con ipconfig en Windows o con ip addr en Linux. Haz la prueba: verás que son completamente distintas, y eso es NAT trabajando frente a tus ojos.

Hay un caso especial que rompe la protección natural de NAT: cuando quieres que alguien de Internet inicie una conexión hacia un equipo de tu red, por ejemplo para entrar a tu computadora desde la oficina, para que tus amigos se conecten a tu servidor de videojuegos, o para ver tus cámaras de seguridad desde el teléfono. Como las IPs privadas no son alcanzables desde afuera, necesitas configurar reenvío de puertos o port forwarding en el router: una regla que dice "todo lo que llegue a mí IP pública por el puerto X, mandalo a la IP privada Y por el puerto Z".

Ejemplo típico: quieres un servidor de Minecraft para jugar con amigos. Tu PC tiene la 192.168.1.20 y el juego usa el puerto 25565. En el router creas la regla: puerto externo 25565 hacia 192.168.1.20 puerto 25565. Ahora tus amigos se conectan a tu IP pública en ese puerto y el router los redirige a tu PC. Por eso este equipo es candidato perfecto para una reserva DHCP: si su IP privada cambiará, la regla de reenvío apuntaría al vacío y el servidor dejaría de ser alcanzable.

Advertencia de seguridad importante: cada regla de port forwarding es una puerta que abres hacia tu red interna. Abre solo los puertos necesarios, solo hacia los equipos necesarios, y asegurate de que el servicio expuesto este actualizado y protegido con contraseña. Un reenvío mal planeado convierte la barrera natural de NAT en una entrada de servicio para atacantes.

Errores comunes de principiantes con NAT

El primero es creer que NAT es un firewall. NAT oculta tus IPs privadas y bloquea conexiones entrantes no solicitadas, pero no inspecciona tráfico ni bloquea salidas maliciosas. Un virus en tu PC puede salir a Internet sin problema a través de NAT. Usa un firewall real además de NAT.

El segundo es configurar port forwarding hacia una IP que cambia por DHCP. La regla deja de funcionar misteriosamente cada cierto tiempo. Solución: reserva DHCP para ese equipo o IP estática fuera del rango DHCP.

El tercero es el doble NAT: conectar un segundo router detrás del primero sin ponerlo en modo puente o AP. Ahora tienes dos traducciones encadenadas, lo que rompe juegos en línea, videollamadas y VPNs de formas difíciles de diagnosticar. Si necesitas más cobertura Wi-Fi, configura el segundo equipo como punto de acceso, no como router.

El cuarto es asumir que tu IP pública es fija. La mayoría de los proveedores residenciales asignan la IP pública por DHCP y puede cambiar. Si montas un servidor casero y dejas de ser alcanzable de un día para otro, probablemente tu IP pública cambio. Para esos casos existen los servicios de DNS dinámico, que actualizan un nombre de dominio automaticamente cada vez que tu IP cambia.

Ejemplos paso a paso

Ejemplo 1: ver tu configuración DHCP en Windows

Abre una terminal (cmd) y ejecuta:

```
C:\> ipconfig /all
```

Entre la salida busca tu adaptador Wi-Fi o Ethernet. Verás algo así:

Adaptador de LAN inalámbrica Wi-Fi:

```
Sufijo DNS específico para la conexión. . . :  
Dirección IPv4. . . . . : 192.168.1.25  
Máscara de subred . . . . . : 255.255.255.0  
Puerta de enlace predeterminada . . . . . : 192.168.1.1  
Servidor DHCP . . . . . : 192.168.1.1  
Servidores DNS. . . . . : 192.168.1.1  
Concesión obtenida. . . . . : sábado, 19 de septiembre de 2026  
08:12:33  
La concesión expira . . . . . : domingo, 20 de septiembre de 2026  
08:12:33
```

Línea por línea: la dirección IPv4 es la que te prestó el servidor; la máscara y la puerta de enlace definen tu red y tu salida; el campo "Servidor DHCP" te dice quién te dio todo esto (aquí es el propio router, 192.168.1.1); y las fechas de concesión muestran el lease en acción: la obtuviste hoy y expira en 24 horas, así que tu equipo intentará renovarla automáticamente al cumplirse 12 horas. Si en vez de 192.168.1.25 vieras una dirección 169.254.x.x, ya sabes el diagnóstico: APIPA, DHCP no respondió.

Para forzar un ciclo DORÁ nuevo manualmente:

```
C:\> ipconfig /release  
C:\> ipconfig /renew
```

El primer comando envía un DHCP Release y suelta tu dirección; el segundo inicia un Discover desde cero. Es la primera cosa que intentas cuando sospechas un problema de DHCP.

Ejemplo 2: renovar DHCP en Linux

En una terminal de Linux:

```
$ sudo dhclient -r
$ sudo dhclient
```

La opción `-r` liberará la concesión actual (equivalente al `release`) y el segundo comando solícita una nueva (equivalente al `renew`). Para ver lo que obtuviste:

```
$ ip addr show
$ cat /etc/resolv.conf
```

El primer comando muestra tu IP y máscara; el segundo muestra los servidores DNS que DHCP te configuró. Si `resolv.conf` está vacío o tiene direcciones extrañas, tu navegación fallará aunque la IP este bien: otro síntoma típico de DHCP a medias.

Ejemplo 3: configurar un servidor DHCP en un router Cisco

En equipos Cisco de práctica (o en el simulador Packet Tracer) se configura así:

```
Router> enable
Router# configure terminal
Router(config)# ip dhcp pool RED-CASA
Router(dhcp-config)# network 192.168.1.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.1.1
Router(dhcp-config)# dns-server 8.8.8.8 1.1.1.1
Router(dhcp-config)# lease 1
Router(dhcp-config)# exit
Router(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.30
```

Explicación: se crea un pool llamado RED-CASA con la red 192.168.1.0/24; `default-router` entrega la puerta de enlace; `dns-server` entrega dos servidores DNS públicos; `lease 1` fija la concesión en 1 día; y la última línea excluye de la repartición las primeras 30 direcciones, reservadas para equipos con IP fija manual o reservas (incluido el propio router en la .1). Para crear una reserva para la impresora con MAC `aaaa.bbbb.cccc`:

```
Router(config)# ip dhcp pool IMPRESORA
Router(dhcp-config)# host 192.168.1.50 255.255.255.0
Router(dhcp-config)# client-identifier 01aa.aabb.bbcc.cc
Router(dhcp-config)# default-router 192.168.1.1
```

Así la impresora siempre recibirá la 192.168.1.50 por DHCP, sin importar cuantas veces se reinicie.

Ejemplo 4: consultar DNS con nslookup

```
C:\> nslookup google.com
Servidor:  router-casa
Address:  192.168.1.1

Respuesta no autoritativa:
Nombre:  google.com
Addresses:  142.250.0.1
           142.250.0.2
```

La primera parte te dice a quién le preguntaste (tu router, que reenvía la consulta). "Respuesta no autoritativa" significa que la respuesta vino de la cache de tu servidor recursivo, no del servidor autoritativo de google.com: es normal y es la prueba de la cache en acción. Para ver los servidores de correo de un dominio:

```
C:\> nslookup -type=mx lucasegaacademy.com
lucasegaacademy.com      MX preference = 10, mail exchanger = mail1.proveedor.com
lucasegaacademy.com      MX preference = 20, mail exchanger = mail2.proveedor.com
```

Ves los dos registros MX con sus prioridades: él 10 es el preferido y el 20 el respaldo. Y para preguntarle directamente a otro servidor DNS, por ejemplo el de Google:

```
C:\> nslookup google.com 8.8.8.8
```

Así comparas respuestas: si tu DNS habitual falla pero 8.8.8.8 responde, el problema está en tu servidor DNS configurado, no en tu conexión.

Ejemplo 5: consultar DNS con dig en Linux

```
$ dig lucasegaacademy.com +short
192.0.2.10
```

La opción +short te da solo la respuesta, ideal para scripts. Sin ella obtienes el detalle completo:

```
$ dig lucasegaacademy.com

;; QUESTION SECTION:
;lucasegaacademy.com.      IN      A

;; ANSWER SECTION:
lucasegaacademy.com.      3600    IN      A      192.0.2.10

;; Query time: 24 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
```

Lee la sección ANSWER: el nombre, el TTL (3600 segundos, o sea una hora de cache), la clase IN y el tipo A con la IP. Al final ves cuanto tardó y a que servidor le preguntaste. Para ver el recorrido completo por la jerarquía, la opción mágica es +trace:

```
$ dig +trace www.ejemplo.com
```

Verás las consultas iterativas una por una: primero a un servidor raíz, luego al TLD .com, luego al autoritativo, exactamente el proceso que describimos en la teoría. Y para otros tipos de registro:

```
$ dig lucasegaacademy.com MX +short
10 mail1.proveedor.com.
20 mail2.proveedor.com.
$ dig lucasegaacademy.com TXT +short
"v=spf1 include:proveedor.com -all"
```

El TXT muestra un registro SPF que autoriza a los servidores del proveedor a enviar correo del dominio: seguridad de correo construida sobre DNS.

Ejemplo 6: configurar PAT en un router Cisco

La configuración típica de una pequeña empresa con una sola IP pública:

```
Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255
Router(config)# ip nat inside source list 1 interface GigabitEthernet0/1 overload
Router(config)# interface GigabitEthernet0/0
Router(config-if)# ip nat inside
Router(config-if)# interface GigabitEthernet0/1
Router(config-if)# ip nat outside
```

Explicación línea por línea: la lista de acceso 1 define que tráfico se traducirá (toda la red 192.168.1.0/24); el comando ip nat crea la regla: traduce el origen de ese tráfico usando la IP de la interfaz de salida (la pública) con overload, que es la palabra mágica que activa PAT; y las dos interfaces se marcan como inside (la de la red local) y outside (la que da a Internet). Con esto, cientos de equipos internos comparten la única IP pública.

Para ver la tabla NAT en acción:

```
Router# show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
tcp 203.0.113.5:50001  192.168.1.10:49152 142.250.0.1:443    142.250.0.1:443
tcp 203.0.113.5:50002  192.168.1.11:49153 142.250.0.1:443    142.250.0.1:443
```

Esta tabla es PAT en estado puro: dos equipos internos distintos (192.168.1.10 y 192.168.1.11) salen con la misma IP pública 203.0.113.5, diferenciados solo por el puerto traducido (50001 y 50002). Ambos hablan con el mismo servidor web en el puerto 443, y el router sabrá devolver cada respuesta a su dueño gracias a esa tabla.

Ejemplo 7: NAT estático y reenvío de puertos

Para un servidor web interno que debe ser visible siempre con la misma IP pública:

```
Router(config)# ip nat inside source static 192.168.1.10 203.0.113.10
```

Mapeo uno a uno permanente: todo lo que salga de 192.168.1.10 se verá como 203.0.113.10, y todo lo que llegue a 203.0.113.10 ira a 192.168.1.10. Y el reenvío de un solo puerto para el servidor de juegos del ejemplo anterior:

```
Router(config)# ip nat inside source static tcp 192.168.1.20 25565 203.0.113.5 25565
```

Lee la regla así: el tráfico TCP que llegue a la IP pública 203.0.113.5 por el puerto 25565 se reenvia a 192.168.1.20 puerto 25565. Tus amigos se conectan a tu IP pública y terminan en tu PC, sin exponer ningún otro puerto ni ningún otro equipo. Recuerda combinar esto con una reserva DHCP para la 192.168.1.20, o la regla se romperá en silencio cuando la IP cambie.

Práctica

1. Ordeña los cuatro mensajes del proceso DORÁ y explica con tus palabras que contiene cada uno. Además responde: qué pasaría si el cliente envía el Discover pero ningún servidor responde, y qué pasaría si hay dos servidores DHCP activos en la misma red.

SOLUCIÓN:

El orden correcto es: 1) Discover, 2) Offer, 3) Request, 4) Acknowledge. El Discover lo envía el cliente por broadcast desde 0.0.0.0 porque aún no tiene IP, y básicamente dice "necesito una dirección, hay algún servidor DHCP". El Offer es la respuesta del servidor con una IP propuesta, la máscara, el tiempo de concesión y su propia dirección. El Request lo envía el cliente también por broadcast para aceptar la oferta elegida y avisar a los demás servidores que liberen sus ofertas. El Acknowledge es la confirmación final del servidor con todos los parámetros completos: IP, máscara, puerta de enlace, DNS y lease. Si ningún servidor responde al Discover, el cliente reintenta varias veces y al final se autoasigna una dirección APIPA del rango 169.254.0.1 a 169.254.255.254, con la que solo podrá hablar con otros equipos APIPA de su red local, sin salida a Internet. Si hay dos servidores DHCP activos sin coordinación, el cliente recibirá dos ofertas y tomará la primera que llegue, pero ambos servidores reparten del mismo rango sin saber lo que hace el otro, así que tarde o temprano asignarán la misma IP a dos equipos distintos y aparecerán conflictos de dirección duplicada con conectividad intermitente.

2. Enciendes tu computadora, abres la terminal y ves que tu dirección IP es 169.254.87.12 con máscara 255.255.0.0. No puedes abrir ninguna página web. Diagnóstica el problema y propone un plan de solución en orden, del paso más simple al más avanzado.

SOLUCIÓN:

El diagnóstico es claro: tienes una dirección APIPA, lo que significa que tu equipo intento obtener configuración por DHCP y ningún servidor respondió. No es que "no tengas IP", es que la IP que tienes es la prueba de que DHCP fallo, y por eso no tienes puerta de enlace ni DNS validos y no puedes navegar. El plan en orden es: paso 1, revisa lo físico, que el cable este bien conectado o que el Wi-Fi este asociado a tu red correcta y con buena señal; paso 2, reinicia el router casero y espera dos minutos a que levante su servicio DHCP; paso 3, en tu equipo liberá y renueva la concesión con `ipconfig /release` e `ipconfig /renew` en Windows o con `dhclient -r` y `dhclient` en Linux, para forzar un DORÁ nuevo; paso 4, revisa en la página del router si su servidor DHCP sigue activado y si le quedan direcciones libres en el pool; paso 5, descarta un segundo servidor DHCP peleando en la red o un switch intermedio con problemas; paso 6, prueba con otro dispositivo: si otro equipo si obtiene IP, el problema está en tu computadora (controlador de red o configuración) y no en la red. Solo como último recurso

temporal podrías poner una IP estática manual dentro del rango de tu red, pero eso es un parche, no la solución.

- Una oficina tiene una impresora de red, dos cámaras de seguridad y un servidor de archivos que deben tener siempre la misma dirección IP. El administrador duda entre configurarles IP estática a mano o usar reservas DHCP. Que le recomiendas y por qué. Además escribe como quedaría la reserva de la impresora (MAC aaaa.bbbb.cccc) para que siempre obtenga 192.168.1.50.

SOLUCIÓN:

Le recomiendo las reservas DHCP. El resultado para los equipos es el mismo (siempre la misma IP), pero la administración es centralizada: todos los parámetros viven en el servidor DHCP, así que si algún día cambian la puerta de enlace, los DNS o el rango de la red, basta actualizar el servidor y los equipos reciben lo nuevo en su próxima renovación, sin ir equipo por equipo. Con IP estática manual cada cambio futuro es trabajo físico en cada aparato, y además hay que acordarse de excluir esas direcciones del pool DHCP para evitar duplicados. La reserva en un router Cisco quedaría así:

```
Router(config)# ip dhcp pool IMPRESORA
Router(dhcp-config)# host 192.168.1.50 255.255.255.0
Router(dhcp-config)# client-identifier 01aa.aabb.bbcc.cc
Router(dhcp-config)# default-router 192.168.1.1
```

La impresora sigue pidiendo su configuración por DHCP con el proceso DORÁ normal, pero el servidor, al reconocer su MAC, siempre le entrega la 192.168.1.50. Lo mismo se repetiría para cada cámara y para el servidor de archivos, cada uno con su pool de reserva y su dirección fija.

- Describe paso a paso que ocurre cuando escribes www.tienda-ejemplo.com en tu navegador por primera vez en el día, indicando en cada paso quien pregunta, a quién le pregunta, y si la consulta es recursiva o iterativa. Incluye el papel de la cache y del TTL.

SOLUCIÓN:

Paso 1: tu equipo revisa su cache DNS local; cómo es la primera vez del día, no hay nada guardado. Paso 2: tu equipo hace una consulta recursiva a su servidor DNS configurado (el de tu proveedor o uno público como 8.8.8.8), exigiéndole la respuesta completa. Paso 3: el servidor recursivo revisa su cache; supongamos que tampoco la tiene. Paso 4: el recursivo hace una consulta iterativa a un servidor raíz preguntando por www.tienda-ejemplo.com; el raíz no sabe la IP pero le responde con los servidores del TLD .com. Paso 5: el recursivo pregunta iterativamente a un servidor del TLD .com, que le responde con los servidores NS

autoritativos de tienda-ejemplo.com. Paso 6: el recursivo pregunta al servidor autoritativo, que sí tiene el registro A y devuelve la IP final. Paso 7: el recursivo guarda esa respuesta en su cache durante el TTL indicado (por ejemplo 3600 segundos) y se la entrega a tu equipo, que también la guarda en su cache local. A partir de ahí, durante la vigencia del TTL, cualquier repetición de la consulta se responde desde la cache en uno o dos milisegundos sin repetir el viaje por la jerarquía. La lección práctica: tu equipo solo hizo una consulta recursiva, y fue el servidor recursivo quien hizo el trabajo iterativo de escalar la jerarquía por referencias.

5. Con las herramientas nslookup o dig averigua lo siguiente de un dominio real (usa el que quieras, por ejemplo wikipedia.org): su dirección IPv4, sus registros MX y un registro TXT. Interpreta cada resultado: que significa cada dato para el funcionamiento del dominio.

SOLUCIÓN:

Primero la IPv4 con ``nslookup wikipedia.org`` o ``dig wikipedia.org +short``: obtendrás una o varias direcciones, por ejemplo 208.80.154.224. Ese es el registro A, la dirección a dónde tu navegador se conecta cuando escribes el dominio; si hay varias, el servidor las rota para repartir la carga. Después los MX con ``nslookup -type=mx wikipedia.org`` o ``dig wikipedia.org MX +short``: verás líneas con números de prioridad y nombres de servidores de correo. Esos registros le dicen al mundo a dónde entregar el correo dirigido a ese dominio, intentando primero el de prioridad más baja y usando los demás como respaldo; sin ellos el dominio no podría recibir correo. Finalmente el TXT con ``dig wikipedia.org TXT +short``: verás cadenas de texto que suelen ser registros SPF o verificaciones de propiedad. Un SPF como "v=spf1 ..." declara que servidores están autorizados a enviar correo en nombre del dominio, y los servidores de correo del mundo lo consultan para decidir si un mensaje es legítimo o spam. En conjunto, el ejercicio demuestra que un dominio no es "una IP", sino un conjunto de registros de distintos tipos que sostienen la web, el correo y la seguridad del dominio.

6. Tu casa sale a Internet con una sola IP pública, 203.0.113.5. Tu laptop tiene la IP privada 192.168.1.10 y tu teléfono la 192.168.1.11. Ambos abren al mismo tiempo una página alojada en 142.250.0.1 por el puerto 443. Explica cómo el router distingue las dos conexiones usando PAT y dibuja como quedaría la tabla NAT. Después configura el reenvío de puertos para que tus amigos puedan entrar a tu servidor de juegos en tu PC (192.168.1.20, puerto TCP 25565) y explica que precaución de DHCP debes tomar para que no deje de funcionar.

SOLUCIÓN:

El router usa PAT: traduce la IP privada de origen a su única IP pública, pero asigna a cada conexión un puerto de origen distinto, de modo que la combinación IP pública más puerto identifica de forma única a cada sesión. La laptop sale como 203.0.113.5 con puerto 50001 y

el teléfono como 203.0.113.5 con puerto 50002. El servidor web ve dos conexiones del mismo origen aparente pero de puertos distintos y responde a cada puerto por separado. La tabla NAT quedaría así:

Pro	Inside global	Inside local	Outside local	Outside global
tcp	203.0.113.5:50001	192.168.1.10:49152	142.250.0.1:443	142.250.0.1:443
tcp	203.0.113.5:50002	192.168.1.11:49153	142.250.0.1:443	142.250.0.1:443

Cuándo llega una respuesta al puerto 50001, el router busca en la tabla, ve que pertenece a 192.168.1.10 y se la entrega a la laptop; lo mismo con el 50002 hacia el teléfono. El reenvío de puertos en el router se configura así:

```
Router(config)# ip nat inside source static tcp 192.168.1.20 25565 203.0.113.5 25565
```

Con esa regla, todo lo que llegue de Internet a tu IP pública por el puerto TCP 25565 se redirige a tu PC en él mismo puerto, y tus amigos se conectan a tu IP pública para entrar al juego. La precaución de DHCP: la regla apunta a la IP privada 192.168.1.20, así que debes crear una reserva DHCP para la MAC de tu PC que siempre le entregue la 192.168.1.20; si la dejarás con DHCP dinámico normal, algún día obtendría otra IP y el reenvío apuntaría al vacío sin que nadie tocará la configuración del router.

Resumen de la unidad

En esta unidad conociste a los tres servicios invisibles que sostienen tu experiencia diaria en Internet. DHCP reparte automáticamente las direcciones IP y todos los parámetros de red mediante el proceso DORÁ de cuatro mensajes: Discover, Offer, Request y Acknowledge, usando los puertos UDP 67 y 68. Las direcciones se prestan por un tiempo llamado concesión o lease, que se renueva al 50 por ciento del tiempo y se reasocia al 87.5 por ciento si el servidor original no responde. Las reservas DHCP te dan direcciones predecibles con administración centralizada, ideales para impresoras, cámaras y servidores, mientras que los rangos de exclusión protegen las IPs fijas manuales. El servidor DHCP vive dentro de tu router casero, y cuando no hay ninguno disponible tu equipo se autoasigna una dirección APIPA del rango 169.254.0.1 a 169.254.255.254: el síntoma inconfundible de que DHCP fallo.

DNS traduce los nombres que escribes a las direcciones IP que las máquinas entienden, funcionando como el directorio telefónico de Internet sobre el puerto 53. Su jerarquía va de los servidores raíz a los TLD, de ahí a los dominios registrados y finalmente a los subdominios, delegando autoridad en cada nivel. Aprendiste los registros esenciales: A y AAAA para

direcciones IPv4 e IPv6, CNAME para aliás, MX con prioridades para el correo, TXT para verificaciones y seguridad, y NS para la delegación. La resolución combina una consulta recursiva de tu equipo con consultas iterativas del servidor recursivo por la jerarquía, y la cache con su TTL en cada nivel es lo que la hace rápida. También conociste los DNS públicos como 8.8.8.8 y 1.1.1.1, y las herramientas nslookup y dig para interrogar al sistema.

NAT resuelve la escasez de IPv4 permitiendo que redes enteras compartan pocas direcciones públicas: traduce la IP privada de origen a una pública al salir y revierte la traducción al regresar. Viste sus tres formas: estático uno a uno permanente, dinámico con pool temporal, y PAT con sobrecarga, que distingue miles de conexiones simultaneas usando puertos de origen distintos sobre una sola IP pública. Repasaste los rangos privados, la diferencia entre IP pública y privada, y el reenvío de puertos para exponer servicios internos, con su precaución de seguridad y su necesidad de reservas DHCP.

Con DHCP, DNS y NAT dominados, ya puedes explicar el viaje completo de un paquete desde qué enciendes tu equipo hasta que se carga tú página favorita. En la Unidad 8 darás el siguiente salto: IPv6, el protocolo que multiplica las direcciones disponibles, y las redes inalámbricas Wi-Fi con su seguridad. Nos vemos ahí.

UNIDAD 8: IPv6 y redes inalámbricas

Bienvenido a la Unidad 8 del Curso Completo de Redes de Lucas EGA Academy. Si la Unidad 7 te presentó a los trabajadores invisibles que hacen funcionar Internet hoy, esta unidad te lleva al presente más avanzado y al futuro de las redes: IPv6, el protocolo con direcciones casi infinitas, y las redes inalámbricas Wi-Fi, la forma en qué la mayoría de las personas se conecta a Internet en su vida diaria, junto con la seguridad que protege esas conexiones que viajan por el aire.

Empieza con una pregunta incómoda: las direcciones IPv4 se acabaron. No es una predicción, es un hecho que ya ocurrió. IPv4 ofrece unos 4,300 millones de direcciones, y el planeta tiene muchos más dispositivos conectados que eso: teléfonos, computadoras, tabletas, televisiones, relojes inteligentes, focos, bocinas, cámaras, automóviles y sensores industriales. En la Unidad 7 viste como NAT nos permitió estirar IPv4 compartiendo direcciones públicas, y fue un truco brillante, pero es un parche, no una solución definitiva. La solución real se llama IPv6, y multiplica el espacio de direcciones de una forma tan brutal que cuesta trabajo imaginarla: en vez de 32 bits usa 128 bits, lo que da un número de direcciones tan grande que cada grano de arena de la Tierra podría tener miles de direcciones propias y aún sobrarían. En esta unidad vas a aprender a leer, escribir, comprimir e identificar direcciones IPv6 como un profesional.

La segunda mitad de la unidad es igual de práctica: el Wi-Fi. Piensa en tu día: despiertas y tu teléfono ya está conectado, desayunas viendo videos sin cables, trabajas con la laptop en el sillón, y todo funciona por arte de magia invisible. Esa magia tiene nombre y apellido: los estándares 802.11, las bandas de 2.4, 5 y 6 GHz, los canales, el SSID de tu red y los puntos de acceso. Vas a entender por qué tu Internet se pone lento cuando el vecino enciende su microondas, por qué la red de 5 GHz es más rápida pero no llega al fondo de la casa, y que significan esas etiquetas de Wi-Fi 4, Wi-Fi 5 y Wi-Fi 6 que ves en las cajas de los equipos.

Y hay un tema que no puede faltar: la seguridad inalámbrica. Tu red Wi-Fi no viaja por un cable dentro de tu pared, viaja por el aire en todas direcciones, y cualquiera con una laptop en la banqueta de enfrente puede intentar escucharla. Por eso existen WEP, WPA, WPA2 y WPA3, y por eso importa enormemente cuál usa tu router. Vas a aprender por qué WEP está muerto y no debe usarse jamás, que cambió cada generación de WPA, y las buenas prácticas que separan una red casera segura de una invitación abierta a los intrusos: contraseñas fuertes, cambio de credenciales del router, desactivación de WPS y red de invitados.

En esta unidad cubres las clases 22, 23 y 24. En la clase 22 dominarás IPv6: por qué se creó, su formato de 128 bits, la notación hexadecimal con dos puntos, la compresión de ceros con el doble dos puntos, los tipos de dirección (unicast global, link-local que empieza con fe80,

multicast, y la ausencia total de broadcast), y cómo conviven IPv4 e IPv6 mediante dual-stack y túneles. En la clase 23 te sumergirás en Wi-Fi: los estándares 802.11 a/b/g/n/ac/ax y sus nombres comerciales Wi-Fi 4/5/6, las bandas de 2.4 GHz contra 5 GHz contra 6 GHz, los canales y su interferencia, que es el SSID, los modos infraestructura y ad-hoc, y los componentes de una red inalámbrica (punto de acceso, controlador y cliente). En la clase 24 conquistarás la seguridad Wi-Fi: la historia de WEP y por qué ya no se usa, WPA, WPA2 y WPA3, los cifrados TKIP y AES, y las buenas prácticas de protección.

Al terminar serás capaz de leer una dirección IPv6 sin miedo, de diagnosticar problemas de Wi-Fi con criterio técnico en vez de a prueba y error, y de blindar una red inalámbrica como lo haría un profesional. Vamos a ello.

Explicación detallada

1. IPv6: el protocolo que nació porque IPv4 se quedó corto

Para entender IPv6 primero hay que entender la magnitud del problema que resuelve. IPv4 usa direcciones de 32 bits, lo que da 2 elevado a 32 combinaciones: unos 4,300 millones de direcciones. En los años ochenta parecía una cifra inagotable; en aquel entonces Internet era un proyecto académico y militar con unas cuantas miles de máquinas. Nadie imaginó un mundo donde cada persona llevaría varios dispositivos conectados en el bolsillo, donde los focos y los refrigeradores tendrían dirección IP, y donde países enteros se conectarían de golpe.

El agotamiento llegó por etapas y fue noticia real en la industria: primero se acabó el bloque central administrado a nivel mundial, después cada región del planeta fue agotando sus reservas una por una. La respuesta inmediata fue NAT, que ya dominas: compartir direcciones públicas entre muchos dispositivos privados. NAT nos compró décadas de tiempo extra, pero tiene costos: rompe el principio de conectividad de extremo a extremo, complica los juegos en línea, las videollamadas y las VPNs, y obliga a trucos como el port forwarding para servicios entrantes. Era evidente que se necesitaba una solución de fondo, no otro parche.

IPv6 es esa solución. En vez de 32 bits usa 128 bits, es decir, 2 elevado a 128 direcciones posibles. Ese número es tan grande que las analogías se quedan cortas, pero intenta esta: es aproximadamente 340 seguido de 36 ceros. Con esa cantidad, cada persona del planeta podría tener miles de millones de direcciones propias, cada dispositivo podría tener su IP pública única sin necesidad de NAT, y aún así el espacio estaría prácticamente vacío. IPv6 no solo resuelve la escasez: devuelve a Internet su diseño original, donde cada equipo puede hablar directamente con cualquier otro.

Otra motivación del diseño fue simplificar. La cabecera de IPv6 es más simple y eficiente que la de IPv4: se eliminaron campos poco usados, el checksum de cabecera desapareció (se confiaba en las capas inferiores), y la fragmentación ya no la hacen los routers intermedios sino solo el equipo origen. Además IPv6 trae de fábrica características que en IPv4 eran agregados: la autoconfiguración de direcciones sin servidor (SLAAC), el descubrimiento de vecinos que reemplaza a ARP, y el soporte nativo para IPsec. No es solo "IPv4 con más bits": es un protocolo rediseñado con treinta años de lecciones aprendidas.

2. El formato de 128 bits: notación hexadecimal con dos puntos

Una dirección IPv6 se escribe como ocho grupos de cuatro dígitos hexadecimales separados por dos puntos. Cada grupo representa 16 bits, y ocho grupos por 16 bits dan los 128 bits totales. Un ejemplo completo:

```
2001:0db8:0000:0000:0000:ff00:0042:8329
```

Si vienes de IPv4, lo primero que choca es el hexadecimal: en vez de solo dígitos del 0 al 9, se usan también las letras a, b, c, d, e y f (se acostumbra escribirlas en minúsculas). Cada dígito hexadecimal representa 4 bits, así que cuatro dígitos forman los 16 bits de cada grupo. No necesitas ser un calculista mental del hexadecimal para trabajar con IPv6: lo importante es reconocer la estructura de ocho grupos y saber leerlos.

Compara los tamaños para apreciar la diferencia. Una dirección IPv4 como 192.168.1.10 ocupa 32 bits y se escribe en unas 15 letras como máximo. Una IPv6 completa ocupa 128 bits y se escribe con 39 caracteres contando los dos puntos. Es más larga de escribir, sí, y por eso existen las reglas de compresión que verás en la siguiente sección: nadie escribe direcciones IPv6 completas en la vida real.

Un detalle práctico que te evitará confusiones: cuando una dirección IPv6 aparece junto a un puerto, por ejemplo en una URL o en una configuración, se encierra entre corchetes para que los dos puntos de la dirección no se confundan con el separador del puerto. Así se ve:

```
http://[2001:db8::1]:8080/pagina
```

Sin los corchetes sería imposible saber dónde termina la dirección y dónde empieza el puerto. Es una convención que verás en navegadores, servidores y documentación.

También es útil saber que los prefijos en IPv6 se escriben igual que en IPv4, con la notación de diagonal. Un /64 en IPv6 significa que los primeros 64 bits son la parte de red, igual que un /24 en IPv4. La diferencia es que en IPv6 el tamaño estándar para una subred de equipos

finales es /64: son tantos bits para hosts que cada subred tiene más direcciones que todo el IPv4 junto. Los proveedores suelen entregar a cada cliente un /56 o un /48, qué a su vez se divide en cientos o miles de subredes /64.

3. La compresión de ceros: el arte del doble dos puntos

Escribir 39 caracteres por dirección sería un suplicio diario, así que IPv6 tiene dos reglas de compresión que todo técnico debe dominar. Son sencillas, pero tienen una trampa que causa errores en exámenes, así que presta atención.

Regla 1: en cada grupo se pueden omitir los ceros a la izquierda. El grupo 0db8 se puede escribir como db8, el grupo 0042 como 42, y el grupo 0000 como 0. Aplicando solo esta regla, nuestro ejemplo queda así:

```
2001:0db8:0000:0000:0000:ff00:0042:8329
2001:db8:0:0:0:ff00:42:8329
```

Regla 2: una secuencia de uno o más grupos consecutivos que sean todos cero se puede reemplazar por un doble dos puntos ::. Aplicandola al resultado anterior:

```
2001:db8:0:0:0:ff00:42:8329
2001:db8::ff00:42:8329
```

Esa es la forma comprimida que verás en la vida real. Ahora la trampa: el :: solo puede usarse una vez en cada dirección. La razón es matemática: él :: significa "aquí faltan grupos de ceros hasta completar ocho", y si apareciera dos veces sería ambiguo cuantos ceros van en cada hueco. Por ejemplo, esta dirección es válida:

```
fe80::1
```

Qué equivale a fe80:0000:0000:0000:0000:0000:0000:0001. Pero esta es inválida:

```
2001::db8::1
```

Porque no hay forma de saber cómo repartir los ceros faltantes entre los dos huecos. Si te encuentras una dirección con dos ::, está mal escrita, punto.

Cuándo haya varias secuencias de ceros candidatas, la convención es comprimir la más larga; si empatan, la primera. Por ejemplo:

```
2001:db8:0:0:1:0:0:0
```

Se comprime como 2001:db8:0:0:1:: (la secuencia final de tres ceros es más larga que la intermedia de dos), no como 2001:db8::1:0:0:0. No es una regla que rompa nada si la ignoras, pero escribirlo bien marca la diferencia entre un aficionado y un profesional.

Práctica mental rápida: expande 2001:db8::a:b. Cuenta los grupos visibles: 2001, db8, a, b son cuatro grupos; faltan cuatro grupos de ceros que van donde está el ::, así que la forma completa es 2001:0db8:0000:0000:0000:0000:000a:000b. Con un poco de práctica lo harás sin pensar.

4. Tipos de direcciones IPv6: quién es quien en el zoológico

En IPv4 estabas acostumbrado a unas cuantas categorías: públicas, privadas, loopback y poco más. IPv6 tiene su propio repertorio y vale la pena conocerlo porque las direcciones se identifican a simple vista por su prefijo, como si llevarán uniforme.

Unicast global: son las direcciones públicas de IPv6, enrutables en todo Internet, el equivalente a las IP públicas de IPv4. Todas empiezan con los bits 2000::/3, lo que en la práctica significa que el primer dígito hexadecimal es 2 o 3. Casi todas las que verás empiezan con 2001 o 2002, como 2001:db8::1. Ojo con un detalle: el prefijo 2001:db8::/32 está reservado para documentación y ejemplos, igual que 192.0.2.0/24 en IPv4; nunca lo verás en una red real. Cuando tu proveedor te da IPv6, te entrega un bloque de direcciones unicast globales, y cada uno de tus dispositivos puede tener su propia IP pública sin NAT de por medio.

Link-local: empiezan con fe80::/10, o sea que los primeros dígitos son fe80, fe81, hasta febf, aunque en la práctica casi siempre verás fe80. Estas direcciones se autoconfiguran solas en cuanto activas IPv6 en una interfaz, sin servidor, sin router y sin configuración manual. Solo son validas dentro del enlace local, es decir, no cruzan routers: sirven para qué los vecinos de la misma red se hablen entre si. Su uso más importante es invisible para ti: los routers las usan como origen de sus anuncios y los equipos las usan para el descubrimiento de vecinos. Si ejecutas un comando para ver tus direcciones IPv6 y ves una fe80::algo, no te asustes: es normal, la tienes aunque tu proveedor no te de IPv6 global.

Unique local: usan el prefijo fc00::/7 y son el equivalente a las direcciones privadas de IPv4 (10.0.0.0/8 y compañeros). Sirven para redes internas que no necesitan salir a Internet con IPv6 o que quieren direcciones estables e independientes del proveedor. En la práctica verás casi siempre el bloque fd00::/8, porque la otra mitad del rango requiere asignación central que casi nadie tramita.

Multicast: empiezan con ff00::/8, el primer grupo es ff. Se usan para enviar un paquete a un grupo de destinatarios a la vez, y en IPv6 tienen un papel mucho más protagonista que en IPv4 porque, atención, en IPv6 no existe el broadcast. Nada de 255.255.255.255: cuándo un equipo necesita hablarle "a todos", usa una dirección multicast bien conocida. La más famosa es ff02::1, que significa "todos los nodos del enlace local", y la usa por ejemplo el descubrimiento de routers. Otra es ff02::2, "todos los routers del enlace local". Esta decisión de diseño reduce el ruido en la red: en vez de interrumpir a todos con broadcasts, los mensajes van solo a quiénes pertenecen al grupo multicast.

Loopback y no especificada: ::1 es la dirección de loopback, el equivalente al 127.0.0.1 de IPv4: apunta a tu propio equipo y sirve para pruebas. Y :: (todo ceros) es la dirección no especificada, el equivalente al 0.0.0.0: significa "no tengo dirección" o "cualquier dirección" según el contexto.

La ausencia de broadcast merece subrayarse porque es una de las diferencias conceptuales más grandes con IPv4. En IPv4, servicios como DHCP y ARP abusan del broadcast, interrumpiendo a todos los equipos del segmento. En IPv6 esos mecanismos se rediseñaron sobre multicast dirigido: solo despiertan a quiénes necesitan escuchar. El resultado son redes más silenciosas y eficientes.

5. Autoconfiguración: SLAAC, DHCPv6 y el descubrimiento de vecinos

Una de las joyas de IPv6 es que los equipos pueden configurarse solos sin ningún servidor, gracias a SLAAC (Stateless Address Autoconfiguration, autoconfiguración sin estado). El proceso es elegante: el router de la red envía periódicamente anuncios de router (Router Advertisements) diciendo "hola, esta red usa el prefijo 2001:db8:abcd::/64". Cada equipo que escucha el anuncio toma ese prefijo, le pega su propio identificador de interfaz (derivado de su MAC o generado aleatoriamente por privacidad) y listo: ya tiene su dirección unicast global completa, sin pedirle nada a nadie. Además el anuncio le dice cuál es la puerta de enlace y dónde buscar DNS.

Compañero inseparable de SLAAC es NDP, el Neighbor Discovery Protocol (protocolo de descubrimiento de vecinos), que funciona sobre ICMPv6 y reemplaza por completo a ARP. En IPv4, para saber la MAC de un vecino se hacía un broadcast ARP que interrumpía a todos. En IPv6, el equipo envía una solicitud de vecino (Neighbor Solicitation) a una dirección multicast calculada a partir de la IP buscada, así que solo los interesados potenciales la procesan. NDP también detecta direcciones duplicadas, descubre routers y mantiene la tabla de vecinos, todo sin broadcasts.

Dónde queda DHCP en este mundo. Existe DHCPv6, y se usa cuando quieres administración centralizada: repartir direcciones de forma controlada, entregar opciones extra o llevar registro de quién tiene que. Muchas redes usan una combinación: SLAAC para la dirección y DHCPv6 en modo "sin estado" solo para entregar el DNS y otros parámetros. La lección importante es que en IPv6 la autoconfiguración es la regla y el servidor DHCP es opcional, al revés que en IPv4 donde sin DHCP (o configuración manual) no hay red.

Un detalle moderno que te conviene conocer: las extensiones de privacidad. Como el identificador de interfaz derivado de la MAC sería el mismo en todas las redes y permitiría rastrear tu dispositivo, los sistemas operativos modernos generan identificadores aleatorios y además rotan direcciones temporales para las conexiones salientes. Por eso tu teléfono puede mostrar varias direcciones IPv6 a la vez: la estable para recibir y las temporales para navegar con privacidad.

6. La convivencia: dual-stack y túneles

IPv6 no reemplazo a IPv4 de la noche a la mañana, y de hecho décadas después ambos siguen conviviendo. La migración es gradual porque hay miles de millones de equipos, routers y aplicaciones que solo hablan IPv4, y no se pueden apagar de golpe. La estrategia dominante para convivir se llama dual-stack (pila doble): los equipos y routers corren IPv4 e IPv6 al mismo tiempo, con direcciones de ambos tipos, y eligen cuál usar según el destino. Si el servidor al que quieres llegar tiene IPv6, usas IPv6; si solo tiene IPv4, usas IPv4. Tu computadora actual probablemente ya es dual-stack sin que lo sepas: tiene su 192.168.1.x y además su fe80:: y quizás una global.

La segunda técnica son los túneles: encapsular paquetes IPv6 dentro de paquetes IPv4 (o al revés) para cruzar zonas de la red que solo hablan un protocolo. Imagina dos islas IPv6 separadas por un océano IPv4: el túnel mete el paquete IPv6 dentro de uno IPv4, lo cruza por el océano, y al llegar a la otra isla lo saca y lo entrega como IPv6. Fue la técnica que permitió los primeros despliegues cuando los proveedores aún no ofrecían IPv6 nativo.

En la práctica, lo que verás es una adopción desigual: muchos proveedores móviles y algunos fijos ya entregan IPv6 nativo a sus clientes, los grandes servicios de Internet (buscadores, redes sociales, redes de distribución de contenido) son accesibles por IPv6, pero infinidad de redes corporativas y pequeños proveedores siguen siendo solo IPv4. Como técnico debes sentirte cómodo en ambos mundos: saber leer una IPv6, configurar dual-stack y diagnosticar problemas en cada protocolo por separado, porque "no me funciona IPv6 pero si IPv4" es un diagnóstico perfectamente válido y común.

Errores comunes de principiantes con IPv6

El primero es usar el :: dos veces en una dirección. Recuerda: solo una vez por dirección, porque con dos el número de ceros omitidos sería ambiguo. Los validadores y los equipos rechazan esas direcciones y los mensajes de error no siempre son claros.

El segundo es confundir link-local con una dirección útil para salir a Internet. Ver una fe80:: en tu equipo no significa que tengas IPv6 global ni que puedas navegar por IPv6: significa solo que tu interfaz tiene IPv6 activado a nivel local. Para salir necesitas una unicast global (que empiece con 2 o 3) entregada por tu proveedor o autoconfigurada por SLAAC.

El tercero es olvidar los corchetes al mezclar IPv6 con puertos. Escribir `http://2001:db8::1:8080` es ambiguo e inválido; lo correcto es `http://[2001:db8::1]:8080`. Es un error tonto que hace perder tiempo en configuraciones de servidores y firewalls.

El cuarto es asumir que con IPv6 ya no hace falta el firewall "porque cada equipo tiene su IP pública". Al contrario: sin el NAT casero que antes te ocultaba, cada dispositivo con IPv6 global es directamente alcanzable desde Internet, así que el firewall del router y el de cada equipo pasan a ser tu única defensa. IPv6 sin firewall es una casa con las puertas abiertas.

7. Wi-Fi y la familia 802.11: del cable al aire

Wi-Fi es el nombre comercial de la familia de estándares IEEE 802.11, que define cómo se comunican los dispositivos por radio en redes locales inalámbricas. La historia empieza modesta: las primeras versiones ofrecían 1 o 2 Mbps, apenas para lo básico. Después llegaron las letras que todavía verás mencionadas: 802.11a (banda de 5 GHz, hasta 54 Mbps), 802.11b (banda de 2.4 GHz, hasta 11 Mbps, la que popularizó el Wi-Fi en los hogares) y 802.11g (2.4 GHz, hasta 54 Mbps, compatible con b). Cada letra era una mejora de velocidad o de banda, pero el esquema de letras se volvió confuso para el público.

Por eso la Wi-Fi Alliance, la organización que certifica los productos, renombró las generaciones recientes con números simples. La equivalencia que debes memorizar es: 802.11n es Wi-Fi 4, 802.11ac es Wi-Fi 5, 802.11ax es Wi-Fi 6 (y Wi-Fi 6E cuando usa la banda de 6 GHz), y 802.11be es Wi-Fi 7. Cuando una caja dice "Wi-Fi 6", ya sabes que habla de 802.11ax sin tener que descifrar letras.

Cada generación trajo más velocidad y mejores técnicas de radio. En números redondos y teóricos (velocidades de laboratorio, no lo que verás en tu casa): 802.11n (Wi-Fi 4) llega hasta 600 Mbps usando las bandas de 2.4 y 5 GHz; 802.11ac (Wi-Fi 5) trabaja solo en 5 GHz y alcanza varios gigabits teóricos; 802.11ax (Wi-Fi 6) usa 2.4 y 5 GHz (y 6 GHz en la variante 6E) con un máximo teórico cercano a 10 Gbps y, más importante, mucho mejor rendimiento

con muchos dispositivos conectados a la vez; 802.11be (Wi-Fi 7) suma la banda de 6 GHz de serie y multiplica la velocidad teórica de nuevo. Fijate que digo "teóricos": en el mundo real la velocidad depende de la distancia, los obstáculos, la interferencia y la cantidad de equipos compartiendo el aire.

Todas las generaciones son compatibles hacia atrás: un teléfono Wi-Fi 6 se conecta sin problema a un router Wi-Fi 4, solo que hablará a la velocidad de la generación más vieja. Esa compatibilidad es la que permite que en tu casa convivan aparatos de diez años de antigüedad con el teléfono nuevo.

8. Las bandas: 2.4 GHz contra 5 GHz contra 6 GHz

Las redes Wi-Fi transmiten en bandas de frecuencia de radio, y cada banda es un compromiso distinto entre alcance, velocidad e interferencia. Entenderlas es lo que te permite elegir bien y diagnosticar problemas reales.

La banda de 2.4 GHz es la veterana. Sus ondas son más largas, así que atraviesan mejor las paredes y llegan más lejos: ideal para cubrir toda la casa. Pero tiene dos problemas graves: es lenta comparada con las bandas altas, y está saturadísima. En 2.4 GHz no solo viven las redes Wi-Fi de todos tus vecinos, también los hornos de microondas, los dispositivos Bluetooth, algunos teléfonos inalámbricos y hasta cámaras de bebe. Todo ese ruido se traduce en interferencia y velocidad irregular. Además el espacio es pequeño: con canales de 20 MHz de ancho solo hay tres canales que no se traslapan entre sí, el 1, el 6 y el 11. Si tu router está en el canal 3 y el del vecino en el 1, se estorban mutuamente aunque "estén en canales distintos". Por eso la regla de oro en 2.4 GHz es usar solo 1, 6 u 11, eligiendo el menos congestionado.

La banda de 5 GHz es la velocista. Ofrece mucho más espacio (muchos más canales que no se traslapan) y canales más anchos (40, 80 y hasta 160 MHz), lo que se traduce en velocidades muy superiores y poquísima interferencia de aparatos no Wi-Fi. Su debilidad es la física: las ondas más cortas se atenían más rápido y les cuesta atravesar paredes. Por eso la red de 5 GHz vuela en la misma habitación del router pero se queda corta al fondo de la casa. La mayoría de los routers modernos emiten ambas bandas, a veces con el mismo nombre de red y a veces con nombres separados como "MiCasa" y "MiCasa_5G".

La banda de 6 GHz es la recién llegada, usada por Wi-Fi 6E y Wi-Fi 7. Es rapidísima y está casi vacía porque pocos dispositivos la usan todavía, pero su alcance es el más corto de las tres: prácticamente exige estar cerca del punto de acceso y con línea de vista despejada. Piensala como el carril expés para quién está al lado del router.

La recomendación práctica: deja que tus dispositivos usen 5 GHz (o 6 GHz) cuando esten cerca del router para máxima velocidad, y que caigan a 2.4 GHz cuando se alejen para mantener la conexión. Si tu router lo permite, actívalo en modo de bandas combinadas con selección inteligente, o configura nombres separados y conecta manualmente cada aparato a la banda que le convenga: la tele fija cerca del router a 5 GHz, el foco inteligente del patió a 2.4 GHz.

9. SSID, modos y componentes de una red inalámbrica

El SSID (Service Set Identifier) es simplemente el nombre de tu red Wi-Fi, el que ves en la lista cuando buscas redes: "MiCasa", "Café_Central", "xX_DarkNet_Xx". Es un identificador, no una medida de seguridad: ocultar el SSID (no difundirlo) no te protege de nadie con conocimientos mínimos, porque el nombre viaja de todos modos en el tráfico de administración y se descubre en segundos. Ponle un nombre reconocible, evita datos personales como tu dirección, y no creas que esconderlo te hace invisible.

Las redes Wi-Fi pueden operar en dos modos. El modo infraestructura es el que usas todos los días: todos los dispositivos se conectan a un punto de acceso central que coordina la red y normalmente les da salida hacia Internet. Tu router casero es un punto de acceso en modo infraestructura. El modo ad-hoc, en cambio, conecta dispositivos directamente entre sí sin ningún punto central, como dos laptops compartiendo archivos o un teléfono compartiendo Internet. Es útil en casos puntuales pero raro en el día a día, y menos seguro por definición.

Los componentes de una red inalámbrica son tres. El punto de acceso (AP, Access Point) es el equipo que emite la red Wi-Fi y al que se conectan los clientes; tu router casero trae uno integrado, y las empresas instalan muchos APs distribuidos por el edificio. El controlador inalámbrico (wireless controller) es un equipo o software que en redes empresariales administra centralizadamente todos los APs: les reparte configuración, balancea clientes entre ellos y gestiona que tu teléfono salté del AP del piso 1 al del piso 2 sin cortar la llamada. En tu casa no lo necesitas, pero en un campus o un centro comercial es indispensable. El cliente (o estación) es cualquier dispositivo que se conecta: teléfonos, laptops, tabletas, impresoras, focos inteligentes.

Un concepto emparentado que escucharás es el de las redes en malla (mesh): varios nodos que se interconectan entre sí para cubrir áreas grandes sin cables, muy populares en casas grandes. Cada nodo es a la vez AP para tus dispositivos y repetidor hacia los demás nodos. Son cómodos pero cada salto inalámbrico reduce la velocidad, así que conviene conectarlos por cable cuando sea posible.

Errores comunes de principiantes con Wi-Fi

El primero es dejar el router en el canal automático de fábrica en 2.4 GHz en un edificio lleno de redes. El "automático" no siempre elige bien; usa una app analizadora de Wi-Fi, mira que canales usan tus vecinos y fíjate manualmente en el 1, 6 u 11 menos ocupado.

El segundo es esconder el router en el peor lugar posible: dentro de un mueble metálico, detrás del televisor, en el sótano o en una esquina de la casa. El Wi-Fi se propaga mejor desde un punto alto, centrado y despejado. Mover el router dos metros puede cambiar más tu velocidad que cualquier configuración.

El tercero es creer que "más barras" significa "más velocidad". Las barras miden intensidad de señal, no velocidad ni calidad: puedes tener señal llena en 2.4 GHz saturado navegando lento, y dos barras en 5 GHz volando. La interferencia y la banda importan tanto como la señal.

El cuarto es mezclar generaciones sin saberlo y culpar al proveedor. Si tu laptop es Wi-Fi 4 y tu plan es de 500 Mbps, nunca pasarás de unos 100-150 Mbps reales por aire aunque el router sea nuevo: el eslabón más viejo manda. Para planes rápidos necesitas equipos con Wi-Fi 5 o 6.

10. Seguridad inalámbrica: WEP, WPA, WPA2 y WPA3

Tu red Wi-Fi viaja por el aire y cualquiera dentro del alcance puede capturar ese tráfico con una laptop. Sin cifrado sería como hablar a gritos en un restaurante: todos escuchan. Por eso existen los protocolos de seguridad inalámbrica, y su historia es una carrera entre atacantes y defensores que debes conocer.

WEP (Wired Equivalent Privacy) fue el primer intento, y hoy es historia de terror: su cifrado se rompe en minutos con herramientas gratuitas por fallas en su diseño. Ver WEP activo en un router en pleno 2026 es como ver una puerta con cerradura de juguete: cualquiera entra. Jamás lo uses; si tu router solo ofrece WEP, ese router debe jubilarse.

WPA (Wi-Fi Protected Access) nació como parche de emergencia para WEP, usando TKIP, un cifrado que envolvía el sistema roto para hacerlo usable mientras llegaba algo mejor. Cumplió su misión en su época, pero TKIP también mostró debilidades con los años y hoy WPA con TKIP se considera obsoleto. Solo aparecerá en equipos muy viejos.

WPA2 fue durante más de una década el estándar serio, basado en AES con el modo CCMP: cifrado robusto de verdad. Es lo mínimo aceptable hoy. Su punto débil famoso fue el ataque KRACK, descubierto en 2017, que aprovechaba una falla en el apretón de manos de la conexión para interceptar tráfico; se corrigió con actualizaciones de firmware, lo que nos lleva a una lección permanente: un WPA2 sin actualizar no es tan seguro como crees.

WPA3 es la generación actual. Su gran mejora es el apretón de manos SAE, que resiste ataques de diccionario fuera de línea: aunque un atacante capture tu tráfico, no puede llevarse a su casa a probar contraseñas con calma como podía con WPA2. También ofrece secreto hacia adelante (si alguien roba tu contraseña mañana, no puede descifrar lo que capturó ayer) y cifrado más fuerte. En modo personal sigue usando contraseña, pero mucho mejor protegida; en modo empresarial usa autenticación individual por usuario. Si tus equipos lo soportan, WPA3 es la elección correcta; si tienes aparatos viejos, el modo mixto WPA2/WPA3 mantiene compatibilidad sin bajar toda la red al nivel más débil más de lo necesario.

Respecto a los cifrados: TKIP es el viejo, asociado a WPA, y debe evitarse; AES (en modo CCMP) es el moderno, asociado a WPA2 y WPA3, y es el que debes seleccionar en la configuración. Si tu router ofrece "WPA2 con TKIP+AES", elige solo AES.

11. Buenas prácticas para blindar tu red Wi-Fi

Primera: usa una contraseña Wi-Fi larga, única y realmente fuerte. Nada de "12345678", el nombre de tu calle o tu fecha de nacimiento: esas son las primeras que prueba cualquier atacante. Una frase de cuatro o cinco palabras con algún número y símbolo es fácil de recordar y difícil de romper. Y que sea única: no reutilices la de tu correo ni la de tu banco.

Segunda: cambia las credenciales de administración del router. Casi todos vienen de fábrica con usuario "admin" y contraseña "admin" o "password", datos públicos que cualquiera conoce. Si un atacante entra a tu red Wi-Fi, lo primero que intentará es abrir la página del router con esas credenciales. Cambialas por algo fuerte y guardalo bien.

Tercera: desactiva WPS. El WPS (Wi-Fi Protected Setup) era un botón o un PIN de 8 dígitos para conectar aparatos sin escribir la contraseña, cómodo pero con una falla grave: el PIN se puede adivinar por fuerza bruta en horas. Aunque no uses el botón, muchos routers dejan el PIN activo. Entra a la configuración y apágalo por completo.

Cuarta: crea una red de invitados. Casi todos los routers modernos permiten una segunda red Wi-Fi aislada para visitas, con su propia contraseña. Así tus invitados navegan sin entrar a tu red principal, donde están tu computadora, tu impresora y tus archivos compartidos. Cambia su contraseña de vez en cuando y no le des la principal a nadie que no viva contigo.

Quinta: manten el firmware del router actualizado. Las vulnerabilidades como KRACK se corrigen con actualizaciones, y un router abandonado por su fabricante acumula fallas conocidas. Revisa cada pocos meses si hay actualizaciones, o activa las automáticas si tu modelo las ofrece. Y cuando el fabricante deje de dar soporte, considera reemplazar el equipo: un router sin parches es un riesgo permanente.

Sexta: usa WPA3 si está disponible, o WPA2 con AES como mínimo. Nunca WEP ni WPA con TKIP. Desactiva la administración remota del router desde Internet (que nadie de afuera pueda abrir tú página de configuración) y, si eres más avanzado, considera una red separada para tus dispositivos inteligentes del hogar, que suelen tener seguridad pobre y no reciben actualizaciones.

12. Caso integrado: un día normal en tu casa moderna

Juntemos todo lo de esta unidad en una historia completa, porque los conceptos sueltos se olvidan y las historias se quedan. Son las 7 de la mañana y enciendes tu teléfono.

Tu teléfono busca redes Wi-Fi y encuentra la tuya, "CasaFamilia_5G". Se conecta usando WPA3 con AES: el apretón de manos SAE verifica tú contraseña sin exponerla a ataques de diccionario, y a partir de ahí todo el tráfico por el aire viaja cifrado. El punto de acceso es tu router Wi-Fi 6, que también emite la red de 2.4 GHz "CasaFamilia" para los aparatos lejanos y una red de invitados aislada que configuraste el mes pasado.

Una vez asociado al AP, tu teléfono necesita direcciones. Por el lado IPv4 hace él DORA que ya conoces y el servidor DHCP del router le entrega 192.168.1.33 con puerta 192.168.1.1 y DNS. Por el lado IPv6 no necesita pedir nada: escucha el anuncio del router con el prefijo 2001:db8:abcd:77::/64, arma su unicast global con SLAAC, genera además una dirección temporal por privacidad y ya tiene su fe80:: link-local para hablar con sus vecinos. Tu teléfono ahora es dual-stack: habla los dos protocolos a la vez.

Abres el navegador y escribes una dirección. Tu teléfono consulta al DNS (recibido por DHCP y por el anuncio del router), obtiene la IP del servidor y elige IPv6 porque el destino la soporta. Los paquetes salen de tu teléfono por radio en 5 GHz hacia el AP, el router los manda a Internet con tu IP pública, y la respuesta vuelve por él mismo camino. Todo esto que acabas de leer ocurrió en menos de un segundo y sin que tocarás nada.

A mediodía llega tu primo de visita y le das la contraseña de la red de invitados. Navega sin problema pero no puede ver tu computadora ni tu impresora, porque la red de invitados está aislada. En la tarde juegas en línea con tu laptop conectada por cable al router: tu juego usa IPv4 con PAT para salir, y ni te enteras. En la noche, desde el balcón, tu teléfono se cambia solo a la red de 2.4 GHz porque la de 5 GHz ya no llega con fuerza: menos velocidad, pero conexión estable gracias al mayor alcance.

Esta historia contiene cada tema de la unidad: generaciones Wi-Fi, bandas, SSID, WPA3, DHCP, SLAAC, link-local, dual-stack, DNS, NAT y red de invitados. Cuando diagnostiques una red real, recorre mentalmente esta misma secuencia y pregunta en cada paso: se asoció al Wi-Fi correcto, tiene IP válida, resuelve DNS, sale a Internet. El fallo estará en el primer paso que no se cumpla.

13. Mitos comunes sobre IPv6 y Wi-Fi

Mito 1: "IPv6 es solo IPv4 con números más largos". Falso. Si bien el cambio más visible es el tamaño de la dirección, IPv6 rediseñó el protocolo: cabecera simplificada, sin broadcast, autoconfiguración nativa con SLAAC, descubrimiento de vecinos con NDP en vez de ARP y soporte integrado para IPsec. Es una nueva generación, no una simple ampliación.

Mito 2: "Con IPv6 ya no necesito firewall porque las direcciones son demasiadas para atacar". Falsísimo y peligroso. Los atacantes no adivinan direcciones al azar: las descubren con DNS, con registros públicos, con tráfico capturado y con técnicas de escaneo inteligente de rangos comunes. Y recuerda que sin el NAT casero como escondite, cada equipo con IPv6 global es directamente alcanzable. El firewall es más importante con IPv6, no menos.

Mito 3: "Ocultar el SSID me protege de intrusos". Falso. El nombre de la red viaja en las tramas de administración y cualquier herramienta básica lo revela en segundos, red oculta o no. La protección real es WPA3 o WPA2 con AES y una contraseña fuerte, no la invisibilidad del nombre.

Mito 4: "Más antenas en el router significa más velocidad". No necesariamente. Las antenas ayudan con la tecnología MIMO (múltiples flujos simultáneos), pero la velocidad real depende de la generación del estándar (Wi-Fi 4, 5 o 6), de la banda usada, del ancho del canal y del equipo cliente. Un router de ocho antenas con Wi-Fi 4 no superará a uno de cuatro antenas con Wi-Fi 6.

Mito 5: "La banda de 5 GHz siempre es mejor que la de 2.4 GHz". Depende de la distancia. Cerca del router, 5 GHz gana por velocidad y limpieza del espectro. Lejos o detrás de varias paredes, 2.4 GHz gana porque su señal llega donde la de 5 GHz muere. La mejor red usa ambas, cada una donde brilla.

Mito 6: "IPv6 va a apagar IPv4 pronto, así que ya no vale la pena aprender IPv4". Falso. La convivencia dual-stack durará muchos años más: incontables redes corporativas, proveedores pequeños y equipos antiguos seguirán en IPv4. Un técnico completo domina ambos protocolos y sabe diagnosticar en cada uno.

Ejemplos paso a paso

Ejemplo 1: comprimir y expandir direcciones IPv6 a mano

Toma esta dirección completa y aplícale las dos reglas, paso a paso:

```
Direccion completa:
2001:0db8:0000:0000:0001:0000:0000:0042

Paso 1 - quitar ceros a la izquierda de cada grupo:
2001:db8:0:0:1:0:0:42

Paso 2 - reemplazar la secuencia mas larga de grupos cero con ::
La secuencia mas larga es 0:0:0 al final (tres grupos).
2001:db8:0:0:1::42
```

Verificación: cuenta los grupos visibles (2001, db8, 0, 0, 1, 42 = seis grupos), así que el :: representa dos grupos de ceros y el total da ocho. Correcto. Ahora al revés, expande está:

```
Direccion comprimida:
fe80::a1b2:c3d4

Grupos visibles: fe80, a1b2, c3d4 = tres grupos.
Grupos faltantes: 8 - 3 = 5 grupos de ceros en el ::.
Direccion completa:
fe80:0000:0000:0000:a1b2:c3d4
```

Espera, cuenta de nuevo: fe80 más cinco grupos de ceros más a1b2 más c3d4 son 1 + 5 + 2 = 8 grupos. Correcto. Este hábito de verificar contando grupos te salvará en exámenes.

Ejemplo 2: ver tus direcciones IPv6 en tu equipo

En Windows:

```
C:\> ipconfig
```

Busca tu adaptador y verás líneas cómo estás:

```
Direccion IPv6 . . . . . : 2001:db8:abcd:12::45
Direccion IPv6 temporal. . . . . : 2001:db8:abcd:12:9c4e:71aa:3f2b:88d1
Direccion IPv6 de vinculo local . : fe80::9c4e:71aa:3f2b:88d1%12
```

Lectura: tienes una unicast global (empieza con 2001) que te dio tu proveedor por SLAAC o DHCPv6, una temporal generada por las extensiones de privacidad para navegar, y la link-local fe80 que existe siempre. El %12 al final de la link-local es el identificador de zona o interfaz: como las fe80 se repiten en cada interfaz, el sistema indica en cuál de ellas vive está. En Linux:

```
$ ip -6 addr show
```

Muestra lo mismo con más detalle técnico, incluyendo el prefijo /64 y si la dirección es temporal o permanente. Prueba de conectividad local:

```
C:\> ping ::1
```

Si responde, tú pila IPv6 funciona: te estás haciendo ping a ti mismo por loopback, igual que con 127.0.0.1 en IPv4. Y para probar IPv6 real hacia Internet (si tu proveedor lo ofrece):

```
$ ping6 2001:4860:4860::8888
```

Esa es la dirección IPv6 del DNS público de Google. Si responde, tienes conectividad IPv6 global de verdad.

Ejemplo 3: elegir el mejor canal Wi-Fi en 2.4 GHz

Imagina que vives en un edificio y tu red anda lenta. El procedimiento profesional es:

- Paso 1: instala una app analizadora de Wi-Fi en tu telefono (muestra las redes vecinas y sus canales).
- Paso 2: anota cuantas redes hay en el canal 1, en el 6 y en el 11.
Ejemplo de lectura:
Canal 1: 6 redes vecinas
Canal 6: 2 redes vecinas
Canal 11: 4 redes vecinas
- Paso 3: entra a la configuracion de tu router (192.168.1.1), seccion inalambrica de 2.4 GHz.
- Paso 4: cambia el canal de "Automatico" al 6, el menos ocupado.
- Paso 5: guarda, espera a que el router reinicie la radio y prueba velocidad cerca y lejos del router.

Por qué funciona: en 2.4 GHz solo 1, 6 y 11 no se traslapan, así que cualquier otro número se estorba con dos canales a la vez. Elegir el menos congestionado de esos tres reduce las colisiones y los reintentos, que son lo que realmente te pone lento el Internet, más que la "velocidad contratada".

Ejemplo 4: configurar la seguridad de tu router paso a paso

Esta es la secuencia de blindaje básico que aplica a casi cualquier router casero:

1. Conectate por cable al router y abre su pagina (192.168.1.1).
2. Entra con las credenciales de fabrica y CAMBIALAS de inmediato:
usuario admin / contraseña nueva larga y unica.
3. Ve a la seccion inalambrica (Wireless / Wi-Fi).
 - Modo de seguridad: WPA3-Personal. Si algun aparato viejo no conecta, usa WPA2/WPA3 mixto. Jamas WEP ni WPA.
 - Cifrado: AES (solo AES, no TKIP ni mixto TKIP+AES).
 - Contraseña Wi-Fi: frase larga y unica, distinta de la de administracion.
4. Desactiva WPS por completo (ni boton ni PIN).
5. Activa la red de invitados con su propia contraseña y aislamiento de clientes activado.
6. Desactiva la administracion remota desde Internet (WAN).
7. Revisa la seccion de firmware y aplica actualizaciones.
8. Guarda, reinicia el router y reconecta tus dispositivos con la contraseña nueva.

Cada paso cierra una puerta real: credenciales nuevas bloquean el acceso a la configuración, WPA3/AES blindo el aire, sin WPS eliminas el PIN vulnerable, la red de invitados aísla a las visitas, y sin administración remota nadie de Internet puede tocar tu router. Hazlo una vez y duerme tranquilo.

Ejemplo 5: leer una tabla de capacidades Wi-Fi antes de comprar

Cuándo compares equipos, traduce la etiqueta a datos útiles:

Etiqueta: "Router Wi-Fi 6, AX3000, doble banda"

Traducción:

- Wi-Fi 6 = estándar 802.11ax.
- AX3000 = velocidad teórica combinada aproximada de 3000 Mbps sumando todas las bandas y antenas (no la veras real, pero sirve para comparar modelos).
- Doble banda = emite en 2.4 GHz y 5 GHz (no incluye 6 GHz; eso sería "tribanda" con 6 GHz, propio de Wi-Fi 6E o Wi-Fi 7).

Conclusión: buen equipo moderno para un hogar con muchos dispositivos, siempre que tus aparatos soporten Wi-Fi 6 para aprovecharlo al máximo.

Este ejercicio te convierte en comprador informado: ya no te venden "más antenas" como sinónimo de "más velocidad", porque sabes que la generación del estándar y la banda pesan más.

Ejemplo 6: auditar tu propia conexión Wi-Fi en dos minutos

Sin instalar nada raro puedes revisar que generación y que seguridad usa tu conexión actual. En Windows:

Paso 1: abre Configuración > Red e Internet > Wi-Fi y entra a las propiedades de tu red conectada.

Paso 2: busca estos dos datos:

- Protocolo: aquí veras algo como "Wi-Fi 6 (802.11ax)". Esa es la generación negociada entre tu equipo y el AP.
- Tipo de seguridad: aquí veras "WPA3-Personal" o "WPA2-Personal". Si dice WEP o WPA, tienes un problema que corregir en el router.

Paso 3: compara el protocolo con tu plan contratado. Si tu plan es de 300 Mbps pero el protocolo dice Wi-Fi 4 (802.11n), tu cuello de botella es el equipo o el router, no el proveedor: ni el mejor plan pasa por una radio vieja.

En Android, en los detalles de la red Wi-Fi conectada verás la "seguridad" (WPA3, WPA2) y a veces la banda (2.4 o 5 GHz). En iPhone la información es más limitada, pero la app del fabricante del router suele mostrarla. Este chequeo de dos minutos te dice de inmediato si tu red está al día o si vives con WEP sin saberlo, qué pasa más seguido de lo que crees en routers viejos heredados.

Práctica

1. Comprime al máximo estas tres direcciones IPv6 aplicando las dos reglas, y después expande estas dos direcciones comprimidas a su forma completa. Explica en cada caso que hiciste: a) 2001:0db8:0000:0000:0000:0000:0001, b) fe80:0000:0000:0000:0000:0000:00a1, c) 2001:0db8:0000:0001:0000:0000:0000:0001, d) 2001:db8::ff00:42:8329, e) ff02::1.

SOLUCIÓN:

a) Primero quito ceros a la izquierda: 2001:db8:0:0:0:0:1. Luego la secuencia más larga de ceros son siete grupos seguidos, que se reemplazan con un solo ::. Resultado: 2001:db8::1. Es, de paso, una dirección de documentación muy usada en ejemplos. b) Quito ceros a la izquierda: fe80:0:0:0:0:0:a1. Comprimo los siete grupos de ceros: fe80::a1. Fijate que el último grupo 00a1 quedo como a1 por la regla 1. c) Quito ceros: 2001:db8:0:1:0:0:1. Aquí hay dos secuencias de ceros: una de un grupo (después de db8) y otra de tres grupos (antes del 1 final). La regla dice comprimir la más larga, así que el resultado es 2001:db8:0:1::1. Comprimir la secuencia corta daría 2001:db8::1:0:0:1, que también es válido pero no es la forma canónica. d) Expansión: grupos visibles son 2001, db8, ff00, 42, 8329, cinco grupos; faltan tres grupos de ceros en el ::. Forma completa: 2001:0db8:0000:0000:ff00:0042:8329. e) Expansión: visibles ff02 y 1, dos grupos; faltan seis grupos de ceros. Forma completa: ff02:0000:0000:0000:0000:0000:0000:0001. Reconocela: es la multicast de "todos los nodos del enlace local".

2. Clasifica cada una de estas direcciones IPv6 según su tipo y explica que significa cada tipo en una red real: a) 2001:db8:abcd::10, b) fe80::1c2d:3e4f:5a6b:7c8d, c) ff02::1, d) ::1, e) fd00::5. Además responde: cuál de ellas podría usar un servidor web para ser visitado desde otro país, y por qué las demás no servirían.

SOLUCIÓN:

a) Unicast global: empieza con 2001, así que es una dirección pública enrutable en Internet. Ojo: 2001:db8::/32 es el rango de documentación, así que en un ejercicio es válida pero en una red real sería de ejemplo. b) Link-local: empieza con fe80, solo válida dentro de su enlace local, se autoconfigura sola y sirve para comunicación entre vecinos y para NDP; no cruza routers. c) Multicast: empieza con ff, es la dirección de grupo "todos los nodos del enlace local", usada para mensajes a todos los vecinos sin broadcast. d) Loopback ::1: apunta al propio equipo, solo para pruebas locales, equivalente a 127.0.0.1. e) Unique local: empieza con fd, es el equivalente a una IP privada de IPv4, para redes internas sin necesidad de salir a Internet con IPv6. Para el servidor web visible desde otro país solo sirve la unicast global (a), porque es la única enrutable en Internet. La link-local no cruza routers, la multicast es para grupos locales, el loopback solo se ve a si mismo y la unique local es privada por diseño.

3. Te mudas a un departamento en un edificio con 20 redes Wi-Fi vecinas visibles. Tu router es doble banda Wi-Fi 6. Disena tu configuración inalámbrica justificando cada decisión: que banda usas para tu laptop de trabajo que está en la misma habitación del router, que banda para el foco inteligente del balcón al fondo del departamento, qué canal eliges en 2.4 GHz y por qué, y dónde colocas físicamente el router.

SOLUCIÓN:

La laptop de trabajo va a la banda de 5 GHz: está cerca del router, así que aprovecha su velocidad alta y sus canales anchos sin sufrir su menor alcance; además en 5 GHz hay poquísima interferencia de vecinos comparada con 2.4 GHz. El foco del balcón va a 2.4 GHz: está lejos y probablemente detrás de paredes, y un foco necesita alcance, no velocidad; 2.4 GHz atraviesa mejor los obstáculos. Para el canal de 2.4 GHz uso una app analizadora, cuento las redes vecinas en el 1, el 6 y el 11, y elijo manualmente el menos ocupado de esos tres, porque son los únicos que no se traslapan con canales de 20 MHz; dejarlo en automático en un edificio saturado suele elegir mal. El router lo colocó en un punto alto, centrado en el departamento y despejado, lejos de microondas, espejos grandes y muebles metálicos: la ubicación física suele mejorar más la experiencia que cualquier ajuste de software. Si el router permite nombres de red separados por banda, los configuré así para decidir yo que aparató va a cada banda en vez de dejarlo al azar.

4. Completa la tabla comparativa de generaciones Wi-Fi con la banda y la velocidad máxima teórica de cada una, y explica con tus palabras que mejoró la Wi-Fi Alliance al introducir los nombres Wi-Fi 4, 5 y 6: 802.11b, 802.11g, 802.11a, 802.11n, 802.11ac, 802.11ax.

SOLUCIÓN:

802.11b: banda 2.4 GHz, hasta 11 Mbps, la que popularizó el Wi-Fi hogareño. 802.11g: 2.4 GHz, hasta 54 Mbps, compatible con b. 802.11a: 5 GHz, hasta 54 Mbps, contemporánea de b

pero en la banda alta. 802.11n (Wi-Fi 4): 2.4 y 5 GHz, hasta 600 Mbps teóricos, primera con múltiples antenas. 802.11ac (Wi-Fi 5): solo 5 GHz, varios gigabits teóricos, enfocada en velocidad. 802.11ax (Wi-Fi 6): 2.4 y 5 GHz (y 6 GHz en la variante 6E), cerca de 10 Gbps teóricos, con gran mejora en eficiencia cuando hay muchos dispositivos conectados. Lo que mejoró la Wi-Fi Alliance con los nombres numéricos fue la comunicación: antes el público tenía que descifrar letras (a, b, g, n, ac, ax) sin orden evidente, y "Wi-Fi 6" transmite de inmediato que es más nuevo y mejor que "Wi-Fi 5", igual que las generaciones de telefonía móvil. Además los números aparecen en los iconos de conexión de los dispositivos, así que el usuario ve en pantalla que generación está usando.

5. Auditas la red Wi-Fi de un pequeño negocio y encuentras esto: seguridad WEP con contraseña "negocio123", WPS activado, usuario y contraseña del router en "admin/admin", firmware de hace 6 años, una sola red para empleados y clientes, y el SSID visible con el nombre del negocio y su dirección. Elabora una lista priorizada de cambios, explicando el riesgo de cada problema y su solución.

SOLUCIÓN:

Prioridad 1, cambiar WEP por WPA3 (o WPA2 con AES como mínimo): WEP se rompe en minutos con herramientas gratuitas, así que hoy cualquiera puede entrar a la red y espiar el tráfico del negocio; es el riesgo más grave y se corrige en la sección inalámbrica del router. Prioridad 2, contraseña Wi-Fi nueva, larga y única: "negocio123" cae ante el primer ataque de diccionario; hay que poner una frase fuerte y no reutilizarla. Prioridad 3, cambiar las credenciales de administración del router: con admin/admin cualquiera dentro de la red puede tomar el control total del equipo, cambiar DNS o abrir puertos. Prioridad 4, desactivar WPS: su PIN de 8 dígitos se adivina por fuerza bruta en horas, y es una puerta trasera aunque la contraseña Wi-Fi sea fuerte. Prioridad 5, actualizar el firmware: seis años sin parches acumulan vulnerabilidades conocidas y públicas; si el fabricante ya no da soporte, hay que reemplazar el equipo. Prioridad 6, crear red de invitados aislada para clientes: hoy los visitantes comparten red con las computadoras del negocio, sus archivos y su impresora; la red de invitados los separa. Prioridad 7, cambiar el SSID por un nombre sin la dirección del negocio: no es una medida de seguridad real (ocultarlo tampoco protege), pero regalar la ubicación exacta en el nombre es información innecesaria para atacantes. Con los siete cambios la red pasa de estar abierta de par en par a un nivel profesional básico.

6. Una pequeña oficina quiere modernizarse: su proveedor ya ofrece IPv6 nativo y también compraron puntos de acceso Wi-Fi 6. Diseña el plan: que tipo de dirección IPv6 recibirá cada computadora y como la obtendrá (SLAAC, DHCPv6 o manual), para qué usarías las direcciones link-local, cómo conviven IPv4 e IPv6 en los equipos, y que configuración de seguridad Wi-Fi aplicarías a la red de empleados y a la de visitantes.

SOLUCIÓN:

Cada computadora recibirá una unicast global (prefijo del proveedor, algo como 2001:..../64) obtenida por SLAAC: el router anuncia el prefijo y cada equipo arma su dirección solo, sin servidor. Para control centralizado se puede complementar con DHCPv6 en modo sin estado que entregue los servidores DNS y el nombre de dominio. Las direcciones link-local fe80:: se autoconfiguran solas en cada interfaz y las usarán los equipos para NDP (descubrimiento de vecinos, reemplazo de ARP) y para hablar con el router; el administrador no necesita configurarlas ni preocuparse por ellas, solo reconocerlas en los diagnósticos. Los equipos trabajarán en dual-stack: conservarán su IPv4 privada (192.168.x.x con NAT para salir) y sumarán su IPv6 global; el sistema elegirá IPv6 cuando el destino la soporte. En Wi-Fi, los APs nuevos se configuran en modo infraestructura con un controlador que los administre centralizadamente y permita roaming entre pisos. La red de empleados llevará WPA3-Personal (o WPA2/WPA3 mixto si hay equipos viejos) con AES y contraseña fuerte única, WPS desactivado y credenciales del controlador cambiadas. La red de visitantes será una red de invitados aislada de la red corporativa, con su propia contraseña rotada periódicamente. Finalmente, como ahora cada equipo tiene IPv6 global alcanzable desde Internet, se verifica que el firewall del router filtre IPv6 entrante: sin el NAT casero como escondite, el firewall es la única defensa.

7. Tu vecino te presume que su Wi-Fi es "invisible y por lo tanto inhackeable" porque oculta el SSID, usa WEP "para que los aparatos viejos se conecten rápido" y dejó el WPS activado "por comodidad". Desmonta cada afirmación con argumentos técnicos y proponle la configuración correcta, explicando que gana con cada cambio.

SOLUCIÓN:

Primera afirmación, falsa: ocultar el SSID no da ninguna protección real. El nombre de la red se anuncia en las tramas beacon y en las respuestas a sondas, y cualquier analizador de Wi-Fi gratuito lo muestra en segundos aunque esté "oculto". Lo único que logra es incomodar a sus propios invitados, que deben escribir el nombre a mano. La seguridad real está en el cifrado, no en esconder el nombre. Segunda afirmación, peligrosa: WEP se rompe en minutos con herramientas gratuitas por fallas de diseño en su cifrado, así que su red está efectivamente abierta. Ninguna compatibilidad con aparatos viejos justifica WEP: esos aparatos deben actualizarse o jubilarse, y mientras tanto se usa WPA2 con AES como mínimo. Con WEP, su vecino podría estar espionando su tráfico esta misma noche. Tercera afirmación, riesgosa: el WPS por PIN se puede adivinar por fuerza bruta en cuestión de horas, así que aunque tuviera buena contraseña, el PIN es una puerta trasera abierta. Debe desactivar WPS por completo. La configuración correcta: SSID visible con nombre neutro, seguridad WPA3-Personal (o WPA2 con AES si hay equipos viejos), contraseña larga y única, WPS desactivado,

credenciales de administración del router cambiadas y firmware actualizado. Con cada cambio gana algo concreto: cifrado real contra espionaje, adiós a la puerta trasera del PIN, control exclusivo de su propio router y protección contra vulnerabilidades conocidas.

8. Explica la diferencia entre dual-stack y túneles como estrategias de convivencia entre IPv4 e IPv6, y dí en que situación usarías cada una. Incluye un ejemplo concreto de cada estrategia aplicada a una empresa con sucursales.

SOLUCIÓN:

Dual-stack significa que los equipos, routers y sistemas operativos corren IPv4 e IPv6 al mismo tiempo: cada interfaz tiene direcciones de ambos protocolos y el sistema elige cuál usar según lo que soporte el destino. Es la estrategia preferida cuando controlas los equipos y la red, porque no hay encapsulamiento ni traducción: cada protocolo funciona de forma nativa y con su máximo rendimiento. Su requisito es que el proveedor entregue IPv6 y que los equipos lo soporten, algo cierto en casi todo el hardware moderno. Los túneles, en cambio, encapsulan paquetes de un protocolo dentro de paquetes del otro para cruzar una zona que solo habla uno de ellos. Son un puente, no un destino: sirven cuando dos extremos hablan IPv6 pero el camino entre ellos solo entiende IPv4 (o al revés). Tienen un pequeño costo de rendimiento por el encapsulamiento y son más complejos de diagnosticar. Ejemplo concreto: una empresa con matriz y tres sucursales, dónde el proveedor de la matriz ya da IPv6 nativo pero los enlaces hacia dos sucursales son antiguos y solo manejan IPv4. En la matriz y en la sucursal moderna se despliega dual-stack en todos los equipos, que es limpio y nativo. Para comunicar las sucursales antiguas con la matriz por IPv6 se configura un túnel entre los routers de borde: los paquetes IPv6 viajan encapsulados en IPv4 por el enlace viejo y salen como IPv6 nativo al otro lado. Cuando el proveedor modernice esos enlaces, los túneles se retiran y todo queda en dual-stack nativo. La moraleja: dual-stack es la meta, los túneles son el puente para llegar a ella.

Resumen de la unidad

En esta unidad disté el salto al IPv6 y al mundo inalámbrico. IPv6 nació porque las 4,300 millones de direcciones de IPv4 se agotaron frente a un planeta lleno de dispositivos conectados; con sus 128 bits ofrece un espacio de direcciones tan vasto que cada equipo puede tener su IP pública sin NAT. Aprendiste su notación de ocho grupos hexadecimales separados por dos puntos, las dos reglas de compresión (quitar ceros a la izquierda y usar :: una sola vez para la secuencia más larga de ceros) y a expandir direcciones contando grupos. Clasificas direcciones a simple vista: unicast global (empieza con 2 o 3) para Internet, link-local fe80:: para el enlace local y NDP, unique local fd00:: como privadas, multicast ff00::/8 para

grupos, ::1 loopback y :: no especificada, recordando siempre que en IPv6 no existe el broadcast.

Viste que SLAAC permite a los equipos autoconfigurarse con los anuncios del router, que NDP sobre ICMPv6 reemplaza a ARP sin broadcasts, y que DHCPv6 queda como opción para administración centralizada. La migración convive con IPv4 mediante dual-stack (ambos protocolos a la vez) y túneles para cruzar zonas de un solo protocolo. En Wi-Fi dominas la familia 802.11 y sus nombres comerciales (n es Wi-Fi 4, ac es Wi-Fi 5, ax es Wi-Fi 6), las bandas de 2.4 GHz (alcance, lenta, saturada, canales 1/6/11), 5 GHz (rápida, menos alcance) y 6 GHz (rapidísima, corto alcance), el SSID como simple nombre, los modos infraestructura y ad-hoc, y los componentes AP, controlador y cliente.

En seguridad quedo claro el veredicto histórico: WEP está muerto y jamás se usa, WPA con TKIP fue un parche temporal, WPA2 con AES es el mínimo aceptable y WPA3 con su apretón SAE es el estándar actual. Tus buenas prácticas de memoria: contraseña Wi-Fi fuerte y única, cambiar credenciales del router, desactivar WPS, red de invitados aislada, firmware actualizado y administración remota apagada. Con las Unidades 7 y 8 completas ya entiendes la red moderna de punta a punta, del cable al aire y de IPv4 a IPv6. Sigue así: en la siguiente unidad el viaje continua.

Para qué esté conocimiento no se quede en teoría, te dejo tres retos para esta semana. Primero, abre la terminal de tu computadora y ejecuta ipconfig o ip addr para encontrar tus direcciones IPv6: identifica cuál es la link-local, si tienes una unicast global y si aparecen direcciones temporales de privacidad. Segundo, entra a la configuración de tu router y verifica con tus propios ojos que seguridad usa tu Wi-Fi: si dice WPA3 o WPA2 con AES, felicidades; si dice WEP o WPA con TKIP, ya sabes exactamente que hacer gracias a esta unidad. Tercero, instala una app analizadora de Wi-Fi y cuenta cuantas redes vecinas comparten tu canal en 2.4 GHz: si estás en un canal saturado, cambia manualmente al 1, 6 u 11 menos ocupado y mide la diferencia. Estos tres ejercicios toman menos de una hora en total y convierten lo que leíste en habilidad real, que es lo que distingue a un técnico de alguien que solo aprobó un examen. El libro continua, y cada unidad construye sobre la anterior: lo que hoy parece mucho mañana será tú segunda naturaleza. Tu red ya no tiene secretos para ti: entiendes cada paquete que sale de tus dispositivos y cada decisión que toma tu router.

UNIDAD 9: Seguridad de redes

Imaginate esto: llegas un lunes por la mañana a la oficina y descubres que ninguna computadora enciende sus archivos. En cada pantalla hay un mensaje que pide un pago en criptomonedas para "liberar" la información. Tu empresa acaba de ser víctima de ransomware. En otro escenario más cercano a tu vida diaria: recibes un correo que parece de tu banco, con su logo y sus colores, pidiéndote que "verifiques tu cuenta" entrando a un enlace. Haces clic, escribes tu usuario y tú contraseña, y al día siguiente tu cuenta está vacía. O tal vez entras a trabajar a una empresa y lo primero que te piden es instalar una VPN para conectarte desde tu casa. Todo esto que acabó de describirte tiene un nombre: seguridad de redes.

Hasta ahora en este curso aprendiste cómo funcionan las redes: direcciones IP, máscaras de subred, enrutamiento, DNS, DHCP, protocolos de transporte y los servicios que corren sobre ellos. Toda esa maquinaria existe para qué los datos viajen de un punto a otro. Pero hay una pregunta que aún no habíamos respondido a fondo: qué pasa cuando alguien con malas intenciones se mete en el camino de esos datos. Esta unidad responde esa pregunta, y lo hace con un enfoque completamente defensivo: vas a aprender a reconocer las amenazas, a entender cómo operan los ataques más comunes y, sobre todo, a protegerte a ti, a tu casa y a tu trabajo.

Por qué importa esto. Primero, porque los ataques ya no son cosa de películas. El ransomware que mencionaba al inicio le pega a hospitales, escuelas, pequeños negocios y hasta a personas comunes que guardan fotos familiares sin respaldo. El phishing es la puerta de entrada número uno de la mayoría de los incidentes: no necesitan "hackear" tu computadora si tu mismo les entregas la contraseña en bandeja de plata. Segundo, porque la seguridad es parte del trabajo de cualquiera que administre redes. Si algún día configuras la red de una oficina, de una escuela o de tu propia casa, las decisiones que tomes aquí son las que separan una red segura de una puerta abierta de par en par. Y tercero, porque en el trabajo moderno te vas a topar con VPNs, firewalls y certificados todo el tiempo; entenderlos te convierte en alguien que resuelve problemas en vez de alguien que solo dice "no tengo internet".

En esta unidad vas a ver tres grandes bloques. En la clase 25 estudiamos las amenazas comunes: el malware en todas sus formas (virus, gusanos, troyanos, spyware y ransomware), la ingeniería social y el phishing, y los ataques típicos contra redes como el escaneo de puertos, el hombre en el medio (MitM), la denegación de servicio (DDoS) y la suplantación ARP. Vas a aprender a reconocerlos y a prevenirlos. En la clase 26 entramos a los firewalls: que son, sus tipos (de red, de host, stateful contra stateless), las zonas de red (LAN, WAN, DMZ), cómo se escriben las reglas de permitir y denegar, y por qué la segmentación de la red

es una de las mejores defensas que existen. En la clase 27 cerramos con las VPNs y los túneles seguros: qué es una VPN, cómo funciona el cifrado, los protocolos principales (IPsec, OpenVPN, WireGuard), la diferencia entre una VPN personal y una corporativa, cómo entra HTTPS y TLS con sus certificados, y las buenas prácticas que sostienen todo lo demás: actualizaciones, contraseñas fuertes, doble factor de autenticación (2FA) y respaldos.

Una advertencia ética importante antes de empezar, y la tomo muy en serio: todo lo que aprendas aquí es para defenderte y para proteger sistemas que están a tu cargo o para los que tienes permiso. Nunca uses este conocimiento para entrar a sistemas ajenos, espiar a otras personas o causar daño. Además de ser delito en México y en casi todo el mundo, es exactamente lo contrario del espíritu de este curso. Un profesional de redes protege; no ataca. Con eso claro, empecemos.

Explicación detallada

Las amenazas: el mapa del territorio

Antes de defenderte necesitas conocer al enemigo. En seguridad de redes una "amenaza" es cualquier cosa capaz de dañar tus sistemas, robar tu información o interrumpir tus servicios. Las amenazas se dividen en dos grandes familias: las que llegan a través de software malicioso (malware) y las que llegan a través de personas engañadas (ingeniería social). Y luego están los ataques directos contra la red misma, que veremos en el siguiente subtema.

Piensa en tu red como en tu casa. El malware sería como una plaga que se mete por las rendijas: a veces la traes tú sin darte cuenta en algo que descargaste. La ingeniería social sería como un estafador que toca tu puerta disfrazado de técnico de la compañía de luz y tu mismo le abres. Los ataques de red serían como alguien que intenta forzar la chapa o que bloquea tu calle para que no puedas salir. Distintas técnicas, mismo objetivo: entrar, robar o destruir.

Malware: virus, gusanos, troyanos, spyware y ransomware

La palabra "malware" viene de "malicious software", software malicioso. Es el término paraguas que cubre todos los programas diseñados para hacer daño. Los principiantes suelen llamar "virus" a todo, pero hay diferencias importantes y vale la pena conocerlas porque cada tipo se previene de forma distinta.

El virus clásico es un programa que se pega a archivos legítimos y necesita que tú lo ejecutes para activarse. Como el virus de la gripa, necesita un huésped. Ejemplo típico de los noventa:

un virus que infectaba documentos de Word y se propagaba cuando compartías el archivo. Hoy los virus puros son menos comunes, pero la idea sigue viva en archivos adjuntos maliciosos: ese "factura.pdf.exe" que te llega por correo es un virus disfrazado esperando que le des doble clic.

El gusano (worm) es más peligroso porque no necesita tu ayuda: se copia solo y se propaga por la red buscando otras máquinas vulnerables. El ejemplo más famoso es WannaCry, el ransomware de 2017 que paralizó hospitales y empresas en más de 150 países en cuestión de horas. Un gusano entra por una vulnerabilidad sin parchear y de ahí salta de computadora en computadora como domino. Moraleja que repetiremos hasta el cansancio: las actualizaciones de seguridad existen para cerrar exactamente esas puertas.

El troyano se disfraza de programa legítimo. Como el caballo de Troya de la historia griega, por fuera parece un regalo y por dentro trae soldados enemigos. Descargas un "programa gratis para editar fotos", lo instalas, y sin que lo notes también instalaste una puerta trasera que le da control de tu máquina a un atacante. Los troyanos son la razón número uno por la que no debes descargar software de sitios dudosos ni usar programas piratas: el "crack" que promete activar tu programa gratis casi siempre trae sorpresa incluida.

El spyware es software espía: se instala en silencio y roba información. Registra lo que escribes en el teclado (keylogger), toma capturas de pantalla, roba tus cookies de sesión para entrar a tus cuentas sin contraseña. A veces viene empaquetado con programas gratuitos ("gratis" casi nunca es gratis). Señales de alerta: tu computadora se pone lenta sin razón, aparecen barras de herramientas en el navegador que tú no instalaste, o tu antivirus se desactiva solo.

El ransomware es la estrella oscura de los últimos años y merece atención especial. Cifra tus archivos con una llave que solo el atacante tiene y te pide un rescate para devolvértelos. No borra nada: lo vuelve ilegible. Imagina que alguien cambia la chapa de tu casa y te pide dinero por la llave nueva. Los ataques modernos son de "doble extorsión": primero roban tus datos y luego los cifran, así que aunque tengas respaldo te amenazan con publicar tu información si no pagas. Casos reales: en 2021 el ataque a Colonial Pipeline dejó sin gasolina a buena parte de la costa este de Estados Unidos; hospitales han teñido que regresar al papel y lápiz por semanas. Y no creas que solo le pasa a las grandes empresas: los atacantes automatizan el envío masivo y le pegan a quién caiga, incluyendo pequeños negocios y personas.

Cómo reconocer una posible infección de malware: archivos que cambian de extensión de golpe, programas que se abren solos, el ventilador trabajando a todo cuando no haces nada pesado, mensajes pidiendo rescate, contactos que reciben correos raros "de tu parte". Como prevenirlo: antivirus actualizado y activado, sistema operativo y programas siempre al día, no

abrir adjuntos inesperados aunque vengan de conocidos (sus cuentas también se hackean), descargar software solo de sitios oficiales, y tener respaldos regulares. Los respaldos son tu seguro de vida contra el ransomware: si tienes copia de todo, el rescate pierde su poder.

Error común de principiante: pensar "a mí no me va a pasar porque no tengo nada importante". Tu computadora es valiosa para un atacante aunque no tengas secretos: la puede usar para minar criptomonedas, para lanzar ataques contra otros, o para robar tus cuentas que sí valen dinero. Otro error: desactivar el antivirus "porque alenta la máquina". Es como quitarte el cinturón de seguridad porque te aprieta.

Ingeniería social y phishing: el ataque a la persona

La ingeniería social es el arte de manipular personas para que entreguen información o acceso. Es el ataque más efectivo que existe porque no necesita romper ninguna tecnología: rompe a la persona. Los atacantes saben que es más fácil engañar a un humano que hackear un servidor bien configurado.

El phishing es la forma más común: mensajes falsos que se hacen pasar por entidades de confianza (tu banco, tu trabajo, una paquetería, una red social) para robarte credenciales o instalarte malware. El nombre viene de "fishing", pescar: lanzan miles de anzuelos y esperan que alguien muerda. Ejemplo realista: recibes un SMS que dice "PAQUETE DETENIDO: confirma tu dirección aquí" con un enlace acortado. El enlace lleva a una página idéntica a la de la paquetería que te pide tu tarjeta "para el pago del envío". Caíste.

Variantes que debes conocer: el spear phishing, dirigido a una persona específica con datos reales sobre ella ("Hola Lic. García, aquí está la factura del proyecto Alfa"); el whaling, dirigido a directivos con acceso a dinero ("Soy el director, haz esta transferencia urgente, es confidencial"); el vishing, por llamada de voz ("hablamos de tu banco, tu cuenta fue comprometida, danos el código que te llegó"); y el smishing, por SMS como el ejemplo de la paquetería. También existe el phishing por código QR en lugares públicos: pegan su QR sobre el QR legítimo de un restaurante o estacionamiento y te llevan a su página falsa.

Cómo reconocer un intento de phishing. Revisa estas señales como checklist: primero, la urgencia artificial ("tu cuenta será bloqueada en 24 horas", "actúa ahora"). Los atacantes usan el miedo y la prisa para que no pienses. Segundo, el remitente: pasa el mouse sobre el nombre y mira la dirección real. "soporte@banc0-seguro.com" no es tu banco, aunque el logo se vea perfecto. Tercero, errores sutiles: dominios parecidos pero no iguales (micr0soft, g00gle), faltas de ortografía, saludos genéricos ("estimado cliente" en vez de tu nombre). Cuarto, enlaces sospechosos: sin hacer clic, pasa el cursor y mira a dónde apunta de verdad. Quinto, adjuntos inesperados, sobre todo archivos .exe, .zip, .docm o .xlsm. Sexto, peticiones

raras: ningún banco legítimo te pide tu contraseña completa, tu NIP o los códigos que te llegan por SMS.

Cómo prevenirlo: desconfía por defecto de mensajes no solicitados que pidan datos o acciones urgentes; nunca entres a tu banco desde un enlace de un correo, mejor escribe tú la dirección o usa la app oficial; activa el doble factor de autenticación en todo lo importante (así aunque roben tu contraseña no entran); verifica por otro canal: si tu "jefe" te pide una transferencia urgente por correo, llámale por teléfono para confirmar; y reporta el phishing en tu correo o a tu equipo de sistemas en el trabajo. En las empresas, la capacitación constante es la mejor defensa: un empleado entrenado vale más que un firewall caro.

Analogía útil: el phishing es como esos vendedores que tocan tu puerta con uniforme falso de la compañía de luz para "revisar tu medidor" y en realidad quieren ver que tienes en casa. La defensa no es una chapa más gruesa: es aprender a pedir identificación y a no abrirle a desconocidos.

Error común de principiante: creer que "yo si me doy cuenta". Los ataques modernos usan inteligencia artificial para escribir correos perfectos sin faltas de ortografía y clonar voces. La humildad es parte de la defensa: ante la duda, no hagas clic y verifica por otro medio.

Ataques de red: escaneo de puertos, MitM, DDoS y suplantación ARP

Hasta aquí hablamos de ataques que llegan a tu computadora o a tu persona. Ahora veamos los ataques que van directo contra la red: como los atacantes exploran, interceptan, saturan y enganan la comunicación entre equipos.

El escaneo de puertos es el reconocimiento del atacante. Antes de robar una casa, el ladrón pasa por la calle viendo que ventanas están abiertas. En redes, el atacante envía paquetes a los puertos de tu equipo o servidor para ver cuáles responden. Si el puerto 22 responde, hay SSH; si el 3389 responde, hay escritorio remoto de Windows; si el 80 o 443 responden, hay un servidor web. Con esa información sabe que servicios atacar y que vulnerabilidades probar. Herramientas como Nmap hacen esto en segundos contra miles de equipos. Como reconocerlo: en los registros de tu firewall verás muchas conexiones rechazadas desde una misma IP en poco tiempo, como alguien tocando todas las puertas de tu edificio. Como prevenirlo: cierra todos los puertos que no necesites, usa un firewall que bloquee el escaneo, y no expongas servicios de administración (SSH, RDP, paneles de control) directamente a internet: ponlos detrás de una VPN.

El ataque de hombre en el medio (Man in the Middle, MitM) es la interceptación de la comunicación. El atacante se coloca en secreto entre tú y el servidor con el que hablas, de modo que todo pasa por sus manos. Imagina que le pasas notitas a tu amigo en clase a través

de un compañero, y ese compañero lee cada notita antes de entregarla, y a veces hasta cambia lo que dice. En redes esto pasa sobre todo en WiFi públicas sin protección: el atacante crea una red falsa con el mismo nombre que la del café ("Café_Gratis") y cuando te conectas, todo tu tráfico pasa por su computadora. Así puede robar sesiones, contraseñas de sitios sin cifrado y datos personales. Como reconocerlo: certificados de seguridad que el navegador marca como inválidos, la red WiFi pide datos raros, o tu conexión se comporta extrañamente. Como prevenirlo: evita hacer banca o meter contraseñas en WiFi públicas; si no hay de otra, usa una VPN que cifre todo tu tráfico; verifica que los sitios importantes usen HTTPS (el candadito) y no ignores las advertencias de certificado del navegador.

La denegación de servicio (DoS) y su versión distribuida (DDoS) buscan tumbar un servicio saturándolo. Es como si mil personas llamarán al mismo tiempo a la pizzería de tu colonia: el teléfono suena y suena, los clientes reales no pueden entrar su pedido y el negocio se paraliza. En un DDoS, el atacante usa miles de equipos infectados (una botnet) para inundar de peticiones a un servidor hasta que colapsa. No roba información: su objetivo es que el servicio deje de funcionar. Lo usan para extorsión ("pagame o tumbo tu tienda en línea en el Buen Fin"), como protesta, o como cortina de humo mientras hacen otro ataque. Como reconocerlo: tu sitio o servicio se vuelve lentísimo o inaccesible de golpe, con picos de tráfico anormal en las gráficas. Como prevenirlo (a nivel empresa): servicios anti-DDoS de proveedores grandes, balanceadores de carga, y tener un plan de respuesta. A nivel personal no puedes hacer mucho contra un DDoS dirigido a ti, pero si te toca administrar algo público, contrata protección antes de necesitarla.

La suplantación ARP (ARP spoofing) es un engaño dentro de tu red local. Recuerda de unidades anteriores: ARP es el protocolo que relaciona direcciones IP con direcciones MAC en la red local, y los equipos confían ciegamente en las respuestas ARP que reciben. El atacante envía mensajes ARP falsos diciendo "yo soy la puerta de enlace" (o "yo soy la computadora de la víctima"), y los demás equipos le creen y le empiezan a mandar su tráfico. Así logra un MitM dentro de la red local sin que nadie lo note. Es el ataque favorito en redes WiFi de oficinas y escuelas mal cuidadas. Como reconocerlo: herramientas de red muestran que dos equipos tienen la misma MAC, o la tabla ARP cambia de forma extraña. Como prevenirlo: en redes empresariales se usan switches con protección "Dynamic ARP Inspection" y se segmenta la red (de eso hablamos en el tema de firewalls); en casa, mantener el router actualizado y no dejar que desconocidos se conecten a tu red ayuda mucho.

Un punto importante sobre todos estos ataques: existen herramientas legítimas para probarlos en tu propio laboratorio (Nmap para escanear, Wireshark para analizar tráfico). Usarlas contra tus propios equipos o en prácticas con permiso es perfectamente legal y es cómo aprenden los profesionales. Usarlas contra redes ajenas sin permiso es delito. La línea es clara: tu red y tus equipos, o permiso escrito del dueño. Todo lo demás está fuera de límites.

Firewalls: el guardia de la puerta

Un firewall es un sistema que filtra el tráfico de red según reglas que tú defines: decide que paquetes pueden pasar y cuáles se bloquean. Es el guardia de seguridad de tu red, parado en la puerta con una lista de invitados. "Tú si pasas, tú no". Sin firewall, cada servicio de tu red está expuesto a todo el internet; con firewall, solo entra lo que tu autorices.

Hay dos grandes tipos según dónde viven. El firewall de red protege a toda una red y suele estar en el borde, entre tu red e internet: puede ser un aparato físico (como los que venden para empresas) o la función de firewall de tu router casero. El firewall de host protege a una sola computadora: el Firewall de Windows, el de macOS o iptables en Linux son ejemplos. La buena práctica es usar ambos en capas: el de red frena lo grueso y el de host cuida cada equipo por si algo se cuele. A esto se le llama defensa en profundidad: no depender de una sola muralla sino de varias capas, como un castillo con foso, muralla y guardia interior.

Otra clasificación importante: stateful contra stateless. Un firewall stateless (sin estado) mira cada paquete por separado, como un guardia que revisa cada persona sin recordar a nadie: "traes credencial válida, pasa". Es rápido pero tonto: no sabe si ese paquete es parte de una conversación legítima o un intruso suelto. Un firewall stateful (con estado) recuerda las conexiones: sabe que tu computadora pidió una página web y por eso permite que la respuesta entre, pero bloquea paquetes que llegan sin que nadie los haya pedido. Analogía: el guardia que además de revisar credenciales lleva un registro de quién entro y solo deja salir y volver a entrar a los que están anotados. Hoy casi todos los firewalls son stateful porque son mucho más seguros; los stateless quedaron para casos muy específicos de alto rendimiento.

También existen los firewalls de aplicaciones (como los WAF, Web Application Firewall), que entienden el tráfico de una aplicación específica, por ejemplo HTTP, y pueden bloquear ataques contra páginas web aunque el tráfico venga por un puerto permitido. Y los firewalls de nueva generación (NGFW) que combinan filtrado con detección de intrusos y control de aplicaciones. No necesitas memorizar todas las siglas: quedate con la idea de qué el firewall evoluciona de "reviso puertos" a "entiendo que aplicación eres y si tu comportamiento es normal".

Zonas de red: LAN, WAN, DMZ y la segmentación cómo defensa

No todas las partes de una red merecen la misma confianza, así que se dividen en zonas. La LAN (red de área local) es tu zona de confianza: las computadoras de la oficina o de tu casa. La WAN, en este contexto, suele ser internet: la zona de no confianza, donde está todo el mundo. Y en medio, para los servicios que deben ser visibles desde internet (como tu página web o tu servidor de correo), existe la DMZ (zona desmilitarizada).

La DMZ es una idea brillante y sencilla: si tu servidor web tiene que estar expuesto a internet porque los clientes deben verlo, no lo pongas dentro de tu LAN junto a tus archivos importantes. Ponlo en una zona intermedia con reglas estrictas: internet puede llegar a la DMZ, la DMZ puede responder a internet, pero la DMZ no puede entrar libremente a tu LAN. Así, si un atacante compromete tu servidor web, se queda atrapado en la DMZ y no llega a tus datos internos. Es como la recepción de un edificio: los visitantes pueden entrar ahí, pero no pueden pasar a las oficinas sin permiso especial.

La segmentación de red lleva esta idea más lejos: dividir la red interna en pedazos separados según su función o su nivel de riesgo. Ejemplo en una empresa: una red para empleados, otra para invitados (el WiFi de visitas no debe tocar los servidores), otra para los sistemas de cobro, otra para las cámaras de seguridad. Cada segmento tiene sus propias reglas de firewall. Por qué es tan poderosa: limita el daño. Si un empleado abre un phishing y su computadora se infecta con un gusano, el firewall entre segmentos impide que el gusano salté al segmento de servidores o al de cobro. Sin segmentación, una sola computadora infectada contamina toda la empresa en minutos, como paso en varios ataques famosos de ransomware.

En tu casa también puedes aplicar una versión sencilla: la mayoría de los routers modernos permiten crear una red de invitados separada. Actívala y dale esa clave a las visitas en vez de la clave de tu red principal. Tus dispositivos personales (computadora, teléfono, discos de respaldo) quedan en la red principal, aislados de lo que hagan los invitados. Cuesta dos minutos configurarlo y es una de las mejoras de seguridad más rentables que existen.

Error común de principiante: pensar que el firewall "ya viene configurado" y no hay que tocarlo. Los firewalls traen reglas genéricas de fábrica; la seguridad real está en adaptarlas a lo que tu red necesita: cerrar lo que no se usa, abrir solo lo necesario y revisar las reglas cada cierto tiempo. Otro error: creer que con firewall ya no hace falta nada más. El firewall no te protege del phishing (tu mismo abres la puerta), ni del malware que entra en una memoria USB, ni de una contraseña débil. Es una capa, no toda la armadura.

Reglas de firewall: permitir, denegar y el orden correcto

Las reglas de un firewall son instrucciones del tipo "si el tráfico cumple estas condiciones, haz esto". Cada regla suele especificar: origen (IP o red de dónde viene), destino (IP o red a dónde va), puerto o servicio, protocolo (TCP/UDP) y acción: permitir (accept/allow) o denegar (deny/drop/reject). La diferencia entre "drop" y "reject": drop tira el paquete en silencio (el atacante ni se entera), reject lo tira pero avisa. Para el tráfico de internet, drop es mejor porque no le das pistas al atacante.

El principio de oro para escribir reglas es "denegar por defecto": todo lo que no este explícitamente permitido, se bloquea. Es la política de la fiesta privada con lista de invitados: si no estás en la lista, no entras. Lo contrarió ("permitir por defecto") es la fiesta de puerta abierta donde solo sacas a los problemáticos conocidos: siempre se te cuela alguien. Cuando configures un firewall, tú última regla debe ser "denegar todo".

El orden de las reglas importa muchísimo porque el firewall las evalúa de arriba hacia abajo y se queda con la primera que coincida. Ejemplo de error clásico: pones primero "permitir todo desde internet al servidor web" y después "denegar el acceso al panel de administración". Como la primera regla ya dejó pasar todo, la segunda nunca se aplica y tu panel queda expuesto. La regla más específica siempre va antes que la general. Piensa en las reglas como un embudo: primero las excepciones finas, al final la regla general de bloqueo.

Buenas prácticas con reglas: dales nombres o comentarios que expliquen para qué sirven ("permitir SSH solo desde la oficina"); revisa la lista cada pocos meses y elimina reglas de proyectos que ya terminaron (las reglas olvidadas son puertas olvidadas); nunca abras un puerto "para probar" y lo dejes abierto; restringe los servicios de administración a IPs específicas en vez de abrirlos al mundo; y lleva un registro de cambios, aunque sea un archivo de texto con fecha y motivo. En empresas grandes esto es obligatorio por auditoría; en tu casa te salva cuando dentro de seis meses te preguntes "por qué abrí este puerto".

Analogía final para cerrar el tema: un firewall bien configurado es como un buen portero de antro: conoce la lista, revisa identificaciones, no deja entrar al que viene agresivo, y si alguien de adentro quiere salir a fumar y volver a entrar, lo reconoce porque ya estaba anotado (stateful). Un firewall mal configurado es el portero que deja pasar a todo el que sonríe.

VPNs y túneles seguros: tu autopista privada por internet

VPN significa Red Privada Virtual (Virtual Private Network). Es una tecnología que crea un "túnel" cifrado entre tu dispositivo e internet (o entre tu dispositivo y la red de tu empresa), de modo que todo lo que viaja por ese túnel va protegido aunque la red por dónde pasa no sea confiable.

La analogía del túnel es literalmente la mejor: imagina que internet es una avenida llena de gente y tú necesitas llevar documentos confidenciales de tu casa a la oficina. Sin VPN, los llevas en las manos a la vista de todos: cualquiera puede leerlos por encima de tu hombro. Con VPN, los metes en un tubo sellado y blindado que va directo de tu casa a la oficina: la gente ve el tubo pasar, pero no puede ver ni tocar lo que va adentro. Técnicamente, la VPN toma tus paquetes, los cifra y los mete dentro de otros paquetes que viajan hasta el servidor VPN, donde se descifran y siguen su camino normal.

Qué te da una VPN y que no te da. Si te da: confidencialidad en redes no confiables (nadie en el café puede leer tu tráfico), ocultamiento de tu IP real ante los sitios que visitas (ven la IP del servidor VPN), y acceso a redes privadas como si estuvieras físicamente ahí (por eso las empresas la exigen para el trabajo remoto: tu computadora "entra" a la red de la oficina por el túnel). Que no te da: no te hace invisible ni anónimo total (el proveedor de VPN si puede ver tu tráfico si quisiera, y los sitios te siguen rastreando con cookies), no te protege del malware ni del phishing (el túnel protege el camino, no lo que haces al llegar), y no te protege si el servidor VPN mismo es malicioso. Por eso importa elegir bien al proveedor.

El corazón de la VPN es el cifrado. Cifrar es transformar tu información en un revoltijo ilegible usando una llave matemática, de modo que solo quien tenga la llave pueda leerla. Hay dos tipos que debes conocer. El cifrado simétrico usa la misma llave para cifrar y descifrar: rápido, ideal para grandes volúmenes de datos (es lo que protege el túnel una vez establecido). El cifrado asimétrico usa una pareja de llaves: una pública (que todos pueden conocer) y una privada (que solo tú guardas). Lo que se cifra con la pública solo se descifra con la privada, y viceversa. Es más lento pero resuelve el problema de "cómo nos ponemos de acuerdo en la llave sin que nadie nos escuche": se usa al inicio para intercambiar de forma segura la llave simétrica que luego protegerá todo. Así funcionan en equipo: el asimétrico hace la presentación segura y el simétrico hace el trabajo pesado. Cuando escuches "AES-256", es un algoritmo simétrico muy fuerte y es el estándar actual; cuando escuches "RSA" o "intercambio Diffie-Hellman", son piezas del mundo asimétrico.

Protocolos de VPN: son las "recetas" que definen cómo se construye el túnel. Los tres que debes conocer:

IPsec es el veterano corporativo. En realidad es un conjunto de protocolos que trabaja a nivel de red (capa 3), lo que significa que protege todo el tráfico del equipo sin que las aplicaciones se enteren. Es el que usan la mayoría de las VPNs empresariales para conectar oficinas entre sí (túneles sitio a sitio) y para acceso remoto. Es muy seguro y está probado por décadas, pero configurarlo a mano es complejo; por eso normalmente lo configuran los equipos de sistemas, no el usuario final.

OpenVPN es el favorito del mundo abierto. Es de código abierto (cualquiera puede revisar su código buscando errores, lo cuál es una ventaja de seguridad), muy configurable y funciona sobre TCP o UDP, incluso sobre el puerto 443, lo que le permite pasar por casi cualquier firewall porque "parece" tráfico web normal. Muchos proveedores de VPN comerciales y muchos routers lo soportan. Su desventaja es que puede ser más lento que las opciones modernas y su configuración también requiere cierto conocimiento.

WireGuard es el nuevo estándar ligero. Tiene un código muchísimo más pequeño que los anteriores (unas 4,000 líneas contra cientos de miles), lo que significa menos lugares donde esconderse un error y auditorías más fáciles. Es rapidísimo, se reconecta al instante cuando cambias de red (ideal en el teléfono cuando pasas de WiFi a datos) y su configuración es sorprendentemente simple. Cada vez más proveedores y empresas lo adoptan. Si vas a montar tu propia VPN hoy, WireGuard suele ser la recomendación por defecto.

VPN personal contra VPN corporativa: no son lo mismo aunque usen la misma tecnología. La VPN personal (las que anuncian en YouTube) la contratas tú para proteger tu tráfico en redes públicas y cambiar tu ubicación aparente. Ojo crítico: estás moviendo tu confianza del café al proveedor de VPN; elige uno con política clara de no guardar registros, buena reputación y auditorías independientes, y desconfía de las VPN "gratis": si no pagas con dinero, pagas con tus datos. La VPN corporativa la provee tu empresa para que trabajes desde casa como si estuvieras en la oficina: el túnel termina en los servidores de la empresa y desde ahí sales a internet con sus filtros y sus reglas. Cuando tu trabajo te pide instalar "la VPN de la empresa", es esto: no es para espiarte por gusto, es para que los recursos internos (sistemas, archivos, impresoras) solo sean accesibles por el túnel cifrado y no queden expuestos a internet.

Error común de principiante: pensar que la VPN reemplaza al antivirus o que "con VPN ya nadie me puede hackear". La VPN protege el camino; si tú descargas un troyano o caes en un phishing, el ataque viaja cómodamente por tu túnel cifrado. La seguridad siempre es por capas.

HTTPS, TLS y certificados: el candadito explicado

Cuándo entras a tu banco en el navegador ves un candadito y la dirección empieza con https. Esa "s" es de "secure" y significa que tu conexión con ese sitio viaja cifrada con TLS (Transport Layer Security, el sucesor del viejo SSL). TLS hace por la web lo mismo que la VPN hace por toda tu conexión: crea un túnel cifrado, pero solo entre tu navegador y ese sitio específico.

Cómo funciona, en versión sencilla: tu navegador le dice al servidor "quiero hablar seguro"; el servidor le muestra su certificado digital, que es como su identificación oficial: dice "yo soy

realmente banco-ejemplo.com" y viene firmado por una autoridad certificadora (CA) en la que tu navegador confiá. Tu navegador verifica la firma; si todo cuadra, ambos negocian una llave de sesión usando cifrado asimétrico y de ahí en adelante hablan cifrado con cifrado simétrico rápido. Todo esto pasa en milisegundos antes de que veas la página.

El certificado es la pieza clave contra el MitM: si un atacante intenta interceptar tu conexión al banco, no puede presentar un certificado válido para ese dominio y tu navegador te mostrará una advertencia aterradora a pantalla completa. Por eso la regla de oro: nunca ignores una advertencia de certificado ni hagas clic en "continuar de todos modos" en sitios donde metas contraseñas o datos bancarios. Esa advertencia es tu navegador gritandote que algo está mal.

Qué te protege HTTPS y que no. Si te protege: que nadie en el camino (tu proveedor de internet, el dueño del WiFi del café, un atacante en la red) lea o modifique lo que intercambias con ese sitio. No te protege: de qué el sitio mismo sea falso (un sitio de phishing también puede tener su candadito: el candado solo dice que la conexión es privada, no que el dueño sea honesto), ni de qué el sitio sea legítimo pero vulnerable o malicioso. Moraleja: el candadito es necesario pero no suficiente; verifica siempre el dominio letra por letra.

Para quién administre un sitio o servicio: conseguir un certificado hoy es gratis y fácil gracias a Let's Encrypt, una autoridad certificadora gratuita y automatizada. No hay excusa para tener un sitio sin HTTPS en estos tiempos; los navegadores marcan como "no seguro" a los sitios sin cifrado y los usuarios desconfían con razón.

Buenas prácticas: los hábitos que sostienen todo

La tecnología de seguridad falla si los hábitos son malos. Estas cuatro prácticas son el cimiento; sin ellas, ni el mejor firewall te salva.

Primero, actualizaciones. Cada actualización de seguridad cierra vulnerabilidades que los atacantes ya están explotando. El gusano WannaCry entro por una falla para la que Microsoft ya había publicado parche meses antes: las víctimas eran equipos sin actualizar. Activa las actualizaciones automáticas en tu sistema operativo, tu navegador y tus aplicaciones, y actualiza el firmware de tu router (mucha gente jamás lo hace y su router queda con fallas conocidas por años). Piensa en las actualizaciones como las vacunas: molestan un poco, pero previenen desastres.

Segundo, contraseñas fuertes y únicas. Una contraseña fuerte es larga (mínimo 12 caracteres, mejor 16 o más) y única por sitio: si un sitio es hackeado y roban su base de datos, los atacantes prueban esas mismas contraseñas en bancos, correos y redes sociales (a esto se le llama "credential stuffing"). Las reglas viejas de "una mayúscula, un número y un símbolo" importan menos que la longitud: una frase de cuatro palabras aleatorias es más fuerte y más

fácil de recordar que una contraseña corta y enredada. Ejemplo: "caballo batería mapa trueno" es mejor que "P@ssw0rd1". Pero no intentes memorizar 50 contraseñas: usa un gestor de contraseñas (hay opciones gratuitas y de código abierto) que las genere y las guarde por ti; tu solo memorizas una contraseña maestra fuerte. Y jamás reutilices la contraseña de tu correo en otros sitios: tu correo es la llave maestra porque con él recuperas todas las demás cuentas.

Tercero, doble factor de autenticación (2FA). Es pedir dos pruebas distintas para entrar: algo que sabes (tú contraseña) más algo que tienes (un código de tu teléfono) o algo que eres (tu huella). Así, aunque un phisher robe tú contraseña, no puede entrar sin el segundo factor. Actívalo en tu correo, tu banco, tus redes sociales y tu trabajo: en ese orden de prioridad. Prefiere una app autenticadora o una llave física de seguridad sobre los códigos por SMS, porque los SMS pueden ser interceptados con técnicas de duplicado de SIM. El 2FA es la medida individual más efectiva que existe contra el robo de cuentas: actívalo hoy mismo en tu correo si aún no lo tienes.

Cuarto, respaldos (backups). La regla 3-2-1: tres copias de tu información importante, en dos tipos de medio distintos, y una copia fuera de tu casa u oficina (en la nube o en un disco en otro lugar). Por qué: el ransomware cifra tus archivos, un robo se lleva tu computadora, una inundación dana tus discos. Con respaldos automáticos y probados, cualquiera de esos desastres se convierte en un mal rato en vez de una tragedia. "Probados" es la palabra clave: un respaldo que nunca restauraste es solo una esperanza; verifica cada cierto tiempo que tus copias realmente se pueden recuperar. Para fotos familiares y documentos importantes, un servicio en la nube con historial de versiones es una excelente red de seguridad.

Bonus que vale oro: principio de mínimo privilegio. En tu computadora no navegues todos los días como administrador; usa una cuenta de usuario normal y la de administrador solo para instalar cosas. En el trabajo, cada persona y cada sistema debe tener solo los permisos que necesita y nada más. Así, si una cuenta se compromete, el daño queda contenido. Es la misma lógica de la segmentación aplicada a las personas.

Plan de respuesta a incidentes: que hacer cuando ya paso

Por más defensas que pongas, algún día algo va a fallar: un empleado abrirá un phishing, un servidor quedará expuesto, un proveedor será comprometido. La diferencia entre un incidente controlado y un desastre no es la suerte, es tener un plan escrito antes de que pase. Los profesionales lo llaman "plan de respuesta a incidentes" y sus fases son siempre las mismas.

Primera fase, preparación: ten lista tú lista de contactos (quién decide, quién ejecuta, a quién avisar), tus respaldos probados, y tus herramientas (un USB de arranque con antivirus, acceso a los registros del firewall). Un plan guardado solo en la computadora que se infectó no sirve: ten una copia impresa o en otro lugar.

Segunda fase, detección y análisis: confirma que el incidente es real y mide su alcance. Que equipos están afectados, que datos tocaron, como entro. Los registros del firewall, del antivirus y del sistema son tus testigos: aprende a leerlos antes de necesitarlos.

Tercera fase, contención: frena el sangrado. Desconecta equipos de la red, bloquea cuentas comprometidas, aísla segmentos. Hay contención corta (desconectar ya) y larga (mantener servicios críticos funcionando de forma limitada mientras limpias). No brinques a borrar todo todavía: primero contiene.

Cuarta fase, erradicación: elimina la causa raíz. Limpia el malware, cierra la vulnerabilidad, cambia credenciales comprometidas, parchea lo que permitió la entrada. Si solo limpias los síntomas sin cerrar la puerta, el atacante vuelve a entrar por la misma puerta.

Quinta fase, recuperación: restaura sistemas y datos desde respaldos limpios, vuelve a conectar por etapas y monitorea de cerca por si quedo algo escondido. Verifica que todo funcione antes de declarar victoria.

Sexta fase, lecciones aprendidas: reune con los involucrados y pregunta sin buscar culpables: que salió bien, que salió mal, que cambiamos. Actualiza el plan con lo aprendido. Esta fase es la que convierte un incidente en una inversión: cada ataque te deja más fuerte si documentas y mejoras.

Dos reglas de oro para incidentes: nunca pagues un rescate como primera opción (financia el crimen y no garantiza nada), y nunca ocultes un incidente que afecte datos de terceros (en muchos países hay obligación legal de avisar). La transparencia a tiempo duele menos que el escándalo después.

Ejemplos paso a paso

La seguridad se aprende haciendo. En esta sección vas a configurar un firewall básico, revisar reglas, verificar un certificado y armar un respaldo automático. Todos son ejemplos defensivos para tus propios equipos. Lee cada bloque línea por línea: no copies y pegues a ciegas, entiende que hace cada instrucción.

Ejemplo 1: firewall básico en Linux con UFW

UFW (Uncomplicated Firewall) es la forma sencilla de manejar el firewall en Ubuntu y derivados. Vamos a dejar un servidor con política de denegar por defecto y abrir solo lo necesario: SSH para administrarlo y HTTP/HTTPS si es un servidor web.

```
# Ver el estado actual del firewall
sudo ufw status verbose

# Política por defecto: denegar todo el tráfico entrante
sudo ufw default deny incoming

# Política por defecto: permitir todo el tráfico saliente
# (tu servidor necesita salir a internet para actualizarse)
sudo ufw default allow outgoing

# Permitir SSH, pero solo desde la IP de tu oficina o tu casa
# Cambia 203.0.113.25 por tu IP real
sudo ufw allow from 203.0.113.25 to any port 22 proto tcp

# Permitir tráfico web para todo el mundo (es un servidor web público)
sudo ufw allow 80/tcp
sudo ufw allow 443/tcp

# Activar el firewall (te pedirá confirmación)
sudo ufw enable

# Revisar las reglas finales, en orden de evaluación
sudo ufw status numbered
```

Línea por línea: primero vemos el estado para saber desde dónde partimos. Luego fijamos "deny incoming" como política por defecto: todo lo no permitido explícitamente se bloquea (el principio de denegar por defecto). "allow outgoing" deja que el servidor inicie conexiones hacia afuera, necesario para descargar actualizaciones. La regla de SSH es la más importante: en vez de abrir el puerto 22 al mundo entero, lo restringimos a una sola IP de confianza; así los bots que escanean internet no pueden ni intentar adivinar tu contraseña. Los puertos 80 y 443 se abren a todos porque el servidor web debe ser público. Finalmente activamos y revisamos la lista numerada para confirmar el orden: las reglas específicas aparecen antes de la política general de denegación.

Si metiste la pata y te bloqueaste, la mayoría de los proveedores de nube ofrecen una consola web de emergencia para entrar y corregir con "sudo ufw delete" seguido del número de regla. Por eso conviene probar primero en una máquina virtual local.

Ejemplo 2: lo mismo con iptables, regla por regla

UFW por dentro usa iptables (o nftables en sistemas nuevos). Ver las reglas crudas te ayuda a entender qué pasa realmente. Este ejemplo muestra el concepto de conexión stateful:

```
# Ver las reglas actuales con numeros de linea
sudo iptables -L INPUT -n --line-numbers -v

# Permitir el trafico de la interfaz local (localhost)
sudo iptables -A INPUT -i lo -j ACCEPT

# Permitir las respuestas a conexiones que TU iniciaste (stateful)
# ESTABLISHED,RELATED significa: "esto es respuesta a algo legitimo"
sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

# Permitir SSH solo desde tu red de administracion
sudo iptables -A INPUT -p tcp -s 203.0.113.0/24 --dport 22 -j ACCEPT

# Bloquear (DROP en silencio) todo lo demas que llegue a INPUT
sudo iptables -A INPUT -j DROP
```

La segunda regla es la magia stateful: cuando tu servidor pide una actualización a internet, la respuesta puede entrar porque el firewall recuerda que tú la pediste. Sin esa regla, o abres todo, o nada funciona. La última regla es el "denegar por defecto" hecho a mano. Nota que el orden importa: si pusieras el DROP antes de las reglas de permitir, nada entraría jamás.

Ejemplo 3: reglas básicas en el Firewall de Windows

En Windows no necesitas la terminal para lo esencial, pero la línea de comandos sirve para documentar y repetir. Con PowerShell:

```
# Ver el estado de los tres perfiles (dominio, privada, publica)
Get-NetFirewallProfile | Select-Object Name, Enabled, DefaultInboundAction

# Bloquear por defecto el trafico entrante en el perfil publico
Set-NetFirewallProfile -Name Public -DefaultInboundAction Block

# Crear una regla que permite RDP solo desde la red de la oficina
New-NetFirewallRule -DisplayName "RDP solo oficina" -Direction Inbound `
  -Protocol TCP -LocalPort 3389 -RemoteAddress 203.0.113.0/24 -Action Allow

# Listar las reglas que permiten trafico entrante, para auditar
Get-NetFirewallRule -Direction Inbound -Action Allow |
  Select-Object DisplayName, Enabled | Sort-Object DisplayName
```

En redes públicas (el WiFi del aeropuerto), Windows debe estar en perfil "Público" con entrante bloqueado: así tu laptop no ofrece servicios a desconocidos. La última instrucción es tu auditoría periódica: revisa que reglas permiten entrada y elimina las que ya no necesites.

Ejemplo 4: verificar el certificado de un sitio con OpenSSL

Cuándo tu navegador se queja de un certificado, puedes inspeccionarlo tu mismo. Este comando se conecta a un sitio y muestra su certificado:

```
# Pedir el certificado de un sitio y ver sus datos principales
echo | openssl s_client -connect www.ejemplo.com:443 -servername www.ejemplo.com
2>/dev/null |
  openssl x509 -noout -subject -issuer -dates

# Salida de ejemplo (datos inventados):
# subject=CN = www.ejemplo.com
# issuer=C = US, O = Let's Encrypt, CN = R10
# notBefore=Sep  1 00:00:00 2026 GMT
# notAfter=Nov 30 23:59:59 2026 GMT
```

Qué lees aquí: "subject" debe coincidir con el dominio que visitaste (si dice otro nombre, algo anda mal); "issuer" te dice que autoridad lo firmó (Let's Encrypt es legítima y gratuita); "notBefore/notAfter" son las fechas de vigencia (un certificado vencido o aún no válido dispara advertencias). Si el issuer dice algo extraño como "MiEmpresa-Proxy" en tu casa, alguien podría estar interceptando tu tráfico.

Ejemplo 5: respaldo automático sencillo en Linux

Un respaldo que depende de tu memoria no es un respaldo. Este script copia tu carpeta de documentos a un disco externo con fecha, y lo programas para que corra solo:

```
# Script: ~/respaldo.sh
#!/bin/bash
FECHA=$(date +%Y-%m-%d)
DESTINO="/media/disco-externo/respaldos"
mkdir -p "$DESTINO"
# rsync copia solo lo que cambio desde el ultimo respaldo
rsync -av --delete ~/Documentos/ "$DESTINO/documentos-$FECHA/"
echo "Respaldo del $FECHA terminado" >> ~/respaldo.log

# Darle permiso de ejecucion
chmod +x ~/respaldo.sh

# Programarlo cada domingo a las 3 am con cron
crontab -e
# Agregar esta linea dentro del editor de cron:
# 0 3 * * 0 /home/tu-usuario/respaldo.sh
```

rsync con "-av" copia en modo archivo preservando permisos y en modo detallado; "--delete" borra del respaldo lo que tú borraste (cuidado: si un ransomware cifra tus archivos y el respaldo sincroniza, también cifra la copia; por eso la regla 3-2-1 pide además una copia desconectada o con versiones). La línea de cron "0 3 * * 0" significa minuto 0, hora 3, cualquier día del mes, cualquier mes, día 0 de la semana (domingo). Cambia "tu-usuario" por tu nombre de usuario real.

Ejemplo 6: generar una contraseña fuerte con la terminal

En vez de inventar contraseñas, genera una frase larga aleatoria:

```
# Generar 5 palabras aleatorias del diccionario como frase de paso
shuf -n 5 /usr/share/dict/words | tr '\n' ' '

# Salida de ejemplo:
# trueno mapa bateria caballo rio

# O una cadena aleatoria de 20 caracteres
openssl rand -base64 15
# Salida de ejemplo:
# k9Xm2pQvR7tYw4ZaB
```

La frase de cinco palabras es fácil de recordar y muy difícil de adivinar por fuerza bruta por su longitud. Usala como base y no la reutilices entre sitios: para eso está el gestor de contraseñas.

Práctica

1. Auditoría de phishing: analiza este mensaje como si lo hubieras recibido. "De: seguridad@banc0nacional-seguro.com | Asunto: URGENTE: tu cuenta será suspendida en 24 horas | Cuerpo: Estimado cliente, detectamos actividad sospechosa. Verifica tu identidad aquí: <http://bit.ly/verifica-cuenta-ya> | Atentamente, Departamento de Seguridad." Enumera al menos cinco señales de alerta y explica que harías paso a paso en vez de hacer clic.

SOLUCIÓN: Señales de alerta: 1) Urgencia artificial: "será suspendida en 24 horas" busca que actúes sin pensar. 2) Remitente sospechoso: "banc0nacional-seguro.com" usa un cero en vez de la letra o y agrega "-seguro", no es el dominio oficial del banco. 3) Saludo genérico: "Estimado cliente" en vez de tu nombre; tu banco real te llama por tu nombre. 4) Enlace acortado: "bit.ly" oculta el destino real; un banco legítimo no usa acortadores para temas de seguridad. 5) El enlace usa "http" y no el dominio del banco. Que hacer paso a paso: primero, no hagas clic ni descargues nada. Segundo, abre tu navegador y escribe tu mismo la dirección del banco o usa su app oficial para revisar si hay algún aviso real. Tercero, si quieres confirmar, llama al número oficial del banco (el de tu tarjeta, no el del correo). Cuarto, marca el mensaje como phishing en tu correo y elimínalo. Quinto, si por error ya hiciste clic y diste datos, cambia tu contraseña de inmediato desde el sitio oficial, revisa movimientos y avisa al banco. Lección: ante la duda, verifica por un canal distinto al que te llegó el mensaje.

2. Configura el firewall de tu propia computadora con política de denegar por defecto. En Linux usa UFW, en Windows usa el Firewall de Windows con PowerShell, en macOS usa

el firewall del sistema. Documenta: que reglas dejaste, por qué cada una es necesaria, y que servicios decidiste no abrir. Luego verifica con un escaneo local que solo estén abiertos los puertos que autorizaste.

SOLUCIÓN: En Linux (Ubuntu): ejecuta "sudo ufw default deny incoming" y "sudo ufw default allow outgoing", luego "sudo ufw enable". Si no necesitas compartir archivos ni impresoras en red, no abras nada más: tu computadora puede navegar y actualizarse sin puertos entrantes abiertos, gracias a la regla stateful implícita que permite las respuestas. Si usas SSH para administrarla desde tu red local, abre solo el puerto 22 restringido a tu red: "sudo ufw allow from 192.168.1.0/24 to any port 22 proto tcp". Documenta cada regla en un archivo de texto con fecha y motivo, por ejemplo: "2026-09-19: abierto 22/tcp solo para 192.168.1.0/24, administración desde laptop". Para verificar, desde otra computadora de tu red ejecuta "nmap 192.168.1.X" (cambia X por tu IP) y confirma que solo aparezcan los puertos autorizados; todo lo demás debe aparecer como "filtered". En Windows: pon el perfil de red en "Público" cuando estes fuera de casa y crea reglas de entrada solo para lo indispensable, listandolas con "Get-NetFirewallRule -Direction Inbound -Action Allow" para auditar. Lección: un firewall con todo cerrado por defecto y excepciones justificadas es cien veces más seguro que uno con todo abierto "por si acaso".

3. Diseña el plan anti-ransomware para tu casa o para un pequeño negocio. Debe incluir: la regla 3-2-1 de respaldos aplicada a datos concretos (que se respalda, a dónde, cada cuando), como evitarías que el ransomware cifre también los respaldos, y que harías en las primeras dos horas después de descubrir el ataque.

SOLUCIÓN: Inventario de datos: documentos de trabajo o escuela, fotos familiares, base de datos de clientes, correos importantes. Regla 3-2-1 aplicada: copia 1 en la computadora; copia 2 en un disco externo que solo se conecta durante el respaldo y luego se desconecta (así el ransomware no lo alcanza); copia 3 en un servicio de nube con historial de versiones (si el ransomware cifra los archivos sincronizados, restauras una versión anterior). Frecuencia: documentos de trabajo diario automático, fotos semanal. Para qué el ransomware no cifre los respaldos: el disco externo permanece desconectado excepto durante la ventana de respaldo; la nube debe tener versiones e idealmente inmutabilidad o papelera con retención; jamás mapees el disco de respaldo como unidad de red permanente. Primeras dos horas del incidente: 1) no pagues el rescate de inmediato (pagar no garantiza recuperar nada y financia el crimen). 2) Desconecta los equipos infectados de la red pero no los apagues (apagar puede borrar evidencia útil). 3) Identifica el alcance: que equipos y que archivos están cifrados. 4) Avisa a tu equipo o familia y cambia contraseñas importantes desde un equipo limpio. 5) Limpia los equipos con antivirus desde un medio de arranque confiable o reinstalando

el sistema. 6) Restaura desde el respaldo más reciente anterior al ataque y verifica que los archivos abran bien. 7) Investiga como entro (correo, USB, servicio expuesto) y cierra esa puerta. Lección: con respaldos 3-2-1 probados, el ransomware pasa de ser una tragedia a ser un fin de semana de trabajo.

4. Una pequeña oficina tiene: 10 computadoras de empleados, 1 servidor con el sistema de cobro, 1 red WiFi para clientes que esperan, y 2 cámaras de seguridad. Todo está hoy en una sola red 192.168.1.0/24 sin firewall interno. Identifica al menos cuatro riesgos concretos de este diseño y propone una segmentación con zonas y reglas de firewall entre ellas.

SOLUCIÓN: Riesgos: 1) Un cliente en el WiFi puede escanear la red y llegar al servidor de cobro o a las computadoras de empleados. 2) Si una computadora de empleado se infecta por phishing, el malware se propaga sin obstáculos al servidor de cobro. 3) Las cámaras, que suelen tener contraseñas de fábrica débiles, son puerta de entrada a toda la red. 4) No hay forma de aplicar políticas distintas: lo que necesita el cobro (máxima restricción) convive con lo que necesitan los clientes (internet abierto). Segmentación propuesta: VLAN 10 empleados (192.168.10.0/24), VLAN 20 invitados (192.168.20.0/24), VLAN 30 servidores/cobro (192.168.30.0/24), VLAN 40 cámaras (192.168.40.0/24). Reglas entre zonas: invitados solo pueden salir a internet, nada hacia las demás VLANs; empleados pueden salir a internet e iniciar conexiones hacia servidores, pero los servidores no pueden iniciar conexiones hacia empleados (solo responder); cámaras solo pueden hablar con el grabador de video, nada de internet directo; el servidor de cobro acepta conexiones únicamente desde las computadoras de caja por los puertos del sistema de cobro, y su administración remota solo desde una IP específica por VPN. Además: cambiar todas las contraseñas de fábrica de las cámaras y activar actualizaciones automáticas donde sea posible. Lección: segmentar convierte "un equipo infectado" en "un problema contenido" en vez de "toda la empresa comprometida".

5. Haz una auditoría de tus propias cuentas: lista tus cinco cuentas más importantes (correo principal, banco, red social principal, trabajo o escuela, almacenamiento en la nube) y verifica en cada una: si la contraseña es única y larga, si tiene 2FA activado y de que tipo, y cuando fue la última vez que la cambiaste. Migra las contraseñas a un gestor y activa 2FA donde falte. Documenta el antes y el después.

SOLUCIÓN: Tabla de ejemplo del "antes": correo: contraseña reutilizada en tres sitios, sin 2FA, cambiada hace dos años; banco: contraseña única pero corta, 2FA por SMS; red social: misma contraseña del correo, sin 2FA; trabajo: contraseña única larga, 2FA con app (bien); nube: contraseña única, sin 2FA. Plan de acción: 1) Instala un gestor de

contraseñas reconocido y crea tú contraseña maestra como frase larga de cinco palabras. 2) Empezando por el correo (es la llave maestra de todas las recuperaciones), genera una contraseña nueva de 16+ caracteres y actívala junto con 2FA por app autenticadora; guarda los códigos de respaldo en papel en un lugar seguro. 3) Repite con banco, nube, red social y trabajo. 4) En cada sitio revisa las sesiones activas y cierra las que no reconozcas. 5) Guarda en el gestor también las respuestas a preguntas de seguridad tratándolas como contraseñas (nadie necesita saber el verdadero nombre de tu primera mascota: genera respuestas aleatorias). El "después": cinco cuentas con contraseñas únicas de 16+ caracteres, 2FA por app en todas, sesiones desconocidas cerradas. Lección: la mayoría de los "hackeos" de cuentas son en realidad contraseñas reutilizadas y sin segundo factor; esta auditoría elimina de raíz ese riesgo.

6. Ejercicio de mesa: eres el encargado de sistemas y el lunes a las 8 am tres empleados reportan que sus archivos tienen extensión rara y hay un mensaje de rescate en pantalla. Escribe tú lista de acciones ordenadas para las primeras cuatro horas, indicando que haces, en qué orden y por qué, sin pagar el rescate.

SOLUCIÓN: Hora 0 a 0:30, contención: desconecta de la red (cable y WiFi) los tres equipos y cualquier otro con síntomas; no los apagues para no perder evidencia volátil; avisa a todo el personal que no abra archivos ni conecte USBs. Hora 0:30 a 1:30, evaluación: identifica la variante del ransomware por el mensaje y la extensión (hay sitios con bases de datos de variantes y algunas tienen descifradores gratuitos); determina el alcance revisando respaldos y preguntando por más síntomas; revisa cómo pudo entrar (correos recientes, USBs, accesos remotos). Hora 1:30 a 3:00, erradicación: pasa antivirus actualizado desde USB de arranque en los equipos afectados o reinstala el sistema operativo desde cero en los más comprometidos; cambia las contraseñas de cuentas importantes desde un equipo limpio; cierra la puerta de entrada (bloquea el remitente del phishing, cierra el puerto expuesto, parchea la vulnerabilidad). Hora 3:00 a 4:00, recuperación: restaura los archivos desde el respaldo más reciente anterior al ataque y verifica que abran correctamente; vuelve a conectar los equipos por grupos, monitoreando; documenta todo con fechas para el reporte. Después: lecciones aprendidas con el equipo, capacitación anti-phishing y revisión del plan de respaldos. Por qué esté orden: primero se frena el sangrado (contención), luego se entiende el problema (evaluación), luego se elimina la causa (erradicación) y al final se vuelve a operar (recuperación). Hacerlo al revés, como restaurar antes de limpiar, garantiza reinfectarse. Lección: en incidentes, el orden importa tanto como las acciones; un checklist escrito evita decisiones de pánico.

Resumen de la unidad

En esta unidad aprendiste que la seguridad de redes no es un producto que se compra, sino una forma de pensar y un conjunto de capas que trabajan juntas. Del lado de las amenazas, ahora distingues el malware por sus tipos: virus que necesitan que los ejecutes, gusanos que se propagan solos por la red, troyanos disfrazados de software legítimo, spyware que roba en silencio y ransomware que cifra tus archivos para extorsionarte. Sabes reconocer las señales de infección y, más importante, sabes prevenirlas: antivirus activo, todo actualizado, descargas solo de sitios oficiales y respaldos regulares.

Aprendiste que el eslabón más atacado no es la tecnología sino la persona: la ingeniería social y el phishing. Ya tienes tu checklist mental: urgencia artificial, remitentes falsos, dominios parecidos, enlaces acortados y peticiones extrañas. Y tienes el antídoto: desconfiar por defecto, verificar por otro canal y activar el doble factor en todo lo importante. Recuerda la lección de humildad: nadie es inmune al engaño, la verificación es para todos.

En ataques de red conociste el escaneo de puertos (el reconocimiento previo), el hombre en el medio (la interceptación en redes no confiables), el DDoS (la saturación que tumba servicios) y la suplantación ARP (el engaño dentro de la red local). Para cada uno sabes cómo se reconoce y cómo se previene, y tienes clara la línea ética: probar en tu laboratorio con permiso está bien; atacar sistemas ajenos es delito.

Del lado de la defensa dominas los firewalls: que son, la diferencia entre firewall de red y de host, por qué los stateful son superiores a los stateless, y como las zonas (LAN, WAN, DMZ) y la segmentación limitan el daño cuando algo falla. Sabes escribir reglas con el principio de denegar por defecto, cuidar el orden de evaluación y auditar tu configuración periódicamente. Y sabes que el firewall es una capa, no toda la armadura.

En conectividad segura entiendes las VPNs: el túnel cifrado, la diferencia entre cifrado simétrico y asimétrico, los protocolos IPsec, OpenVPN y WireGuard, y la diferencia entre una VPN personal y la corporativa que te pide tu trabajo. Entiendes HTTPS y TLS: que significa el candadito, para qué sirven los certificados y por qué jamás debes ignorar una advertencia de certificado en un sitio importante.

Finalmente, tienes los cuatro hábitos que sostienen todo: actualizaciones automáticas, contraseñas largas y únicas con gestor, doble factor de autenticación empezando por tu correo, y respaldos con la regla 3-2-1 probados de verdad. Más el principio de mínimo privilegio como filosofía general.

La próxima unidad cambia de ritmo: dejamos la defensa y tomamos las herramientas del diagnóstico. Cuando algo falle en una red, y va a fallar, sabrás exactamente por dónde empezar a buscar. Nos vemos en la Unidad 10.

Un último consejo antes de cerrar: la seguridad es un hábito, no un proyecto con fecha de entrega. Agenda en tu calendario una revisión trimestral: actualizaciones al día, reglas del firewall auditadas, respaldos probados y 2FA activado en tus cuentas clave. Treinta minutos cada tres meses te ahorran el peor lunes de tu vida. La red segura no es la que nunca es atacada, es la que está lista cuando el ataque llega, y la que se recupera rápido después de él.

UNIDAD 10: Diagnóstico y resolución de problemas

Hay una verdad que todo profesional de redes aprende tarde o temprano: las redes fallan. No importa que tan bien disenes todo, algun dia algo va a dejar de funcionar. El internet se "cae", una página no abre, la videollamada se congela, el servidor no responde. Y cuando eso pasa, hay dos tipos de personas: las que reinician todo a ver si se arregla solo, y las que diagnostican. Esta unidad es para que seas del segundo tipo.

Diagnosticar es el arte de encontrar la causa real de un problema siguiendo un método, en vez de adivinar. Piensa en un doctor: cuando llegas con fiebre no te opera de inmediato; te pregunta síntomas, te toma la temperatura, te manda análisis y va descartando causas de lo más simple a lo más complejo. En redes hacemos exactamente lo mismo con herramientas que ya tienes en tu computadora: ping, ipconfig, traceroute, nslookup, netstat y compañías. Son gratis, vienen instaladas, y un técnico que las domina resuelve en diez minutos lo que a otro le toma todo el día.

Por qué importa esto para ti. Primero, porque es la habilidad más práctica de todo el curso: la teoría de las unidades anteriores cobra sentido cuando la usas para cazar un problema real. Segundo, porque en cualquier trabajo donde toques computadoras o redes, "se cayó el internet" va a ser la frase que más escuches, y quien sabe diagnosticar se vuelve indispensable. Tercero, porque te ahorra dinero y corajes en tu propia casa: la próxima vez que tu WiFi falle, en vez de llamar al técnico y esperar tres días, vas a saber decirle exactamente dónde está el problema, o mejor aún, lo vas a arreglar tu.

En esta unidad vas a ver tres bloques. En la clase 28 estudiamos los comandos básicos de diagnóstico: ping (que mide y como leer su salida, incluyendo el TTL), ipconfig, ifconfig e ip addr para leer tu propia configuración, y tracert/traceroute para ver la ruta que siguen tus paquetes salto por salto. En la clase 29 sumamos más herramientas: nslookup y dig para interrogar al DNS, netstat y ss para ver conexiones y puertos abiertos, arp para revisar la tabla ARP, y pathping y mtr que combinan lo mejor de ping y traceroute. Vas a leer salidas reales y a interpretarlas como un profesional. En la clase 30 entramos a Wireshark, el analizador de paquetes más famoso del mundo: qué es, como hacer una captura básica y como usar filtros simples como "dns" o "tcp.port == 80". Y cerramos con lo más valioso de la unidad: una metodología de resolución de problemas basada en el modelo de capas, de abajo hacia arriba, con un checklist práctico (capa física, dirección IP, puerta de enlace, DNS) y la disciplina de documentar cada problema.

Una nota sobre el enfoque: diagnosticar no es adivinar más rápido, es descartar con método. La mayoría de los problemas de red son tontos: un cable suelto, una IP mal puesta, un DNS caído. El método de abajo hacia arriba que vas a aprender existe precisamente para atrapar esos problemas tontos en los primeros cinco minutos, antes de que te metas a cazar fantasmas en configuraciones avanzadas. Empecemos por la herramienta más famosa de todas.

Un detalle que te ayudará a aprovechar esta unidad al máximo: ten tu computadora a la mano mientras lees y ejecuta cada comando que veas. La lectura te da la teoría, pero el diagnóstico se aprende con los dedos en el teclado: ver tu propia puerta de enlace responder al ping, leer tu propia tabla ARP o capturar tus propios paquetes DNS convierte estos conceptos en reflejos. Cada ejemplo de esta unidad está diseñado para que lo repliques en tu red casera sin riesgo alguno, porque todas son herramientas de lectura y prueba, no de modificación ni de ataque. si algo sale distinto a lo que describe el libro, mejor todavía: acabas de encontrar tu primer caso real para diagnosticar de verdad.

Explicación detallada

ping: el "hola, sigues ahí" de las redes

ping es el comando de diagnóstico más conocido del mundo y también el más subestimado. Su trabajo es simple: manda un pequeño paquete de prueba (un "echo request" del protocolo ICMP) a un destino y mide cuanto tarda en volver la respuesta (el "echo reply"). Es como gritar "hola" en un túnel y medir cuanto tarda el eco en regresar: si el eco vuelve rápido, el túnel está libre; si tarda mucho, algo lo está obstruyendo; si no vuelve, el túnel está bloqueado o no hay nadie al otro lado.

Qué mide ping exactamente. Tres cosas: primero, alcanzabilidad: si hay respuesta, hay conectividad básica hasta ese destino. Segundo, latencia: el tiempo de ida y vuelta en milisegundos (ms); mientras más bajo, mejor. Tercero, pérdida de paquetes: que porcentaje de los paquetes no volvió; 0% es lo ideal, y cualquier pérdida arriba del 2-5% ya se nota en llamadas y juegos.

Los tiempos típicos te dicen mucho: menos de 1 ms significa que el destino está en tu red local (tu router, otra compu de tu casa). Entre 5 y 30 ms es normal dentro de tu ciudad o país. Entre 100 y 200 ms es normal hacia otro continente. Más de 300 ms o tiempos muy variables (un paquete tarda 20 ms y el siguiente 400 ms) indican congestión o un problema en el camino. La variación del retardo se llama jitter, y es el enemigo número uno de las videollamadas: no importa tanto que el retardo sea alto, importa que sea inestable.

El TTL que aparece en la respuesta de ping merece explicación porque confunde a muchos. TTL significa "tiempo de vida" y es un contador que cada paquete lleva: cada router por el que pasa le resta 1, y si llega a cero el paquete muere. Existe para que los paquetes perdidos no den vueltas eternas por internet. Los sistemas operativos ponen un valor inicial típico: Windows usa 128, Linux y macOS usan 64, muchos routers usan 255. Entonces, si haces ping a un servidor y la respuesta dice TTL=117, puedes deducir que empezó en 128 (Windows) y paso por 11 routers (128 menos 117). Si dice TTL=52, probablemente empezó en 64 y paso por 12 saltos. No es una ciencia exacta, pero te da una idea de que tan lejos está el destino y por qué sistema corre.

Cómo se usa ping en un diagnóstico real. La técnica clásica es "ping por capas": primero haz ping a tu propia puerta de enlace (tu router, normalmente 192.168.1.1 o 192.168.0.1). Si responde, tu red local funciona. Luego haz ping a una IP pública conocida, por ejemplo 8.8.8.8 (el DNS de Google). Si responde, tu conexión a internet funciona. Luego haz ping a un nombre, por ejemplo www.ejemplo.com. Si la IP respondía pero el nombre no, tu problema es de DNS, no de conectividad. Este encadenamiento de tres pings te ubica el problema en menos de un minuto: red local, internet o DNS. Memorízalo, lo usarás toda la vida.

Errores comunes de principiante: primero, creer que "sí no responde al ping, está caído". Muchos servidores y firewalls bloquean ICMP por seguridad, así que un servidor perfectamente sano puede no responder al ping. El ping que no responde significa "no hay respuesta ICMP", no "no hay servicio": confirma con el puerto real del servicio. Segundo, hacer ping una sola vez y sacar conclusiones: la red varía, manda al menos 10 o 20 paquetes para ver el patrón. Tercero, asustarse con el primer paquete lento: en muchos equipos el primer ping tarda más porque el router aún no tenía la dirección MAC en cache (ARP); es normal, mira el promedio.

En Windows el comando es "ping" y por defecto manda 4 paquetes; usa "ping -t" para que no pare hasta que lo detengas con Ctrl+C, y "ping -n 20" para mandar 20. En Linux y macOS, ping no para solo: mandalo con "ping -c 10" para limitar a 10 paquetes. Guarda estas banderas, las necesitarás en la práctica.

ipconfig, ifconfig e ip addr: lee tu propia configuración

Antes de diagnosticar la red, diagnosticate a ti: la mitad de los problemas están en la configuración de tu propio equipo. Estos comandos muestran tu dirección IP, tu máscara de subred, tu puerta de enlace y tus servidores DNS. Si alguno de esos datos está mal, nada más va a funcionar, así que siempre se revisan primero.

En Windows el comando es `ipconfig`. "`ipconfig`" a secas te muestra lo esencial de cada adaptador; "`ipconfig /all`" te muestra todo: dirección física (MAC), si el DHCP está activado, la fecha en que se obtuvo la IP, los servidores DNS y hasta el nombre del equipo. "`ipconfig /release`" suelta tu IP actual y "`ipconfig /renew`" pide una nueva al servidor DHCP: es el famoso "renovar la IP" que arregla muchos problemas caseros. "`ipconfig /flushdns`" vacía la cache de DNS de tu equipo, útil cuando una página cambio de servidor y tu compu sigue recordando la dirección vieja.

En Linux el comando moderno es "`ip addr`" (parte de la suite `iproute2`); el clásico "`ifconfig`" sigue existiendo en muchos sistemas pero está en retirada. "`ip addr show`" lista tus interfaces con sus IPs y máscaras; "`ip route show`" muestra tú tabla de rutas, incluyendo cuál es tu puerta de enlace por defecto (la línea que dice "default vía 192.168.1.1"). En macOS tienes `ifconfig` y también "`ipconfig`" con sintaxis distinta a la de Windows (herencia de Unix): "`ipconfig getifaddr en0`" te da tu IP en WiFi.

Qué buscar cuando lees la salida. Primero, tienes IP o tienes una de esas raras 169.254.x.x: esa es una IP automática (APIPA) que Windows se asigna cuando no encuentra servidor DHCP; traducido: tu equipo no está hablando con el router, revisa cable, WiFi o el servidor DHCP. Segundo, tu puerta de enlace: debe ser la IP de tu router; si está vacía o es 0.0.0.0, no tienes salida a internet. Tercero, tus DNS: si apuntan a un servidor que no responde, navegarás fallando aunque el ping a IPs funcione. Cuarto, la máscara: una máscara mal puesta te deja fuera de tu propia red local.

Analogía: leer tu configuración IP es como revisar tu credencial antes de culpar al guardia del edificio. Si tu credencial dice otro edificio (IP de otra red) o no trae foto (sin puerta de enlace), el problema eres tu, no la puerta.

tracert y traceroute: el mapa de tu paquete

Si ping te dice "si hay camino y cuanto tarda", traceroute te dibuja el camino: muestra cada router (cada "salto" o hop) por el que pasan tus paquetes hasta el destino, con los tiempos de cada tramo. Es tu mapa de carreteras de internet.

Cómo funciona es ingenioso: envía paquetes con el TTL empezando en 1. El primer router le resta 1, el TTL llega a cero, el router descarta el paquete y te avisa con un mensaje ICMP de "tiempo excedido". Así descubres al primer router. Luego manda con TTL=2 y descubre al segundo, y así hasta llegar al destino. Cada salto se prueba normalmente tres veces y ves tres tiempos.

En Windows el comando es "`tracert`" (con una sola t en medio, detalle que confunde); en Linux y macOS es "`traceroute`". Ejemplo de lectura: las primeras líneas con 1 ms son tu red local y tu

proveedor; luego verás nombres de routers intermedios que a veces revelan ciudades o empresas; al final, el destino. Los asteriscos (*) significan que ese router no respondió a la prueba: no necesariamente está caído, muchos routers ignoran estas pruebas por seguridad o por carga. Unos cuantos asteriscos en medio son normales; una pared de asteriscos hasta el final suele indicar un firewall bloqueando la prueba o un problema real a partir de cierto punto.

Cómo interpretar los tiempos: lo importante no es el tiempo absoluto de cada salto sino dónde aparece el salto brusco. Si los saltos 1 a 5 van a 10 ms y del salto 6 en adelante todo va a 250 ms, el problema (o simplemente la distancia geográfica) está entre el 5 y el 6. Si un salto intermedio muestra tiempos altísimos pero los siguientes vuelven a la normalidad, probablemente ese router solo tardó en responder la prueba porque tenía trabajo más importante (responder pruebas es su última prioridad); no es necesariamente congestión real. La clave está en el patrón, no en un número aislado.

Uso práctico: cuando un sitio tarda en cargar, un traceroute te dice si el problema está en tu casa (primeros saltos lentos), en tu proveedor (saltos intermedios) o en el destino (últimos saltos). Esa información vale oro cuando llamas a soporte: "mi tráfico se atora en el salto 4, que es su router" te pone en otro nivel de conversación.

Error común: obsesionarse con los asteriscos o con un salto lento aislado y declarar "ahí está el problema" sin ver el patrón completo. Otro error: olvidar que la ruta de ida y la de vuelta pueden ser distintas (rutas asimétricas), así que el tiempo de un salto no siempre cuenta la historia completa.

nslookup y dig: interrogando al DNS

Cuando escribes "www.ejemplo.com" y la página abre, hubo una pregunta invisible al DNS: "¿qué IP tiene este nombre?". Cuando la página no abre pero el ping a 8.8.8.8 sí funciona, el sospechoso número uno es el DNS. nslookup y dig son tus interrogadores: les preguntas directamente a un servidor DNS y ves que responde, sin intermediarios ni caches que te confundan.

nslookup viene en Windows, Linux y macOS, así que es tu herramienta universal. "nslookup www.ejemplo.com" te dice qué servidor DNS usaste y qué IP te devolvió. Pero su verdadero poder está en preguntarle a un servidor específico: "nslookup www.ejemplo.com 8.8.8.8" le pregunta al DNS de Google ignorando tu configuración local. Si tu DNS normal falla pero el de Google responde, acabas de probar que el problema es tu servidor DNS configurado, no tu internet. También puedes pedir otros tipos de registros: "nslookup -type=mx ejemplo.com" muestra los servidores de correo del dominio, útil cuando el correo no llega.

dig (domain information groper) es el favorito en Linux y macOS, más detallado y más preciso. "dig www.ejemplo.com" te muestra la pregunta, la respuesta, que servidor respondió y en cuantos milisegundos. "dig +short www.ejemplo.com" te da solo la IP, perfecto para scripts. "dig mx ejemplo.com" pide los registros de correo. "dig -x 8.8.8.8" hace la pregunta inversa: que nombre tiene esta IP. Y "dig +trace www.ejemplo.com" te muestra la consulta recorriendo toda la jerarquía DNS desde la raíz: es como ver el tramite completo del DNS paso a paso, excelente para entender la unidad de DNS en acción.

Qué buscar en las salidas. Primero, el tiempo de respuesta: un DNS local debe responder en 1-5 ms; si tarda cientos de ms o expira el tiempo (timeout), tu navegación se sentirá lenta aunque tu internet vuele. Segundo, respuestas vacías o errores como NXDOMAIN (el dominio no existe): si escribiste bien el nombre y el DNS dice que no existe, prueba con otro servidor DNS para descartar un problema de tu proveedor. Tercero, respuestas inconsistentes: si tu DNS te devuelve una IP distinta a la que devuelve 8.8.8.8 para él mismo sitio, alguien podría estar manipulando tus respuestas (o tu proveedor hace redirecciones). Cuarto, en dig fijate en los "flags": la bandera "aa" significa respuesta autoritativa (viene del servidor dueño del dominio) y "ra" significa que el servidor hizo recursión por ti.

Caso típico que resuelves con esto: "el internet funciona pero no abre ninguna página". Haces ping a 8.8.8.8 y responde: hay internet. Haces "nslookup www.ejemplo.com" y expira el tiempo: el DNS configurado no responde. Solución temporal: cambia tus DNS a 8.8.8.8 y 1.1.1.1; solución definitiva: reporta a tu proveedor o revisa tu router. Sin nslookup habrías reiniciado el router tres veces sin resultado.

netstat y ss: quién está hablando con quién

netstat (estadísticas de red) y su sucesor moderno ss (socket statistics) te muestran las conexiones activas de tu equipo y los puertos en los que tus programas están escuchando. Es como pedir la lista de llamadas entrantes y salientes de tu teléfono: ves quién se conectó, a dónde y en qué estado está cada conversación.

"netstat -an" es la forma básica: -a muestra todo (conexiones y puertos en escucha), -n muestra números en vez de resolver nombres (más rápido y más claro para diagnosticar). En la salida verás columnas de dirección local, dirección remota y estado. Los estados importantes: LISTENING (o LISTEN) significa que un programa está esperando conexiones en ese puerto, por ejemplo tu servidor web en el 80; ESTABLISHED es una conexión activa en este momento; TIME_WAIT es una conexión recién cerrada esperando para liberar recursos (ver muchas es normal después de navegar mucho); CLOSE_WAIT puede indicar un programa que no cierra bien sus conexiones.

"netstat -anb" en Windows (con b) te dice que programa (binario) abrió cada conexión: indispensable cuando ves una conexión sospechosa y quieres saber que procesó la originó. En Linux, "ss -tulpn" es la combinación mágica: -t solo TCP, -u solo UDP, -l solo puertos en escucha, -p muestra el proceso, -n numérico. Si sospechas que hay un programa raro en tu máquina, "ss -tulpn" te muestra todo lo que escucha y quién es el responsable.

Usos prácticos de diagnóstico. Primero, "mi programa no se puede conectar al servidor": revisa con netstat/ss si el servidor realmente está escuchando en el puerto que crees (si no hay LISTEN en ese puerto, el servicio está caído o mal configurado, y ningún diagnóstico de red lo va a arreglar). Segundo, "el puerto dice estar ocupado": la salida te muestra que procesó lo tiene y decides si detenerlo o cambiar tu configuración. Tercero, auditoría de seguridad básica: puertos escuchando que no reconoces merecen investigación; cada puerto abierto es una puerta que alguien podría tocar. Cuarto, conexiones establecidas raras: si ves tu equipo conectado a IPs extrañas en horarios extraños, investiga el proceso dueño antes de entrar en pánico (muchas son actualizaciones o servicios legítimos en la nube).

Error común: asustarse al ver decenas de conexiones ESTABLISHED. Navegar la web moderna abre muchísimas conexiones (cada pestaña, cada anuncio, cada video). Lo sospechoso no es la cantidad sino lo desconocido: procesos que no reconoces escuchando puertos, o conexiones a países con los que no tienes relación a las 3 am.

arp: la tabla de vecinos de tu red local

El comando arp muestra la tabla ARP de tu equipo: la lista que relaciona direcciones IP de tu red local con direcciones MAC físicas. Es tu "directorio de vecinos": para hablar con 192.168.1.20, tu compu consulta esta tabla para saber a que MAC enviarle la trama.

"arp -a" en Windows, Linux y macOS muestra la tabla completa. Verás entradas dinámicas (aprendidas automáticamente) y a veces estáticas (configuradas a mano). En un diagnóstico, la tabla ARP sirve para dos cosas. Primera: verificar que tu puerta de enlace este bien resuelta; si la entrada de tu router muestra una MAC incompleta o dice "incomplete", tu equipo no logra hablar con el router a nivel físico: revisa cable, WiFi o que el router este encendido. Segunda: detectar suplantación ARP (la que viste en la Unidad 9); si dos IPs distintas muestran la misma MAC, o la MAC de tu puerta de enlace cambia de repente, alguien podría estar haciendo ARP spoofing en tu red.

"arp -d" borra una entrada (o toda la tabla según el sistema) y obliga a tu equipo a preguntar de nuevo: útil cuando cambiaste un equipo de IP y tu compu sigue recordando la MAC vieja, el clásico "cambie el router y ahora no lo veo". Es un truco pequeño que resuelve problemas misteriosos después de cambios de hardware.

pathping y mtr: lo mejor de dos mundos

ping te dice el destino final, traceroute te muestra el camino; pathping (Windows) y mtr (Linux/macOS, "my traceroute") combinan ambas ideas y agregan lo más valioso: estadísticas de pérdida por cada salto durante un período de tiempo. En vez de una foto instantánea, te dan una película de unos minutos.

Cómo funcionan: hacen un traceroute y luego mandan muchos pings a cada salto durante un rato (pathping tarda unos 5 minutos por defecto; mtr corre en tiempo real hasta que lo detienes). El resultado es una tabla donde cada salto muestra su pérdida de paquetes y su latencia promedio. Esto te permite ver exactamente dónde empieza la pérdida: si los saltos 1-4 tienen 0% de pérdida y del salto 5 en adelante hay 20%, el problema está en el salto 5 o en el enlace que le sigue. Con traceroute normal no verías eso porque solo prueba cada salto tres veces.

Cuándo usarlos: son tus herramientas para problemas intermitentes o de calidad, no para cortés totales. "Mi videollamada se entrecorta cada tanto", "el juego tiene lag en las noches", "la página a veces tarda muchísimo": ahí brillan pathping y mtr. Para un corte total ("no hay internet"), el ping por capas de la primera sección es más rápido.

Cómo leer la salida sin caer en trampas. Primera trampa: un salto intermedio con 100% de pérdida pero los saltos siguientes perfectos. Eso casi siempre significa que ese router ignora las pruebas (muy común en routers de núcleo), no que esté caído: si estuviera caído, nada pasaría más allá de él. Segunda trampa: la pérdida que aparece en un salto y se mantiene igual en todos los siguientes: el problema es de ese salto en adelante, no se suma. Tercera: tiempos altos en saltos lejanos geográficamente hablando: 150 ms hacia otro continente es física, no falla (la luz tarda lo que tarda).

En Windows: "pathping www.ejemplo.com" y espera unos minutos al reporte final. En Linux: instala mtr si no lo tienes y corre "mtr www.ejemplo.com" para ver la tabla en vivo, o "mtr --report www.ejemplo.com" para un reporte estático de 10 ciclos. En macOS también existe mtr instalable. Estas dos herramientas son las favoritas del soporte técnico de los proveedores de internet: cuando les llevas un reporte de mtr mostrando pérdida en su red, tu ticket se atiende distinto.

Wireshark: ver los paquetes con tus propios ojos

Wireshark es el analizador de protocolos más famoso del mundo: un programa gratuito que captura los paquetes que viajan por tu red y te los muestra uno por uno, desarmados por capas, para que veas exactamente que se están diciendo los equipos. Si las herramientas anteriores son como llamar por teléfono para preguntar qué pasa, Wireshark es como poner una cámara en la carretera y ver los autos pasar.

Qué es y que no es. Es una herramienta de diagnóstico y aprendizaje potentísima: sirve para entender protocolos, cazar problemas esquivos y auditar tu propia red. No es una herramienta de espionaje para usar en redes ajenas: capturar tráfico de otros sin permiso es delito en México y en casi todo el mundo. Úsalo en tu red, en tu laboratorio o donde tengas autorización escrita. Con esa regla clara, es de lo más divertido que vas a aprender en este curso.

Captura básica paso a paso. Primero, instala Wireshark desde su sitio oficial (wireshark.org) y ábrelo con permisos de administrador (en Linux normalmente necesitas estar en el grupo `wireshark` o usar `sudo`). Segundo, elige la interfaz de red: verás una lista (WiFi, Ethernet, adaptador virtual); haz doble clic en la que estes usando y la captura empieza de inmediato. Tercero, genera tráfico interesante: abre una página web, haz un ping, entra a tu correo. Cuarto, deten la captura con el botón cuadrado rojo. Ya tienes cientos o miles de paquetes frente a ti.

Cómo leer la pantalla. Arriba está la lista de paquetes: cada fila es un paquete con su número, tiempo, origen, destino, protocolo e información resumida. En medio está el detalle del paquete seleccionado, desarmado por capas: puedes expandir "Ethernet", "IP", "TCP", "DNS" y ver cada campo, exactamente los encabezados que estudiaste en las unidades de protocolos. Abajo están los bytes crudos en hexadecimal. Haz clic en un paquete DNS y expande su sección: verás la pregunta ("que IP tiene www.ejemplo.com") tal cuál viaja por la red. Esa es la magia de Wireshark: la teoría del curso convertida en algo visible.

Los filtros display son lo que hace usable a Wireshark: con miles de paquetes, necesitas un colador. Se escriben en la barra de filtro y se aplican con Enter. Los esenciales para empezar: "dns" muestra solo tráfico DNS (perfecto para diagnosticar problemas de resolución de nombres); "tcp.port == 80" muestra solo tráfico web sin cifrar hacia el puerto 80; "ip.addr == 192.168.1.1" muestra solo lo que habla con tu router; "icmp" muestra solo pings y sus respuestas; "arp" muestra solo tráfico ARP de tu red local. Puedes combinarlos: "dns and ip.addr == 8.8.8.8" muestra solo tus consultas al DNS de Google. Si el filtro queda en rojo, la sintaxis está mal; en verde, está bien aplicado.

Un diagnóstico real con Wireshark, ejemplo: "una página no abre". Capturas mientras intentas abrirla y filtras por "dns": ves tus consultas saliendo pero ninguna respuesta volviendo, o respuestas con error. Diagnóstico: tu DNS no responde, y lo viste con tus ojos en vez de

adivinarlo. Otro ejemplo: filtras por "tcp" e intentas entrar a un sitio: ves tu paquete SYN salir, pero nunca vuelve el SYN-ACK. Diagnóstico: el servidor o un firewall en el camino está bloqueando la conexión TCP. Wireshark no te dice la solución mágica, pero te dice exactamente dónde se rompe la conversación, y eso es el 80% del diagnóstico.

Buenas prácticas con Wireshark: captura solo lo necesario (unos segundos o un par de minutos bastan; capturas largas son océanos imposibles de analizar); usa filtros de captura si vas a grabar mucho tiempo para no llenar tu disco; nunca publiques capturas sin revisarlas porque pueden contener contraseñas o datos personales (el tráfico sin cifrar muestra todo tal cuál); y etiqueta tus archivos de captura con fecha y descripción ("2026-09-19_problema-dns-oficina.pcapng") para encontrarlos después.

Error común de principiante: abrir Wireshark, ver miles de paquetes y entrar en pánico. Respira: aplica un filtro, enfocate en una sola conversación (clic derecho, "seguir flujo TCP") y analiza esa. Wireshark premia la paciencia y castiga la prisa.

Metodología de resolución: de abajo hacia arriba, siempre

Las herramientas sin método son solo juguetes. La metodología profesional para resolver problemas de red se basa en el modelo de capas que ya conoces: se empieza por la capa más baja (la física) y se sube capa por capa, descartando niveles hasta encontrar al culpable. Se le llama "bottom-up" (de abajo hacia arriba) y funciona porque la mayoría de los problemas están abajo, y porque no tiene sentido diagnosticar DNS si ni siquiera tienes IP.

El método tiene cinco pasos. Paso 1: define el problema con precisión. "No hay internet" no es una definición útil; "mi laptop no abre páginas web pero el teléfono con WiFi sí navega" sí lo es, porque ya te dice que el problema está en la laptop, no en el router ni en el proveedor. Pregunta siempre: ¿qué falla exactamente, desde cuándo, a quién afecta (uno o todos), y qué cambió recientemente. El "qué cambió recientemente" resuelve más casos de los que crees: se actualizó algo, se movió un cable, se cambió una clave.

Paso 2: empieza por la capa física. Está el cable conectado, el WiFi activado, el router encendido, los focos del equipo en estado normal. Parece obvio y por eso se olvida: una cantidad vergonzosa de tickets de soporte se resuelven aquí. Revisa también lo físico menos obvio: un cable dañado que funciona "a veces", un puerto del switch quemado, un eliminador de corriente flojo.

Paso 3: sube a la capa de red. Tienes IP válida (ipconfig), puedes hacer ping a tu puerta de enlace, puedes hacer ping a una IP pública como 8.8.8.8. Si el ping a la puerta de enlace falla, tu problema es local: cable, WiFi, DHCP o el router. Si la puerta responde pero 8.8.8.8 no, el problema está entre tu router y tu proveedor. Cada prueba que pasa descarta una capa entera: eso es eficiencia.

Paso 4: sube a resolución de nombres y servicios. Si las IPs responden pero los nombres no, es DNS (nslookup te lo confirma). Si el DNS resuelve pero la página no abre, prueba el puerto del servicio y revisa si el servidor escucha (netstat en el servidor, o un simple intento de conexión). Aquí también entra revisar firewalls: una regla mal puesta es una causa clásica de "todo se ve bien pero no conecta".

Paso 5: documenta y verifica. Anota que encontraste, que cambiaste y si el problema se resolvió. Luego verifica con el usuario o con tus propias pruebas que todo funciona, y monitorea un rato por si el problema era intermitente. Un problema "arreglado" que vuelve a los dos días no estaba arreglado: te faltó encontrar la causa raíz.

Por qué esté orden y no otro. Porque es el que descarta más rápido lo más probable. Empezar por arriba ("debe ser el DNS, voy a reinstalar el servidor") cuando el problema era un cable suelto te hace perder horas y tocar cosas que estaban bien, con el riesgo de romperlas. La disciplina del método es lo que separa al técnico del adivinador. Con el tiempo harás estos pasos casi sin pensar, pero al principio siguelos en orden religiosamente.

Checklist rápido: físico, IP, puerta de enlace, DNS

Para pegarlo en tu pared o guardarlo en tu teléfono, este es el checklist de los primeros cinco minutos ante un "no hay internet":

1. Físico: equipo encendido, cable bien conectado o WiFi conectado a la red correcta, focos del router en estado normal, otros equipos funcionan o también fallan (esto último te dice si el problema es tuyo o general).
2. IP: ejecuta ipconfig (o ip addr) y confirma que tienes una IP válida de tu red, no una 169.254.x.x, con máscara correcta.
3. Puerta de enlace: haz ping a tu puerta de enlace. Si responde, tu red local está sana.
4. Internet: haz ping a 8.8.8.8. Si responde, tienes salida a internet.
5. DNS: haz ping a un nombre (www.ejemplo.com) o usa nslookup. Si la IP funciona pero el nombre no, cambia temporalmente tus DNS a 8.8.8.8 y 1.1.1.1 y reporta el problema.

Si llegaste al paso 5 con todo en verde y aún así una página específica no abre, el problema probablemente está en el destino (servidor caído) o en un firewall intermedio: un traceroute te mostrará hasta dónde llegan tus paquetes. Cinco minutos, cinco pasos, cero adivinanzas.

Documentar el problema: tu yo del futuro te lo agradecerá

El último hábito profesional es el menos glamoroso y el más rentable: documentar. Cada problema que resuelvas, anotalo: fecha, síntomas, que pruebas hiciste, cuál fue la causa raíz y que lo arregló. Con el tiempo construyes tu propia base de conocimiento y los problemas repetidos se resuelven en minutos porque "esto ya me paso en marzo".

Qué anotar como mínimo: cuando empecé y a quién afectaba; los resultados de tus pruebas clave (los tres pings, el nslookup); la causa encontrada; la solución aplicada; y si quedo algo pendiente (por ejemplo, "cambiar el cable dañado del switch 2 la próxima semana"). En empresas esto se lleva en un sistema de tickets; en tu casa basta un archivo de texto o una libreta. Lo importante es el hábito, no la herramienta.

Documentar también te protege: cuando algo vuelve a fallar y te preguntan "que hiciste la última vez", tienes la respuesta exacta en vez de un vago "creó que reinicie algo". Y cuando entregues un trabajo o ayudes a alguien, un reporte claro de "problema, causa, solución" es tu mejor carta de presentación como técnico serio.

Las trampas mentales del diagnóstico: errores que cuestan horas

Las herramientas ya las tienes; lo que separa al buen técnico del malo suele estar en la cabeza. Estos son los errores mentales más comunes al diagnosticar, los que convierten un problema de diez minutos en una tarde perdida.

Trampa 1: empezar por la hipótesis favorita. "Seguro es el DNS" dices, y te pasas una hora tocando el DNS mientras el problema era un cable. La hipótesis favorita es cómoda pero ciega: el método de abajo hacia arriba existe justamente para obligarte a descartar lo simple primero. Regla: las pruebas mandan, no las corazonadas. Si tu hipótesis favorita vive en la capa 7 y ni siquiera verificaste la capa 1, estás adivinando.

Trampa 2: cambiar varias cosas a la vez. Reinicias el router, cambias los DNS, actualizas el controlador de red y "ya funciona". Que lo arregló. No lo sabes, y cuando vuelva a fallar no sabrás por dónde empezar. En diagnóstico se cambia una cosa a la vez y se prueba después de cada cambio. Es más lento en el momento y muchísimo más rápido a la larga, porque cada prueba te da información confiable.

Trampa 3: confundir correlación con causa. "Se cayó justo cuando instale la actualización, entonces la actualización lo rompió". A veces si, pero a veces la actualización solo reinicio el equipo y el problema real era un servicio que no arranca solo desde hace meses. Antes de revertir la actualización, verifica con pruebas: si el servicio X no responde en su puerto, el culpable es el servicio X, no lo último que instalaste.

Trampa 4: el túnel de la herramienta favorita. Hay técnicos que todo lo quieren resolver con ping y técnicos que todo lo quieren resolver con Wireshark. Cada herramienta ve una parte: ping no ve DNS, Wireshark no te dice si el cable está suelto. El diagnóstico completo usa varias herramientas en orden, como un doctor que no diagnostica solo con el termómetro.

Trampa 5: no preguntar "que cambió". La pregunta más rentable del diagnóstico es también la más olvidada. "Funciono durante un año y hoy no" casi siempre tiene una respuesta en algo que cambió: una actualización, un equipo nuevo, una contraseña cambiada, alguien que "solo movió un cablecito". Pregunta siempre, y pregunta a todos: el usuario jura que "no toco nada" hasta que recuerda que su sobrino "arreglo" el router el domingo.

Trampa 6: rendirse en el primer callejón sin salida. Hiciste los tres pings, todo responde, las páginas abren en el teléfono pero no en la laptop, y te quedas en blanco. Ese es el momento de subir de nivel, no de rendirse: compara configuraciones entre el equipo que funciona y el que no (ipconfig en ambos), revisa el proxy del navegador, prueba otro navegador, revisa el firewall del equipo, mira los registros del sistema. Los problemas "imposibles" casi siempre son una configuración distinta entre dos equipos que creías idénticos.

Trampa 7: arreglar el síntoma y no la causa. Lograste que funcione reiniciando el router cada mañana durante una semana. Eso no es una solución, es un ritual. La causa raíz podría ser un equipo sobrecalentado, un firmware con fuga de memoria o un conflicto de IPs que aparece cuando llega cierta laptop. Persigue la causa hasta que puedas explicar por qué fallaba; si no puedes explicarlo, no lo arreglaste, solo lo escondiste.

El antídoto contra todas estas trampas es él mismo: método, una cosa a la vez, pruebas que hablan y documentación. Con el tiempo notarás que los problemas se repiten con disfraces distintos, y tu base de notas se vuelve tu superpoder.

Ejemplos paso a paso

Aquí vas a leer salidas reales de las herramientas, como las verías en tu pantalla, con explicación línea por línea. Los datos (IPs, tiempos, nombres) son ejemplos ilustrativos; los tuyos serán distintos pero la forma de leerlos es la misma.

Ejemplo 1: ping a tu puerta de enlace y a internet

```
C:\> ping 192.168.1.1
```

Haciendo ping a 192.168.1.1 con 32 bytes de datos:

Respuesta desde 192.168.1.1: bytes=32 tiempo<1ms TTL=64

Respuesta desde 192.168.1.1: bytes=32 tiempo<1ms TTL=64

Respuesta desde 192.168.1.1: bytes=32 tiempo<1ms TTL=64

Respuesta desde 192.168.1.1: bytes=32 tiempo<1ms TTL=64

Estadísticas de ping para 192.168.1.1:

Paquetes: enviados = 4, recibidos = 4, perdidos = 0 (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:

Minimo = 0ms, Maximo = 0ms, Media = 0ms

```
C:\> ping 8.8.8.8
```

Haciendo ping a 8.8.8.8 con 32 bytes de datos:

Respuesta desde 8.8.8.8: bytes=32 tiempo=18ms TTL=117

Respuesta desde 8.8.8.8: bytes=32 tiempo=21ms TTL=117

Respuesta desde 8.8.8.8: bytes=32 tiempo=19ms TTL=117

Respuesta desde 8.8.8.8: bytes=32 tiempo=22ms TTL=117

Estadísticas de ping para 8.8.8.8:

Paquetes: enviados = 4, recibidos = 4, perdidos = 0 (0% perdidos),
Minimo = 18ms, Maximo = 22ms, Media = 20ms

Lectura: el primer ping va a tu router (192.168.1.1): menos de 1 ms es lo esperado en red local, 0% de pérdida, todo sano. El TTL=64 sugiere que el router corre Linux. El segundo ping va a internet (8.8.8.8): 20 ms de media es un excelente tiempo dentro del país, 0% de pérdida. El TTL=117 indica que el paquete paso por unos 11 routers (venia de un 128 de Windows del lado del servidor). Conclusión del diagnóstico: tu red local funciona y tu salida a internet funciona. Si aún así no abren las páginas, el siguiente sospechoso es el DNS.

Ejemplo 2: ipconfig /all en Windows

```
C:\> ipconfig /all
```

Adaptador de LAN inalambrica Wi-Fi:

```
Nombre de DNS especifico de la conexion . . :  
Descripcion . . . . . : Intel Wireless-AC 9560  
Direccion fisica. . . . . : 3C-22-FB-9A-44-1D  
DHCP habilitado . . . . . : si  
Direccion IPv4. . . . . : 192.168.1.25  
Mascara de subred . . . . . : 255.255.255.0  
Puerta de enlace predeterminada . . . . . : 192.168.1.1  
Servidor DHCP . . . . . : 192.168.1.1  
Servidores DNS. . . . . : 192.168.1.1
```

Lectura línea por línea: la dirección física es tu MAC (identificador de tu tarjeta WiFi). DHCP habilitado en "si" significa que tu IP la asignó el router automáticamente. Tu IPv4 es 192.168.1.25, una IP privada normal de red casera, con máscara /24 (255.255.255.0): estás en la red 192.168.1.0. Tu puerta de enlace es 192.168.1.1, o sea tu router, y es también tu servidor DHCP y tu DNS (el router reenvía tus consultas DNS). Todo consistente: si tuvieras aquí una IP 169.254.x.x o la puerta vacía, sabrías que el DHCP no te habló. Este es el comando número uno ante cualquier falla: treinta segundos y ya sabes si tu configuración está sana.

Ejemplo 3: traceroute hacia un sitio

```
$ traceroute www.ejemplo.com  
traceroute to www.ejemplo.com (93.184.216.34), 30 hops max, 60 byte packets  
1  router.casa (192.168.1.1)  0.8 ms  0.6 ms  0.5 ms  
2  10.20.0.1 (10.20.0.1)  8.2 ms  7.9 ms  9.1 ms  
3  nodo-proveedor-3.ciudad.mx (201.150.44.1)  12.4 ms  11.8 ms  13.0 ms  
4  enlace-nacional-7.proveedor.mx (201.150.200.9)  22.5 ms  21.9 ms  23.1 ms  
5  * * *  
6  frontera-usa.proveedor.mx (201.150.210.14)  45.3 ms  44.8 ms  46.0 ms  
7  servidor-destino (93.184.216.34)  48.1 ms  47.5 ms  49.2 ms
```

Lectura: el salto 1 es tu router (menos de 1 ms, perfecto). El salto 2 es el primer equipo de tu proveedor (8 ms, normal). Los saltos 3 y 4 recorren la red del proveedor con tiempos crecientes pero sanos. El salto 5 no responde a las pruebas (* * *): como los saltos siguientes si responden bien, es un router que ignora estas pruebas, no un problema. El salto 6 cruza hacia el extranjero (el tiempo sube a 45 ms por la distancia) y él 7 es el destino final a 48 ms. Patrón general: tiempos creciendo de forma gradual con la distancia y sin pérdidas. Si el

problema fuera lentitud, buscarías un salto donde el tiempo se dispara de golpe y se mantenga alto en adelante. Nota: los nombres e IPs son inventados para el ejemplo; los tuyos mostrarán los routers reales de tu proveedor.

Ejemplo 4: nslookup y dig comparando servidores DNS

```
C:\> nslookup www.ejemplo.com
Servidor:  router.casa
Address:  192.168.1.1

Respuesta no autoritativa:
Nombre:  www.ejemplo.com
Address:  93.184.216.34

C:\> nslookup www.ejemplo.com 8.8.8.8
Servidor:  dns.google
Address:  8.8.8.8

Respuesta no autoritativa:
Nombre:  www.ejemplo.com
Address:  93.184.216.34

$ dig +short www.ejemplo.com
93.184.216.34

$ dig mx ejemplo.com +short
10 correo1.ejemplo.com.
20 correo2.ejemplo.com.
```

Lectura: la primera consulta usa tu DNS configurado (el router) y resuelve bien: 93.184.216.34. La segunda pregunta directamente a Google y da él mismo resultado: tu DNS local funciona correctamente. Si la primera fallará y la segunda funcionará, el diagnóstico sería "tu DNS configurado no responde" y la solución temporal sería cambiar tus DNS. El "dig +short" es la versión minimalista para scripts. La última consulta pide los registros MX: el dominio ejemplo.com recibe correo en correo1 (prioridad 10, se intenta primero) y correo2 (prioridad 20, respaldo). Si el correo de una empresa no llega, esta es la primera consulta que haces.

Ejemplo 5: ss mostrando puertos en escucha (Linux)

```
$ ss -tulpn
Netid  State  Recv-Q  Send-Q  Local Address:Port  Peer Address:Port  Process
tcp    LISTEN  0        128      0.0.0.0:22          0.0.0.0:*
users: (("sshd",pid=820,fd=3))
tcp    LISTEN  0        128      127.0.0.1:3306      0.0.0.0:*
users: (("mysqld",pid=1104,fd=21))
tcp    LISTEN  0        511      0.0.0.0:80          0.0.0.0:*
users: (("apache2",pid=1330,fd=4))
udp    UNCONN  0         0        0.0.0.0:68          0.0.0.0:*
users: (("dhclient",pid=700,fd=6))
```

Lectura: sshd escucha en el puerto 22 en todas las interfaces (0.0.0.0): acepta SSH desde cualquier red que lo alcance; evalúa si eso es lo que quieres o si deberías restringirlo. mysqld escucha en 3306 pero solo en 127.0.0.1 (localhost): la base de datos solo acepta conexiones locales, buena práctica de seguridad. apache2 escucha en el puerto 80 en todas las interfaces: es un servidor web público, correcto si esa es su función. dhclient usa UDP 68: es el cliente DHCP pidiendo tu IP, totalmente normal. Con esta salida auditas tu equipo en diez segundos: cada línea LISTEN es una puerta abierta; si ves algo que no reconoces, investiga el proceso antes de decidir.

Ejemplo 6: tabla ARP y reporte de mtr

```
C:\> arp -a

Interfaz: 192.168.1.25 --- 0xa
  Direccion IP      Direccion fisica  Tipo
  192.168.1.1       a4-2b-8c-10-ff-02 dinamico
  192.168.1.20      b8-27-eb-3f-11-9a dinamico
  192.168.1.30      b8-27-eb-3f-11-9a dinamico
```

Lectura: tu router (192.168.1.1) tiene su MAC registrada como dinámica, todo normal. Pero mira las dos últimas líneas: 192.168.1.20 y 192.168.1.30 comparten la misma MAC (b8-27-eb-3f-11-9a). Eso es anormal: dos IPs no deberían tener la misma dirección física. Posibles causas: alguien configuró dos IPs en el mismo equipo (inocente), o alguien está haciendo suplantación ARP en tu red (malicioso). Si no hay explicación inocente, investiga ese equipo.

```
$ mtr --report www.ejemplo.com
```

HOST: mi-laptop	Loss%	Snt	Last	Avg	Best	Wrst	StDev
1. router.casa	0.0%	10	0.8	0.7	0.5	1.0	0.1
2. 10.20.0.1	0.0%	10	8.1	8.4	7.6	9.8	0.6
3. nodo-proveedor-3	0.0%	10	12.2	12.8	11.5	15.3	1.1
4. enlace-nacional-7	30.0%	10	85.4	62.1	21.0	120.5	28.4
5. frontera-usa	30.0%	10	90.2	66.3	44.0	125.1	24.9
6. servidor-destino	0.0%	10	48.0	48.5	47.1	50.2	0.9

Lectura: mtr mando 10 pruebas a cada salto. Los saltos 1 a 3 están perfectos: 0% de perdida y tiempos estables. Los saltos 4 y 5 muestran 30% de perdida y tiempos muy variables (StDev alto): ahí hay un problema real de calidad en la red del proveedor. Pero el salto 6, el destino, tiene 0% de perdida y 48 ms estables: interesante, el destino final está sano. Conclusión: hay congestión o falla intermitente en el tramo del proveedor (saltos 4-5) que afecta a parte del tráfico pero no tumba la conexión completa; es el típico caso de "a veces se entrecorta". Este reporte, guardado en un archivo, es exactamente lo que le mandas al soporte de tu proveedor para qué tu reporte se tome en serio.

Práctica

1. Tu vecino te dice "se me fue el internet". Aplica el método de los tres pings en orden: primero a la puerta de enlace, luego a 8.8.8.8, luego a www.ejemplo.com. Escribe que comandó usarías en cada paso, que resultado esperarías si todo está bien, y que conclusión sacarías en cada uno de estos tres casos: a) falla el primer ping, b) el primero funciona pero falla el segundo, c) los dos primeros funcionan pero falla el tercero.

SOLUCIÓN: Paso 1: averigua la puerta de enlace con "ipconfig" (Windows) o "ip route show" (Linux); supongamos 192.168.1.1. Comando: "ping 192.168.1.1". Esperado: respuestas de menos de 1 ms con 0% de perdida. Paso 2: "ping 8.8.8.8". Esperado: respuestas de 10-40 ms con 0% de perdida. Paso 3: "ping www.ejemplo.com". Esperado: primero resuelve el nombre a una IP y luego responde como en el paso 2. Caso a) falla el primer ping: el problema es tu red local; revisa en orden físico: cable conectado, WiFi conectado a la red correcta, router encendido; luego revisa tu IP con ipconfig (si tienes 169.254.x.x el DHCP no te habló). Caso b) el primero funciona pero el segundo falla: tu red local está sana pero no sales a internet; el problema está en el router, en el módem o en tu proveedor; reinicia módem y router en orden (primero módem, espera dos minutos, luego router) y si sigue fallando llama a tu proveedor diciendo "tengo red local pero no salgo a internet, el ping a 8.8.8.8 falla". Caso c) los dos primeros funcionan pero el tercero falla: tienes internet pero no resuelves nombres,

es un problema de DNS; confirma con "nslookup www.ejemplo.com 8.8.8.8": si con el DNS de Google si resuelve, cambia temporalmente tus servidores DNS a 8.8.8.8 y 1.1.1.1 y reporta la falla de DNS a tu proveedor. Lección: tres pings ordenados te ubican el problema en un minuto sin adivinar.

2. Analiza está salida de ping e indica si hay un problema y cuál: "Respuesta desde 8.8.8.8: bytes=32 tiempo=24ms TTL=117 / Respuesta desde 8.8.8.8: bytes=32 tiempo=412ms TTL=117 / Respuesta desde 8.8.8.8: bytes=32 tiempo=19ms TTL=117 / Se agotó el tiempo de espera para esta solicitud / Respuesta desde 8.8.8.8: bytes=32 tiempo=388ms TTL=117". Estadísticas: enviados 5, recibidos 4, perdidos 1 (20% perdidos).

SOLUCIÓN: Si hay problema, y es de calidad de conexión, no de corte total. Evidencias: 20% de pérdida de paquetes (1 de 5), muy por arriba del 0% ideal y del 2-5% tolerable; tiempos brutalmente variables: 19 ms, luego 412 ms, luego 19 ms, luego 388 ms. Esa variación extrema es jitter alto: la latencia salta sin patrón. Con estos síntomas, navegar se siente "a ratos", las videollamadas se entrecortan y los juegos tienen lag. El TTL estable en 117 descarta que los paquetes esten dando vueltas raras; el problema es congestión o un enlace inestable en el camino. Que harías: primero descarta tu red local haciendo ping a tu puerta de enlace (si ahí también hay jitter, el problema es tu WiFi o tu router); si la red local está limpia, corre "mtr 8.8.8.8" por unos minutos para ubicar en que saltó empieza la pérdida y lleva ese reporte a tu proveedor. También prueba en otro horario: si de noche mejora, es congestión del proveedor en horas pico. Lección: no mires solo si "responde o no responde"; la pérdida y la variación cuentan la historia de la calidad.

3. En tu trabajo "el internet funciona pero no abre ninguna página". Ya hiciste ping a 8.8.8.8 y responde perfecto. Describe paso a paso cómo confirmas que es un problema de DNS usando nslookup y dig, como encuentras una solución temporal para seguir trabajando, y que revisarías para encontrar la causa raíz.

SOLUCIÓN: Confirmación: ejecuta "nslookup www.ejemplo.com" y observa si expira el tiempo o da error; luego ejecuta "nslookup www.ejemplo.com 8.8.8.8": si está segunda sí resuelve, confirmaste que tu servidor DNS configurado falla pero internet funciona. Con dig sería "dig www.ejemplo.com" (falla o tarda muchísimo) contra "dig @8.8.8.8 www.ejemplo.com" (responde rápido). Solución temporal: cambia tus servidores DNS a 8.8.8.8 y 1.1.1.1 en tu equipo (en Windows: propiedades del adaptador, IPv4, DNS manual; en Linux: /etc/resolv.conf o tu gestor de red) y vacía la cache con "ipconfig /flushdns"; así sigues trabajando de inmediato. Causa raíz: revisa en orden: tu router (reinicialo, revisa que DNS tiene configurados y si su firmware está actualizado), si otros equipos tienen él mismo problema (si es solo tu equipo, el problema es tu

configuración; si son todos, es el router o el proveedor), y llama a tu proveedor preguntando por fallas en su DNS. También verifica que no haya un malware cambiando tus DNS (revisa que tus DNS sean los que tú pusiste). Lección: separar "conectividad" de "resolución de nombres" con una prueba directa contra otro servidor DNS convierte un misterio en un diagnóstico de dos minutos.

4. Te pasan este traceroute y te dicen que "la página tarda mucho en cargar". Encuentra dónde está el problema: "1 router.casa 0.7ms / 2 10.20.0.1 8ms / 3 nodo1.proveedor 12ms / 4 nodo2.proveedor 280ms / 5 nodo3.proveedor 285ms / 6 destino 290ms". Explica tu razonamiento y que acción tomarías.

SOLUCIÓN: El problema está entre el salto 3 y el salto 4. Razonamiento: los saltos 1 a 3 tienen tiempos sanos y crecientes de forma gradual (0.7, 8, 12 ms): tu red local y la entrada a tu proveedor están bien. En el salto 4 el tiempo se dispara a 280 ms y se mantiene alto en todos los saltos siguientes (285, 290 ms): el retardo aparece ahí y ya no baja, lo que indica congestión o un enlace lento a partir de ese punto, dentro de la red de tu proveedor o en su salida internacional. No es tu casa, no es el destino: es el tramo intermedio. Acción: primero confirma que no sea algo temporal repitiendo la prueba en unos minutos y con "mtr" para ver si hay pérdida además de retardo; luego llama a tu proveedor con datos concretos: "a partir del salto 4 (nodo2.proveedor) mi latencia sube de 12 a 280 ms de forma sostenida", y pregunta por congestión o mantenimiento en ese tramo. Si el problema es en horario pico y mejora de noche, es congestión: evalúa con tu proveedor un plan mejor o reporta la saturación. Lección: en traceroute no busques el número más alto aislado, busca dónde el tiempo salta de golpe y se queda alto: ahí vive el problema.

5. Auditoría de seguridad con netstat/ss: ejecuta "netstat -anb" (Windows) o "ss -tulpn" (Linux) en tu equipo y clasifica cada puerto en escucha en tres grupos: esperado (sabes que programa es y por qué escucha), investigable (no reconoces el programa) y sospechoso (escucha en todas las interfaces un servicio que debería ser local, o un proceso con nombre raro). Para cada puerto investigable o sospechoso, describe como averiguarías qué es y qué decisión tomarías.

SOLUCIÓN: Ejemplo de clasificación en un equipo típico. Esperados: puerto 22 con sshd (tu acceso remoto, si lo usas), 80/443 con tu servidor web (si corres uno), 3306 de MySQL solo en 127.0.0.1 (base de datos local, correcto), 68 UDP de dhclient (tu DHCP, normal). Investigables: un puerto alto como 52341 en LISTEN con un proceso llamado "mi-app-rara": buscarías el nombre del proceso en internet, revisarías la ruta del ejecutable (en Windows el -b te da el nombre; en Linux "ps -p PID -o cmd" te da el comando completo), y verificarías si corresponde a un programa que instalaste.

Sospechosos: un servicio escuchando en 0.0.0.0:3389 (escritorio remoto abierto a todo el mundo) cuando nunca lo activaste, o un proceso con nombre extraño escuchando en un puerto poco común: ahí detienes el servicio, pasas el antivirus, revisas programas instalados recientemente y cambias contraseñas desde otro equipo limpio si sospechas infección. **Decisiones:** lo esperado se documenta, lo investigable se identifica y se decide (mantener, restringir a localhost o desinstalar), lo sospechoso se aísla primero y se pregunta después. **Regla práctica:** si un servicio solo lo usas tu desde tu misma máquina, configuralo para escuchar solo en 127.0.0.1; cada puerto que dejes en 0.0.0.0 es una puerta que ofreces a toda tu red. **Lección:** netstat/ss convierte tu computadora de caja negra a lista transparente de puertas abiertas.

6. Caso completo con metodología: eres el técnico de una pequeña oficina. El lunes a las 9 am todos reportan que "no hay internet", pero el viernes todo funcionaba y el fin de semana se fue la luz en la zona. Aplica la metodología de abajo hacia arriba paso a paso: que verifiques en cada capa, que herramientas usas, y cuales serían las dos causas más probables con su solución.

SOLUCIÓN: Paso 1, define: afecta a todos los equipos, empezó hoy lunes, el viernes funcionaba, hubo corte de luz el fin de semana. "Que cambió recientemente": el corte de luz. Paso 2, capa física: verifica que módem, router y switches estén encendidos y con focos normales; un corte de luz suele dejar equipos apagados o a medio arrancar; revisa que los cables del módem al router sigan conectados (alguien pudo moverlos). Herramienta: tus ojos y tus manos. Paso 3, capa de red: en un equipo ejecuta ipconfig y confirma IP válida y puerta de enlace; haz ping a la puerta de enlace: si responde, la red local está sana. Luego ping a 8.8.8.8: si falla, no hay salida a internet. Paso 4, DNS y servicios: si el ping a IPs funciona pero no abren páginas, revisa DNS con nslookup. Causa probable 1: el módem o el router quedaron colgados tras el corte de luz (muy común): solución, reinicio ordenado: apaga todo, enciende el módem, espera dos minutos a que sincronice (focos estables), luego enciende el router, espera un minuto, y prueba los tres pings. Causa probable 2: el corte dañó la configuración o el equipo quedó con IP estática vieja: si ipconfig muestra 169.254.x.x, el DHCP del router no está respondiendo; verifica que el servicio DHCP esté activo en el router o renueva con "ipconfig /renew". Paso 5, documenta: anota fecha, causa (equipos colgados tras corte de luz), solución (reinicio ordenado) y pendiente (comprar un UPS o regulador para módem y router, y dejar escrito el procedimiento de reinicio para que cualquiera pueda hacerlo). **Lección:** el "que cambió recientemente" (el corte de luz) te llevó directo a la capa física y al reinicio ordenado, en vez de perder la mañana reinstalando controladores.

7. Captura con Wireshark mientras intentas abrir una página que no carga, con el filtro display "dns" aplicado. Ves tus consultas DNS saliendo hacia tu servidor configurado, pero no vuelve ninguna respuesta. Luego cambias el filtro a "icmp", haces ping a 8.8.8.8 y ves los echo request salir y los echo reply volver sin problema. Con esta evidencia: a) dónde está el problema exactamente y por qué lo sabes, b) que tres acciones tomarías en orden, c) que filtró usarías después para verificar que tu solución funcione.

SOLUCIÓN: a) El problema está en tu servidor DNS configurado, no en tu conectividad. Lo sabes porque la evidencia es directa y no una suposición: con el filtro "dns" viste las preguntas salir pero jamás viste respuestas volver, mientras que con el filtro "icmp" viste la conversación completa de ida y vuelta hacia 8.8.8.8. Si el problema fuera tu red local o tu salida a internet, los pings tampoco volverían. Wireshark te mostró exactamente dónde se rompe la conversación: en la resolución de nombres. b) Acciones en orden: primero, solución temporal para seguir trabajando: cambia tus DNS a 8.8.8.8 y 1.1.1.1 y vacía la cache con "ipconfig /flushdns". Segundo, ataca la causa: reinicia tu router (la mayoría de los DNS caseros fallan por el router colgado) y verifica que equipo es tu DNS configurado con ipconfig; si el problema persiste, prueba "nslookup www.ejemplo.com 8.8.8.8" para confirmar y reporta la falla a tu proveedor. Tercero, documenta: anota fecha, síntoma, evidencia de la captura y solución, y guarda la captura con nombre descriptivo por si el problema regresa. c) Para verificar, repite la captura con el filtro "dns" e intenta abrir la página: ahora deberías ver cada consulta seguida de su respuesta con la IP resuelta, y con el filtro "tcp.port == 80" o "tcp.port == 443" verías la conversación web establecerse (SYN, SYN-ACK, ACK). Si ves preguntas y respuestas DNS sanas, tu solución funciona. Lección: Wireshark convierte "no abre la página" en "miro exactamente que paquete falta", y eso es diagnosticar de verdad.

Resumen de la unidad

En esta unidad te convertiste en detective de redes. Aprendiste que diagnosticar no es adivinar: es seguir un método que descarta capas de abajo hacia arriba hasta encontrar la causa real. Y ahora tienes las herramientas para hacerlo.

De la clase 28 te llevas los comandos básicos que resuelven el 80% de los casos. `ping` te dice si hay camino, cuanto tarda y cuanta perdida hay; ya sabes leer su latencia, su porcentaje de perdida y su TTL para estimar distancia y sistema operativo. `ipconfig`, `ifconfig` e `ip addr` te muestran tu propia configuración: IP, máscara, puerta de enlace y DNS; y sabes que una IP 169.254.x.x grita "el DHCP no me habló". `tracert` y `traceroute` te dibujan la ruta salto por salto para ubicar dónde el tiempo se dispara o dónde mueren los paquetes. Y memorizaste la técnica de oro: los tres pings en orden (puerta de enlace, IP pública, nombre) te dicen en un minuto si el problema es tu red local, tu salida a internet o tu DNS.

De la clase 29 sumaste herramientas de precisión. `nslookup` y `dig` te permiten interrogar al DNS directamente y comparar servidores para confirmar fallas de resolución. `netstat` y `ss` te muestran conexiones activas y puertos en escucha con sus procesos dueños: tu auditoría de puertas abiertas. `arp` te muestra la tabla de vecinos de tu red local y te ayuda a detectar suplantaciones. Y `pathping` y `mtr` combinan `ping` y `traceroute` con estadísticas por salto para cazar problemas intermitentes de calidad, esos que "a veces fallan" y vuelven loco a quién no tiene método.

De la clase 30 te llevas dos tesoros. Wireshark: sabes hacer una captura básica, leer un paquete desarmado por capas y usar filtros display como "`dns`", "`tcp.port == 80`", "`icmp`" o "`ip.addr == 192.168.1.1`" para encontrar exactamente dónde se rompe una conversación. Y la metodología completa: definir el problema con precisión, empezar por la capa física, subir por red, DNS y servicios, documentar todo y verificar la solución. Más tu checklist de cinco minutos (físico, IP, puerta de enlace, internet, DNS) para pegarlo en la pared.

El consejo final de la unidad y del curso en este tema: la calma diagnóstica más que la prisa. Ante un problema, respira, sigue el orden y deja que las herramientas hablen. El técnico que reinicia todo a ver si se arregla depende de la suerte; el que diagnostica por capas depende de su método, y el método no falla. Práctica estos comandos en tu propia red esta semana: haz `ping` a tu router, corre un `traceroute` a tu sitio favorito, abre Wireshark y mira una consulta DNS viajar. La próxima vez que alguien diga "se cayó el internet", tú vas a ser la persona que pregunta "a ver, que muestran los tres pings", y eso, creeme, se nota.

Tu kit mínimo de diagnóstico, para tenerlo siempre a la mano: `ping` con sus banderas (`-t` en Windows, `-c` en Linux), `ipconfig /all` o `ip addr` para tu configuración, `tracert/traceroute` para la ruta, `nslookup` o `dig` para el DNS, `netstat -anb` o `ss -tulpn` para conexiones y puertos, `arp -a` para tu red local, `pathping` o `mtr` para problemas de calidad, y Wireshark para cuándo necesites ver los paquetes de verdad. No necesitas memorizar cada bandera: necesitas saber que herramienta responde que pregunta. "No resuelve nombres" es pregunta de `nslookup`; "dónde se atora" es pregunta de `traceroute`; "que programa escucha aquí" es pregunta de `netstat`. Con esa asociación clara, el diagnóstico deja de ser una lista de comandos y se vuelve

un instinto: síntoma, pregunta, herramienta, evidencia, conclusión. Ese instinto es lo que te llevas de esta unidad para toda tu carrera en redes y sistemas.

EXAMEN FINAL

Este examen final pone a prueba todo lo que aprendiste en el Curso Completo de Redes (Networking) de Lucas EGA Academy. Son 50 preguntas: 30 de opción múltiple, 10 de verdadero o falso y 10 abiertas. Hazlo con calma y sin ver las respuestas: el objetivo no es la calificación, es descubrir qué temas dominas y cuáles debes repasar. Para las preguntas de cálculo (subneteo) usa papel y lápiz; en la vida real tendrás calculadora, pero resolverlos a mano te demuestra que entiendes el concepto. Cuando termines, revisa la sección de respuestas y soluciones: cada respuesta explica por qué es correcta y por qué las demás opciones fallan. Si sacas menos de 40 aciertos, repasa las unidades donde fallaste antes de dar el curso por terminado. Éxito.

PREGUNTA 1: Una escuela conecta 40 computadoras dentro de un mismo edificio para compartir archivos e impresoras. Que tipo de red es está?

A) WAN B) LAN C) MAN D) PAN

PREGUNTA 2: En una red con arquitectura cliente-servidor, cuál es la función del servidor?

A) Solicitar recursos y servicios a otros equipos B) Proveer recursos y servicios a los equipos que los solicitan C) Conectar físicamente los cables de la red D) Traducir nombres de dominio a direcciones IP

PREGUNTA 3: Tu proveedor te ofrece 200 Mbps de bajada. En condiciones ideales, a cuantos megabytes por segundo (MB/s) equivale esa velocidad?

A) 200 MB/s B) 25 MB/s C) 1600 MB/s D) 20 MB/s

PREGUNTA 4: (Verdadero o falso) El ancho de banda y el throughput son exactamente lo mismo: la velocidad real a la que viajan tus datos.

PREGUNTA 5: (Pregunta abierta) Una oficina pequeña con 20 equipos necesita compartir archivos e impresoras y salir a internet. Describe que dispositivos pondrías, como los conectarías y por qué elegiste esa topología.

PREGUNTA 6: Un router toma decisiones de reenvío leyendo la dirección IP destino. En qué capa del modelo OSI trabaja principalmente?

A) Capa 1 (física) B) Capa 2 (enlace de datos) C) Capa 3 (red) D) Capa 7 (aplicación)

PREGUNTA 7: Cuando un segmento TCP sale de tu computadora, en que se encapsula primero para poder viajar por la red?

A) En una trama Ethernet B) En un paquete (datagrama) IP C) En bits físicos directamente D) En una sesión de aplicación

PREGUNTA 8: Alguien corta el cable de red de tu oficina y toda comunicación se detiene. En qué capa del modelo OSI se origina este problema?

A) Capa 7 (aplicación) B) Capa 4 (transporte) C) Capa 3 (red) D) Capa 1 (física)

PREGUNTA 9: (Verdadero o falso) TCP y UDP son protocolos de la capa de transporte del modelo OSI.

PREGUNTA 10: (Pregunta abierta) Explica que hace cada capa del modelo OSI (de la 7 a la 1) usando como ejemplo el envío de un correo electrónico.

PREGUNTA 11: Necesitas conectar dos switches entre si usando cable UTP. Que tipo de cable es el adecuado según la regla clásica?

A) Cable directo (straight-through) B) Cable cruzado (crossover) C) Cable coaxial D) Cable de fibra óptica

PREGUNTA 12: En una red, si falla una computadora solo esa queda fuera de servicio, pero si falla el dispositivo central toda la red cae. Que topología es?

A) Bus B) Anillo C) Estrella D) Malla completa

PREGUNTA 13: qué categoría de cable UTP soporta 10 Gbps hasta 55 metros?

A) Cat 5 B) Cat 5e C) Cat 6 D) Cat 3

PREGUNTA 14: (Verdadero o falso) En una topología en bus, si el cable troncal se rompe, toda la red deja de funcionar.

PREGUNTA 15: (Pregunta abierta) Compara el par trenzado, el cable coaxial y la fibra óptica en velocidad, distancia máxima e inmunidad a interferencias, e indica en que situación usarías cada uno.

PREGUNTA 16: La dirección 172.16.5.10 pertenece a que clase?

A) Clase A B) Clase B C) Clase C D) Clase D

PREGUNTA 17:Cuál de las siguientes es una dirección IP privada?

A) 8.8.8.8 B) 192.168.1.1 C) 172.32.0.1 D) 203.0.113.5

PREGUNTA 18: Con la IP 192.168.10.77 y máscara 255.255.255.0, cuál es la dirección de red?

A) 192.168.10.0 B) 192.168.10.77 C) 192.168.10.255 D) 192.168.0.0

PREGUNTA 19: (Verdadero o falso) La dirección 127.0.0.1 sirve para comunicarte con otros equipos de tu red local.

PREGUNTA 20: (Pregunta abierta) Lee esta salida de ipconfig y explica que significa cada dato. Qué problema detectas?

Dirección IPv4: 169.254.12.44 Máscara: 255.255.0.0 Puerta de enlace: (vacía)

PREGUNTA 21: La red 192.168.1.0/26, cuántas direcciones IP utilizables ofrece para hosts?

A) 62 B) 64 C) 126 D) 30

PREGUNTA 22:Cuál es la máscara en formato decimal punteado del prefijo /27?

A) 255.255.255.192 B) 255.255.255.224 C) 255.255.255.240 D) 255.255.255.128

PREGUNTA 23: Tienes la red 192.168.0.0/24 y necesitas una subred para 50 hosts y otra para 12 hosts, desperdiciando lo menos posible. Que asignación es correcta con VLSM?

A) 192.168.0.0/26 y 192.168.0.64/28 B) 192.168.0.0/24 y 192.168.1.0/24 C) 192.168.0.0/28 y 192.168.0.16/26 D) 192.168.0.0/25 y 192.168.0.128/25

PREGUNTA 24: (Verdadero o falso) Con VLSM puedes usar máscaras de diferente tamaño dentro de la misma red para no desperdiciar direcciones IP.

PREGUNTA 25: (Pregunta abierta) Divide 10.0.0.0/16 en subredes para: 4000 hosts, 500 hosts y un enlace punto a punto de 2 hosts. Para cada una indica el bloque CIDR, el rango utilizable y la dirección de broadcast.

PREGUNTA 26: Un switch aprende direcciones MAC con el objetivo de:

A) Asignar direcciones IP a los equipos B) Reenviar cada trama solo por el puerto donde está el equipo destino C) Traducir direcciones privadas a públicas D) Cifrar el tráfico de la red local

PREGUNTA 27: Un router recibe un paquete cuya red destino no está en su tabla de ruteo y no tiene ruta por defecto configurada. Que hace?

A) Lo reenvía por todos sus puertos B) Lo guarda hasta que aparezca una ruta C) Lo descarta y normalmente avisa con un mensaje ICMP de destino inalcanzable D) Lo fragmenta y lo envía de vuelta al origen

PREGUNTA 28: Tienes dos VLANs en el mismo switch y los equipos de una no pueden comunicarse con los de la otra. Que se necesita para permitirlo de forma controlada?

A) Un router (o switch capa 3) que haga ruteo entre VLANs B) Conectar más switches en cascada C) Cambiar todos los cables a fibra óptica D) Desactivar el protocolo STP

PREGUNTA 29: (Verdadero o falso) Un hub reenvía las tramas que recibe únicamente al puerto del equipo destino.

PREGUNTA 30: (Pregunta abierta) Explica la diferencia entre ruteo estático y ruteo dinámico, en que casos conviene cada uno y que protocolo dinámico usarías en una empresa mediana con varios routers. Justifica tu elección.

PREGUNTA 31: Cuál es el orden correcto del proceso DHCP (DORÁ)?

A) Discover, Offer, Request, Acknowledge B) Request, Discover, Acknowledge, Offer C) Offer, Discover, Acknowledge, Request D) Discover, Request, Offer, Acknowledge

PREGUNTA 32: Que tipo de registro DNS asocia un nombre de dominio con una dirección IPv4?

A) A B) AAAA C) MX D) CNAME

PREGUNTA 33: Tu red interna usa 192.168.1.0/24 y todos los equipos salen a internet con una sola IP pública. Que tecnología lo hace posible?

A) DHCP B) DNS C) NAT D) VLAN

PREGUNTA 34: (Verdadero o falso) El DNS traduce los nombres de dominio que escribes en el navegador a direcciones IP.

PREGUNTA 35: (Pregunta abierta) Un equipo nuevo hace ping a 8.8.8.8 pero no abre ninguna página web. Explica paso a paso cómo determinas si el problema es de DHCP, de DNS o de NAT, indicando que prueba o comando usas en cada paso.

PREGUNTA 36: Cuál de las siguientes es una dirección IPv6 válida?

A) 2001:db8::1 B) 2001:db8::g1 C) 2001:db8::1::2 D) 2001:db8:1

PREGUNTA 37: En Wi-Fi, que banda ofrece mayor velocidad a corta distancia pero menor alcance y peor penetración de muros?

A) 2.4 GHz B) 5 GHz C) Ambas ofrecen lo mismo D) Ninguna, la banda no afecta

PREGUNTA 38: Las direcciones que empiezan con fe80::/10 en IPv6 se usan para:

A) Comunicación global en internet B) Enlace local (link-local), solo dentro del mismo segmento de red C) Multicast a todos los nodos D) Loopback del propio equipo

PREGUNTA 39: (Verdadero o falso) IPv6 usa direcciones de 128 bits, así que hay direcciones suficientes para cada dispositivo y ya no se necesita NAT para compartir una sola IP pública.

PREGUNTA 40: (Pregunta abierta) Tu Wi-Fi es muy lenta en un departamento rodeado de muchas redes vecinas. Explica las causas probables (canal, banda, interferencias) y que acciones concretas tomarías para mejorarla.

PREGUNTA 41: Un firewall "stateful" se distingue porque:

A) Solo filtra por dirección MAC B) Recuerda el estado de las conexiones y permite el tráfico de respuesta legítimo C) Cifra todo el tráfico que pasa por el D) Asigna direcciones IP a los equipos internos

PREGUNTA 42: Un atacante satura tu servidor con miles de peticiones por segundo desde cientos de direcciones IP distintas. Que tipo de ataque es?

A) Phishing B) DDoS C) Man-in-the-middle D) Spoofing de ARP

PREGUNTA 43: Para la red Wi-Fi de tu empresa, el protocolo de seguridad que debes usar hoy en día es:

A) WEP B) WPA con TKIP C) WPA3 D) Red abierta con filtrado por MAC

PREGUNTA 44: (Verdadero o falso) El cifrado WEP sigue siendo una opción segura para proteger una red inalámbrica doméstica.

PREGUNTA 45: (Pregunta abierta) Detectas tráfico saliendo de tu red hacia internet a las 3 de la mañana, algo inusual. Describe tu plan: cómo confirmas si es una amenaza, como contienen el problema y que medidas preventivas aplicas después.

PREGUNTA 46: Haces ping a tu puerta de enlace y obtienes "Tiempo de espera agotado", pero el ping a 127.0.0.1 responde perfecto. Que concluyes?

A) Tu tarjeta de red y tu stack TCP/IP local funcionan; el problema está en el camino hacia la puerta de enlace B) El servidor DNS está caído C) Tu cable de red está perfecto y el problema es del ISP D) La puerta de enlace responde pero tu PC no la ve por un virus

PREGUNTA 47: Que comandó te muestra la ruta (los saltos) que siguen los paquetes hasta un destino?

A) ping B) ipconfig C) tracert (traceroute en Linux) D) nslookup

PREGUNTA 48: Un usuario no puede navegar. Siguiendo un diagnóstico ordenado de abajo hacia arriba en el modelo OSI, que revisas primero?

A) La configuración del proxy en el navegador B) Los servidores DNS configurados C) El cable, los LEDs del puerto y el estado del enlace físico D) Reinstalar el sistema operativo

PREGUNTA 49: (Verdadero o falso) Si el ping a una dirección IP responde pero el ping al nombre de dominio falla, el problema probablemente está en el DNS.

PREGUNTA 50: (Pregunta abierta) Te reportan "internet lento en toda la oficina desde las 10:00". Describe tu metodología de diagnóstico paso a paso: que verificas, con que comandos y que descartas en cada etapa.

Respuestas y soluciones

Revisa tus respuestas aquí. Cada solución explica por qué la opción correcta lo es y por qué las demás fallan; usalas para repasar, no solo para calificarte.

RESPUESTA 1: B. Una LAN (red de área local) cubre un área pequeña como un edificio o una oficina y es administrada por una sola organización, justo el caso de la escuela. A) es incorrecta: una WAN cubre áreas geográficas grandes (ciudades, países) y normalmente usa enlaces contratados a terceros. C) es incorrecta: una MAN cubre una ciudad completa, no un solo edificio. D) es incorrecta: una PAN es para dispositivos personales a pocos metros, como tu teléfono y tus audífonos, no para 40 computadoras. Tip para el examen: LAN = Local, MAN = Metropolitana, WAN = Amplia (wide); el alcance geográfico es la pista.

RESPUESTA 2: B. El servidor centraliza y provee recursos (archivos, impresoras, páginas web, correo) a los clientes que los solicitan. A) describe al cliente, no al servidor: es el que pide, no el que da. C) es incorrecta: conectar cables físicamente es función del cableado y los switches, no del modelo cliente-servidor. D) es incorrecta: traducir nombres a IPs es función del DNS. En redes pequeñas también existe el modelo punto a punto (peer-to-peer), donde no hay servidor dedicado y todos los equipos comparten por igual.

RESPUESTA 3: B. Hay 8 bits en cada byte, así que divides 200 entre 8 y obtienes 25 MB/s teóricos. A) es incorrecta: confunde bits con bytes, el error más común al leer velocidades de internet. C) es incorrecta: multiplica por 8 en vez de dividir, lo que daría kilobits, no megabytes. D) es incorrecta: divide entre 10 en vez de entre 8; la relación bit-byte es base 8, no base 10. Tip práctico: cuando tu navegador descarga a "25 MB/s" habla de megabytes, cuando el ISP anuncia "200 Mbps" habla de megabits; para convertir, siempre divide entre 8.

RESPUESTA 4: F. El ancho de banda es la capacidad máxima teórica del enlace (lo que contratas, por ejemplo 200 Mbps). El throughput es la velocidad real medida, siempre menor por el overhead de los protocolos, la latencia y la congestión. Ejemplo: contratas 200 Mbps de ancho de banda pero en hora pico mides 140 Mbps de throughput; la diferencia se la comen la congestión y los encabezados de los protocolos. Por eso tú descarga real rara vez alcanza el número contratado: uno es el techo teórico y el otro es lo que de verdad viaja.

RESPUESTA 5: Respuesta modelo: instalaría un switch central de 24 puertos en topología estrella, con cable UTP categoría 5e o 6 desde cada equipo hasta el switch, y un router conectado al módem del ISP como puerta de enlace. La estrella es la elección correcta porque es fácil de administrar y de ampliar, si falla un cable solo cae un equipo y el switch evita las colisiones del hub. El router separa la red interna de internet y normalmente aporta NAT y DHCP. La impresora se conecta por red directamente al switch para que todos la compartan. Como extra: reservaría IPs estáticas para la impresora y el router, dejaría al DHCP del router asignar direcciones a los 20 equipos y documentaría el diagrama físico y lógico. Si la oficina crece, el switch de 24 puertos deja 4 libres para expansiones inmediatas.

RESPUESTA 6: C. La capa 3 (red) es donde vive el direccionamiento lógico IP y el ruteo entre redes. A) es incorrecta: la capa 1 solo maneja señales eléctricas, conectores y bits. B) es incorrecta: la capa 2 usa direcciones MAC y es el terreno de los switches, no de los routers. D) es incorrecta: la capa 7 es para servicios y aplicaciones del usuario, como el navegador o el correo. Truco para el examen: asocia cada dispositivo con su capa: hub en capa 1, switch en capa 2, router en capa 3; el firewall puede operar en capas 3, 4 y hasta 7.

RESPUESTA 7: B. El orden de encapsulación es: segmento (capa 4) dentro de un paquete o datagrama IP (capa 3), luego dentro de una trama Ethernet (capa 2) y al final como bits (capa 1). A) es incorrecta: la trama viene después del paquete, no antes. C) es incorrecta: los bits son el último paso, sobre el medio físico. D) es incorrecta: no existe una "sesión de aplicación" como unidad de encapsulación en este orden. Piensalo como meter una carta en sobres cada vez más grandes: cada capa agrega su encabezado, y al recibir se hace lo inverso (desencapsulación), quitando un sobre por capa.

RESPUESTA 8: D. Un cable cortado es un problema del medio físico: sin señal eléctrica, nada de las capas superiores puede funcionar. A), B) y C) son incorrectas: aplicación, transporte y red dependen de que la capa física entregue bits; si el cable está cortado, el diagnóstico empieza y termina en la capa 1. En la práctica, ante una caída total primero

miras los LEDs del switch y de la tarjeta de red: si están apagados, el problema es físico antes de pensar en configuraciones. Por eso el diagnóstico ordenado siempre empieza abajo.

RESPUESTA 9: V. La capa 4 (transporte) ofrece comunicación extremo a extremo entre aplicaciones: TCP orientado a conexión y confiable, UDP sin conexión y más rápido. Ambos viven en la misma capa; la diferencia está en el servicio que ofrecen (confiabilidad contra velocidad), no en la capa a la que pertenecen. Mnemotécnica: la capa 4 es el "transporte", como la paquetería que lleva tus segmentos; TCP es correo certificado (llega seguro, con acuse) y UDP es correo normal (rápido, sin garantía).

RESPUESTA 10: Respuesta modelo: capa 7 aplicación, el cliente de correo donde redactas el mensaje; capa 6 presentación, da formato al contenido y puede cifrarlo; capa 5 sesión, establece y mantiene la sesión con el servidor de correo; capa 4 transporte, TCP divide el mensaje en segmentos, les pone números de puerto y garantiza la entrega ordenada; capa 3 red, IP pone las direcciones origen y destino y los routers lo encaminan por la mejor ruta; capa 2 enlace de datos, Ethernet lo mueve con direcciones MAC dentro de tu red local; capa 1 física, convierte todo en señales eléctricas que viajan por el cable. Para memorizar el orden de la 7 a la 1 usa la frase "Todas Las Personas Necesitan Transporte Seguro Físico": Aplicación, Presentación, Sesión, Transporte, Red, Enlace (seguro = security no, aquí es enlace), Física.

RESPUESTA 11: B. La regla clásica dice: dispositivos iguales (switch con switch, PC con PC) se conectan con cable cruzado, y dispositivos diferentes (PC con switch) con cable directo. A) es incorrecta: el directo es para PC a switch. C) y D) son incorrectas: el coaxial y la fibra son otros medios físicos, no tipos de terminación UTP. Nota: la mayoría de los switches modernos trae auto-MDIX y negocia solo el tipo de cable, pero en equipos viejos y en certificaciones la regla directo/cruzado sigue siendo pregunta segura.

RESPUESTA 12: C. En estrella cada nodo se conecta a un dispositivo central (switch): el fallo de un nodo no afecta a los demás, pero el central es punto único de falla. A) es incorrecta: en bus todos comparten un cable troncal y su ruptura tumba toda la red. B) es incorrecta: en anillo cada nodo depende de sus dos vecinos. D) es incorrecta: en malla completa no hay un dispositivo central único del que todo dependa. Por eso en redes críticas el dispositivo central se respalda con fuentes redundantes o se duplica: se elimina el punto único de falla.

RESPUESTA 13: C. Cat 6 soporta 10GBASE-T hasta 55 metros (y 1 Gbps hasta 100 metros). A) es incorrecta: Cat 5 solo llega a 100 Mbps. B) es incorrecta: Cat 5e llega a 1

Gbps, no a 10. D) es incorrecta: Cat 3 es para telefonía y redes de 10 Mbps. Para el examen memoriza la escalera: Cat5 = 100 Mbps, Cat5e = 1 Gbps, Cat6 = 10 Gbps (55 m), Cat6a = 10 Gbps (100 m).

RESPUESTA 14: V. En bus todos los nodos comparten el mismo cable troncal; al romperse, la señal no llega a ningún segmento y la red completa cae. El bus se reemplazó por la estrella justamente por esto: aislar las fallas por segmento en vez de tumbar toda la red con un solo corte en el cable.

RESPUESTA 15: Respuesta modelo: el par trenzado (UTP) es barato y fácil de instalar, llega a 1 o 10 Gbps hasta 100 metros, pero es vulnerable a interferencias electromagnéticas; ideal para el cableado de oficinas y hogares. El coaxial tiene mejor blindaje y más alcance que el UTP, se usa en TV por cable y en instalaciones antiguas. La fibra óptica es inmune a interferencias, alcanza decenas de kilómetros y velocidades altísimas, pero es más cara y frágil de instalar; ideal para backbones y enlaces entre edificios. Dato extra: la fibra puede ser monomodo (largas distancias, láser) o multimodo (cortas, LED); el par trenzado se divide en blindado (STP) y no blindado (UTP).

RESPUESTA 16: B. La clase B va de 128.0.0.0 a 191.255.255.255 (primer octeto entre 128 y 191); 172 cae dentro de ese rango. A) es incorrecta: la clase A va de 1 a 126 en el primer octeto. C) es incorrecta: la clase C va de 192 a 223. D) es incorrecta: la clase D va de 224 a 239 y es para multicast, no para asignar a hosts. Memoriza los rangos por el primer octeto: A 1-126, B 128-191, C 192-223, D 224-239 (multicast), E 240-255 (experimental).

RESPUESTA 17: B. Los rangos privados son 10.0.0.0/8, 172.16.0.0/12 y 192.168.0.0/16; 192.168.1.1 pertenece al tercero. A) es incorrecta: 8.8.8.8 es pública (DNS de Google). C) es la trampa clásica: parece privada pero NO lo es, porque el rango privado de clase B termina en 172.31.255.255 y 172.32.0.1 ya es pública. D) es incorrecta: 203.0.113.5 es pública del rango de documentación TEST-NET-3. El rango 172.16.0.0/12 es el más tramposo del examen: solo de 172.16.x.x a 172.31.x.x es privado; 172.15.x.x y 172.32.x.x ya son públicos.

RESPUESTA 18: A. Con máscara 255.255.255.0 (/24) los primeros tres octetos son red y el último es host, así que la red es 192.168.10.0. B) es incorrecta: 192.168.10.77 es la dirección del host, no de la red. C) es incorrecta: 192.168.10.255 es la dirección de broadcast de esa red. D) es incorrecta: mezcla octetos; la red es 192.168.10.x, no 192.168.0.x. Truco rápido: con /24 la dirección de red siempre termina en .0 y el broadcast en .255; solo cambia si la máscara es distinta.

RESPUESTA 19: F. 127.0.0.1 es la dirección de loopback: apunta a tu propia máquina y el tráfico nunca sale a la red física. Sirve para probar que tu stack TCP/IP local funciona, no para comunicarte con otros equipos. Todo el rango 127.0.0.0/8 es loopback, aunque en la práctica solo se usa 127.0.0.1.

RESPUESTA 20: Respuesta modelo: la dirección 169.254.12.44 es APIPA: el equipo no pudo obtener IP por DHCP y se autoasigna una del rango 169.254.0.0/16, lo que confirma la máscara 255.255.0.0. La puerta de enlace vacía significa que no hay salida hacia internet ni hacia otras redes. El problema detectado es una falla de DHCP: el servidor puede estar caído, el cable desconectado o el puerto del switch sin servicio. Pasos: revisar el enlace físico, luego el servidor DHCP y su alcance de direcciones. Si el servidor está bien, verifica que el alcance no se haya agotado y que no haya un DHCP pirata (un equipo dando IPs falsas) en la red.

RESPUESTA 21: A. Un /26 deja 6 bits para hosts: $2^6 = 64$ direcciones, menos la de red y la de broadcast, quedan 62 utilizables. B) es incorrecta: olvida restar la dirección de red y la de broadcast. C) es incorrecta: 126 utilizables corresponden a un /25. D) es incorrecta: 30 utilizables corresponden a un /27. Fórmula general: 2 elevado a los bits de host, menos 2. Para /26: $32 - 26 = 6$ bits, $64 - 2 = 62$.

RESPUESTA 22: B. Un /27 tiene 27 bits en 1; en el último octeto quedan 11100000, que es $128+64+32 = 224$. A) es incorrecta: 192 (11000000) corresponde a /26. C) es incorrecta: 240 (11110000) corresponde a /28. D) es incorrecta: 128 (10000000) corresponde a /25. Memoriza la tabla del último octeto: /25=128, /26=192, /27=224, /28=240, /29=248, /30=252.

RESPUESTA 23: A. Con VLSM das a cada subred solo lo que necesita: 50 hosts requieren 6 bits de host (/26 = 62 utilizables), así que 192.168.0.0/26 cubre de .0 a .63; 12 hosts requieren 4 bits (/28 = 14 utilizables), y el siguiente bloque libre es 192.168.0.64/28 (de .64 a .79). B) es incorrecta: desperdicia dos /24 completos y la segunda red ni siquiera está dentro de 192.168.0.0/24. C) es incorrecta: un /28 solo da 14 direcciones, insuficientes para 50 hosts. D) funciona pero es incorrecta por desperdicio: dos /25 entregan 126 direcciones útiles cada uno para necesidades de 50 y 12. Regla de oro de VLSM: ordeña las subredes de mayor a menor tamaño y asigna bloques alineados; así evitas traslapes y huecos.

RESPUESTA 24: V. VLSM (máscara de subred de longitud variable) permite usar máscaras de distinto tamaño dentro de la misma red, asignando a cada subred solo los bits de host que necesita. Sin VLSM, con tamaño fijo, para subredes de 50 y 12 hosts tendrías que entregar dos /26 y desperdiciar 48 direcciones en la segunda subred. VLSM es la base del diseño eficiente de redes modernas.

RESPUESTA 25: Respuesta modelo: 4000 hosts necesitan 12 bits de host ($2^{12} - 2 = 4094$), o sea un /20: bloque 10.0.0.0/20, rango utilizable 10.0.0.1 a 10.0.15.254, broadcast 10.0.15.255. Para 500 hosts se necesitan 9 bits ($2^9 - 2 = 510$), o sea un /23, tomando el siguiente espacio libre: bloque 10.0.16.0/23, utilizables 10.0.16.1 a 10.0.17.254, broadcast 10.0.17.255. El enlace punto a punto necesita solo 2 direcciones: un /30, bloque 10.0.18.0/30, utilizables 10.0.18.1 y 10.0.18.2, broadcast 10.0.18.3. Verificación: los tres bloques no se traslapan y caben dentro de 10.0.0.0/16; aún sobra espacio desde 10.0.18.4 hasta 10.0.255.255 para crecer.

RESPUESTA 26: B. El switch construye su tabla CAM asociando cada dirección MAC con el puerto por dónde la vio, y así reenvía las tramas unicast solo al puerto correcto en vez de inundar la red. A) es incorrecta: asignar IPs es función de DHCP. C) es incorrecta: traducir direcciones privadas a públicas es función de NAT en el router. D) es incorrecta: un switch básico no cifra tráfico. Dato de seguridad: la tabla CAM tiene tamaño limitado; un ataque de MAC flooding la llena para forzar al switch a comportarse como hub, por eso existe la seguridad de puerto (port security).

RESPUESTA 27: C. Sin una ruta válida (ni específica ni por defecto) el router no puede reenviar el paquete: lo descarta y, si los ICMP no están filtrados, avisa al origen con "destino inalcanzable". A) es incorrecta: reenviar por todos los puertos es comportamiento de hub o de broadcast en switch, no de un router. B) es incorrecta: los routers no almacenan paquetes esperando rutas futuras. D) es incorrecta: la fragmentación ocurre por tamaño de MTU, no por falta de ruta. En la práctica verás este ICMP como "Destination host unreachable" al hacer ping a una red que tu router no conoce.

RESPUESTA 28: A. Las VLANs separan dominios de broadcast en capa 2, así que para pasar tráfico de una a otra se necesita ruteo inter-VLAN en capa 3, ya sea con un router o con un switch capa 3. B) es incorrecta: más switches en cascada no cruzan la segmentación lógica de las VLANs. C) es incorrecta: cambiar el medio físico no cambia la segmentación lógica. D) es incorrecta: STP evita bucles; desactivarlo no conecta VLANs y puede tumbar la red. El estándar que lo implementa es 802.1Q con etiquetado, y al enlace que lleva varias VLANs entre switch y router se le llama troncal (trunk).

RESPUESTA 29: F. El hub es un repetidor multipuerto de capa 1: repite todo lo que recibe por TODOS sus puertos, sin distinguir destinos. El que reenvía únicamente al puerto del equipo destino es el switch, gracias a su tabla de direcciones MAC. Por eso los hubs quedaron obsoletos: generan un solo dominio de colisión y desperdician ancho de banda repitiendo todo a todos.

RESPUESTA 30: Respuesta modelo: en el ruteo estático el administrador escribe las rutas a mano; es simple, no genera tráfico de protocolos y es ideal para redes pequeñas o para rutas por defecto, pero no se adapta solo ante fallos. En el ruteo dinámico los routers intercambian información y recalculan rutas automáticamente; es ideal para redes medianas y grandes con redundancia. En una empresa mediana con varios routers usaría OSPF: es estándar abierto (funciona con equipos de cualquier marca), converge rápido y se organiza por áreas. RIP quedo corto (convergencia lenta y límite de 15 saltos) y EIGRP históricamente fue propietario de Cisco. Menciona también la distancia administrativa: si una ruta estática (distancia 1) compite con una de OSPF (110) por el mismo destino, gana la estática.

RESPUESTA 31: A. DORÁ resume el proceso: el cliente envía Discover por broadcast buscando servidor, el servidor responde con Offer proponiendo una IP, el cliente envía Request solicitando esa IP y el servidor cierra con Acknowledge confirmando la concesión. Las demás opciones alteran el orden y rompen la lógica: no puedes solicitar una IP antes de descubrir servidores (B), ni confirmar antes de ofrecer (C), ni pedir antes de que te ofrezcan (D). Dato técnico: los mensajes DHCP viajan en UDP con puerto 67 en el servidor y 68 en el cliente; el Discover inicial es un broadcast porque el cliente aún no tiene IP.

RESPUESTA 32: A. El registro A (address) mapea un nombre de dominio a una dirección IPv4. B) es incorrecta: AAAA es su equivalente para IPv6. C) es incorrecta: MX define los servidores de correo del dominio. D) es incorrecta: CNAME crea un aliás de un nombre hacia otro nombre, no hacia una IP. Otros registros útiles que verás en la práctica: NS (servidores autoritativos del dominio), TXT (verificaciones como SPF) y PTR (resolución inversa, de IP a nombre).

RESPUESTA 33: C. NAT traduce las direcciones privadas internas a la IP pública del router (y de regreso), multiplexando muchas conexiones internas en una sola dirección pública mediante puertos. A) es incorrecta: DHCP asigna las IPs internas, no las traduce hacia internet. B) es incorrecta: DNS resuelve nombres, no traduce direcciones. D) es incorrecta: VLAN segmenta la LAN, no da salida a internet. El NAT de tu casa suele ser PAT (NAT con sobrecarga): distingue cada conexión por su puerto de origen, y así miles de sesiones comparten una sola IP pública sin confundirse.

RESPUESTA 34: V. Esa es exactamente la función del DNS: resolver los nombres legibles que escribes (como `lucasegaacademy.com`) a las direcciones IP numéricas que las máquinas entienden. El proceso completo se llama resolución: tu equipo pregunta a un DNS recursivo, este recorre los servidores raíz, los de TLD y el autoritativo hasta devolverte la IP. Sin DNS tendrías que memorizar números para cada sitio que visitas.

RESPUESTA 35: Respuesta modelo: primero descarto DHCP con `ipconfig`: si el equipo tiene una IP válida, máscara y puerta de enlace, DHCP funciona; si tiene `169.254.x.x` (APIPA), el problema es DHCP. Segundo, hago ping a la puerta de enlace y a `8.8.8.8`: si responden, hay conectividad IP y el fallo al navegar apunta a DNS. Tercero, pruebo con `nslookup google.com`: si no resuelve, el problema es DNS (reviso los servidores DNS configurados en el equipo o en el DHCP). El NAT solo entra en escena si ningún equipo de la red interna sale a internet: ahí reviso la configuración de NAT en el router. En este caso, como el ping a `8.8.8.8` si funciona, lo más probable es un problema de DNS. Comando extra útil: `"ipconfig /all"` muestra también los DNS asignados; si están vacíos o mal, ahí está la falla aunque el ping funcione.

RESPUESTA 36: A. Es válida: 8 grupos hexadecimales con `::` comprimiendo los ceros una sola vez. B) es inválida: la letra "g" no es un dígito hexadecimal. C) es inválida: `::` solo puede usarse una vez en una dirección. D) es inválida: está incompleta, tiene 3 grupos sin compresión válida. Regla de compresión: el `::` se usa una sola vez y solo para el grupo de ceros más largo; `"2001:db8:0:0:0:0:1"` se escribe `"2001:db8::1"`.

RESPUESTA 37: B. A mayor frecuencia hay más velocidad potencial pero menor alcance y peor penetración de muros: 5 GHz es rápida a corta distancia. A) es incorrecta: es al revés, 2.4 GHz llega más lejos y atraviesa mejor los muros, pero es más lenta y suele estar congestionada. C) y D) son incorrectas: ignoran la física de las ondas de radio, donde la frecuencia sí determina alcance y velocidad. Recomendación práctica: 5 GHz para velocidad cerca del router y 2.4 GHz para llegar lejos o atravesar muros.

RESPUESTA 38: B. `fe80::/10` son direcciones link-local: se autoconfiguran en cada interfaz IPv6 y solo son válidas dentro del mismo segmento físico, nunca se rutean a internet. A) es incorrecta: la comunicación global usa unicast global (`2000::/3`). C) es incorrecta: multicast es `ff00::/8`. D) es incorrecta: loopback es `::1`. La verás en `"ipconfig"` como una dirección `fe80::` seguida de un `"%"` con el número de interfaz; es normal y no indica ningún problema.

RESPUESTA 39: V. Con 128 bits el espacio de direcciones es prácticamente inagotable y cada dispositivo puede tener su propia IP global; NAT nació para paliar la escasez de

direcciones IPv4, así que en IPv6 ya no se necesita para compartir una IP. Para dimensionarlo: con 128 bits hay 340 sextillones de direcciones, podrías asignar una IP a cada grano de arena de la Tierra y sobrarían. Ojo: los firewalls siguen existiendo en IPv6 para controlar el tráfico, solo que ya no hace falta traducir direcciones.

RESPUESTA 40: Respuesta modelo: causas probables: saturación de canales en 2.4 GHz (solo los canales 1, 6 y 11 no se traslapan y los vecinos los saturan), interferencia de microondas o Bluetooth, demasiados dispositivos conectados y router mal ubicado o con firmware viejo. Acciones: analizar el espectro con una app Wi-Fi y cambiar a un canal libre, migrar los equipos que lo soporten a la banda de 5 GHz, colocar el router en alto y al centro del departamento, actualizar su firmware y, si nada basta, considerar una red en malla o un repetidor bien ubicado. También verificar que la seguridad sea WPA2 o WPA3. Si el problema persiste, mide con speedtest por cable: si por cable va bien y por Wi-Fi no, el problema es 100% inalámbrico y no del ISP.

RESPUESTA 41: B. El firewall stateful guarda una tabla con el estado de las conexiones activas y permite los paquetes de respuesta de conexiones iniciadas desde dentro, bloqueando el tráfico no solicitado. A) es incorrecta: filtrar solo por MAC es un filtrado básico de capa 2, no stateful. C) es incorrecta: cifrar el tráfico es función de VPN o TLS, no del firewall. D) es incorrecta: asignar IPs es función de DHCP. Un firewall sin estado (stateless) filtra cada paquete por reglas fijas sin contexto; el stateful es más inteligente pero consume más memoria.

RESPUESTA 42: B. Es un DDoS (ataque distribuido de denegación de servicio): muchas fuentes coordinadas saturan los recursos del objetivo hasta dejarlo sin servicio. A) es incorrecta: el phishing es engaño por correo o mensajes para robar credenciales. C) es incorrecta: man-in-the-middle es interceptar la comunicación entre dos partes, no saturar un servidor. D) es incorrecta: el spoofing de ARP falsifica mensajes en la LAN; por si solo no genera saturación masiva desde cientos de IPs. Defensas típicas: servicios anti-DDoS en la nube, limitar la tasa de peticiones (rate limiting) y esconder la IP real del servidor tras un proxy o CDN.

RESPUESTA 43: C. WPA3 es el estándar actual: usa cifrado más fuerte con el método SAE y protege contra ataques de diccionario. A) es incorrecta: WEP está roto desde hace años y se crackea en minutos. B) es incorrecta: WPA con TKIP quedo obsoleto y es vulnerable. D) es incorrecta: el filtrado por MAC no es seguridad real, las direcciones MAC se falsifican con facilidad. WPA3-Personal usa SAE (apretón de manos simultáneo de iguales), que evita el ataque de diccionario offline que sufría WPA2.

RESPUESTA 44: F. WEP se rompió hace más de 15 años: su vector de inicialización débil permite recuperar la clave con herramientas comunes en cuestión de minutos. Herramientas como Aircrack-ng recuperan una clave WEP capturando suficientes vectores de inicialización, a veces en menos de 5 minutos. Para una red doméstica usa WPA2 como mínimo y WPA3 si tus equipos lo soportan.

RESPUESTA 45: Respuesta modelo: primero confirmo. Reviso los logs del firewall para identificar la IP y la MAC de origen, analizo el tráfico con Wireshark o netflow para ver a dónde se conecta y que protocolo usa, y reviso los procesos del equipo sospechoso. Si confirma actividad maliciosa, contengo: aislo el equipo de la red (sin apagarlo para no perder evidencia volátil) y bloqueo la IP destino en el firewall. Después aplico medidas preventivas: antivirus y antimalware actualizados, cambio de credenciales, parches al día, segmentación con VLANs, un IDS/IPS y monitoreo continuo del tráfico saliente. Documenta todo con fechas y horas: si el incidente escala, ese registro es evidencia. Y comunica al equipo: la seguridad también es cultura.

RESPUESTA 46: A. El ping a 127.0.0.1 prueba tu propio stack TCP/IP: si responde, tu tarjeta de red y tu software están bien. El "tiempo de espera agotado" hacia la puerta de enlace apunta entonces al camino entre tu PC y el router: cable, puerto del switch o el propio router. B) es incorrecta: hiciste ping a una IP numérica, el DNS ni siquiera participa en la prueba. C) es incorrecta: no puedes asegurar que el cable este perfecto; de hecho es uno de los primeros sospechosos. D) es contradictoria: si la puerta de enlace respondiera, no habría tiempo de espera agotado. Orden de descarte sugerido: 1) ping a 127.0.0.1 (tu stack), 2) ping a tu propia IP (tu NIC), 3) ping al gateway (tu LAN), 4) ping a internet (tu salida). Dónde se rompa la cadena, ahí está la falla.

RESPUESTA 47: C. tracert (traceroute en Linux) lista cada salto hasta el destino con sus tiempos de respuesta, ideal para ubicar exactamente dónde se pierde o se atora el tráfico. A) es incorrecta: ping solo dice si hay respuesta y cuanto tarda, no muestra la ruta. B) es incorrecta: ipconfig muestra tu configuración IP local. D) es incorrecta: nslookup consulta servidores DNS, no traza rutas. Para leer la salida: cada línea es un salto; asteriscos o tiempos muy altos en un salto específico delatan dónde está el problema.

RESPUESTA 48: C. La metodología bottom-up empieza en la capa 1: sin enlace físico, nada de lo demás importa, así que primero revisas cable, LEDs del puerto y estado del enlace. A) y B) son incorrectas: el proxy y el DNS son capas altas; revisarlas primero es perder tiempo si el cable está desconectado. D) es incorrecta: reinstalar el sistema es la medida más drástica y casi nunca es el primer paso de un diagnóstico ordenado. Este enfoque se resume en "físico primero": cerca del 70% de las fallas de red en oficinas son de capa 1 (cables, conectores, energía).

RESPUESTA 49: V. Si llegas al destino por su número, la conectividad IP funciona; la falla está en la resolución de nombres: servidor DNS mal configurado, caído o bloqueado. Es la prueba clásica para separar un problema de red de un problema de DNS. Prueba de bolsillo: "ping 8.8.8.8" bien más "ping google.com" mal = DNS. Así de simple y así de útil en campo.

RESPUESTA 50: Respuesta modelo: primero defino el alcance: pregunto si afecta a todos o a algunos equipos, y si pasa en cableado, en Wi-Fi o en ambos. Segundo, mido por capas: ping a la puerta de enlace (si la latencia local es alta, el problema está en la LAN), ping a 8.8.8.8 (si falla o es lento, el problema es la salida a internet) y tracert para ubicar el salto lento. Tercero, reviso el consumo: alguien descargando, un respaldo programado justo a las 10:00 o un equipo infectado pueden saturar el enlace; un speedtest lo confirma. Cuarto, reviso el router: CPU, tabla de sesiones NAT saturada y logs. Quinto, pruebo DNS con nslookup por si la "lentitud" es en realidad resolución lenta de nombres. Voy descartando por etapas: si la LAN va bien y solo falla hacia afuera, es el enlace del ISP o el router; si es un solo equipo, el problema es local. Cierra el ciclo documentando: que encontraste, que hiciste y a que hora se normalizó; ese historial acelera el próximo diagnóstico.

Curso Completo de Redes (Networking)

Bienvenido a "Curso Completo de Redes (Networking)", el libro de Lucas EGA Academy para aprender desde cero cómo funcionan las redes que conectan al mundo. Este libro nació del curso en video de 30 clases de la academia, pero aquí tienes todo explicado con mucho más detalle: conceptos a fondo, analogías de la vida real, errores comunes de principiantes, buenas prácticas de la industria, ejemplos paso a paso con comandos reales para probar en tu computadora, prácticas con soluciones explicadas y un examen final para medir lo que aprendiste.

lucasegaacademy.com

Colibrí Editorial EGA