

Curso Completo de Wireless

Autor: Esteban

lucasegaacademy.com

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

Curso Completo de Wireless

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 inalámbricas (Clases 1 a 3)	9
UNIDAD 2: Bandas, canales y el espectro WiFi (Clases 4 a 6)	33
UNIDAD 3: Los estándares WiFi 802.11 (Clases 7 a 9)	56
UNIDAD 4: Tu router, pieza por pieza (Clases 10 a 12)	82
UNIDAD 5: Seguridad inalámbrica (Clases 13 a 15)	107
UNIDAD 6: Antenas y cobertura (Clases 16 a 18)	136
UNIDAD 7: Repetidores, puntos de acceso y redes mesh (Clases 19 a 21)	161
UNIDAD 8: Redes de invitados, control parental y QoS (Clases 22 a 24)	186
UNIDAD 9: Diagnóstico y solución de problemas (Clases 25 a 27)	209
UNIDAD 10: WiFi en el mundo real y lo que viene (Clases 28 a 30)	236
EXAMEN FINAL	258

PRÓLOGO

Bienvenido a "Curso Completo de Redes Inalámbricas (Wireless)", el libro de Lucas EGA Academy para entender de una vez por todas ese mundo invisible que te conecta con todo: el WiFi. 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 para aplicar en tu casa o tu negocio, prácticas con soluciones explicadas y un examen final para medir lo que aprendiste.

Piénsalo un momento: hoy casi todo lo que haces pasa por una red inalámbrica. Te despiertas y el celular ya se conectó solo al WiFi de tu casa. Trabajas en videollamadas que viajan por el aire de tu sala al router. Ves películas que llegan sin cables hasta tu pantalla. Incluso cuando sales, el café, el aeropuerto y el centro comercial te ofrecen su red. El WiFi es tan común que ya ni lo notas... hasta que falla. Y cuando falla, se siente como si se hubiera ido la luz.

Lo curioso es que casi nadie entiende cómo funciona. La mayoría de la gente trata su red WiFi como una caja mágica: si va lento, la reinician; si no llega al cuarto del fondo, se resignan; si el vecino se cuelga de su red, ni se enteran. Este libro existe para que tú no seas de esos. Al terminar, vas a entender qué viaja por el aire de tu casa, por qué unas redes son rápidas y otras no, cómo configurar tu router como un profesional, cómo proteger tu red de intrusos y cómo diagnosticar cualquier problema como lo haría un técnico.

A quién va dirigido este libro

Este libro es para ti si en tu casa el WiFi no llega bien a todos lados y ya te cansaste de adivinar. Es para ti si quieres montar la red de tu negocio, tu oficina o tu local y hacerlo bien desde el principio. Es para ti si estudias sistemas, redes o telecomunicaciones y quieres una base sólida y práctica antes de meterte a certificaciones. Y es para ti si simplemente eres curioso y quieres entender la tecnología que usas todos los días.

No necesitas saber programar ni tener conocimientos previos de redes. Empezamos desde cero absoluto: qué es una onda de radio, qué significa eso de 2.4 GHz que ves en la caja del router, por qué tu red se llama SSID en la configuración. Cada concepto se construye sobre el anterior, con analogías de la vida cotidiana para que nada se quede en el aire.

Si vienes de otros cursos de Lucas EGA Academy, este libro encaja perfecto: ya sabes de computadoras, de internet y de tecnología, y ahora vas a dominar la parte que conecta todo sin cables.

Por qué las redes inalámbricas son una habilidad que vale oro

Hablemos de frente: todo negocio moderno necesita WiFi que funcione. Restaurantes, cafés, oficinas, escuelas, consultorios, hoteles: todos dependen de una red inalámbrica estable, y casi ninguno tiene a alguien que la entienda de verdad. Saber diseñar, configurar y reparar redes WiFi es un servicio que se cobra bien y que siempre tiene demanda, porque el problema nunca desaparece: cada casa nueva, cada local nuevo, cada oficina nueva necesita su red.

Además es la puerta de entrada al mundo de las redes en general. Los conceptos que aprenderás aquí (bandas, canales, direccionamiento, seguridad, diagnóstico) son la base para después estudiar redes cableadas, certificaciones y administración de infraestructura. Muchos técnicos e ingenieros de redes empezaron justo aquí: configurando el router de su casa y preguntándose por qué no llegaba la señal al segundo piso.

Y en lo personal, el beneficio es inmediato: vas a dejar de sufrir tu propio WiFi. Vas a saber exactamente qué cambiar cuando algo falle, en lugar de reiniciar la caja y rezar.

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: qué verás y por qué importa.
- Explicación detallada: conceptos a fondo, analogías, errores comunes y buenas prácticas.
- Ejemplos paso a paso: configuraciones y comandos reales para aplicar de inmediato, explicados línea por línea.
- Práctica: ejercicios con soluciones explicadas paso a paso. Las redes se aprenden metiendo las manos, no solo leyendo.
- Resumen: los puntos clave para repasar rápido.

Al final hay un EXAMEN FINAL con 50 preguntas: opción múltiple, verdadero o falso y preguntas abiertas donde describirás configuraciones y resolverás casos. Cada respuesta viene explicada en las soluciones. Si lo resuelves con confianza, estás listo para configurar y cuidar redes inalámbricas reales.

Este es tu mapa:

Unidad 1: Fundamentos de las redes inalámbricas (Clases 1 a 3)

Desde cero absoluto. Clase 1: qué es una red inalámbrica y por qué cambió el mundo. Clase 2: ondas de radio, frecuencia y longitud de onda explicados sin fórmulas aterradoras. Clase 3: cómo viajan los datos por el aire. Terminas entendiendo el fenómeno físico que hace posible todo lo demás.

Unidad 2: Bandas, canales y el espectro WiFi (Clases 4 a 6)

El "terreno" donde vive el WiFi. Clase 4: las bandas de 2.4 GHz, 5 GHz y 6 GHz, con sus ventajas y desventajas. Clase 5: canales y ancho de canal, y por qué tus vecinos te pueden arruinar la velocidad. Clase 6: interferencia: qué la causa y cómo evitarla. Aprenderás a elegir el mejor canal como un profesional.

Unidad 3: Los estándares WiFi 802.11 (Clases 7 a 9)

El abecedario del WiFi. Clase 7: la familia 802.11 desde la b hasta la ac. Clase 8: WiFi 6, 6E y 7. Clase 9: velocidades teóricas contra velocidades reales, y por qué nunca alcanzas el número de la caja. Sabrás leer las especificaciones sin que te mareen.

Unidad 4: Tu router, pieza por pieza (Clases 10 a 12)

Manos a la obra con el aparato central. Clase 10: el router por dentro. Clase 11: primer encendido y panel de administración. Clase 12: configurar tu WiFi completo: nombre de red, bandas, canal y potencia. Terminas con un router configurado por ti, bien hecho.

Unidad 5: Seguridad inalámbrica (Clases 13 a 15)

La unidad que protege tu casa. Clase 13: WEP, WPA y WPA2, y la historia de por qué WEP está muerto. Clase 14: WPA3 y el cifrado moderno. Clase 15: contraseñas fuertes, WPS y tu lista de verificación de seguridad. Nadie se va a colgar de tu red sin que te enteres.

Unidad 6: Antenas y cobertura (Clases 16 a 18)

Para que la señal llegue a todos lados. Clase 16: tipos de antenas. Clase 17: ganancia, polarización y MIMO. Clase 18: dónde poner el router y cómo orientar las antenas. Adiós a las zonas muertas.

Unidad 7: Repetidores, puntos de acceso y redes mesh (Clases 19 a 21)

Cuando un solo router no basta. Clase 19: repetidores, cómo funcionan y sus trampas. Clase 20: puntos de acceso cableados, la solución profesional. Clase 21: sistemas mesh y roaming sin cortes. Sabrás elegir la solución correcta para cada casa.

Unidad 8: Redes de invitados, control parental y QoS (Clases 22 a 24)

Tu red, bajo control. Clase 22: red de invitados separada y segura. Clase 23: control parental con horarios y filtros. Clase 24: QoS para que las videollamadas y los juegos nunca se traben.

Unidad 9: Diagnóstico y solución de problemas (Clases 25 a 27)

Piensa como técnico. Clase 25: medir tu red e interpretar los números. Clase 26: herramientas de diagnóstico. Clase 27: los problemas más comunes y cómo resolverlos paso a paso.

Unidad 10: WiFi en el mundo real y lo que viene (Clases 28 a 30)

Del hogar al mundo. Clase 28: WiFi para negocios. Clase 29: cómo protegerte en redes públicas. Clase 30: el futuro: WiFi 7, LiFi y las tendencias que vienen.

Cómo estudiar este libro

No lo leas como novela. Cada unidad está diseñada para estudiarse en una o dos sesiones: lee la explicación, haz los ejemplos en tu propio router o con tu celular, resuelve la práctica sin mirar las soluciones primero y cierra con el resumen. Si un concepto no te queda claro a la primera, las analogías están ahí para eso: vuelve a leerlas.

Ten a la mano tu celular y, si puedes, acceso al panel de tu router. La mitad del aprendizaje de este libro ocurre cuando comparas lo que lees con lo que ves en tu propia red. Mide tu señal en cada cuarto, revisa en qué canal estás, entra a la configuración y reconoce cada opción que el libro menciona. Esa práctica convierte la teoría en habilidad.

No te saltes las prácticas. Están diseñadas para que te equivoques en un ambiente seguro y aprendas de cada error, con la solución explicada paso a paso. Y cuando termines las 10 unidades, haz el examen final completo, de una sentada, como si fuera real. Si sacas menos de 80, repasa las unidades donde fallaste y vuelve a intentarlo.

Una nota sobre marcas y modelos

En este libro hablamos de routers, configuraciones y opciones de forma genérica: los menús cambian entre marcas, pero los conceptos son los mismos en todos. Cuando veas una ruta de menú como "Inalámbrico > Seguridad", úsala como guía y busca el equivalente en tu modelo. Lo importante no es memorizar dónde está cada botón, sino entender qué hace cada ajuste y por qué lo estás cambiando.

¿Listo? Vamos a conquistar el aire. Empieza la Unidad 1.

UNIDAD 1: Fundamentos de las redes inalámbricas (Clases 1 a 3)

Esta unidad reúne las tres primeras clases del curso: Clase 1, qué es una red inalámbrica y por qué cambió el mundo; Clase 2, ondas de radio, frecuencia, longitud de onda y cómo viajan; y Clase 3, cómo viajan los datos por el aire, es decir, señal analógica contra señal digital, modulación básica y ancho de banda. Al terminar, tendrás los cimientos sobre los que se construye todo lo demás del libro: sin entender qué es una onda de radio y cómo se le montan los datos encima, el resto de las unidades (WiFi, seguridad, antenas, enlaces, redes móviles) parecería magia. No es magia. Es física sencilla, y esta unidad la va a convertir en intuición.

Introducción

Piensa en la última vez que hiciste algo inalámbrico sin pensar en ello. Despertaste y apagaste la alarma del celular, te conectaste al WiFi de la casa sin escribir nada porque el teléfono se acordó solo, mandaste un mensaje de voz por WhatsApp mientras el microondas calentaba el café, te subiste al carro y el Bluetooth enlazó el teléfono con el estéreo antes de que cerraras la puerta. Nada de eso existía de manera práctica hace treinta años. Tus abuelos, para llamar por teléfono, estaban atados a un cable pegado a la pared; si querían cambiar de canal de televisión, se levantaban del sillón; y "conectarse" a algo era enchufar un cable con un ruido seco de plástico.

Lo inalámbrico no es solo una comodidad. Es una de las transformaciones más profundas que ha vivido la humanidad desde la electricidad. Antes de las redes inalámbricas, cada dato necesitaba un camino físico: un cable de cobre, una fibra de vidrio, una carretera de metal que uniera el punto A con el punto B. Si no había cable, no había comunicación. Eso significaba que llevar internet a un pueblo de la sierra, a una ranchería, a una comunidad pesquera en la costa, costaba cavar zanjas, colgar postes y tender kilómetros de cable que a veces nadie podía pagar. Las redes inalámbricas rompieron esa barrera: el aire se convirtió en el camino. El aire es gratis, está en todas partes y no hay que cavar nada para usarlo.

Por eso esta unidad importa más de lo que parece. No estamos estudiando un tema de "tecnología para nerds". Estamos estudiando la infraestructura invisible sobre la que corre la vida moderna: el trabajo remoto que te permite ganar en dólares viviendo en tu pueblo, la videollamada con tu familia, la clase en línea de tu hijo, el pago con tarjeta en la tiendita de la esquina, el Uber que llega porque el conductor tiene datos móviles. Todo eso viaja por el aire en forma de ondas de radio. Entender cómo lo hace te convierte de usuario pasivo en alguien

que puede diagnosticar problemas, mejorar su propia red, ayudar a otros y, si quieres, ganarte la vida con esto.

¿Qué lograrás al terminar esta unidad? Cuatro cosas concretas. Primera: vas a poder explicar con tus propias palabras qué es una red inalámbrica y por qué cambió el mundo, sin recitar definiciones de memoria, sino entendiendo el antes y el después. Segunda: vas a dominar el vocabulario de las ondas: frecuencia, longitud de onda, amplitud, espectro electromagnético, y las unidades Hz, kHz, MHz y GHz, que aparecen en cada caja de router, en cada ficha técnica de celular y en cada examen de certificación. Tercera: vas a entender cómo los datos viajan por el aire, es decir, la diferencia entre una señal analógica y una digital, qué es la modulación y qué es el ancho de banda, que son las ideas que explican por qué tu WiFi es rápido o lento. Cuarta: vas a poder abrir una terminal o la configuración de tu celular y ver con tus propios ojos la señal, la frecuencia y la velocidad de tu red, usando comandos reales de diagnóstico. Teoría más práctica, desde el día uno: esa es la filosofía de Lucas EGA Academy.

El panorama general de la unidad es el siguiente. Empezamos con la Clase 1: la historia y el concepto. Veremos qué es exactamente una red inalámbrica, qué tipos existen (las vas a conocer por sus nombres: WPAN, WLAN, WMAN, WWAN), y haremos un recorrido por cómo pasamos del telégrafo sin hilos de Marconi a los 5G de hoy. Después, la Clase 2 nos mete a la física: las ondas de radio. Aquí aprenderás que una onda de radio es lo mismo que la luz, solo que con otra frecuencia; que la frecuencia se mide en hertz; que la longitud de onda y la frecuencia están casadas por una fórmula sencillísima; y que las ondas se propagan, rebotan, se absorben y se debilitan según el medio. Con analogías de la vida real (la radio AM/FM de tu abuelo, gritar en una fiesta ruidosa, tirar piedras a un estanque) todo esto se vuelve obvio. Finalmente, la Clase 3 responde la pregunta del millón: ¿cómo viajan los DATOS por el aire? Veremos la diferencia entre señal y datos (una distinción que confunde a casi todos los principiantes), qué es una señal analógica y qué es una digital, cómo la modulación "monta" los unos y ceros sobre la onda, y qué es el ancho de banda y por qué determina la velocidad.

Una advertencia honesta antes de empezar: esta unidad tiene matemáticas, pero son matemáticas de primaria. La fórmula más difícil que vas a ver es una división: longitud de onda igual a velocidad de la luz entre frecuencia. Si sabes dividir, ya estás del otro lado. Y tiene física, pero es física de sentido común: las paredes frenan las ondas, el metal las refleja, el agua las absorbe. Todo lo que sigue se construye sobre ideas que ya conoces de la vida diaria; nuestro trabajo es darles nombre técnico.

Cómo usar esta unidad: lee la explicación detallada con calma, sin prisa por llegar a los comandos. Las analogías están ahí por una razón: cuando en la Unidad 5 hablemos de por qué tu WiFi de 5 GHz no atraviesa dos paredes, vas a recordar la analogía de esta unidad y todo va a encajar. Haz los ejemplos paso a paso frente a tu computadora o tu celular, no solo

con los ojos: escribe los comandos, mira tu propia señal, recorre tu casa midiendo. Y haz la práctica de verdad, con lápiz y papel para los cálculos; los ejercicios están diseñados para que el conocimiento se te quede en las manos, no solo en la cabeza.

Al final de la unidad hay un resumen para repaso rápido. Úsalo antes de pasar a la Unidad 2, y vuelve a él cada vez que un concepto posterior te suene a medias. Los fundamentos no se aprenden una vez: se repasan siempre. Vamos a empezar.

Explicación detallada

Qué es una red inalámbrica, en palabras simples

Una red inalámbrica es un conjunto de dispositivos que se comunican entre sí sin necesidad de un cable físico que los una, usando ondas electromagnéticas que viajan por el aire (y en general por el espacio). Eso es todo. Cuando tu celular se conecta al WiFi de tu casa, cuando tus audífonos se enlazan por Bluetooth, cuando la torre de telefonía te da datos móviles, estás usando una red inalámbrica.

Fíjate en lo que NO dice la definición: no dice "internet". Internet y red inalámbrica no son lo mismo. Internet es la red mundial de redes; lo inalámbrico es solo el medio por el que viajan los datos en el último tramo. Tu WiFi casero, por ejemplo, es inalámbrico entre tu celular y el router, pero del router al proveedor de internet casi siempre hay un cable (fibra óptica, cable coaxial o par de cobre). Decir "no tengo internet" cuando se cayó el WiFi es técnicamente impreciso: lo que se cayó fue tu red inalámbrica local, o el enlace de tu proveedor, y son cosas distintas. Esta distinción te va a ahorrar horas de diagnóstico en el futuro: cuando algo falle, lo primero es preguntar ¿dónde se rompió la cadena? ¿En el tramo inalámbrico o en el tramo cableado?

Tampoco dice la definición que lo inalámbrico sea "mejor" que lo cableado. Es más cómodo y más flexible, pero un cable casi siempre es más rápido, más estable y más seguro que el aire. El aire es un medio compartido: todos los vecinos, el microondas, los audífonos Bluetooth y la red del café de enfrente están usando el mismo aire que tú. Un cable es un camino privado. Guarda esta idea: lo inalámbrico gana en movilidad y pierde en control del medio. Esa tensión explica casi todos los problemas y todas las soluciones que verás en este libro.

Los cuatro tamaños de las redes inalámbricas: WPAN, WLAN, WMAN y WWAN

Las redes inalámbricas se clasifican por su alcance, es decir, por qué tan lejos llegan. Hay cuatro categorías y conviene aprenderlas desde ahora porque aparecen en todas las

certificaciones y en toda la documentación técnica. Piensa en ellas como círculos concéntricos alrededor de tu cuerpo.

La WPAN (Wireless Personal Area Network, red inalámbrica de área personal) es la más pequeña: unos cuantos metros alrededor de ti. Es tu espacio personal. Bluetooth es el ejemplo clásico: tus audífonos, tu reloj inteligente, el control de tu consola, el teclado inalámbrico. Alcance típico: de 1 a 10 metros. Velocidades modestas, consumo de energía bajísimo. Su trabajo no es mover películas en 4K, sino conectar tus cosas contigo.

La WLAN (Wireless Local Area Network, red inalámbrica de área local) es la de tu casa, tu escuela o tu oficina: decenas de metros. WiFi es el ejemplo por excelencia. Alcance típico: de 30 a 100 metros en interiores, más en espacios abiertos. Es la red que más vas a configurar, diagnosticar y optimizar en tu vida, y por eso gran parte de este libro gira alrededor de ella.

La WMAN (Wireless Metropolitan Area Network, red inalámbrica de área metropolitana) cubre una ciudad o una zona amplia: kilómetros. El ejemplo histórico es WiMAX, una tecnología que quiso llevar internet inalámbrico a ciudades enteras. Hoy este espacio lo ocupan más bien los enlaces punto a punto de los proveedores y algunas redes comunitarias. Alcance: varios kilómetros.

La WWAN (Wireless Wide Area Network, red inalámbrica de área amplia) es la de los celulares: la red móvil. 4G, 5G y sus antecesoras. Cubre ciudades, carreteras, países enteros mediante miles de torres (radiobases) que se pasan tu llamada o tus datos de una a otra mientras te mueves. Alcance: decenas de kilómetros por torre, cobertura nacional por el conjunto.

Un truco para no confundirlas: PAN es Personal (tu cuerpo), LAN es Local (tu casa), MAN es Metropolitana (tu ciudad), WAN es Wide, amplia (tu país). Y fíjate que el WiFi y el Bluetooth, aunque los usas todos los días, viven en categorías distintas: Bluetooth es PAN, WiFi es LAN. Cuando alguien dice "se me desconectó la red", un técnico lo primero que ubica es en qué categoría está el problema, porque cada una tiene sus herramientas y sus culpables habituales.

Por qué cambió el mundo: el antes y el después

Para entender la revolución, hay que recordar el mundo con cables. En los años noventa, una oficina típica era una jungla de cables: cada computadora necesitaba un cable de red hasta un switch, cada teléfono un cable hasta la pared, cada impresora su cable. Mover un escritorio de lugar era un proyecto de media tarde. Instalar internet en una escuela rural implicaba obra civil. Y el teléfono móvil, cuando por fin llegó, era un ladrillo caro que solo servía para hablar.

La primera gran ruptura fue la telefonía móvil: por primera vez, la voz viajó sin cables a escala masiva. La segunda, más profunda, fue el WiFi: por primera vez, los DATOS viajaron sin cables a escala masiva y barata. La combinación de ambas (un celular con WiFi y datos móviles) creó el mundo en el que vives: la oficina sin cables, el café convertido en lugar de trabajo, la educación a distancia, el comercio electrónico desde el teléfono, las redes sociales, el trabajo remoto.

El cambio económico es igual de importante. Tender un cable cuesta dinero por cada metro: materiales, mano de obra, permisos, zanjas. Cubrir con cable una comunidad rural dispersa puede costar más de lo que esa comunidad puede pagar en años. Una torre inalámbrica, en cambio, cubre kilómetros a la redonda desde un solo punto. Por eso en México y en toda América Latina el internet llegó a muchísimos lugares primero por aire que por cable: las redes comunitarias, los WISP (proveedores inalámbricos locales) y la telefonía móvil conectaron pueblos enteros con una antena en un cerro y equipos baratos en los techos. Lo inalámbrico no solo es cómodo: es la tecnología que democratizó el acceso.

Y hay un tercer cambio, más sutil: lo inalámbrico cambió nuestra relación con el espacio. Antes, "estar conectado" significaba "estar en un lugar específico", sentado frente a la computadora de la casa o de la oficina. Hoy significa "estar dentro de una burbuja de cobertura". Trabajas desde la hamaca, desde el parque, desde el camión. Esa libertad tiene un precio (baterías, interferencia, seguridad), pero nadie quiere regresar.

Un poco de historia: de Marconi al 5G

La historia de lo inalámbrico empieza con un joven italiano, Guillermo Marconi, que a finales del siglo XIX logró enviar señales telegráficas sin hilos usando ondas de radio. En 1901 cruzó el Atlántico con una señal inalámbrica: la letra "S" en código Morse viajó de Inglaterra a Canadá por el aire. Imagina el asombro: un mensaje que cruza el océano sin ningún cable. Marconi ganó el Premio Nobel en 1909 y fundó la primera industria inalámbrica.

Durante la primera mitad del siglo XX, la radio se volvió el medio masivo: noticias, música, radionovelas. La Segunda Guerra Mundial aceleró todo: radares, comunicaciones militares cifradas, walkie-talkies. De la guerra salieron dos regalos: el espectro radioeléctrico quedó organizado y regulado por los gobiernos, y la electrónica se abarató.

En los años setenta y ochenta nació la telefonía celular: la idea genial de dividir el territorio en "celdas", cada una con su torre, reutilizando las mismas frecuencias en celdas lejanas. Así se pudo atender a millones de usuarios con un espectro limitado. En los noventa llegó el WiFi, nacido de una banda de frecuencias que los gobiernos liberaron para uso sin licencia (las bandas ISM, de las que hablaremos en la Unidad 2). Y en los 2000 el celular se volvió computadora: 3G, 4G, y ahora 5G, cada generación multiplicando la velocidad.

La lección de la historia es un patrón que se repite: cada salto inalámbrico combina una idea física (una nueva forma de usar las ondas), una decisión regulatoria (liberar frecuencias) y una caída de precios (electrónica más barata). Cuando veas una tecnología nueva anunciada con bombo, pregúntate cuál de esas tres patas le falta: muchas "revoluciones" se quedan en promesa porque el espectro no está libre o porque el equipo sigue caro.

El espectro electromagnético: la carretera invisible

Todo lo inalámbrico viaja sobre ondas electromagnéticas. La luz que ves, el calor que sientes del sol, las ondas de tu WiFi y los rayos X de una radiografía son exactamente el mismo fenómeno: ondas electromagnéticas. La única diferencia entre ellas es la frecuencia, es decir, qué tan rápido oscilan.

El espectro electromagnético es el mapa completo de todas esas ondas, ordenadas por frecuencia. De menor a mayor frecuencia: ondas de radio, microondas, infrarrojo, luz visible, ultravioleta, rayos X y rayos gamma. Las redes inalámbricas viven en la zona de radio y microondas, que es la zona de frecuencias bajas: desde unos cuantos kHz hasta unos cuantos GHz.

¿Por qué las comunicaciones usan frecuencias bajas y no, por ejemplo, luz visible? Por tres razones prácticas. Primera: las ondas de baja frecuencia atraviesan obstáculos mejor (ya veremos por qué). Segunda: es más barato generarlas y detectarlas con electrónica sencilla. Tercera: las frecuencias altas (como los rayos X) son peligrosas para la salud porque tienen suficiente energía para dañar células; las de radio no. Tu WiFi no te va a hacer daño: su energía por onda es minúscula comparada con la de la luz solar que te pega todos los días.

El espectro es un recurso limitado y por eso los gobiernos lo administran. En México, el Instituto Federal de Telecomunicaciones (IFT) decide quién puede transmitir en qué frecuencia, igual que un gobierno decide quién puede construir en qué terreno. Algunas bandas requieren licencia (las de telefonía celular, por ejemplo: las compañías pagan miles de millones por ellas), y otras son de uso libre (como las del WiFi), con reglas de potencia máxima para que nadie abuse. Esta es la razón por la que tu router WiFi no necesita permiso del gobierno pero una radiodifusora sí.

Frecuencia: el latido de la onda

La frecuencia es el concepto más importante de toda esta unidad. Grábatelo: frecuencia es cuántas veces oscila una onda por segundo. Una onda de radio es una perturbación electromagnética que sube y baja, como las olas del mar. Cada subida y bajada completa es un ciclo. Si la onda completa 100 ciclos en un segundo, su frecuencia es de 100 hertz.

El hertz (Hz) es la unidad de frecuencia y significa "ciclos por segundo". Como las frecuencias de radio son enormes, usamos múltiplos: el kilohertz (kHz) son mil hertz, el megahertz (MHz) son un millón de hertz, y el gigahertz (GHz) son mil millones de hertz. Tu WiFi casero trabaja típicamente en 2.4 GHz y 5 GHz: eso significa que su onda oscila 2,400 millones y 5,000 millones de veces por segundo, respectivamente. Tu cerebro no puede ni imaginar esa velocidad, pero a la electrónica le parece de lo más normal.

Analogía de la radio AM/FM, que es perfecta aquí. Cuando sintonizas "la 94.5 de FM", estás eligiendo una frecuencia: 94.5 MHz, es decir, una onda que oscila 94.5 millones de veces por segundo. La estación transmite en esa frecuencia y tu radio "escucha" solo esa, ignorando las demás. El WiFi hace exactamente lo mismo: tu router transmite en un canal (una frecuencia específica dentro de la banda de 2.4 GHz o 5 GHz) y tu celular sintoniza ese canal. Si dos vecinos usan el mismo canal, se estorban, igual que dos estaciones de radio en la misma frecuencia se encimarían. Esta analogía te va a servir toda la vida: cada vez que oigas "interferencia" o "canal", piensa en dos estaciones de radio peleando por la misma frecuencia.

Error común de principiante número uno: confundir la frecuencia de la onda con la velocidad de los datos. Que tu WiFi sea de 5 GHz NO significa que descargue a 5 gigabits por segundo. Los 5 GHz son qué tan rápido oscila la onda portadora; la velocidad de descarga depende del ancho de banda y de la modulación, que veremos más adelante. Es como confundir la velocidad a la que gira el motor de un carro con la velocidad a la que avanza: están relacionadas, pero no son lo mismo. Cuando veas una caja de router que dice "AC1200" o "AX3000", esos números son velocidades teóricas en megabits por segundo, no la frecuencia.

Longitud de onda: el tamaño de la ola

Si la frecuencia es qué tan rápido oscila la onda, la longitud de onda es qué tan larga es cada oscilación: la distancia entre una cresta y la siguiente. Se representa con la letra griega lambda y se mide en metros (o centímetros, milímetros, según el caso).

Frecuencia y longitud de onda están casadas por una fórmula sencilla, la más importante de este libro:

longitud de onda = velocidad de la luz / frecuencia

La velocidad de la luz (y de todas las ondas electromagnéticas, incluyendo las de radio) es de aproximadamente 300,000 kilómetros por segundo, o 300 millones de metros por segundo. Entonces, para una frecuencia de 2.4 GHz (2,400 millones de Hz):

$\text{longitud de onda} = 300,000,000 / 2,400,000,000 = 0.125 \text{ metros} = 12.5 \text{ centímetros}$

La onda de tu WiFi de 2.4 GHz mide 12.5 cm de cresta a cresta. Para 5 GHz: $300,000,000 / 5,000,000,000 = 0.06 \text{ metros} = 6 \text{ centímetros}$. Fíjate en la relación: a mayor frecuencia, menor longitud de onda. Son inversamente proporcionales, como una cuerda de guitarra: entre más corta la cuerda, más agudo el sonido (mayor frecuencia).

¿Por qué importa el tamaño de la onda? Porque determina cómo interactúa con los objetos. Regla de oro intuitiva: una onda "siente" los objetos de tamaño parecido a su longitud de onda. Una onda de 12.5 cm se ve afectada por objetos de unos centímetros: marcos de puerta, muebles, tuberías. Las ondas larguísimas de la radio AM (cientos de metros) pasan por encima de edificios como si nada, porque los edificios les parecen piedritas. Las ondas cortitas de 5 GHz (6 cm), en cambio, chocan con casi todo. Por eso la señal de 5 GHz es más rápida pero atraviesa peor las paredes que la de 2.4 GHz: su onda es más pequeña y "choca" más. Esta sola idea explica la mitad de los problemas de cobertura WiFi del mundo.

Analogía de tirar piedras al estanque: si tiras una piedra grande, las olas son grandes y pasan por encima de las hojitas flotando; si haces olas pequeñitas con el dedo, cualquier hoja las frena. La frecuencia alta es el dedo; la frecuencia baja es la piedra grande.

Amplitud: qué tan fuerte viene la ola

La amplitud es la altura de la onda: qué tan grande es cada oscilación. En la práctica, la amplitud se traduce en potencia, en qué tan "fuerte" sale la señal del transmisor y qué tan fuerte llega al receptor. Más amplitud (más potencia) significa más alcance y mejor resistencia al ruido, pero también más consumo de energía y más interferencia a los vecinos.

Piensa en hablar en una fiesta ruidosa, que es la analogía estrella de las redes inalámbricas. Tú quieres que tu amigo te escuche al otro lado del salón. Si hablas bajito (poca amplitud), no te oye. Si gritas (muchísima amplitud), te oye, pero también molestas a las demás mesas y te cansas más rápido. El WiFi hace lo mismo: el router puede subir su potencia de transmisión para llegar más lejos, pero a cambio contamina el aire de los vecinos y gasta más luz. Por eso los routers permiten ajustar la potencia, y por eso la ley limita la potencia máxima: para que tu "grito" no deje sordos a los demás.

La potencia en redes inalámbricas se mide en decibelios (dB) y en dBm, unidades que al principio asustan pero que son solo una forma compacta de hablar de proporciones. No

necesitas dominarlas a fondo en esta unidad; basta con la intuición: en la escala de señal WiFi que verás en los comandos (esos números negativos como -65 dBm), mientras más cercano a cero, más fuerte la señal. -40 dBm es excelente (estás al lado del router), -70 dBm es apenas usable, y -90 dBm es casi nada. Guarda esa escala mental: te va a acompañar todo el libro.

Cómo viajan y mueren las ondas: propagación y obstáculos

Una onda de radio sale de la antena y se expande en todas direcciones (o en una dirección preferente, según la antena). En el vacío viajaría para siempre, pero en el mundo real le pasan cuatro cosas, y las cuatro tienen nombre técnico que debes conocer.

Reflexión: la onda rebota en superficies, como la luz en un espejo o como tu voz en una pared (el eco). El metal es el gran reflector: una lámina, un refrigerador, un carro, rebotan las ondas de WiFi. Por eso a veces tienes señal en un cuarto sin línea directa al router: la onda llegó rebotando por el pasillo, como una pelota de billar.

Refracción: la onda cambia de dirección al pasar de un medio a otro (del aire al vidrio, por ejemplo), igual que un lápiz se ve "quebrado" dentro de un vaso de agua. En interiores es un efecto menor, pero existe.

Difracción: la onda "dobla" alrededor de los bordes de los obstáculos, como el sonido que dobla la esquina y te permite oír a alguien que no ves. Gracias a la difracción, la señal llega a zonas sin línea de vista directa, aunque más débil.

Absorción: el obstáculo se traga parte de la energía de la onda y la convierte en calorcito. Esta es la gran asesina de la señal en casas. ¿Y qué absorbe más? El agua. Las paredes con humedad, las peceras, las tuberías de agua, e incluso el cuerpo humano (somos 60% agua) absorben señal WiFi. El microondas calienta la comida a 2.4 GHz precisamente porque el agua absorbe esa frecuencia: tu microondas y tu WiFi pelean en la misma banda, y cuando calientas la comida, el WiFi sufre. No es coincidencia: es física.

Atenuación es el nombre general de la pérdida de fuerza con la distancia y los obstáculos. Cada pared que cruza la onda le roba una parte de su energía. Regla práctica de técnico: una pared de ladrillo o concreto te puede robar entre 6 y 12 dB (muchísimo), una pared de tabla roca unos 3 dB, y un piso completo de concreto entre 12 y 20 dB. Por eso el router en la planta baja apenas llega al segundo piso: cada losa de concreto es como un muro para la onda.

Error común de principiante número dos: creer que "más rayitas" en el celular significa "más velocidad de internet". Las rayitas miden la fuerza de la señal del tramo inalámbrico (qué tan fuerte llega la onda), no la velocidad de tu conexión a internet. Puedes tener las cinco rayitas y navegar lento porque tu proveedor está saturado, o tener dos rayitas y navegar de maravilla.

Señal fuerte es condición necesaria pero no suficiente para buena velocidad. Cuando diagnostiques, separa siempre las dos preguntas: ¿me llega bien la onda? y ¿me llegan bien los datos?

Buena práctica desde el día uno: el router va en el centro de la casa, elevado (a la altura de un librero, no en el piso), lejos del microondas, de la pecera, del refrigerador y de los espejos grandes. Cada metro que lo acerques al centro te ahorra paredes cruzadas, y cada pared que evitas es señal que no se pierde. Parece consejo de abuela, pero es física pura y resuelve más problemas que cualquier configuración avanzada.

La diferencia entre señal y datos: la distinción que todo lo aclara

Aquí llegamos a la Clase 3 y a una de las distinciones más importantes del libro: señal no es lo mismo que datos. La señal es la onda física que viaja por el aire (lo que hemos estudiado hasta ahora: frecuencia, amplitud, longitud de onda). Los datos son la información que queremos transmitir (tus mensajes, tus fotos, el video que estás viendo). La señal es el camión; los datos son la carga. Un camión puede ir vacío, lleno o a medias: igual la señal puede existir sin llevar datos útiles, o llevarlos mal.

¿Cómo se sube la carga al camión? Con la modulación. Modular es modificar alguna característica de la onda (su amplitud, su frecuencia o su fase) siguiendo un patrón que representa los datos. El ejemplo más simple: imagina que quedas con tu amigo en que vas a prender y apagar una lámpara para mandarle mensajes en código Morse. La luz de la lámpara es la señal; el prender y apagar (modular la amplitud: luz alta, luz baja) es la modulación; y el mensaje en Morse son los datos. El WiFi hace exactamente eso, solo que miles de millones de veces por segundo y con trucos matemáticos sofisticados.

Señal analógica contra señal digital

El mundo físico es analógico: el sonido de tu voz, la luz del atardecer, la temperatura del día, todo varía de forma continua, sin saltos. Una señal analógica es la que varía de forma continua en el tiempo: puede tomar infinitos valores. Si dibujas tu voz en un papel, sale una curva suave y ondulada.

Una señal digital, en cambio, solo toma valores discretos, normalmente dos: encendido o apagado, 1 o 0. Es como un interruptor contra un dimmer: el dimmer (analógico) puede dar cualquier brillo intermedio; el interruptor (digital) solo conoce prendido y apagado. Las computadoras hablan en digital porque sus circuitos son interruptores microscópicos: todo lo que procesan son unos y ceros.

Entonces, ¿cómo viaja algo digital (tus datos) sobre algo físico (la onda, que es analógica por naturaleza)? Con la modulación: el transmisor toma la onda analógica y la "corta" en patrones discretos que representan unos y ceros. El receptor mide la onda que llega, identifica los patrones y reconstruye los unos y ceros. Del otro lado, tu computadora vuelve a convertir esos bits en la foto, el mensaje o el video.

¿Por qué no mandar todo en analógico, como la radio AM/FM de música? Porque lo digital es mucho más resistente al ruido. Si mandas música en analógico y hay interferencia, se oye el chisporroteo mezclado con la música: la señal se degrada poco a poco. Si mandas datos en digital y hay un poco de ruido, el receptor todavía distingue si era un 1 o un 0, y los datos llegan perfectos: o llegan bien o no llegan, no hay punto medio borroso. Por eso tu llamada de WhatsApp o se escucha clara o se corta, pero rara vez se escucha "a medias con estática" como la radio vieja. Lo digital cambió el juego porque permite corrección de errores: se pueden agregar bits extra para detectar y hasta reparar los bits dañados por el camino, algo imposible con una señal analógica pura.

Modulación básica: los tres trucos

Hay tres formas básicas de modular una onda, y sus nombres describen qué característica de la onda se modifica. Las tres se entienden con la analogía de la fiesta ruidosa.

Modulación por amplitud: se varía la altura de la onda. Fuerte = 1, débil = 0. En la fiesta: gritas para decir "sí" y susurras para decir "no". Es el truco más simple y el más vulnerable al ruido: si alguien mete ruido en el salón, tu amigo puede confundir un susurro con un grito apagado por el ruido.

Modulación por frecuencia: se varía qué tan rápido oscila la onda. Rápido = 1, lento = 0. En la fiesta: hablas agudo para decir "sí" y grave para decir "no". Aguanta mejor el ruido que la amplitud, porque el ruido de la fiesta suele cambiar el volumen, no el tono.

Modulación por fase: se varía el punto del ciclo donde empieza la onda, como adelantar o atrasar el paso al bailar. Es el truco más eficiente y el que más usan las redes modernas (WiFi, 4G, 5G), combinado con los otros dos. Las modulaciones modernas con nombres raros (QPSK, QAM) son combinaciones sofisticadas de amplitud y fase que meten muchos bits en cada "paso" de la onda: en vez de mandar un bit por paso (1 o 0), mandan 2, 4, 6 o más bits por paso usando muchas combinaciones de amplitud y fase. Mientras más bits por paso, más velocidad... pero también más delicadeza: con mucho ruido, el receptor confunde las combinaciones. Por eso tu WiFi baja la velocidad automáticamente cuando la señal es mala: cambia a una modulación más simple y robusta. Esa negociación constante se llama modulación adaptativa y ocurre sin que te enteres, cientos de veces por segundo.

Ancho de banda: el ancho de la carretera

El ancho de banda es cuánta "porción" del espectro ocupa una señal, medido en Hz. Si la frecuencia es en qué punto de la carretera vas, el ancho de banda es cuántos carriles ocupas. Un canal WiFi de 20 MHz ocupa 20 millones de hertz de espectro; uno de 40 MHz ocupa el doble.

¿Por qué importa? Porque el ancho de banda determina cuántos datos por segundo puedes mandar: a más carriles, más camiones por hora. Un canal de 40 MHz puede mover aproximadamente el doble de datos que uno de 20 MHz, en igualdad de condiciones. Por eso los routers modernos ofrecen canales de 40, 80 y hasta 160 MHz: más carriles, más velocidad.

Pero hay un precio, y es doble. Primero: el espectro es limitado. Si tú ocupas 80 MHz, quedan menos canales libres para tus vecinos, y todos se estorban más. En la banda de 2.4 GHz, que es estrecha, usar canales de 40 MHz es casi un acto de guerra contra los vecinos: no caben. Segundo: una señal más ancha reparte su potencia entre más frecuencias, así que cada pedacito llega más débil y es más vulnerable al ruido. Más carriles, pero cada carril con camiones más pequeños y frágiles.

Analogía final de la fiesta: el ancho de banda es qué tan ancha es tu mesa. Con una mesa angosta (poco ancho de banda) pasan pocos meseros con charolas (datos); con una mesa de banquete pasan muchos a la vez. Pero la mesa de banquete ocupa casi todo el salón y estorba a las demás mesas. El buen técnico elige el ancho de banda como el buen anfitrión elige las mesas: suficientes para atender bien, sin invadir a los vecinos.

Error común de principiante número tres: creer que el "ancho de banda" que vende tu proveedor de internet (50 megas, 100 megas) es lo mismo que el ancho de banda del canal WiFi (20/40/80 MHz). Se llaman igual por accidente histórico, pero son cosas distintas: lo del proveedor se mide en megabits por segundo (velocidad de datos) y lo del canal WiFi se mide en MHz (porción de espectro). Están relacionados (más MHz permiten más Mbps), pero no son intercambiables. Cuando tu proveedor dice "100 megas", habla de velocidad; cuando tu router dice "canal de 40 MHz", habla de espectro. No los confundas en un examen ni frente a un cliente.

Cómo piensa un técnico inalámbrico: el método de las tres preguntas

Antes de pasar a los ejemplos prácticos, conviene adoptar el hábito mental que distingue a un técnico de un usuario avanzado. Cuando algo falla en una red inalámbrica, el técnico no adivina: hace tres preguntas en orden, y cada respuesta lo acerca a la causa.

Primera pregunta: ¿hay señal? Es decir, ¿la onda llega con fuerza suficiente? Se responde mirando los dBm o el porcentaje de señal junto al dispositivo. Si la señal es de -85 dBm o peor, ya no importa nada más: el problema es de cobertura. La solución vive en el mundo físico: mover el router, quitar obstáculos, agregar un punto de acceso. Ninguna configuración de software arregla una onda que no llega.

Segunda pregunta: ¿hay interferencia? La señal puede ser fuerte y aun así los datos pueden llegar dañados, porque el aire está sucio: vecinos en el mismo canal, un microondas encendido, una red Bluetooth saturando la banda. Se responde con un escaneo de redes (los comandos que verás en los ejemplos): si tu canal está lleno de vecinos fuertes, cambia de canal. La interferencia es el culpable invisible más común en departamentos y oficinas.

Tercera pregunta: ¿hay capacidad más allá? Si la señal es buena y el canal está limpio, pero la velocidad sigue mala, el problema no es tu WiFi: es tu proveedor, su red saturada, o el servidor al que te conectas. Se responde comparando la prueba de velocidad por WiFi contra la prueba con cable directo al router o con datos móviles. Si por cable todo vuela y por WiFi no, el problema es inalámbrico; si por cable también está lento, el problema es del proveedor y hay que llamarlo con números en la mano.

Este método (señal, interferencia, capacidad) te ahorra el error más caro del principiante: cambiar cosas al azar. El que no diagnostica, adivina; y adivinar en redes significa comprar equipos que no se necesitaban y mover configuraciones que estaban bien. Cada vez que en este libro veas un problema, vuelve a estas tres preguntas: son la brújula de todo el curso.

Ejemplos paso a paso

En esta sección vas a ver tu propia red inalámbrica con tus propios ojos. Nada de teoría flotando: vas a abrir la terminal o la configuración de tu dispositivo y vas a leer la señal, la frecuencia, el canal y la velocidad de tu WiFi. Haz cada ejemplo frente a tu computadora o tu celular, no solo leyéndolo. Si un comando no existe en tu sistema, no te preocupes: lee el ejemplo de todos modos, porque la lógica es la misma en todos lados.

Ejemplo 1: Ver tu conexión WiFi en Windows con netsh

En Windows, abre el Símbolo del sistema (tecla Windows, escribe "cmd", Enter) y ejecuta:

```
netsh wlan show interfaces
```

Vas a ver algo parecido a esto (los valores cambian según tu equipo):

Nombre	: Wi-Fi
Descripción	: Intel(R) Wireless-AC 9560
GUID	: 8a3f2c1d-4e5b-4f6a-9c8d-2e1f0a9b8c7d
Dirección física	: a4:c3:f0:12:34:56
Estado	: conectado
SSID	: CASA_ESTEBAN
BSSID	: f0:9f:c2:aa:bb:cc
Tipo de red	: Infraestructura
Tipo de radio	: 802.11ac
Autenticación	: WPA2-Personal
Cifrado	: CCMP
Canal	: 36
Velocidad de recepción	: 866.7 Mbps
Velocidad de transmisión	: 866.7 Mbps
Señal	: 82%

Línea por línea. "Nombre: Wi-Fi" es el nombre que Windows le da a tu adaptador inalámbrico. "Descripción" es el modelo de tu tarjeta WiFi: aquí una Intel Wireless-AC 9560, que soporta el estándar 802.11ac. "Dirección física" es la dirección MAC de tu tarjeta, su identificador único de fábrica, como su CURP: a4:c3:f0:12:34:56. "Estado: conectado" confirma que estás enlazado a una red.

"SSID: CASA_ESTEBAN" es el nombre de la red WiFi a la que estás conectado, el que ves en la lista de redes. "BSSID" es la dirección MAC del punto de acceso (el router): si hay varios routers con el mismo nombre de red, el BSSID te dice exactamente a cuál estás conectado. "Tipo de red: Infraestructura" significa que te conectas a través de un punto de acceso central (el modo normal de casa y oficina), en contraste con el modo "ad hoc", donde los dispositivos se conectan directamente entre sí sin router.

"Tipo de radio: 802.11ac" es el estándar WiFi que estás usando (lo veremos a fondo en la Unidad 3). "Autenticación: WPA2-Personal" y "Cifrado: CCMP" te dicen que la red está protegida con contraseña (bien) y con cifrado moderno (bien). Si aquí dijera "Abierta" y "Ninguno", estarías en una red sin protección.

"Canal: 36" es el canal de frecuencia que usa tu router. Los canales del 36 en adelante pertenecen a la banda de 5 GHz. Si dijera canal 6 u 11, estarías en 2.4 GHz. "Velocidad de recepción/transmisión: 866.7 Mbps" es la velocidad de enlace negociada entre tu tarjeta y el router en este momento: no es tu velocidad de internet, es la velocidad del tramo inalámbrico. Cambia sola según la señal y la modulación (¿te acuerdas de la modulación adaptativa?). "Señal: 82%" es la fuerza con la que te llega la onda, en porcentaje. Arriba de 70% es bueno, entre 50% y 70% es regular, abajo de 50% es malo.

Para ver las redes vecinas y sus canales (útil para elegir un canal libre), ejecuta:

```
netsh wlan show networks mode=bssid
```

Te lista cada red con su SSID, tipo de autenticación y, por cada punto de acceso, la señal en porcentaje y el canal. Si ves que todos tus vecinos están en el canal 6 de 2.4 GHz, ya sabes a qué canal NO poner tu router.

Ejemplo 2: Ver tu conexión WiFi en Linux con iwconfig

En Linux, abre la terminal y ejecuta (puede pedir sudo según tu distribución):

```
iwconfig
```

Salida típica:

```
wlp2s0    IEEE 802.11  ESSID:"CASA_ESTEBAN"
          Mode:Managed  Frequency:5.18 GHz  Access Point: F0:9F:C2:AA:BB:CC
          Bit Rate=866.7 Mb/s   Tx-Power=22 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
          Link Quality=58/70  Signal level=-52 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0  Missed beacon:0
```

Línea por línea. "wlp2s0" es el nombre de tu interfaz inalámbrica en Linux (los nombres varían: wlan0, wlp3s0, etc.). "IEEE 802.11" confirma que es una interfaz WiFi. "ESSID" es el equivalente al SSID: el nombre de la red.

"Mode:Managed" significa modo infraestructura (conectado a un punto de acceso), igual que en Windows. "Frequency:5.18 GHz" te dice la frecuencia exacta: 5.18 GHz corresponde al canal 36 de la banda de 5 GHz. "Access Point" es la MAC del router (el BSSID).

"Bit Rate=866.7 Mb/s" es la velocidad de enlace negociada, igual que en Windows. "Tx-Power=22 dBm" es la potencia con la que TU tarjeta transmite: 22 dBm es una potencia típica y saludable. "Link Quality=58/70" es una medida relativa de calidad del enlace según el driver. "Signal level=-52 dBm" es la joya: la fuerza de la señal en dBm. Recuerda la escala: -52 dBm es buena señal (cerca del router o con poca obstrucción). Si ves -80 dBm o peor, estás lejos o detrás de varias paredes.

Las últimas líneas son contadores de errores: "Rx invalid crypt" cuenta paquetes que llegaron con cifrado inválido (si crece rápido, puede haber un problema de contraseña o un ataque), "Tx excessive retries" cuenta retransmisiones (si es alto, hay interferencia o señal débil). En una red sana, todos estos contadores están en cero o casi.

Ejemplo 3: Escanear redes vecinas en Linux con iwlist

Para ver todas las redes que tu tarjeta alcanza a oír, con detalle técnico completo:

```
sudo iwlist wlp2s0 scan
```

(Cambia wlp2s0 por el nombre de tu interfaz, el que te mostró iwconfig.) La salida es larga; cada red aparece en un bloque "Cell" como este:

```
Cell 01 - Address: F0:9F:C2:AA:BB:CC
        Channel:36
        Frequency:5.18 GHz
        Quality=58/70  Signal level=-52 dBm
        Encryption key:on
        ESSID:"CASA_ESTEBAN"
        Bit Rates:6 Mb/s; 9 Mb/s; 12 Mb/s; 18 Mb/s
        IE: IEEE 802.11i/WPA2 Version 1
```

Línea por línea. "Cell 01" numera cada red encontrada. "Address" es la MAC del punto de acceso. "Channel:36" y "Frequency:5.18 GHz" te ubican en el espectro: canal 36, banda de 5 GHz. "Quality" y "Signal level" ya los conoces del ejemplo anterior.

"Encryption key:on" significa que la red tiene cifrado activado (protegida). Si dijera "off", es una red abierta. "ESSID" es el nombre. "Bit Rates" lista las velocidades básicas que anuncia el punto de acceso. "IE: IEEE 802.11i/WPA2" confirma el tipo de seguridad: WPA2, el estándar moderno (WPA3 es su sucesor, lo veremos en la unidad de seguridad).

Este comando es oro para elegir canal: escanea, anota en qué canales están tus vecinos en la banda que te interesa, y configura tu router en el canal más despejado. En 2.4 GHz los canales que no se enciman son el 1, 6 y 11: si tus vecinos están en el 6, tú vete al 1 o al 11, nunca al 7 (que se encimaría con el 6).

Ejemplo 4: Ver la señal en Android y en iPhone

En Android (los menús varían por marca, pero la ruta es parecida): ve a Ajustes, luego a "Redes e Internet" o "Conexiones", luego a "WiFi". Toca el engrane o el nombre de la red a la

que estás conectado. Verás datos como intensidad de señal (a veces en dBm exactos, por ejemplo -55 dBm), frecuencia (2.4 GHz o 5 GHz), velocidad de enlace y seguridad. En muchos Android, si tocas varias veces "Versión de compilación" en Ajustes del teléfono activas las opciones de desarrollador, donde hay aún más datos de red.

En iPhone, Apple muestra menos datos por defecto: en Ajustes, WiFi, toca la "i" azul junto a tu red y verás la dirección IP y poco más. Para ver la señal en dBm necesitas una app de análisis (ver ejemplo 5). Un truco rápido sin apps: el ícono del WiFi en la barra de estado te da una idea gruesa (tres arcos llenos es buena señal), pero para trabajo serio usa una app.

En ambos sistemas, el dato más útil es la intensidad en dBm caminando por la casa: párate junto al router y anota el valor, luego ve al cuarto más lejano y anótalo de nuevo. Esa diferencia te dice cuánta señal se comen tus paredes. Este es exactamente el ejercicio 3 de la sección de práctica.

Ejemplo 5: Analizar el espectro con una app de WiFi

Instala una app analizadora de WiFi (en Android hay varias gratuitas muy buenas; busca "WiFi Analyzer" en la Play Store; en iPhone las opciones son más limitadas por restricciones de Apple, pero existen apps que muestran redes y canales). Ábrela y verás una gráfica con el espectro: en el eje horizontal, los canales (1 al 11 o 13 en 2.4 GHz, 36 en adelante en 5 GHz); en el eje vertical, la intensidad de señal en dBm; cada red es una curva con su nombre.

Cómo leerla, paso a paso. Primero, identifica tu red por su nombre y mira en qué canal está su curva. Segundo, mira qué otras curvas se enciman con la tuya: cada curva que comparta tu canal o un canal vecino es interferencia potencial, como estaciones de radio encimadas. Tercero, compara alturas: una curva vecina más alta que la tuya en tu zona significa que ese vecino te llega más fuerte que tu propio router en ese punto (típico en departamentos). Cuarto, cambia de banda en la app (2.4 GHz contra 5 GHz) y compara: verás que en 2.4 GHz hay pocas curvas pero anchas y encimadas (poco espectro, mucha pelea), y en 5 GHz hay muchas curvas separadas (mucho espectro, poca pelea).

Con esa gráfica decides el canal de tu router en dos minutos, sin adivinar. Este es el procedimiento profesional básico de un técnico de redes inalámbricas, y acabas de aprenderlo.

Ejemplo 6: Probar el efecto de los obstáculos con un ping

Este ejemplo demuestra la atenuación con números. En Windows (cmd) o Linux/macOS (terminal), ejecuta:

```
ping -t 192.168.1.1
```

En Windows el "-t" hace que el ping no se detenga (detenlo con Ctrl+C); en Linux y macOS el ping ya es continuo por defecto, así que usa simplemente "ping 192.168.1.1". Cambia 192.168.1.1 por la IP de tu router (la ves en la salida de ipconfig en Windows o ip route en Linux, como "puerta de enlace").

Verás líneas como:

```
Respuesta desde 192.168.1.1: bytes=32 tiempo=3ms TTL=64  
Respuesta desde 192.168.1.1: bytes=32 tiempo=2ms TTL=64  
Respuesta desde 192.168.1.1: bytes=32 tiempo=4ms TTL=64
```

Cada línea es un paquetito que fue al router y regresó: "tiempo=3ms" es lo que tardó el viaje redondo. Ahora camina con la laptop o el celular: párate junto al router y mira los tiempos (2 a 5 ms es normal), luego vete al cuarto más lejano, detrás de dos paredes, y mira de nuevo. Verás tiempos más altos y más variables (20 ms, 50 ms, a veces "tiempo de espera agotado", que significa que el paquete se perdió). Esa degradación es la atenuación y las retransmisiones en acción: la onda llega débil, los datos se dañan, y hay que reintentar.

Este experimento de dos minutos vale más que mil diapositivas: acabas de medir con tus manos cómo las paredes se comen tu red.

Práctica

Haz estos ejercicios de verdad, con lápiz, papel y tus dispositivos. La teoría sin práctica se olvida en una semana; la práctica convierte la teoría en intuición. Cada ejercicio trae su solución explicada paso a paso para que verifiques tu trabajo.

Ejercicio 1: Calcula longitudes de onda

Calcula la longitud de onda de estas frecuencias usando la fórmula $\text{longitud de onda} = 300,000,000 / \text{frecuencia (en Hz)}$. Expresa el resultado en metros y en centímetros.

- a) 2.4 GHz (WiFi banda baja)
- b) 5.8 GHz (WiFi banda alta)
- c) 94.5 MHz (una estación de FM)
- d) 900 MHz (telefonía celular antigua)

Solución paso a paso. Primero convierte todo a Hz: 2.4 GHz = 2,400,000,000 Hz; 5.8 GHz = 5,800,000,000 Hz; 94.5 MHz = 94,500,000 Hz; 900 MHz = 900,000,000 Hz. Este es el paso donde más se equivoca la gente: si divides entre 2.4 en lugar de entre 2,400,000,000, el resultado sale mal por miles de millones. Convierte primero, divide después.

a) $300,000,000 / 2,400,000,000 = 0.125$ metros = 12.5 centímetros. b) $300,000,000 / 5,800,000,000 = 0.0517$ metros, redondeado 0.052 metros = 5.2 centímetros. c) $300,000,000 / 94,500,000 = 3.17$ metros = 317 centímetros. d) $300,000,000 / 900,000,000 = 0.333$ metros = 33.3 centímetros.

Interpreta los resultados: la onda de FM mide más de 3 metros (por eso la radio FM llega lejos y dobla esquinas: los edificios le parecen pequeños), la de celular 900 MHz mide 33 cm, y las de WiFi miden entre 5 y 12.5 cm (por eso "chocan" con los muebles y las paredes les roban tanta señal). Con este ejercicio ya puedes mirar cualquier frecuencia y visualizar el tamaño de su onda.

Ejercicio 2: Convierte unidades de frecuencia

Un router anuncia que trabaja en "2400 MHz a 2483.5 MHz". Otro dice "5 GHz". Responde:

a) ¿A cuántos GHz equivalen 2400 MHz? b) ¿A cuántos MHz equivalen 5 GHz? c) ¿Qué ancho de banda (en MHz) cubre el primer router, de 2400 a 2483.5 MHz? d) Si un canal WiFi ocupa 20 MHz, ¿cuántos canales de 20 MHz caben, en teoría, en ese rango?

Solución paso a paso. Recuerda: 1 GHz = 1000 MHz.

a) $2400 \text{ MHz} / 1000 = 2.4 \text{ GHz}$. b) $5 \text{ GHz} \times 1000 = 5000 \text{ MHz}$. c) Ancho de banda = frecuencia final menos frecuencia inicial = $2483.5 - 2400 = 83.5 \text{ MHz}$. Ese es, redondeado, el famoso rango de 2.4 GHz. d) $83.5 / 20 = 4.175$, es decir, caben 4 canales de 20 MHz sin encimarse (en la práctica, por la forma en que están definidos los canales WiFi, solo 3 quedan realmente libres de traslape: el 1, el 6 y el 11; el cálculo teórico te da el límite físico y la ingeniería te da el límite práctico).

Moraleja del ejercicio: la banda de 2.4 GHz es angosta (83.5 MHz) y por eso vive saturada; la de 5 GHz tiene cientos de MHz disponibles y por eso respira mejor. Cuando en la Unidad 3 hablemos de bandas y canales, estos números van a ser tus viejos conocidos.

Ejercicio 3: Mapa de señal de tu casa

Con tu celular Android (o con una app analizadora en iPhone), mide la intensidad de la señal WiFi en dBm en estos 5 puntos: 1) junto al router, 2) en tu cuarto, 3) en la cocina, 4) en el baño

más lejano, 5) en la puerta de la calle o el patio. Anota cada valor en una tabla: punto, distancia aproximada al router, obstáculos en medio (paredes, pisos, electrodomésticos), señal en dBm.

Solución (ejemplo de cómo analizar tus resultados; tus números serán distintos). Una tabla típica se ve así:

Punto 1, junto al router: -35 dBm. Referencia de señal excelente. Punto 2, tu cuarto (una pared de tabla roca): -55 dBm. Se perdieron 20 dB en una pared y unos metros de distancia. Punto 3, cocina (dos paredes, y el refrigerador en medio): -68 dBm. El refrigerador (metal) y las paredes se comieron otros 13 dB. Punto 4, baño lejano (dos paredes más una de concreto con tubería de agua): -80 dBm. Apenas usable; el agua de las tuberías absorbe muchísimo. Punto 5, patio (muro exterior de ladrillo): -85 dBm. Casi sin servicio.

Cómo interpretar: cada caída de 10 dB significa que la señal se redujo a la décima parte de su potencia. Del punto 1 al punto 5 se perdieron 50 dB: la señal del patio es 100,000 veces más débil que junto al router. Y sin embargo el celular a veces todavía se conecta: las modulaciones modernas son heroicas, pero la velocidad en el punto 5 será una fracción de la del punto 1.

Ahora la parte de técnico: con tu mapa en la mano, decide dónde debería estar el router para minimizar la peor caída. Casi siempre la respuesta es "más al centro de la casa y más elevado". Si el punto más débil te importa (tu cuarto de trabajo, por ejemplo), ya sabes por qué en unidades posteriores hablaremos de repetidores, mallas y puntos de acceso adicionales.

Ejercicio 4: Detectives de obstáculos

Recorre tu casa y haz una lista de los 5 peores enemigos de tu señal WiFi que encuentres, clasificados por mecanismo: reflexión, absorción o atenuación por distancia. Para cada uno escribe qué mecanismo aplica y una acción concreta para mitigarlo.

Solución (ejemplo; adáptalo a tu casa):

1. El refrigerador entre el router y la cocina: REFLEXIÓN. El metal rebota la onda. Acción: mover el router de modo que el refrigerador no quede en la línea directa hacia dónde más usas el WiFi.
2. La pecera de la sala: ABSORCIÓN. El agua se traga la señal de 2.4 GHz. Acción: alejar el router de la pecera; no poner nunca un punto de acceso detrás de una pecera.
3. El espejo grande del pasillo: REFLEXIÓN. Los espejos tienen una capa metálica que refleja las ondas. Acción: no colocar el router frente a un espejo grande.

4. El microondas junto al router: INTERFERENCIA más absorción. Trabaja en 2.4 GHz, la misma banda del WiFi. Acción: separar el router del microondas al menos un par de metros, o usar la banda de 5 GHz para lo importante.
5. La losa de concreto entre la planta baja y el cuarto de arriba: ATENUACIÓN. Cada piso de concreto roba 12 a 20 dB. Acción: subir el router a la planta alta si ahí se usa más, o planear un segundo punto de acceso (tema de unidades futuras).

Si encontraste al menos 3 de estos 5 en tu casa, ya diagnosticas como un técnico: la mayoría de los "mi internet está lento" se resuelven moviendo el router y alejándolo de metal, agua y microondas, sin comprar nada.

Ejercicio 5: ¿Señal o velocidad? El experimento de las dos preguntas

Conéctate a tu WiFi junto al router y haz una prueba de velocidad (busca "speed test" en Google y usa el medidor integrado). Anota: señal en dBm o porcentaje, y velocidad de bajada en Mbps. Ahora vete al punto más débil de tu casa (el del ejercicio 3) y repite: anota señal y velocidad. Finalmente, desconecta el WiFi y haz la prueba con datos móviles en ese mismo punto débil. Responde: ¿la velocidad siguió a la señal? ¿En qué caso hubo buena señal pero mala velocidad, o viceversa?

Solución (cómo leer tus resultados). Caso típico A: junto al router, -40 dBm y 95 Mbps; en el punto débil, -78 dBm y 12 Mbps. Aquí la velocidad sí siguió a la señal: el tramo inalámbrico es el cuello de botella, y la modulación adaptativa bajó la velocidad para sobrevivir con poca señal. Diagnóstico: problema de cobertura; solución: reubicar el router o agregar un punto de acceso.

Caso típico B: junto al router, -40 dBm (excelente señal) pero solo 15 Mbps, y con datos móviles en el mismo lugar obtienes 60 Mbps. Aquí hay buena señal pero mala velocidad: el tramo inalámbrico está sano y el problema está "más allá": tu proveedor, su red saturada, o el plan contratado. Diagnóstico: problema del ISP, no de tu WiFi; llamar al proveedor con estos números en la mano.

Caso típico C: señal débil (-80 dBm) pero la velocidad apenas baja de 40 a 35 Mbps. Pasa cuando tu plan de internet es modesto: el WiFi degradado todavía alcanza a entregar lo que el proveedor da. Diagnóstico: no hay problema real; la cobertura es fea pero suficiente para lo contratado.

La lección del ejercicio es el hábito de oro del diagnóstico: separa siempre las dos preguntas, ¿me llega bien la onda? y ¿me llegan bien los datos? El 90% de los principiantes mezcla ambas y termina comprando un router nuevo cuando el problema era el proveedor, o peleando con el proveedor cuando el problema era una pared.

Ejercicio 6: Elige el mejor canal como un profesional

Abre una app analizadora de WiFi (ejemplo 5 de la sección anterior) y observa la banda de 2.4 GHz. Anota qué canales están ocupados por tus vecinos y con qué intensidad. Luego responde: ¿en qué canal pondrías tu router y por qué? Repite para la banda de 5 GHz.

Solución (ejemplo). Supón que en 2.4 GHz ves: canal 1 con dos redes débiles (-85 dBm), canal 6 con cuatro redes fuertes (-60 dBm la más fuerte), canal 11 con una red media (-75 dBm). La respuesta profesional: canal 1, porque es uno de los tres canales que no se traslapan (1, 6 y 11) y es el menos congestionado; nunca elijas un canal intermedio como el 3 o el 9, porque se encimaría parcialmente con dos canales a la vez y eso es peor que compartir limpiamente uno congestionado.

En 5 GHz supón que ves redes en los canales 36, 40, 44 y 149, todas débiles. Aquí hay espectro de sobra: elige el 36 o el 149, el que tenga menos vecinos, y considera usar un ancho de canal de 40 u 80 MHz para más velocidad, ya que hay espacio. La regla general: en 2.4 GHz usa canales de 20 MHz y los canales 1, 6 u 11; en 5 GHz tienes libertad para canales más anchos.

Con este ejercicio cerramos el círculo de la unidad: empezaste aprendiendo qué es una frecuencia y terminaste eligiendo una como lo hace un profesional. Eso es exactamente lo que significa dominar los fundamentos.

Resumen de la unidad

- Una red inalámbrica comunica dispositivos sin cables, usando ondas electromagnéticas que viajan por el aire. Internet y red inalámbrica no son lo mismo: lo inalámbrico suele ser solo el último tramo.
- Lo inalámbrico gana en movilidad y flexibilidad; el cable gana en velocidad, estabilidad y seguridad. El aire es un medio compartido con vecinos e interferencias.
- Las redes se clasifican por alcance: WPAN (personal, Bluetooth, metros), WLAN (local, WiFi, decenas de metros), WMAN (metropolitana, kilómetros) y WWAN (amplia, telefonía móvil 4G/5G).

- Las redes inalámbricas cambiaron el mundo porque eliminaron el costo del cable por metro, llevaron conectividad a zonas rurales y liberaron a las personas de un lugar fijo para estar conectadas.
- Hitos históricos: Marconi y la radio sin hilos, la radiodifusión, la telefonía celular por celdas, el WiFi en bandas libres y las generaciones móviles hasta 5G.
- Todo lo inalámbrico viaja sobre el espectro electromagnético; las comunicaciones usan la zona de radio y microondas por su alcance, su bajo costo y su seguridad para la salud.
- Frecuencia = ciclos por segundo, medida en Hz; kHz = miles, MHz = millones, GHz = miles de millones. La frecuencia es como sintonizar una estación de radio: cada red "escucha" su canal.
- Longitud de onda = $300,000,000 / \text{frecuencia (Hz)}$. A mayor frecuencia, menor longitud de onda. La onda de WiFi 2.4 GHz mide 12.5 cm y la de 5 GHz mide 6 cm: por eso la de 5 GHz choca más con obstáculos.
- Amplitud = fuerza de la onda (potencia). Más potencia da más alcance pero más interferencia a vecinos y más consumo; la ley limita la potencia máxima.
- La señal se mide en dBm con números negativos: cerca de cero es fuerte (-40 dBm excelente), lejos de cero es débil (-80 dBm apenas usable).
- Las ondas sufren reflexión (rebotan en metal), refracción (cambian de dirección), difracción (doblan esquinas) y absorción (el agua se traga la señal). Cada pared y cada piso atenúan la señal; el concreto, el metal, el agua y el microondas son los peores enemigos.
- Las "rayitas" miden fuerza de señal del tramo inalámbrico, no velocidad de internet. Son dos preguntas distintas: ¿me llega bien la onda? y ¿me llegan bien los datos?
- Señal no es lo mismo que datos: la señal es la onda física, los datos son la información; la modulación "monta" los datos sobre la onda, como prender y apagar una lámpara en clave Morse.
- Señal analógica: varía de forma continua (la voz, un dimmer). Señal digital: solo valores discretos, 1 y 0 (un interruptor). Lo digital resiste mejor el ruido y permite corrección de errores.
- Tres modulaciones básicas: por amplitud (fuerte=1, débil=0), por frecuencia (rápido=1, lento=0) y por fase (adelantar o atrasar la onda). Las redes modernas combinan amplitud y fase para meter varios bits por paso, y ajustan la modulación automáticamente según la calidad de la señal.

- Ancho de banda del canal = porción de espectro ocupada, en MHz. Más MHz permiten más velocidad, pero consumen espectro escaso y cada pedacito de señal llega más débil.
- No confundir: el "ancho de banda" del proveedor (Mbps, velocidad) no es el ancho de banda del canal WiFi (MHz, espectro).
- Comandos y herramientas de diagnóstico: ``netsh wlan show interfaces`` y ``netsh wlan show networks mode=bssid`` en Windows; ``iwconfig`` y ``sudo iwlist scan`` en Linux; la configuración de red en Android/iPhone; apps analizadoras de WiFi para ver canales e interferencia; ``ping`` al router para medir el efecto de los obstáculos.
- Buenas prácticas de técnico: router al centro de la casa, elevado, lejos de metal, agua, espejos y microondas; en 2.4 GHz usar solo los canales 1, 6 u 11 con 20 MHz; separar siempre el diagnóstico de señal del diagnóstico de velocidad.

UNIDAD 2: Bandas, canales y el espectro WiFi

(Clases 4 a 6)

Introducción

Imagina que llegas a una casa nueva, conectas tu computadora y descubres que el WiFi funciona lento, se corta cuando alguien usa el microondas y en las tardes parece que todos los vecinos se conectaron a tu red a la vez. La computadora dice que la señal está "excelente", pero los videos se quedan congelados. ¿Qué está pasando? No es que tu internet sea malo, ni que el router esté descompuesto: lo más probable es que tu red inalámbrica esté peleando por un pedazo del aire con las redes de todos los vecinos, con el Bluetooth de tu celular, con el control del Xbox y hasta con el microondas de la cocina.

Esta unidad existe para explicarte exactamente eso: el aire. Bueno, más precisamente, el espectro radioeléctrico, que es el "terreno invisible" donde viven todas las redes WiFi. La Unidad 1 te enseñó qué es una red inalámbrica y cómo se conectan los dispositivos. Ahora vamos a entender el medio por el que viaja todo: las ondas de radio que llevan tus datos del router a tu celular. Sin este conocimiento, configurar un router es como manejar un carro con los ojos vendados: llegas a algún lado, pero no sabes por qué te funciona o por qué te choca.

Cuando termines esta unidad vas a lograr cosas muy concretas. Vas a entender por qué la red de 2.4 GHz de tu router llega hasta la calle pero la de 5 GHz no cruza ni dos paredes, y vas a saber en qué casos conviene usar cada una. Vas a poder abrir una aplicación analizadora de redes WiFi, ver qué canales están usando tus vecinos y elegir manualmente el mejor canal para tu red en lugar de dejar que el router decida por ti (los routers casi siempre deciden mal). Vas a saber qué significa que el ancho de canal sea 20, 40, 80 o 160 MHz, y por qué "más ancho" no siempre significa "más rápido". Vas a reconocer las fuentes de interferencia más comunes en una casa -el microondas, el Bluetooth, las redes vecinas, hasta algunos teléfonos inalámbricos viejos- y vas a tener un plan claro para evitarlas. Y vas a manejar con confianza conceptos técnicos que escucharás por todos lados: espectro no licenciado, canales solapados, DFS, UNII, ruido de fondo y relación señal a ruido. Esas palabras que hoy suenan a chino, al final de esta unidad van a ser herramientas de tu vocabulario diario.

Esta unidad está formada por tres clases que se engranan entre sí como piezas de un rompecabezas. La Clase 4, "Las bandas de 2.4 GHz, 5 GHz y 6 GHz", te presenta los tres grandes terrenos del WiFi moderno: cada banda tiene su personalidad, sus ventajas y sus limitaciones, y entender la diferencia entre alcance y velocidad es la decisión más importante

que vas a tomar al configurar tu red. La Clase 5, "Canales, ancho de canal y canales solapados", baja al detalle: dentro de cada banda hay canales, como carriles de una autopista, y saber cómo se organizan -y cómo se pisan unos a otros cuando están mal configurados- es lo que separa a una red que vuela de una que se arrastra. La Clase 6, "Interferencia", cierra con el problema más frustrante de todos: todo lo que comparte el aire contigo y cómo defenderte. Verás que muchas "fallas de internet" no son del internet en absoluto, sino de interferencia que tú mismo puedes resolver en diez minutos.

Una advertencia honesta antes de empezar: esta unidad tiene más teoría que las otras. No vas a configurar nada con las manos en las primeras páginas. Pero esa teoría es la que te va a permitir, en la segunda mitad de la unidad, abrir el panel de tu router y hacer cambios que de verdad mejoran tu red. La teoría sin práctica es aburrida; la práctica sin teoría es adivinanza. Esta unidad te da las dos, en ese orden, porque así es cómo se aprende de verdad.

También quiero que sepas algo importante: todo lo que aprendas aquí aplica para cualquier router, de cualquier marca, en cualquier casa. No importa si tu router es el que te dio tu proveedor de internet o uno que compraste aparte, ni si vives en un departamento de 50 metros cuadrados o en una casa de dos pisos. Las leyes del espectro son las mismas para todos. Cuando un técnico te diga "cámbiese a 5 GHz" o "ponga el canal en automático", vas a saber exactamente qué significa, cuándo tiene razón y cuándo no. Esa independencia -no depender de que alguien más te arregle la red- es el verdadero objetivo de este curso.

Así que ponte cómodo. Vamos a hablar de autopistas invisibles, de cuartos ruidosos, de microondas asesinos de Netflix y de cómo convertirte en el dueño absoluto del aire de tu casa. Empezamos.

Explicación detallada

El espectro: el terreno invisible donde vive el WiFi

Antes de hablar de bandas y canales, hay que entender el concepto más grande de todos: el espectro radioeléctrico. El espectro es el conjunto de todas las frecuencias de ondas electromagnéticas que existen: desde las ondas de radio larguísimas que usan las estaciones de AM, pasando por la FM, la televisión, los celulares, el WiFi, hasta la luz visible y más allá. Es como un terreno gigantesco dividido en lotes, donde cada servicio de comunicación tiene asignado su pedazo.

Aquí viene lo interesante: ese terreno no es libre. Los gobiernos de cada país, a través de organismos reguladores, deciden quién puede transmitir en qué frecuencia. Las estaciones de

radio y televisión, los celulares, la policía, los aviones: todos necesitan una licencia para usar su pedazo del espectro, y pagan por ella o la reciben por concesión. Pero hay pedacitos del espectro que los reguladores declararon de uso libre, sin licencia: cualquiera puede transmitir ahí sin pedir permiso, siempre y cuando respete ciertas reglas de potencia. Esos pedacitos se llaman bandas ISM (Industrial, Scientific and Medical, por sus siglas en inglés: industrial, científico y médico), porque originalmente se reservaron para equipos industriales, científicos y médicos que generaban ondas de radio como efecto secundario de su funcionamiento. El microondas de tu cocina, por ejemplo, calienta la comida usando ondas de radio en 2.4 GHz: por eso esa banda es de uso libre, porque ya estaba "contaminada" por los microondas desde antes de que existiera el WiFi.

El WiFi vive precisamente en esas bandas de uso libre, y eso es una bendición y una maldición al mismo tiempo. Bendición porque no necesitas permiso de nadie para poner un router en tu casa: lo compras, lo conectas y funciona. Maldición porque, como nadie necesita permiso, todo el mundo transmite ahí: tus vecinos, el Bluetooth, los controles de videojuegos inalámbricos, las cámaras de seguridad baratas, los focos inteligentes, el microondas. El espectro no licenciado es como un parque público: gratis para todos, pero a veces está tan lleno que no hay dónde sentarse. Toda esta unidad trata, en el fondo, de cómo conseguirte el mejor lugar en ese parque.

Las tres bandas principales del WiFi moderno son 2.4 GHz, 5 GHz y 6 GHz. Cada una es un rango de frecuencias: la de 2.4 GHz va aproximadamente de 2400 a 2500 MHz, la de 5 GHz va de 5150 a 5850 MHz (con algunas variaciones por país) y la de 6 GHz va de 5925 a 7125 MHz. No necesitas memorizar estos números, pero sí entender la idea central: son tres terrenos distintos, con reglas distintas, y tu router moderno probablemente puede transmitir en los tres (o al menos en 2.4 y 5).

Frecuencia, longitud de onda y la ley fundamental: alcance contra velocidad

Para entender por qué las bandas se comportan diferente, necesitas una sola idea de física, y es muy intuitiva. Las ondas de radio tienen una frecuencia (cuántas veces oscilan por segundo, medida en GHz, gigahertz) y una longitud de onda (la distancia física entre una cresta y la siguiente). Frecuencia y longitud de onda están inversamente relacionadas: a mayor frecuencia, menor longitud de onda, y viceversa. Las ondas de 2.4 GHz tienen una longitud de onda de unos 12.5 centímetros; las de 5 GHz, de unos 6 centímetros; las de 6 GHz, de unos 5 centímetros.

¿Por qué importa el tamaño de la onda? Porque las ondas interactúan con los objetos de tamaño parecido a su longitud de onda. Una onda de 12.5 cm (2.4 GHz) "ve" una pared como un obstáculo relativamente pequeño y la atraviesa con cierta facilidad, perdiendo algo de

fuerza pero llegando al otro lado. Una onda de 5 o 6 cm (5 y 6 GHz) "ve" la misma pared como un obstáculo más grande en proporción, choca más con ella y pierde mucha más fuerza al cruzarla. Es como la diferencia entre aventar una pelota de playa contra una cortina (la atraviesa fácil) y aventar canicas (se atorán más). Por eso la regla de oro del WiFi: a menor frecuencia, mayor alcance y mejor penetración de paredes; a mayor frecuencia, menor alcance pero mayor velocidad potencial.

Y la velocidad, ¿por qué es mayor en frecuencias altas? Porque las bandas de mayor frecuencia son más anchas: hay más espectro disponible, caben más canales y canales más anchos, y los estándares WiFi más nuevos (que son los más rápidos) se diseñaron para aprovechar esas bandas. No es que la onda viaje más rápido -todas las ondas de radio viajan a la velocidad de la luz-, sino que hay más "espacio" para meter datos. Piensa en una carretera: no es que los carros vayan más rápido, es que hay más carriles.

Esta es la ley fundamental que debes grabarte: alcance y velocidad están en tensión. La banda de 2.4 GHz llega lejos pero es lenta y está saturada. La de 5 GHz es rápida pero no cruza bien las paredes. La de 6 GHz es rapidísima pero su alcance es corto y casi no atraviesa obstáculos. Elegir banda es elegir qué sacrificas. Un buen administrador de red no usa una sola banda para todo: usa cada una para lo que es buena.

Clase 4: La banda de 2.4 GHz, la veterana universal

La banda de 2.4 GHz es la más vieja del WiFi: existe desde el primer estándar inalámbrico popular, el 802.11b de 1999. Todos los dispositivos WiFi del planeta la soportan, desde el celular más nuevo hasta la impresora de hace quince años, pasando por focos inteligentes, cámaras baratas, enchufes inteligentes y asistentes de voz. Es la banda de la compatibilidad universal: si un aparato dice "WiFi", casi seguro habla 2.4 GHz.

Sus características son claras. Alcance: excelente, la mejor de las tres bandas; en campo abierto puede llegar a más de 100 metros, y dentro de una casa cruza varias paredes sin mucho problema. Velocidad: modesta; con los estándares viejos apenas daba 11 o 54 Mbps, y con los modernos (WiFi 4 y WiFi 6 en 2.4 GHz) puede llegar en teoría a varios cientos de Mbps, pero en la práctica, con la saturación que tiene, rara vez verás más de 50 a 100 Mbps reales. Penetración: la mejor, como ya explicamos. Saturación: la peor; es la banda más congestionada porque todo el mundo la usa, incluidos los dispositivos que no son WiFi.

La banda de 2.4 GHz es como la avenida principal de un pueblo: llega a todos lados, todos la usan, pero a la hora pico es un estacionamiento. Úsala para dispositivos que necesitan estar conectados siempre pero no necesitan velocidad: focos inteligentes, cámaras, sensores, impresoras, y para dar cobertura en las zonas más lejanas de la casa donde la señal de 5 GHz

ya no llega. No la uses para ver películas en 4K ni para jugar en línea si tienes 5 GHz disponible.

Un detalle técnico importante: en 2.4 GHz solo hay tres canales que no se solapan entre sí: el 1, el 6 y el 11 (en la mayor parte del mundo; en algunos países hay pequeñas variaciones). Esto lo veremos a fondo en la Clase 5, pero adelanto la idea: si vives en un edificio con veinte redes vecinas, es matemáticamente imposible que no se pisen entre sí, porque solo hay tres canales "limpios" y hay muchas más redes que eso. Esa es la tragedia de 2.4 GHz en zonas densas, y es la razón número uno por la que conviene mover todo lo que se pueda a 5 GHz.

Clase 4: La banda de 5 GHz, la veloz de alcance medio

La banda de 5 GHz llegó con el estándar 802.11a (también de 1999, pero se popularizó mucho después) y se volvió la banda principal del WiFi moderno con el 802.11n (WiFi 4) y sobre todo con el 802.11ac (WiFi 5), que solo funciona en 5 GHz. Hoy es donde ocurre la mayor parte del tráfico rápido: streaming en alta definición, videojuegos en línea, videollamadas, descargas grandes.

Sus características: alcance medio, claramente menor que 2.4 GHz; dentro de una casa típica cubre bien una planta, pero dos paredes de concreto ya la debilitan mucho. Velocidad: alta; con WiFi 5 y WiFi 6 puedes alcanzar velocidades reales de 300 a 900 Mbps en condiciones buenas, suficientes para todo lo doméstico. Penetración: regular; cruza paredes de tabla roca o ladrillo delgado, sufre con concreto y metal. Saturación: mucho menor que 2.4 GHz, porque hay muchos más canales disponibles y menos dispositivos viejos la usan.

La gran ventaja de 5 GHz es el espacio: mientras 2.4 GHz tiene apenas unos 80 MHz de espectro útil, 5 GHz tiene varios cientos de MHz, lo que permite canales anchos de 40, 80 y hasta 160 MHz. Es como comparar una calle de dos carriles con una autopista de ocho. Por eso las velocidades son tan superiores.

Pero 5 GHz tiene una complicación que 2.4 GHz no tiene: los canales DFS. DFS significa Dynamic Frequency Selection (selección dinámica de frecuencia). Parte del espectro de 5 GHz lo comparten los radares: radares meteorológicos, radares de aeropuertos, radares militares. La ley dice que el WiFi es un invitado secundario en esas frecuencias: si tu router detecta la señal de un radar en el canal que está usando, debe abandonar ese canal inmediatamente y cambiarse a otro. Esto causa desconexiones misteriosas: tu red funciona perfecto y de pronto, sin razón aparente, todos los dispositivos se desconectan unos segundos y vuelven. Si vives cerca de un aeropuerto o de una estación meteorológica, los canales DFS pueden ser un dolor de cabeza, y conviene evitarlos manualmente. Los canales DFS en 5 GHz son los del rango 52 a 144 (con variaciones por país). Los routers suelen marcarlos o advertir sobre ellos en su panel de configuración.

Relacionado con esto está el concepto de UNII. UNII significa Unlicensed National Information Infrastructure (infraestructura nacional de información no licenciada): es el nombre que le dio el regulador de Estados Unidos (la FCC) a los bloques del espectro de 5 GHz de uso libre. Se dividen en UNII-1 (canales 36 a 48), UNII-2 (canales 52 a 64, con DFS), UNII-2e o extendido (canales 100 a 144, con DFS) y UNII-3 (canales 149 a 165). No necesitas memorizar los números de memoria, pero sí la idea: no todos los canales de 5 GHz son iguales; algunos requieren DFS y otros no. Cuando configures tu router, preferir los canales no-DFS (36-48 y 149-165) te evita las desconexiones por radar. En México y Latinoamérica las reglas son parecidas, aunque los canales permitidos exactos pueden variar: tu router ya viene configurado para tu región y solo te muestra los canales legales.

Clase 4: La banda de 6 GHz, la nueva autopista vacía

La banda de 6 GHz es la más nueva: se abrió para WiFi en Estados Unidos en 2020 y poco a poco en otros países, y es el territorio del estándar WiFi 6E y WiFi 7. Su gran atractivo es que nació vacía: no hay dispositivos viejos, no hay microondas, no hay Bluetooth (el Bluetooth no usa 6 GHz). Es una autopista recién inaugurada donde casi nadie circula todavía.

Características: alcance corto, el menor de las tres bandas; está pensada para una misma habitación o espacios abiertos sin muchas paredes. Velocidad: la más alta; con canales de hasta 320 MHz en WiFi 7, las velocidades teóricas superan los varios gigabits por segundo, y en la práctica puedes ver más de 1 Gbps reales si tu internet lo permite. Penetración: pobre; una pared gruesa puede matar la señal. Saturación: mínima, por ahora.

Hay dos limitaciones prácticas importantes. Primera: solo los dispositivos nuevos la soportan; si tu celular o tu laptop tienen más de tres o cuatro años, probablemente no tienen radio de 6 GHz, y no hay forma de agregárselo por software. Segunda: la disponibilidad por país es desigual; en algunos países de Latinoamérica la banda de 6 GHz aún no está autorizada o

está parcialmente autorizada, así que un router "WiFi 6E" comprado en otro país podría no poder usarla donde vives. Antes de invertir en equipos 6 GHz, verifica que tus dispositivos la soporten y que esté permitida en tu país.

¿Vale la pena 6 GHz hoy? Si tienes internet de más de 500 Mbps, dispositivos nuevos y trabajas en la misma habitación que el router, sí: es la forma de exprimir al máximo tu conexión. Para el resto de los casos, 5 GHz sigue siendo la mejor combinación de velocidad, alcance y compatibilidad. Piensa en 6 GHz como el carril exprés: fantástico si tu carro puede entrar, inútil si no.

Tabla comparativa de las tres bandas

Para tenerlo todo de un vistazo, aquí está la comparación directa:

- Frecuencia y longitud de onda: 2.4 GHz (~12.5 cm), 5 GHz (~6 cm), 6 GHz (~5 cm).
- Alcance: 2.4 GHz el mayor, 5 GHz medio, 6 GHz el menor.
- Penetración de paredes: 2.4 GHz buena, 5 GHz regular, 6 GHz pobre.
- Velocidad máxima práctica: 2.4 GHz hasta ~100 Mbps, 5 GHz hasta ~900 Mbps, 6 GHz más de 1 Gbps.
- Congestión típica: 2.4 GHz muy alta, 5 GHz media-baja, 6 GHz mínima.
- Compatibilidad: 2.4 GHz universal, 5 GHz casi universal en equipos de la última década, 6 GHz solo equipos nuevos (2021 en adelante, aproximadamente).
- Interferencias típicas: 2.4 GHz microondas, Bluetooth y vecinos; 5 GHz radares (canales DFS) y vecinos; 6 GHz casi ninguna por ahora.

La estrategia ganadora para una casa típica: usa 5 GHz como tu banda principal para todo lo que necesita velocidad (celulares, laptops, TV, consolas), deja 2.4 GHz para los aparatos inteligentes y las zonas lejanas, y usa 6 GHz solo si tienes los equipos y la necesitas de verdad. Muchos routers modernos tienen una función llamada "band steering" (dirección de banda) que intenta mover automáticamente cada dispositivo a la mejor banda, pero no siempre acierta; a veces conviene separar las redes con nombres distintos (por ejemplo, "MiCasa" y "MiCasa_5G") para tener control manual. Hablaremos de esto en unidades posteriores.

Clase 5: Los canales, carriles de la autopista invisible

Dentro de cada banda, el espectro se divide en canales. Un canal es un pedazo del espectro con una frecuencia central y un cierto ancho, donde el router transmite. La analogía clásica -y

la mejor- es la de la autopista: la banda es la autopista completa y los canales son los carriles. Cada red WiFi "maneja" por uno (o varios) carriles. Si dos redes usan el mismo carril, se estorban; si usan carriles separados, cada una va a su velocidad sin molestar a la otra.

En 2.4 GHz hay 14 canales numerados del 1 al 14 (en la práctica, del 1 al 11 o 13 según el país; el 14 solo se usa en Japón para un estándar viejo). Cada canal tiene 20 MHz de ancho nominal y sus centros están separados por solo 5 MHz. Haz la cuenta: si cada canal mide 20 MHz de ancho pero los centros están a 5 MHz de distancia, los canales se enciman unos sobre otros como tejas de un techo. El canal 1, por ejemplo, ocupa en realidad desde aproximadamente 2401 hasta 2423 MHz, y el canal 2 desde 2406 hasta 2428: se solapan en su mayor parte. Por eso se habla de canales solapados: en 2.4 GHz, casi todos los canales se pisan entre sí.

Solo hay tres combinaciones de canales que no se solapan: 1, 6 y 11. El canal 1 ocupa hasta ~2423 MHz, el 6 va de ~2426 a ~2448, y el 11 de ~2451 a ~2473: entre ellos hay suficiente separación para no interferirse. Por eso la regla de oro de 2.4 GHz: usa solo los canales 1, 6 u 11, y elige el que esté menos ocupado por tus vecinos. Usar el canal 3, por ejemplo, es el peor error posible: se solapa con el 1 y con el 6, así que recibes interferencia de los dos lados sin el beneficio de compartir limpiamente con ninguno. Es como manejar a caballo entre dos carriles: estorbas a todos y nadie te deja pasar.

En 5 GHz la situación es mucho más cómoda: los canales están separados por 20 MHz y no se solapan cuando usan ancho de 20 MHz. Hay muchos más canales disponibles (más de veinte según el país), así que es raro que te quedes sin un canal limpio. En 6 GHz, todavía mejor: hay espacio de sobra y canales que no se tocan.

El ancho de canal: 20, 40, 80 y 160 MHz

El ancho de canal es cuántos MHz de espectro usa tu red para transmitir. Más ancho significa más velocidad potencial, porque caben más datos por segundo: es como ensanchar el carril para que pasen más carros a la vez. Los anchos típicos son 20 MHz (el básico), 40 MHz (doble), 80 MHz (cuádruple) y 160 MHz (óctuple, solo en 5 y 6 GHz con equipos nuevos).

Aquí viene el matiz que muchos tutoriales omiten: más ancho NO siempre es mejor, porque un canal más ancho ocupa el lugar de varios canales. Un canal de 40 MHz en 2.4 GHz ocupa el equivalente a dos canales de 20 MHz; uno de 80 MHz en 5 GHz ocupa cuatro. Y lo más importante: un canal ancho también recoge más interferencia, porque "escucha" un pedazo más grande del espectro. Es como abrir más ventanas en un cuarto ruidoso: entra más aire fresco, pero también más ruido de la calle.

Las buenas prácticas por banda son claras. En 2.4 GHz, usa siempre 20 MHz, sin excepción en zonas con vecinos. Activar 40 MHz en 2.4 GHz (algunos routers lo llaman "ancho de canal automático" o "20/40") es uno de los errores más comunes: en teoría duplica la velocidad, pero en la práctica ocupa dos de los tres únicos canales limpios (1, 6 y 11), se pelea con todas las redes vecinas y el resultado neto suele ser peor velocidad y más cortes. Solo tendría sentido en una casa aislada en el campo sin vecinos a kilómetros, y aun así la ganancia es dudosa. En 5 GHz, 40 u 80 MHz es lo recomendable para la mayoría de los casos: hay espacio suficiente y la ganancia de velocidad es real. Usa 160 MHz solo si vives en una zona con pocos vecinos en 5 GHz y tus dispositivos lo soportan; en un edificio de departamentos, 160 MHz casi garantiza que te vas a pisar con alguien. En 6 GHz, puedes usar 80 o 160 MHz con tranquilidad porque la banda está vacía.

Otro concepto clave: el ancho de canal afecta la velocidad real, no solo la teórica. Duplicar el ancho de 20 a 40 MHz, en condiciones ideales, casi duplica la velocidad de transmisión. Pero las condiciones ideales casi nunca existen: con interferencia, un canal de 80 MHz lleno de ruido puede rendir menos que uno de 40 MHz limpio. Por eso la regla práctica es: elige el ancho más grande que puedas usar SIN pisar a nadie. La cortesía espectral -no acaparar más aire del necesario- no es solo amabilidad con los vecinos: es lo que hace que tu propia red funcione mejor.

Ruido de fondo y relación señal a ruido: cómo "escucha" tu dispositivo

Tu celular no solo escucha a tu router: escucha todo lo que hay en el aire en esa frecuencia. El ruido de fondo (noise floor) es el nivel de "murmullo" constante del espectro: la suma de todas las señales débiles, interferencias y ruido electrónico que siempre están presentes. Se mide en dBm (decibelios relativos a un milivatio), igual que la señal, y típicamente anda por -90 a -95 dBm en un ambiente limpio. Mientras más negativo el número, menos ruido: -95 dBm es más silencioso que -85 dBm.

La relación señal a ruido (SNR, Signal-to-Noise Ratio) es la diferencia entre qué tan fuerte llega la señal de tu router y qué tan alto está el ruido de fondo. Si tu señal llega a -60 dBm y el ruido está en -90 dBm, tu SNR es de 30 dB. Mientras mayor el SNR, mejor: con un SNR alto, el dispositivo distingue claramente la señal del ruido y puede usar las modulaciones más rápidas; con un SNR bajo, tiene que usar modulaciones lentas y robustas, y si el SNR es muy bajo, los datos se pierden y hay que retransmitirlos.

Los rangos de referencia que debes conocer: un SNR mayor a 25 dB es excelente (velocidades máximas), entre 15 y 25 dB es bueno (velocidades altas con buena estabilidad), entre 10 y 15 dB es apenas aceptable (velocidad reducida, cortes ocasionales) y menor a 10 dB es malo (la conexión se arrastra o se cae). Cuando veas que tu celular dice "señal

excelente" pero todo va lento, casi siempre el problema es el SNR, no la señal: la señal de tu router llega fuerte, pero el ruido -de vecinos, de interferencias- está igual de fuerte, y el dispositivo no puede distinguir una cosa de la otra. Es como tratar de escuchar a alguien que te habla fuerte en un concierto de rock: el volumen de la voz no es el problema, el problema es el ruido alrededor.

Esto conecta directamente con los canales: cambiarte a un canal menos ocupado baja tu ruido de fondo, sube tu SNR y tu velocidad mejora aunque la "intensidad de señal" no cambie ni un poco. Por eso el análisis de canales que harás en la sección de ejemplos es la herramienta más poderosa de esta unidad.

Clase 6: Interferencia, el enemigo invisible

Interferencia es cualquier señal no deseada que comparte tu frecuencia y estorba a tu red. Es el tema más frustrante del WiFi porque es invisible, cambia con la hora del día y muchas veces la "culpa" no es de tu internet ni de tu router. Vamos a conocer a los sospechosos habituales.

El microondas es el criminal más famoso. Un horno de microondas calienta la comida emitiendo ondas de radio a 2.4 GHz con una potencia brutal (cientos de watts, contra los 0.1 watts de tu router). Los hornos están blindados, pero siempre se escapa algo de radiación, y ese "algo" es suficiente para saturar por completo la banda de 2.4 GHz en varios metros a la redonda. El síntoma clásico: el Netflix se congela o el Zoom se corta exactamente cuando alguien calienta la comida, y vuelve a la normalidad dos minutos después. Si tu router está en la cocina o cerca de ella, muévelo; y si el problema persiste, la solución definitiva es usar 5 GHz, que el microondas no toca.

El Bluetooth es el segundo sospechoso. El Bluetooth también vive en 2.4 GHz y usa una técnica llamada salto de frecuencia: brinca entre 79 canalitos 1600 veces por segundo. Cada salto es una pequeña interferencia para el WiFi. Un audífono Bluetooth o un mouse no causan gran daño, pero varios dispositivos Bluetooth activos cerca del router o de tu laptop sí degradan la red de 2.4 GHz de forma medible. Además, muchos celulares y laptops comparten la misma antena entre WiFi y Bluetooth para ahorrar espacio, lo que empeora el problema. Si usas audífonos Bluetooth y tu laptop está en 2.4 GHz, prueba cambiar la laptop a 5 GHz: la diferencia puede ser notable.

Los vecinos son la tercera fuente, y en edificios de departamentos, la más importante. Cada red vecina en tu mismo canal o en un canal solapado es interferencia directa: no solo "ocupan" el aire, sino que el protocolo WiFi los obliga a turnarse para hablar (es el mecanismo CSMA/CA, que veremos en la Unidad 3). Con veinte redes vecinas, tu router pasa más tiempo esperando su turno que transmitiendo. La defensa es la que ya conoces: analiza los canales,

elige el menos ocupado entre 1, 6 y 11 en 2.4 GHz, y mueve todo lo posible a 5 GHz donde hay más espacio.

Hay más sospechosos en la lista: los teléfonos inalámbricos viejos (los DECT modernos no interfieren, pero algunos inalámbricos baratos de 2.4 GHz sí), las cámaras de seguridad analógicas inalámbricas baratas, los monitores de bebé antiguos, algunos controles de drones y juguetes de radio control, e incluso los focos LED baratos con fuentes de poder mal blindadas que generan ruido eléctrico de banda ancha. También las paredes y objetos físicos: un espejo grande, un acuario (el agua absorbe las ondas de 2.4 GHz de maravilla) o una pared con malla metálica pueden atenuar la señal tanto como una interferencia. La interferencia no siempre es otra señal de radio: a veces es física.

¿Cómo evitar la interferencia? El plan de defensa tiene cinco pasos. Primero, ubica bien el router: en un lugar central, elevado (sobre un mueble, no en el piso), lejos del microondas, de espejos grandes y de peceras, y no encerrado dentro de un mueble metálico. Segundo, analiza el espectro con una app analizadora y elige manualmente el mejor canal en cada banda, como aprenderás en los ejemplos. Tercero, usa el ancho de canal correcto: 20 MHz en 2.4 GHz, 40 u 80 MHz en 5 GHz. Cuarto, mueve los dispositivos que necesitan velocidad a 5 GHz (o 6 GHz) y deja 2.4 GHz para los aparatos simples. Quinto, si nada de eso basta porque vives en un edificio saturadísimo, considera soluciones de la Unidad 5 en adelante: un segundo punto de acceso cableado, una red en malla (mesh) o, en casos extremos, llevar la señal por cable Ethernet o por la red eléctrica (PLC) a las zonas problemáticas. La interferencia se combate con física, no con "más potencia": subir la potencia del router casi nunca ayuda, porque el ruido sube igual y además molestas más a los vecinos.

Errores comunes que debes evitar

Cierra esta explicación con la lista de errores que veo una y otra vez, para que no los cometas. Error uno: dejar el canal en "Auto" para siempre. El modo automático elige un canal al encender el router y rara vez lo vuelve a evaluar; con el tiempo, los vecinos cambian, aparecen redes nuevas y tu canal "automático" termina siendo el peor de todos. Revisa tus canales cada pocos meses, o cuando notes degradación. Error dos: activar 40 MHz en 2.4 GHz creyendo que "más ancho es más rápido". Ya vimos por qué es una trampa: ocupas dos de los tres canales limpios y te peleas con todos. Error tres: usar canales intermedios en 2.4 GHz (3, 4, 8, 9...). Solo 1, 6 y 11 no se solapan; cualquier otro se pisa con dos canales a la vez. Error cuatro: poner el router junto al microondas, dentro de un mueble o en el piso en una esquina de la casa. La ubicación física importa tanto como la configuración. Error cinco: comprar un router "gamer" carísimo esperando que resuelva un problema de interferencia. Un router caro con el canal equivocado en una banda saturada rinde peor que un router barato bien

configurado. La configuración correcta le gana al hardware caro casi siempre. Error seis: ignorar la banda de 5 GHz por flojera ("la de 2.4 me llega a todos lados"). Sí, llega más lejos, pero si tu problema es velocidad y no cobertura, 5 GHz es la respuesta. Y error siete: cambiar de proveedor de internet cuando el problema es el WiFi. Si la velocidad por cable es buena pero por WiFi es mala, el proveedor no tiene la culpa: el problema está en el aire de tu casa, y esta unidad te acaba de dar las herramientas para arreglarlo.

Los estándares WiFi y las bandas: quién puede usar qué

A lo largo de la unidad mencioné los estándares 802.11b, g, n, ac, ax y be. Vale la pena ordenarlos porque cada estándar "habla" en ciertas bandas, y eso explica por qué algunos aparatos viejos no ven tu red de 5 GHz por más que la configures perfecto.

El 802.11b (1999) y el 802.11g (2003) solo usan 2.4 GHz: son los abuelos, lentos (11 y 54 Mbps teóricos), pero todos los aparatos los entienden. El 802.11n, conocido como WiFi 4 (2009), fue el primero en usar las dos bandas, 2.4 y 5 GHz: si tienes un aparato de hace más de diez años que sí ve redes 5G, casi seguro es WiFi 4. El 802.11ac, o WiFi 5 (2013), abandonó 2.4 GHz y solo trabaja en 5 GHz: fue el estándar que convirtió a 5 GHz en la banda principal de velocidad. El 802.11ax, o WiFi 6 (2019), volvió a las dos bandas, 2.4 y 5 GHz, con mejoras de eficiencia; su primo el WiFi 6E es el mismo WiFi 6 pero con permiso de usar además la banda de 6 GHz. Y el 802.11be, o WiFi 7 (2024), usa las tres bandas y agrega canales de hasta 320 MHz en 6 GHz.

¿Por qué te importa esta genealogía? Por tres razones prácticas. Primera: si un aparato no detecta tu red de 5 GHz, no es que esté descompuesto: probablemente es 802.11b/g y solo habla 2.4 GHz; la solución es dejarle su red de 2.4 GHz funcionando, no pelearte con él. Segunda: cuando un router anuncia "compatible con WiFi 6", verifica en qué bandas: un router WiFi 6 barato puede ser solo 2.4 GHz mejorado, mientras que uno WiFi 6E incluye la radio de 6 GHz, que es hardware distinto y más caro. Tercera: los aparatos viejos en 2.4 GHz pueden frenar a los nuevos, porque el punto de acceso a veces baja su ritmo para hacerse entender con el más lento (es el tema de la eficiencia del aire, que veremos a fondo en la Unidad 3). Por eso conviene aislar: deja a los aparatos viejos y simples en 2.4 GHz y reserva 5 GHz para los modernos que necesitan velocidad. No es discriminación, es ingeniería: cada generación en su carril rinde más.

Un truco final de compra: cuando veas un router que dice "AX3000" o "BE6500", ese número es la suma de las velocidades teóricas máximas de todas sus bandas juntas, no la velocidad que obtendrás en un solo aparato. Un AX3000 típico suma unos 600 Mbps en 2.4 GHz más unos 2400 Mbps en 5 GHz. Ningún dispositivo tuyo va a descargar a 3000 Mbps con ese router: el número sirve para comparar routers entre sí, no para predecir tu velocidad real. Tu

velocidad real depende de tu internet contratado, de tu distancia al router, del canal que elegiste con lo aprendido en esta unidad y de la generación WiFi de tu dispositivo. Ya sabes: la configuración correcta le gana al número grande de la caja.

La cortesía del espectro: tu red también es el vecino de alguien

Cierro la explicación con una idea que pocos mencionan y que te convierte en un verdadero profesional: el espectro es compartido, así que tu configuración afecta a tus vecinos igual que la de ellos te afecta a ti. Cada decisión que tomas -el canal, el ancho, la potencia- dibuja tu "huella" en el aire del edificio.

La cortesía del espectro tiene tres reglas simples. Primera: no uses más ancho del necesario. Si tu internet es de 100 Mbps, un canal de 20 MHz en 5 GHz te sobra; poner 160 MHz "porque se puede" solo te expone a más interferencia y le quita aire a los demás sin beneficiarte en nada. Segunda: no subas la potencia de transmisión al máximo por defecto. Más potencia no atraviesa mejor las paredes gruesas (la física no se soborna) y en cambio tu red llega más lejos, molestando a más vecinos y recibiendo más interferencia de vuelta. La potencia media o automática suele ser el punto ideal en casas y departamentos. Tercera: si detectas que un vecino usa un canal intermedio que se solapa con todos (el famoso canal 3 o el 9), una conversación amable con estos datos en la mano resuelve más que cualquier configuración: explícale lo de 1, 6 y 11 y ambos ganan velocidad. En edificios, el WiFi es un bien común: cuando todos configuran bien, todos navegan mejor. Y cuando seas tú el que entienda del tema en tu edificio, ya sabes quién va a recibir las llamadas de "oye, ¿me ayudas con mi internet?".

Ejemplos paso a paso

Ejemplo 1: Ver qué redes y canales hay a tu alrededor en Windows

Vamos a lo práctico. El primer paso para dominar tu espectro es verlo: saber qué redes WiFi te rodean, en qué banda y canal transmite cada una y con qué intensidad llega su señal. En Windows puedes hacerlo sin instalar nada, con un comando del sistema.

Paso 1: Abre la terminal de Windows. Presiona la tecla Windows, escribe "cmd" y abre el Símbolo del sistema (no necesitas permisos de administrador para esto).

Paso 2: Escribe el siguiente comando y presiona Enter:

```
netsh wlan show networks mode=bssid
```

Paso 3: El sistema te muestra la lista de todas las redes WiFi que tu tarjeta inalámbrica puede detectar. Por cada red verás varios datos. Los que nos importan ahora son:

```
SSID 1 : MiVecino_5G
  Tipo de red      : Infraestructura
  Autenticación   : WPA2-Personal
  Cifrado         : CCMP
  BSSID 1        : aa:bb:cc:11:22:33
    Señal         : 72%
    Tipo de radio  : 802.11n
    Banda         : 5 GHz
    Canal         : 44
```

El SSID es el nombre de la red. El BSSID es la dirección física del punto de acceso (cada red puede aparecer varias veces si tiene varios BSSID). La señal en porcentaje te dice qué tan fuerte llega: mientras más alto, más cerca o más potente. La banda te dice si es 2.4 o 5 GHz. El canal es el dato de oro: te dice en qué carril de la autopista va cada vecino.

Paso 4: Repite el comando un par de veces en distintos momentos del día (mañana, tarde y noche). Las redes vecinas cambian: hay routers que se apagan, celulares compartiendo internet que aparecen y desaparecen. Anota en un papel qué canales de 2.4 GHz (1 al 11) aparecen más ocupados y cuáles están libres. Esa anotación es tu mapa del espectro, y la vas a usar en el Ejemplo 3.

Limitación honesta: este comando muestra las redes WiFi, pero no muestra interferencias que no son WiFi (microondas, Bluetooth). Para eso necesitas una app analizadora con gráfica de espectro, como veremos en el Ejemplo 2. Pero como primer reconocimiento, `netsh` es gratis, no instala nada y te da el 80% de la información que necesitas.

Ejemplo 2: Analizar el espectro con una app en el celular

Las aplicaciones analizadoras de WiFi convierten tu celular en un pequeño laboratorio de espectro. Muestran en una gráfica qué canales están ocupados, qué tan fuerte llega cada red y cuál es el mejor canal disponible. Hay varias gratuitas y confiables; busca en tu tienda de aplicaciones "WiFi Analyzer" (en Android hay excelentes opciones gratuitas; en iPhone las opciones están más limitadas por el sistema, pero existen alternativas).

Paso 1: Instala la aplicación y ábrela. Al abrirla verás una gráfica con el eje horizontal numerado del 1 al 11 (o más, según la banda): esos son los canales. Cada red vecina aparece como una curva con forma de campana centrada en su canal; mientras más alta la curva, más fuerte llega su señal.

Paso 2: Cambia a la vista de 2.4 GHz. Observa las curvas: verás que las redes bien configuradas están centradas en 1, 6 u 11, y las mal configuradas aparecen a caballo entre dos canales, con su campana pisando a los vecinos de ambos lados. Esos son los que más daño hacen, y no puedes hacer nada con ellos salvo alejarte a un canal limpio.

Paso 3: Cambia a la vista de 5 GHz. Notarás dos cosas: hay menos redes y las curvas no se enciman (los canales de 5 GHz no se solapan en 20 MHz). Busca un canal donde no haya ninguna curva alta: ese es tu candidato.

Paso 4: La mayoría de estas apps tienen una pantalla de "recomendación" o "mejor canal": te dicen directamente qué canal usar según lo que midieron. Úsala como sugerencia, no como verdad absoluta: la app mide desde dónde estás tú parado, y lo ideal es medir cerca del lugar donde está el router, que es donde la interferencia le pega a él. Camina hasta el router, mide ahí y anota la recomendación.

Paso 5: Repite la medición en la noche, que es cuando más redes están activas (todos en casa viendo videos). El canal que esté libre en la noche es el que te conviene de verdad.

Con estos dos ejemplos ya sabes diagnosticar. Ahora vamos a actuar: cambiar el canal en el router.

Ejemplo 3: Cambiar el canal de tu router paso a paso (panel web genérico)

Cambiar el canal es la intervención más rentable del WiFi doméstico: toma diez minutos y puede duplicar tu velocidad real. Los menús cambian según la marca (TP-Link, Huawei, Arris, Technicolor, ZTE...), pero la lógica es la misma en todos. Aquí va el procedimiento genérico.

Paso 1: Conéctate a tu red (por WiFi o mejor aún por cable Ethernet a la computadora, para no perder el acceso a mitad del cambio). Abre el navegador y en la barra de direcciones escribe la dirección del router. Las más comunes son:

```
192.168.1.1  
192.168.0.1  
192.168.1.254
```

Si ninguna funciona, en Windows abre cmd y escribe `ipconfig`; la "Puerta de enlace predeterminada" es la dirección de tu router. En el celular, está en los detalles de la conexión WiFi como "Puerta de enlace" o "Router".

Paso 2: Inicia sesión en el panel. Te pedirá usuario y contraseña. Los valores de fábrica más comunes son admin/admin, admin/1234 o usuario/clave; casi siempre vienen impresos en una etiqueta pegada debajo o detrás del router. Si tu proveedor te instaló el router, a veces la

contraseña es la misma que la del WiFi o te la dieron en una hoja. Si nunca la cambiaste y no la encuentras, tendrás que reiniciar el router a valores de fábrica (botón de reset 10 segundos), pero ojo: eso borra toda la configuración, úsalo como último recurso.

Paso 3: Busca la sección inalámbrica. Suele llamarse "Wireless", "Inalámbrico", "WiFi", "Red inalámbrica" o estar dentro de "Configuración avanzada" o "Advanced". Dentro encontrarás, separadas, la configuración de 2.4 GHz y la de 5 GHz (a veces en pestañas distintas).

Paso 4: En la sección de 2.4 GHz, busca el campo "Canal" (Channel). Estará en "Auto" o en un número. Cámbialo al canal que elegiste con tu análisis del Ejemplo 1 o 2: solo 1, 6 u 11, el menos ocupado. Busca también el campo "Ancho de canal" (Channel Width o Bandwidth) y ponlo en 20 MHz. Guarda los cambios (botón Apply, Guardar o Aceptar). El router puede tardar un minuto en aplicar el cambio y es normal que el WiFi se desconecte unos segundos.

Paso 5: En la sección de 5 GHz, busca el campo "Canal" y elige un canal no-DFS poco ocupado (de preferencia entre 36 y 48, o entre 149 y 165 según los que te ofrezca tu router). Pon el ancho de canal en 40 MHz o 80 MHz. Guarda.

Paso 6: Verifica. Vuelve a correr el análisis del Ejemplo 1 o 2: tu red debe aparecer ahora en el canal que elegiste. Haz una prueba de velocidad (por ejemplo en speedtest.net) antes y después del cambio, a la misma hora y desde el mismo lugar, para comparar con datos reales y no con sensaciones. Anota los resultados: es tu evidencia de que el cambio funcionó.

Paso 7 (opcional pero recomendado): si tu router transmite las dos bandas con el mismo nombre de red, considera ponerles nombres distintos (por ejemplo "MiCasa" y "MiCasa_5G") para poder elegir manualmente en cada dispositivo. Está en el mismo panel, en el campo SSID o "Nombre de red". Así tus aparatos inteligentes se quedan en 2.4 GHz y tu celular y tu laptop usan 5 GHz sin que el "band steering" automático decida por ti.

Precaución: no cambies nada más en el panel si no sabes qué es. En particular, no toques la configuración de seguridad (debe quedar en WPA2 o WPA3), ni el DHCP, ni el firmware a menos que sepas lo que haces. El objetivo de hoy es solo el canal y el ancho de canal.

Ejemplo 4: Elegir el mejor canal con datos reales (caso de un edificio)

Vamos a hacer el razonamiento completo con un caso típico, para que veas cómo se decide. Supón que vives en un departamento y tu análisis con `netsh` mostró estas redes en 2.4 GHz:

```
Red VecinoA, canal 1, señal 80%
Red VecinoB, canal 1, señal 45%
Red VecinoC, canal 6, señal 70%
Red VecinoD, canal 6, señal 60%
Red VecinoE, canal 9, señal 55%
Red VecinoF, canal 11, señal 40%
```

Tu router está en "Auto" y cayó en el canal 6. ¿Qué haces?

Paso 1: Descarta los canales solapados. El canal 9 se solapa con el 6 y el 11, así que VecinoE está molestando a dos canales a la vez. Tus opciones reales son 1, 6 u 11.

Paso 2: Evalúa cada candidato. Canal 1: dos redes (80% y 45%). Canal 6: dos redes (70% y 60%) más el solapamiento parcial de VecinoE en el 9. Canal 11: una red al 40% más el solapamiento parcial de VecinoE.

Paso 3: Elige el 11. Tiene la menor cantidad de redes directas y la señal competidora más débil (40%). El solapamiento de VecinoE le pega un poco, pero menos que lo que le pega al 6, donde hay dos redes fuertes más el solapamiento. Configura tu router en canal 11, ancho 20 MHz.

Paso 4: Verifica una semana después. Los vecinos cambian de canal, aparecen redes nuevas. Si VecinoE se mueve o aparece alguien fuerte en el 11, repite el análisis. Esto no se hace una vez en la vida: se revisa cada pocos meses.

La lección del ejemplo: no existe el "mejor canal" en abstracto; existe el mejor canal para tu ubicación, hoy. El análisis manda, no la superstición ("el 6 siempre es el bueno").

Ejemplo 5: Diagnosticar si tu problema es interferencia o falta de señal

Muchas personas confunden "poca señal" con "mucho interferencia" y toman la decisión equivocada (comprar un repetidor cuando lo que necesitan es cambiar de canal). Este ejemplo te enseña a distinguirlas con dos pruebas simples.

Prueba A: mide la velocidad junto al router y lejos de él. Ponte a un metro del router y haz una prueba de velocidad. Luego ve al cuarto donde tienes el problema y repítela. Si junto al router la velocidad es buena y lejos es mala, tu problema es de cobertura (señal que no llega): necesitas mejor ubicación, un punto de acceso adicional o red mesh. Si la velocidad es mala incluso junto al router, tu problema NO es de cobertura: es interferencia, saturación del canal o un problema con tu proveedor. Cambiar de canal es el primer paso.

Prueba B: compara 2.4 GHz contra 5 GHz en el mismo lugar. Conéctate a cada banda desde el mismo sitio y mide la velocidad en ambas. Si 5 GHz va mucho más rápido que 2.4 GHz, la banda de 2.4 está saturada o interferida en tu zona (lo normal en edificios). Si ambas van mal, el problema puede ser el router saturado, interferencia en ambas bandas o tu conexión de internet en sí: conecta una computadora por cable Ethernet directo al router y mide; si por cable va bien, el problema es 100% tu WiFi; si por cable también va mal, llama a tu proveedor, porque el problema está antes de tu router.

Con estas dos pruebas, en quince minutos sabes exactamente dónde está tu problema y no gastas dinero adivinando. Esa es la diferencia entre un usuario que "le mueve a ver si jala" y uno que diagnostica como profesional.

Práctica

Ejercicio 1: Elige el mejor canal en 2.4 GHz

Escenario: analizaste tu zona y encontraste estas redes en 2.4 GHz: dos redes en el canal 1 (señal 65% y 50%), una red en el canal 4 (señal 75%), tres redes en el canal 6 (señal 80%, 55% y 40%) y ninguna red en el canal 11, aunque hay una red débil en el canal 9 (señal 25%). ¿Qué canal eliges para tu router y por qué? ¿Qué ancho de canal configuras?

Solución paso a paso. Paso 1: recuerda la regla: solo 1, 6 y 11 son opciones válidas; el canal 4 se solapa con el 1 y el 6, así que ni lo consideres como opción propia, solo como interferencia ajena. Paso 2: evalúa el canal 1: tiene dos redes directas (65% y 50%) más el solapamiento de la red del canal 4 (75%, fuerte y cercana en frecuencia). Mal candidato. Paso 3: evalúa el canal 6: tres redes directas, una de ellas muy fuerte (80%), más el solapamiento de la del canal 4. El peor candidato. Paso 4: evalúa el canal 11: cero redes directas y solo el solapamiento parcial de una red débil en el canal 9 (25%). El canal 9 se solapa parcialmente con el 11, pero una señal de 25% a esa distancia de frecuencia es un estorbo menor. Ganador: canal 11. Paso 5: ancho de canal 20 MHz, siempre en 2.4 GHz con vecinos. Conclusión: canal 11, 20 MHz. La clave del ejercicio era no dejarse llevar por "el 1 tiene solo dos redes": el solapamiento del canal 4 lo contamina, y el 11 está prácticamente libre.

Ejercicio 2: Calcula el solapamiento de un canal mal elegido

Escenario: tu vecino configuró su router en el canal 3 de 2.4 GHz con ancho de 20 MHz. Tú estás en el canal 1 y otro vecino está en el canal 6. ¿A quiénes interfiere tu vecino del canal 3? ¿Qué le recomendarías?

Solución paso a paso. Paso 1: recuerda que cada canal de 20 MHz en 2.4 GHz ocupa en realidad unos 22 MHz alrededor de su frecuencia central, y que los centros están separados por 5 MHz. Paso 2: el canal 1 ocupa aproximadamente de 2401 a 2423 MHz; el canal 3, de 2411 a 2433 MHz; el canal 6, de 2426 a 2448 MHz. Paso 3: compara rangos. El canal 3 (2411-2433) se solapa con el canal 1 (2401-2423) en el rango 2411-2423: interferencia directa contra ti. También se solapa con el canal 6 (2426-2448) en el rango 2426-2433: interferencia directa contra el otro vecino. Paso 4: conclusión: el vecino del canal 3 interfiere a los dos, y además recibe interferencia de los dos. Es el peor escenario posible: todos pierden. Paso 5: recomendación: explícale (con amabilidad, lleva estos números) que se cambie al 1, al 6 o al 11 según cuál esté menos ocupado; si el 1 y el 6 ya están tomados por ustedes dos, que use el 11. Un canal "intermedio" nunca es la respuesta en 2.4 GHz.

Ejercicio 3: Plan de canales para una casa de dos pisos

Escenario: tienes una casa de dos pisos. En la planta baja está el router principal (planta baja, sala) y en la planta alta pusiste un segundo punto de acceso conectado por cable Ethernet al router (está en el estudio). Necesitas planear los canales de 2.4 GHz y 5 GHz para los dos equipos de modo que no se interfieran entre sí. Los vecinos usan: en 2.4 GHz, canal 1 (fuerte) y canal 11 (medio); en 5 GHz, canal 44 (fuerte) y canal 36 (débil).

Solución paso a paso. Paso 1: en 2.4 GHz, tus opciones son 1, 6 y 11. El 1 está fuerte con el vecino y el 11 está medio: elige el 6 para uno de tus equipos, que está libre. Paso 2: el segundo equipo necesita otro canal que no se solape con el 6 ni con los vecinos: el 11 tiene un vecino medio, el 1 tiene un vecino fuerte. Entre esos dos males, el 11 es mejor. Asigna: router planta baja en canal 6, punto de acceso planta alta en canal 11. Así tus dos equipos no se pisan (6 y 11 no se solapan) y cada uno evita al vecino más fuerte. Paso 3: en 5 GHz hay más margen. El vecino fuerte está en 44 y el débil en 36. Elige canales no-DFS alejados: por ejemplo, el router en el canal 48 (cerca del 44 pero sin solaparse en 20 MHz... ojo: con ancho de 40 MHz, 44 y 48 sí se solaparían, porque 40 MHz ocupa dos canales de 20). Mejor: usa 20 o 40 MHz con planeación. Opción limpia: router en canal 36 con 40 MHz (ocupa 36+40... en realidad el par 36-40) y punto de acceso en canal 149 con 40 u 80 MHz, lejos de todo. Los canales 149-165 (UNII-3) no tienen DFS y el vecino no los usa: son tu mejor opción para el segundo equipo. Paso 4: anchos: 20 MHz en 2.4 GHz en ambos equipos; 40 u 80 MHz en 5 GHz. Paso 5: verifica con la app analizadora caminando por la casa: cada equipo debe verse fuerte en su zona y débil en la zona del otro (si se ven muy fuertes entre sí, baja la potencia de transmisión en lugar de subirla; hablaremos de potencia en la Unidad 4). La lección: en 5 GHz el espacio sobra, úsalo; en 2.4 GHz cada canal limpio vale oro, no los desperdicies.

Ejercicio 4: El caso del microondas asesino de Netflix

Escenario: cada noche, entre 7 y 8, tu videollamada se congela y el streaming se corta por 2 o 3 minutos, siempre a la misma hora. La señal del WiFi dice "excelente". Tu laptop está conectada a la red de 2.4 GHz. El router está sobre el refrigerador, al lado del microondas. ¿Qué está pasando y cómo lo arreglas? Dame el plan en orden.

Solución paso a paso. Paso 1: diagnostica por el patrón. Cortes a la misma hora, de 2 a 3 minutos, con señal excelente: no es falta de señal (la señal es excelente) ni es tu proveedor (sería a horas aleatorias o constante). Es interferencia periódica de un aparato que se enciende a esa hora: el microondas calentando la cena. Encaja perfecto: el microondas emite en 2.4 GHz y el router está a su lado. Paso 2: confirma. Una noche, pide que no usen el microondas durante tu llamada, o calienta tu propia comida en ese horario y observa si el corte coincide exactamente con el microondas encendido. Si coincide, caso cerrado. Paso 3: el arreglo inmediato y gratis: cambia tu laptop a la red de 5 GHz (el microondas no interfiere en 5 GHz). Si tu laptop no tiene 5 GHz, ese es un buen motivo para considerar un adaptador USB WiFi moderno, que cuesta poco. Paso 4: el arreglo físico: mueve el router lejos del microondas y del refrigerador (el metal del refri también bloquea señal): a un lugar central y elevado de la casa. Paso 5: el arreglo de configuración: revisa que tu 2.4 GHz esté en 20 MHz y en el mejor canal (1, 6 u 11), para que al menos esa banda rinda lo mejor posible para los aparatos que sí la necesitan. Orden del plan: primero cambia de banda (5 GHz), luego reubica el router, luego optimiza el canal. La lección: cuando el síntoma tiene horario fijo, busca el aparato con horario fijo.

Ejercicio 5: ¿Interferencia o cobertura? Decide con pruebas

Escenario: en tu cuarto el WiFi va lento. Hiciste las dos pruebas del Ejemplo 5 con estos resultados: junto al router, por WiFi, mides 180 Mbps; en tu cuarto mides 15 Mbps. En tu cuarto, la red de 2.4 GHz da 15 Mbps y la de 5 GHz da 12 Mbps. Conectaste la laptop por cable Ethernet al router y mediste 200 Mbps. ¿Dónde está el problema y qué haces? ¿Qué NO debes hacer?

Solución paso a paso. Paso 1: interpreta la prueba A. Junto al router 180 Mbps, en el cuarto 15 Mbps: la velocidad se desploma con la distancia. Eso apunta a problema de cobertura: la señal no llega bien al cuarto (paredes, distancia). Paso 2: interpreta la prueba B. En el cuarto, 2.4 GHz (15 Mbps) rinde parecido a 5 GHz (12 Mbps): si fuera interferencia en 2.4 GHz, la de 5 GHz debería ir notablemente más rápido. Que ambas vayan mal parejo refuerza que el problema es que la señal llega débil al cuarto, no que haya interferencia. Paso 3: interpreta la prueba por cable. 200 Mbps por cable: tu internet y tu router están perfectos; el proveedor no tiene la culpa. Diagnóstico final: problema de cobertura en el cuarto, el WiFi simplemente no

llega con fuerza. Paso 4: qué hacer, en orden de costo: primero reubica el router a un punto más central y elevado; segundo, si no basta, agrega un punto de acceso conectado por cable Ethernet en la planta o zona del cuarto (la mejor solución); tercero, considera una red mesh si no puedes pasar cable. Paso 5: qué NO hacer: no subas la potencia del router al máximo (apenas ayuda y satura más el ambiente), no compres un repetidor barato de los que repiten por WiFi a la mitad de velocidad sin diagnosticar primero, no cambies de proveedor (tu cable da 200 Mbps, el problema no es él) y no cambies de canal esperando un milagro (el canal no arregla la distancia). La lección: diagnosticar antes de gastar; cada síntoma tiene su remedio y los remedios no son intercambiables.

Ejercicio 6: Configura 5 GHz evitando DFS (repaso integrador)

Escenario: tu router ofrece en 5 GHz los canales 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 136, 140, 149, 153, 157, 161 y 165. Vives a 3 km de un aeropuerto. Tu análisis muestra redes vecinas fuertes en 36 y 44, una red media en 149 y nada más. Quieres usar 80 MHz de ancho. ¿Qué canal eliges y por qué? ¿Qué riesgo evitas?

Solución paso a paso. Paso 1: con 80 MHz de ancho necesitas un bloque de cuatro canales de 20 MHz contiguos. Los bloques típicos de 80 MHz son 36-48, 52-64, 100-112, 132-144 y 149-161. Paso 2: descarta bloques con vecinos fuertes. El bloque 36-48 tiene vecinos fuertes en 36 y 44: descartado. El bloque 149-161 tiene un vecino medio en 149: posible pero no ideal. Paso 3: considera los bloques DFS (52-64, 100-112): están vacíos, pero vives a 3 km de un aeropuerto y los radares usan esas frecuencias; si tu router detecta un radar, te saca del canal y tus dispositivos se desconectan. Riesgo real y molesto: descártalos como primera opción. Paso 4: elige el bloque 149-161 (canal central 155 en la configuración de 80 MHz), que no es DFS y solo tiene un vecino medio en el 149. En la práctica, con 80 MHz el vecino del 149 comparte parte de tu bloque, pero es un solo vecino medio contra dos fuertes en la otra opción y contra el riesgo de radar en los DFS. Paso 5: configura el router en el canal correspondiente al bloque 149-161 con 80 MHz, haz prueba de velocidad y monitorea una semana: si el vecino del 149 te molesta mucho, evalúa bajar a 40 MHz en un sub-bloque más limpio (por ejemplo 157-161 en 40 MHz). El riesgo que evitas es doble: la congestión de los canales bajos y las desconexiones por radar de los DFS. La lección integradora: elegir canal es balancear tres cosas a la vez: vecinos, DFS y ancho de canal. Quien domina ese triángulo, domina su WiFi.

Resumen de la unidad

- El WiFi vive en bandas de espectro no licenciado (2.4, 5 y 6 GHz): gratis para todos, pero compartido con todos, incluidos los que no son WiFi.
- Ley fundamental: a menor frecuencia, mayor alcance y mejor penetración de paredes; a mayor frecuencia, mayor velocidad potencial pero menor alcance. Alcance y velocidad siempre están en tensión.
- 2.4 GHz: alcance máximo y compatibilidad universal, pero lenta y saturadísima (microondas, Bluetooth, vecinos). Úsala para aparatos inteligentes y zonas lejanas, siempre en 20 MHz.
- 5 GHz: la banda principal para velocidad (streaming, juegos, videollamadas). Más canales y menos congestión, pero ojo con los canales DFS (52-144): si hay radares cerca, el router te saca del canal sin avisar. Prefiere 36-48 y 149-165.
- 6 GHz: la autopista nueva y vacía (WiFi 6E/7), rapidísima pero de corto alcance y solo para dispositivos nuevos. Verifica compatibilidad y regulación en tu país antes de invertir.
- En 2.4 GHz solo los canales 1, 6 y 11 no se solapan: cualquier otro canal se pisa con dos a la vez. Nunca uses canales intermedios.
- El ancho de canal (20/40/80/160 MHz) multiplica la velocidad pero también ocupa más espectro y recoge más interferencia: 20 MHz en 2.4 GHz siempre; 40 u 80 MHz en 5 GHz; 160 MHz solo si la zona está despejada.
- El ruido de fondo (noise floor) y la relación señal a ruido (SNR) explican por qué una red con "señal excelente" puede ir lenta: lo que importa no es solo qué tan fuerte llega tu router, sino qué tan fuerte llega comparado con el ruido.
- Interferencia típica: el microondas (mata 2.4 GHz por minutos), el Bluetooth (degrada 2.4 GHz), las redes vecinas (te obligan a turnarte en el aire) y los aparatos viejos de 2.4 GHz. La defensa: buena ubicación del router, mejor canal manual, ancho correcto y migrar velocidad a 5 GHz.
- Errores que ya no vas a cometer: dejar el canal en Auto para siempre, activar 40 MHz en 2.4 GHz, usar canales intermedios, poner el router junto al microondas, comprar hardware caro para arreglar un problema de configuración y culpar al proveedor cuando el cable da buena velocidad.
- Tu herramienta más rentable: analizar el espectro (`netsh wlan show networks mode=bssid` o una app analizadora), elegir el canal menos ocupado y medir antes y después. Diez minutos que pueden duplicar tu velocidad real.

- Diagnóstico en 15 minutos: velocidad junto al router vs. lejos (cobertura), 2.4 vs. 5 GHz (interferencia) y prueba por cable (proveedor vs. WiFi). Con esas tres pruebas sabes exactamente dónde está el problema antes de gastar un peso.

UNIDAD 3: Los estándares WiFi 802.11 (Clases 7 a 9)

Si alguna vez has entrado a una tienda de electrónica a comprar un router, ya sabes lo que se siente estar frente a esta unidad del libro en la vida real: cajas que gritan "AC1200", "AX3000", "AXE5400", "BE19000" con letras plateadas, números que prometen velocidades de ciencia ficción y vendedores que aseguran que "este es el bueno porque es WiFi 6". Sales de la tienda con una caja de 2,000 pesos, la conectas en tu casa, y tu internet sigue igual de lento que antes. ¿Te timaron? No necesariamente. Lo que pasó es que nadie te explicó la familia 802.11: el árbol genealógico completo del WiFi, con sus generaciones, sus apellidos de letras, sus promesas teóricas y sus verdades incómodas.

Esta unidad existe para que eso no te vuelva a pasar. Cuando termines estas tres clases, vas a poder leer la caja de cualquier router como quien lee la etiqueta de un producto en el supermercado: sabrás qué significa cada letra, qué número es marketing y qué número es real, qué generación tiene tu celular y si vale la pena gastar en el siguiente salto. Más importante aún: vas a entender por qué tu conexión nunca alcanza la velocidad que dice la caja, y no, no es (solo) culpa de tu proveedor de internet.

En la Clase 7 recorreremos la familia completa desde sus orígenes humildes: 802.11b y 802.11g, que llevaron el WiFi a los hogares a principios de los 2000, pasando por 802.11n, el estándar que nos enseñó la palabra MIMO y que todavía hoy sigue vivo en millones de routers viejos, hasta 802.11ac, el que bautizó la era del gigabit inalámbrico y que probablemente sea el que tienes en casa si tu router tiene unos años. Es la historia de cómo pasamos de 11 megabits por segundo a casi 7 gigabits teóricos en menos de quince años, y de por qué cada salto necesitó cambiar algo fundamental en la forma de usar el aire.

En la Clase 8 nos meteremos con la generación moderna: WiFi 6 (802.11ax), su hermano con esteroides WiFi 6E, y WiFi 7 (802.11be), lo más nuevo que existe al momento de escribir este libro. Aquí aparecen las siglas que suenan a magia negra pero que tienen lógica: OFDMA, que es como pasar de mandar un camión por cliente a mandar un solo camión repartiendo paquetes a varios clientes a la vez; TWT, que deja que tus focos inteligentes duerman en lugar de estar despiertos preguntando "¿ya llegamos?" cada dos segundos; y MLO, la gran apuesta de WiFi 7, que permite que un dispositivo use dos bandas al mismo tiempo como si tuviera dos carriles en lugar de uno. También entenderás por qué la banda de 6 GHz es el terreno virgen que WiFi 6E estrenó y por qué no todos los países la han abierto por completo.

En la Clase 9 llegamos a la parte que más dinero te va a ahorrar: velocidades teóricas contra velocidades reales. Desarmaremos el número de la caja pieza por pieza. Verás qué es MIMO y MU-MIMO con la analogía de los carriles y los camiones, qué significa que una modulación sea 256-QAM o 1024-QAM (pista: es como la diferencia entre hablar deletreando y hablar a velocidad normal), por qué el "ancho de canal" es el factor que más influye y el que menos gente conoce, y haremos cuentas reales: si la caja dice 1200 Mbps, ¿cuánto vas a ver en tu celular de verdad? Cuando termines esta clase, ningún vendedor te va a poder vender humo.

Al terminar la unidad completa serás capaz de: identificar qué estándar usa cada dispositivo que tienes en casa con comandos reales en Windows, Linux, macOS y Android; leer e interpretar una tabla comparativa de estándares sin que te mareen las siglas; calcular una expectativa realista de velocidad antes de comprar cualquier equipo; decidir con criterio si te conviene actualizar tu router o si el cuello de botella está en otro lado; y explicarles a otros (tu familia, tus clientes, tus compañeros) por qué "tener WiFi 6" en el router no sirve de nada si el celular es de 2018.

Una advertencia honesta antes de empezar: esta unidad tiene muchos números y muchas siglas. Es normal que al principio se sientan como sopa de letras. La estrategia es no memorizar, sino entender la lógica: cada generación nueva hace tres cosas, siempre las mismas tres cosas: mete más datos en cada transmisión (mejor modulación), usa más aire a la vez (canales más anchos y más antenas), y organiza mejor el tráfico cuando hay muchos dispositivos (mejores técnicas de acceso al medio). Si entiendes esas tres ideas, cada sigla nueva que aparezca en el futuro será solo un nombre nuevo para una de esas tres cosas. Esa es la brújula de toda la unidad. Guárdala.

También vale la pena que sepas desde ahora el secreto peor guardado de la industria: los nombres "WiFi 4", "WiFi 5", "WiFi 6" y "WiFi 7" no los inventó el IEEE, el organismo técnico que escribe los estándares. Los inventó la WiFi Alliance, la organización comercial, porque se dio cuenta de que nadie en su sano juicio iba a decir "mi router es 802.11ax" en una conversación normal. Es exactamente lo mismo que pasó con los celulares: nadie dice "mi teléfono es 3GPP Release 15", todos dicen "tengo 5G". Los números generacionales son marketing útil, y en este libro los usaremos porque facilitan la vida, pero debajo de cada número bonito hay un documento técnico del IEEE con letras y números que es el que de verdad manda. Aprenderás a moverte entre los dos mundos sin confundirte.

Empecemos por el principio: qué es el IEEE, por qué el WiFi se llama 802.11, y cómo una familia de estándares nacida en 1997 para conectar dos computadoras en una oficina terminó siendo el aire que respira el internet moderno.

Explicación detallada

Clase 7: La familia 802.11, de 802.11b/g/n a 802.11ac

Antes de hablar de letras, hablemos del apellido: IEEE. Son las siglas del Institute of Electrical and Electronics Engineers, el Instituto de Ingenieros Eléctricos y Electrónicos, una organización internacional de ingenieros que escribe las reglas técnicas que permiten que los aparatos de distintas marcas se entiendan entre sí. Piensa en el IEEE como la Real Academia de la lengua, pero para la tecnología: no fabrica nada, pero define cómo deben hablar los aparatos para que un router chino se entienda con un celular coreano y una laptop americana. Sin el IEEE, cada marca inventaría su propio idioma inalámbrico y nada funcionaría con nada.

Dentro del IEEE hay comités numerados por áreas. El comité 802 se encarga de las redes de área local, las LAN. Por eso todo lo que es red local cableada o inalámbrica empieza con 802: 802.3 es Ethernet por cable, 802.15 es Bluetooth, y 802.11 es... el WiFi. El "11" es simplemente el número del grupo de trabajo que se encargó de las redes inalámbricas de área local. Así que cuando dices "802.11", estás diciendo "las reglas del IEEE para redes inalámbricas locales". Y cada letra que sigue (b, g, n, ac, ax, be) es una enmienda, una actualización del documento original. Es como las ediciones de un libro: 802.11 es el título, y la letra es el número de edición.

El 802.11 original se publicó en 1997 y era modestísimo: velocidades de 1 y 2 megabits por segundo, pensado para conectar computadoras en una oficina sin cables. Para que te des una idea, con 2 Mbps descargar una canción de 5 MB tardaba como tres minutos. Pero era revolucionario: por primera vez había una regla común. Dos años después, en 1999, nacieron los gemelos que iniciaron la era comercial del WiFi: 802.11a y 802.11b.

El 802.11b trabajaba en la banda de 2.4 GHz y alcanzaba 11 Mbps teóricos. Fue el que pegó en el mercado porque era barato de fabricar y porque Apple lo metió en sus laptops iBook con el famoso AirPort. De pronto el WiFi dejó de ser cosa de oficinas y llegó a las casas. Su técnica de modulación se llamaba CCK y DSSS, que para efectos prácticos significa que era robusto pero ineficiente: mandaba los datos de forma muy redundante, como si para asegurarte de que te entiendan repitieras cada palabra tres veces. Funciona, pero desperdicia aire.

El 802.11a, su gemelo olvidado, era técnicamente superior: 54 Mbps usando la banda de 5 GHz y una técnica llamada OFDM. Pero llegó en el momento equivocado: los chips para 5 GHz eran caros, y casi nadie lo adoptó en esos años. Su legado, sin embargo, fue enorme, porque OFDM se convirtió en la base de todo lo que vino después. Piensa en OFDM como la diferencia entre mandar cartas una por una en bicicleta (lo que hacía 802.11b) contra mandar

un camión lleno de cartas bien organizadas en compartimentos (OFDM). El camión aprovecha mucho mejor el viaje.

En 2003 llegó 802.11g, el estándar que de verdad masificó el WiFi en los hogares. Tomó lo mejor de los dos mundos: la banda barata de 2.4 GHz del 802.11b y la velocidad de 54 Mbps con OFDM del 802.11a. Además era compatible hacia atrás con 802.11b, así que podías mezclar aparatos viejos y nuevos en la misma red. Si naciste antes del 2000, probablemente el primer router que viste en tu casa era 802.11g, con sus antenitas y su lucecita verde parpadeando. Duró años como el estándar dominante.

Y entonces, en 2009, llegó el que cambió las reglas del juego: 802.11n, conocido hoy como WiFi 4. Fue el primer estándar con MIMO, esas siglas que significan Multiple Input Multiple Output, múltiples entradas y múltiples salidas. Hasta aquí, todos los estándares usaban una sola "conversación" de radio a la vez entre el router y el dispositivo. MIMO introdujo la idea de usar varias antenas para mandar varios flujos de datos simultáneos por el mismo canal, como abrir varios carriles en la misma carretera. Un router 802.11n típico tenía 2 o 3 antenas y podía mandar 2 o 3 flujos espaciales a la vez, multiplicando la velocidad.

El 802.11n también trajo los canales de 40 MHz: si los estándares anteriores usaban canales de 20 MHz de ancho (piensa en el ancho como el número de carriles de la carretera), el n podía juntar dos canales vecinos para formar uno de 40 MHz, duplicando el ancho disponible. Y funcionaba en las dos bandas, 2.4 y 5 GHz. ¿El resultado? Velocidad teórica máxima de 600 Mbps con 4 flujos espaciales y canal de 40 MHz, aunque lo más común en routers caseros era 300 Mbps (2 flujos) o 150 Mbps (1 flujo). De 54 Mbps a 300 Mbps en un salto: por eso el n se quedó tantos años. Todavía hoy, en 2026, hay millones de routers 802.11n funcionando en casas y oficinas pequeñas, y para navegar y ver videos en HD siguen siendo suficientes.

En 2013 llegó 802.11ac, el actual WiFi 5, y con él la era del gigabit inalámbrico. El ac tomó todo lo del n y lo llevó más lejos, pero con una decisión importante: solo trabaja en la banda de 5 GHz. ¿Por qué abandonar la de 2.4? Porque la banda de 2.4 GHz estaba saturadísima: ahí viven los hornos de microondas, los teléfonos inalámbricos viejos, el Bluetooth, las cámaras de seguridad baratas y las redes de todos tus vecinos. Es como una avenida del centro a la hora pico. La banda de 5 GHz, en cambio, era una autopista nueva con mucho espacio libre. El ac apostó todo a la autopista nueva.

Las mejoras del 802.11ac fueron tres. Primera: modulación 256-QAM en lugar de 64-QAM. La modulación QAM es la técnica para empaquetar bits en cada transmisión de radio; 64-QAM mete 6 bits por símbolo y 256-QAM mete 8 bits por símbolo. Es como la diferencia entre escribir con abreviaturas (64-QAM) y escribir con taquigrafía profesional (256-QAM): en el mismo espacio metes más información, pero necesitas "escuchar" con más claridad, o sea,

necesitas buena señal. Por eso el 256-QAM solo funciona bien cuando estás relativamente cerca del router.

Segunda mejora: canales de hasta 80 MHz, y opcionalmente 160 MHz. Si el canal de 20 MHz es una carretera de dos carriles, el de 80 MHz es una autopista de ocho carriles. Más aire, más datos por segundo. Tercera mejora: MU-MIMO en bajada, es decir, Multi-User MIMO. El MIMO del 802.11n era SU-MIMO, de un solo usuario: el router le hablaba a un dispositivo a la vez, aunque fuera rapidísimo turnándose. MU-MIMO permite que el router le hable a varios dispositivos al mismo tiempo usando sus antenas para dirigir flujos separados a cada uno, como un profesor que puede dar instrucciones distintas a cuatro alumnos a la vez sin que se confundan. Ojo: en 802.11ac el MU-MIMO solo funcionaba en bajada (del router hacia los dispositivos), y además casi ningún dispositivo cliente lo implementó bien en esa época, así que en la práctica fue una función más prometedora que real.

La velocidad teórica máxima del 802.11ac es de 6.93 Gbps con 8 flujos espaciales y canal de 160 MHz. En la práctica, los routers caseros típicos eran "AC1200" o "AC1900", números que ya desarmaremos en la Clase 9. Lo importante por ahora: el ac fue el estándar que hizo normal ver velocidades de cientos de megabits por WiFi en una casa, suficiente para 4K, videojuegos y videollamadas simultáneas.

Un detalle que te va a servir toda la vida: la compatibilidad hacia atrás. Todos estos estándares están diseñados para que lo nuevo hable con lo viejo. Un router 802.11ac acepta clientes 802.11n, g e incluso b. Un cliente 802.11n se puede conectar a un router 802.11g. La regla de oro es que la conexión siempre negocia la mejor velocidad que AMBOS extremos soportan: si tu router es ac pero tu laptop es n, la conexión será n. El eslabón más débil manda. Grábate esa frase, porque explica la mitad de los "¿por qué mi internet está lento?" del mundo.

Clase 8: WiFi 6 (802.11ax), WiFi 6E y WiFi 7 (802.11be)

Si la Clase 7 fue la historia de "cada vez más velocidad para un dispositivo", la Clase 8 es la historia de "velocidad decente para muchísimos dispositivos a la vez". El cambio de mentalidad es importante. Para 2019, cuando se publicó el 802.11ax, el problema ya no era que un solo dispositivo necesitara más velocidad: el problema era que en una casa había 20 o 30 dispositivos peleando por el mismo aire (celulares, tablets, teles, focos inteligentes, bocinas, cámaras, el refri que nadie pidió que fuera inteligente). El 802.11ax, bautizado WiFi 6, se diseñó para la era de la multitud.

La mejora estrella de WiFi 6 se llama OFDMA, Orthogonal Frequency Division Multiple Access. Para entenderla, vuelve a la analogía del camión. Con OFDM (la técnica del ac), cada

transmisión era un camión que llevaba paquetes para UN solo cliente: si el cliente solo necesitaba una cajita pequeña, el camión viajaba casi vacío, desperdiciando espacio. OFDMA divide el camión en compartimentos pequeños llamados unidades de recurso, y en un solo viaje reparte paquetes a VARIOS clientes a la vez. Resultado: menos viajes desperdiciados, menos espera, y una latencia mucho menor cuando hay muchos dispositivos. En las pruebas, WiFi 6 no siempre se ve "más rápido" que WiFi 5 para un solo celular descargando un archivo, pero con 30 dispositivos conectados la diferencia es abismal: todo responde más rápido porque nadie se queda esperando su turno.

Segunda mejora grande: 1024-QAM. Si 256-QAM metía 8 bits por símbolo, 1024-QAM mete 10 bits. Es un aumento del 25 por ciento en la cantidad de datos por transmisión. La analogía: si 64-QAM era hablar deletreando, 256-QAM era hablar normal y 1024-QAM es hablar rápido como locutor de radio: transmites más información por segundo, pero necesitas que la señal sea clarísima. En la práctica, el 1024-QAM solo se activa cuando estás cerca del router con buena señal; en cuanto te alejas, el equipo baja automáticamente a modulaciones más robustas. Esto es normal y se llama adaptación de tasa: el WiFi siempre elige la modulación más ambiciosa que la calidad de la señal permite en ese momento.

Tercera mejora: MU-MIMO completo, en bajada Y en subida. El ac solo lo tenía en bajada y casi nadie lo usaba; WiFi 6 lo implementó en ambas direcciones y los fabricantes por fin lo adoptaron en serio. Además, WiFi 6 permite que el MU-MIMO y el OFDMA trabajen juntos: el router puede atender a varios usuarios a la vez Y repartirles el canal en porciones. Es la combinación que hace que un estadio o una oficina llena de gente funcione.

Cuarta mejora: TWT, Target Wake Time, o tiempo de activación programado. Antes de WiFi 6, los dispositivos pequeños (un sensor, un foco inteligente, una pulsera) tenían que estar despertando a cada rato para preguntarle al router "¿tienes algo para mí?", gastando batería en cada pregunta. Con TWT, el router y el dispositivo acuerdan un horario: "duérmete, te despierto cada 10 minutos". Es como la diferencia entre un empleado que está tocando la puerta de su jefe cada cinco minutos y uno que tiene una cita agendada. Para los aparatos de internet de las cosas, esto significa baterías que duran meses o años en lugar de semanas.

Quinta mejora: BSS Coloring, el "color" de la red. En edificios de departamentos, tu router escucha las transmisiones de las redes vecinas y, por cortesía del protocolo, se calla y espera su turno aunque esas transmisiones no le afecten realmente. BSS Coloring le pone una etiqueta de color a cada red, y tu router aprende a distinguir "esta transmisión es de mi red (me callo)" de "esta transmisión es de la red vecina y está lo suficientemente lejos como para que yo pueda hablar al mismo tiempo (hablo)". Es como estar en un restaurante ruidoso y aprender a ignorar las conversaciones de las mesas lejanas para concentrarte en la tuya. En zonas densas, esto recupera una cantidad sorprendente de tiempo de aire.

Las especificaciones de WiFi 6: bandas de 2.4 y 5 GHz (como el n), canales de hasta 160 MHz, hasta 8 flujos espaciales, y velocidad teórica máxima de 9.6 Gbps. Pero ojo con ese número: 9.6 Gbps requiere 8 flujos espaciales y canal de 160 MHz, algo que ningún celular ni laptop normal tiene. Un celular típico WiFi 6 tiene 2 flujos espaciales, así que su máximo teórico real anda por los 1.2 Gbps en 80 MHz o 2.4 Gbps en 160 MHz. Ya haremos estas cuentas con calma en la Clase 9.

Ahora, WiFi 6E. La "E" es de Extended, extendido. Técnicamente es el mismo 802.11ax, con las mismas mejoras, pero con permiso para usar una banda completamente nueva: la de 6 GHz. ¿Por qué importa una banda nueva? Porque las bandas de 2.4 y 5 GHz están llenas de aparatos viejos que obligan a usar mecanismos de compatibilidad que desperdician tiempo. La banda de 6 GHz, en cambio, nació limpia: solo entran dispositivos WiFi 6E o WiFi 7, así que no hay que hablarle despacito a ningún abuelo tecnológico. Además, en 6 GHz hay muchísimo espectro disponible: hasta siete canales de 160 MHz que no se traslapan, contra los dos que apenas caben en 5 GHz. Es como inaugurar una autopista nueva donde solo circulan carros modernos.

El detalle físico que debes conocer: a mayor frecuencia, menor alcance y menor capacidad de atravesar paredes. Los 6 GHz llegan menos lejos que los 5 GHz y mucho menos que los 2.4 GHz. En la práctica, WiFi 6E brilla en el mismo cuarto que el router o en el cuarto de al lado; a dos cuartos de distancia, tu dispositivo probablemente se cambie solo a 5 GHz. No es un defecto, es física. Por eso los routers 6E son tribanda (2.4 + 5 + 6 GHz): el dispositivo usa la mejor banda disponible en cada momento.

Otro detalle práctico: la banda de 6 GHz requiere que los países la autoricen, y no todos lo han hecho igual ni al mismo tiempo. En México y Estados Unidos hay espectro generoso de 6 GHz disponible; en varios países de Europa y América Latina la apertura ha sido parcial o más lenta. Si compras un router 6E, verifica que tus dispositivos lo soporten (muchos celulares de gama media no tienen radio de 6 GHz) y que en tu país la banda esté habilitada. Un router 6E con clientes que no son 6E es simplemente un buen router WiFi 6: la banda de 6 GHz se queda vacía esperando.

Y llegamos a WiFi 7, nombre técnico 802.11be, publicado en 2024. Si WiFi 6 fue la generación de la multitud, WiFi 7 es la generación de la ambición: está pensado para realidad virtual, streaming en 8K, videojuegos en la nube y todas las aplicaciones que necesitan muchísimo ancho de banda con latencia bajísima. Sus tres grandes novedades son:

Primera: canales de 320 MHz. El doble del máximo de WiFi 6. Si el canal de 80 MHz era una autopista de ocho carriles, el de 320 MHz es una autopista de 32 carriles. Eso sí: estos canales gigantes solo caben en la banda de 6 GHz, donde hay espectro de sobra. En 5 GHz no hay espacio para un canal de 320 MHz sin pisar a los vecinos.

Segunda: 4096-QAM, que mete 12 bits por símbolo. Cada salto de QAM da un aumento modesto (de 10 a 12 bits es un 20 por ciento), pero sumado a todo lo demás, contribuye. Como siempre, solo funciona con señal excelente, o sea, cerquita del router.

Tercera, y la más interesante: MLO, Multi-Link Operation, operación multi-enlace. Hasta WiFi 6E, un dispositivo se conectaba al router por UNA banda a la vez: o 2.4, o 5, o 6 GHz. Si la banda se saturaba o tenía interferencia, el dispositivo tenía que cambiarse de banda, con una pequeña interrupción. MLO permite que un dispositivo mantenga conexiones simultáneas en dos o más bandas (por ejemplo, 5 GHz y 6 GHz a la vez) y reparta el tráfico entre ellas dinámicamente. Es como tener dos carriles en dos carreteras distintas e ir cambiando de carril sobre la marcha según cuál esté más libre. Esto no solo suma velocidad: reduce la latencia de forma dramática, porque si un paquete se atora en una banda, el siguiente ya va por la otra. Para videojuegos en la nube y realidad virtual, donde un retardo de milisegundos se siente, MLO es la función más importante de WiFi 7.

WiFi 7 también trae hasta 16 flujos espaciales (el doble que WiFi 6) y una técnica llamada preamble puncturing, que permite usar un canal ancho aunque una porción pequeña esté ocupada por interferencia: en lugar de desechar toda la autopista porque un carril está bloqueado, simplemente no usa ese carril. La velocidad teórica máxima de WiFi 7 es de 46 Gbps, un número tan grande que ningún dispositivo doméstico lo va a alcanzar en años, porque requeriría los 16 flujos y el canal de 320 MHz juntos.

Una pregunta que seguro te estás haciendo: ¿vale la pena comprar WiFi 7 hoy? La respuesta honesta de este libro: depende de tus dispositivos. Si tu celular, tu laptop y tu tele son WiFi 6 o anteriores, un router WiFi 7 te dará una red WiFi 7 vacía esperando clientes que no existen, y funcionará como un buen router WiFi 6. La tecnología más nueva del router no puede darle superpoderes a un cliente viejo. Compra la generación que corresponda a la generación de tus dispositivos, o como máximo una generación arriba si planeas renovarlos pronto. En la sección de práctica haremos este análisis con números.

Tabla comparativa de los estándares

Llegó el momento de poner orden en la sopa de letras. Esta tabla resume la familia completa. No la memorices: úsala como referencia cada vez que veas una caja o una especificación.

Estándar	Nombre comercial	Año	Bandas	Ancho de canal máx.	Modulación máx.	Flujos espaciales máx.	Velocidad teórica máx.
802.11b	(sin nombre)	1999	2.4 GHz	20 MHz	CCK	1	11 Mbps
802.11a	(sin nombre)	1999	5 GHz	20 MHz	64-QAM	1	54 Mbps
802.11g	(sin nombre)	2003	2.4 GHz	20 MHz	64-QAM	1	54 Mbps
802.11n	WiFi 4	2009	2.4 / 5 GHz	40 MHz	64-QAM	4	600 Mbps
802.11ac	WiFi 5	2013	5 GHz	160 MHz	256-QAM	8	6.93 Gbps
802.11ax	WiFi 6	2019	2.4 / 5 GHz	160 MHz	1024-QAM	8	9.6 Gbps
802.11ax	WiFi 6E	2020	2.4 / 5 / 6 GHz	160 MHz	1024-QAM	8	9.6 Gbps
802.11be	WiFi 7	2024	2.4 / 5 / 6 GHz	320 MHz	4096-QAM	16	46 Gbps

Fíjate en tres patrones. Primero: cada generación multiplica la velocidad teórica anterior por un factor de entre 2 y 7. Segundo: el ancho de canal se duplica cada dos generaciones (20, 40, 80/160, 320). Tercero: la modulación sube de a 2 bits por símbolo por generación (6, 8, 10, 12 bits). Si dentro de diez años sale WiFi 8 con 8192-QAM y canales de 640 MHz, no te sorprenderá: es el mismo patrón.

Otro patrón útil: fíjate en qué generaciones comparten bandas. WiFi 4 usa 2.4 y 5; WiFi 5 solo 5; WiFi 6 vuelve a 2.4 y 5; 6E y 7 agregan 6. Esto explica por qué la banda de 2.4 GHz sigue viva después de 25 años: cada generación la sigue soportando para alcance largo y compatibilidad, aunque las velocidades altas siempre vivan en 5 y 6 GHz.

Clase 9: Velocidades teóricas contra velocidades reales

Esta es la clase que te ahorra dinero. Vamos a desarmar el número de la caja y a entender por qué nunca lo alcanzas. Y cuando digo nunca, es nunca: ni con el mejor router, ni pegado a él, ni a las 3 de la mañana. El número de la caja es un máximo teórico calculado en condiciones de laboratorio que tu casa jamás va a reunir. Pero no es una mentira: es un número real bajo supuestos irreales. Entender los supuestos es entender el WiFi.

Empecemos por la fórmula conceptual. La velocidad teórica de una conexión WiFi depende de cuatro factores multiplicados:

1. El ancho del canal (20, 40, 80, 160 o 320 MHz).
2. La modulación (cuántos bits mete cada símbolo: 6, 8, 10 o 12).
3. El número de flujos espaciales (cuántas "conversaciones" simultáneas por antenas MIMO).
4. La eficiencia del protocolo (qué porción del tiempo se usa para datos reales y no para encabezados, turnos y cortesías).

Los fabricantes calculan el número de la caja usando los tres primeros factores en su valor máximo y asumiendo el cuarto factor como si fuera perfecto. En la vida real, el cuarto factor se come entre el 30 y el 50 por ciento, y los tres primeros casi nunca están en su máximo al mismo tiempo en un dispositivo normal. Hagamos las cuentas con un ejemplo concreto.

Toma un router "AX3000", uno de los más vendidos. ¿Qué significa 3000? Es la suma de dos máximos teóricos: 574 Mbps en la banda de 2.4 GHz más 2402 Mbps en la banda de 5 GHz. Ya desde aquí hay una trampa: ningún dispositivo usa las dos bandas a la vez (salvo MLO en WiFi 7), así que ese 3000 es la suma de dos velocidades que jamás se alcanzan juntas. Es como si un carro anunciara "300 km/h" sumando la velocidad máxima en carretera más la velocidad máxima en reversa. Cada banda por separado tiene su propio límite.

Desarmemos los 2402 Mbps de la banda de 5 GHz: vienen de un canal de 160 MHz, modulación 1024-QAM y 2 flujos espaciales. Ahora la realidad de tu celular típico: la mayoría de los celulares solo soportan canales de 80 MHz (no 160), así que el máximo teórico ya baja a 1201 Mbps. Con buena señal, la modulación 1024-QAM sí se activa, así que digamos 1201 Mbps teóricos. Ahora aplica la eficiencia del protocolo: en la práctica, el throughput real (los datos útiles que de verdad cruzan) anda entre el 50 y el 70 por ciento del máximo teórico por todo el tiempo que se pierde en encabezados, confirmaciones de recepción, turnos de espera y demás burocracia del aire. El 60 por ciento de 1201 son unos 720 Mbps. Y eso pegado al router, sin paredes, sin vecinos. A una distancia normal en tu casa, con paredes de por medio, ver 400 a 500 Mbps en un speedtest es un resultado excelente para un equipo AX3000. El número de la caja decía 3000; la realidad dice 500. Y está bien: 500 Mbps son más que suficientes para todo lo doméstico.

La lección no es que te engañen, sino que el número de la caja mide el potencial del ROUTER, no lo que TU DISPOSITIVO va a obtener. Para estimar tu velocidad real necesitas conocer los límites de tu dispositivo: ¿cuántos flujos espaciales tiene? ¿soporta 160 MHz? ¿qué generación de WiFi es? El eslabón más débil manda, ¿recuerdas?

MIMO y MU-MIMO: los carriles y los camiones

Vamos a fijar la analogía que usarás el resto del libro. Imagina que el canal WiFi es una carretera entre el router y tu dispositivo, y que los datos son camiones cargados de paquetes.

Sin MIMO (los estándares viejos b, g, a): la carretera tiene UN carril y circula UN camión a la vez. Cada camión va, entrega, regresa, y luego sale el siguiente. Simple, pero lento.

Con SU-MIMO, Single-User MIMO (el del 802.11n): la carretera se amplía a 2, 3 o 4 carriles, y circulan 2, 3 o 4 camiones EN PARALELO, todos para el MISMO cliente. Si cada camión lleva 150 Mbps de carga, 2 camiones son 300 Mbps y 4 camiones son 600 Mbps. Cada camión es

un "flujo espacial", y cada flujo necesita su propia antena en cada extremo. Por eso los routers no tenían varias antenas: cada antena es un carril. Pero ojo: los camiones solo van a un cliente a la vez. El router atiende a tu celular con sus 2 camiones, termina, y luego atiende a la tablet con sus 2 camiones. Rapidísimo turnándose, pero turnándose al fin.

Con MU-MIMO, Multi-User MIMO (bien implementado desde WiFi 6): el router puede mandar camiones a VARIOS clientes SIMULTÁNEAMENTE, cada uno por sus carriles. Tu celular recibe sus 2 camiones mientras la tablet recibe los suyos y la tele los suyos, todo al mismo tiempo. Aquí hay un detalle que casi nadie explica: el número total de camiones (flujos espaciales) del router se REPARTE entre los clientes. Si el router tiene 8 flujos y atiende a 4 dispositivos, a cada uno le pueden tocar 2. MU-MIMO no multiplica la velocidad de un solo dispositivo: reparte mejor la capacidad total entre varios. Por eso MU-MIMO se nota en casas con muchos dispositivos, no cuando solo hay uno conectado.

Y aquí va el error común número uno de esta unidad: creer que más antenas en el router automáticamente te dan más velocidad. Las antenas del router son los carriles disponibles, pero tu dispositivo también necesita sus propios carriles (sus propias antenas y flujos). Un router de 8 flujos con un celular de 2 flujos establece una conexión de 2 flujos. Los otros 6 carriles se quedan esperando a otros clientes. Las antenas de más sirven para atender a más dispositivos a la vez, no para acelerar a uno solo. Cuando veas un router con 8 antenas como araña, piensa "atiende bien a muchos", no "me va a dar 8 veces más velocidad".

Modulación QAM: hablar deletreando contra hablar de corrido

La modulación es la técnica para convertir bits en ondas de radio. QAM significa Quadrature Amplitude Modulation, modulación de amplitud en cuadratura, pero lo único que necesitas recordar es el número que la acompaña y esta tabla:

- 64-QAM: 6 bits por símbolo (WiFi 4 y anteriores en su máximo).
- 256-QAM: 8 bits por símbolo (WiFi 5).
- 1024-QAM: 10 bits por símbolo (WiFi 6 y 6E).
- 4096-QAM: 12 bits por símbolo (WiFi 7).

Piensa en cada "símbolo" como una sílaba que el router le grita al dispositivo por el aire. Con 64-QAM, cada sílaba lleva 6 bits de información: es como hablar deletreando, lento pero clarísimo, se entiende hasta con ruido. Con 4096-QAM, cada sílaba lleva 12 bits: es como hablar rapidísimo, transmites el doble de información por segundo, pero si hay tantito ruido, se pierde la sílaba completa y hay que repetirla.

Por eso el WiFi ajusta la modulación automáticamente según la señal: cerquita del router usa la modulación más ambiciosa (más bits por sílaba), y conforme te alejas o hay interferencia, baja a modulaciones más robustas (menos bits, pero más resistentes). Este ajuste se llama adaptación de tasa y ocurre cientos de veces por segundo sin que te des cuenta. Cuando ves que la "velocidad de enlace" de tu conexión sube y baja al moverte por la casa, estás viendo la adaptación de tasa en acción.

La consecuencia práctica: los números máximos de QAM de cada generación (1024, 4096) solo se alcanzan con señal excelente. A distancia normal, tu equipo probablemente esté usando 256-QAM o 64-QAM aunque tu router y tu celular sean WiFi 6. Y está bien: es el sistema funcionando como debe, eligiendo confiabilidad sobre ambición cuando el aire está difícil.

Beamforming: el router que apunta

Mención especial para el beamforming, que el 802.11ac popularizó y que todas las generaciones siguientes conservan. Sin beamforming, el router transmite su señal en todas direcciones por igual, como un foco que ilumina todo el cuarto. Con beamforming, el router usa sus múltiples antenas para concentrar la señal en la dirección donde está tu dispositivo, como una lámpara con reflector que apunta el haz de luz. No es magia: las antenas emiten la misma onda con pequeños desfases calculados para que las ondas se refuercen en la dirección del cliente y se cancelen en otras direcciones.

El efecto práctico es una señal más fuerte y estable a mayor distancia, lo que permite mantener modulaciones altas (más velocidad) donde antes habría que bajarlas. Funciona mejor cuando el router sabe dónde estás, y para eso el cliente tiene que cooperar mandando información de vuelta (beamforming explícito). Casi todos los dispositivos modernos lo soportan. No es algo que configures: viene activado por defecto y trabaja solo. Solo recuerda que existe cuando alguien te pregunte por qué el WiFi 5 se siente más estable que el n a la misma distancia: parte de la respuesta es el beamforming.

Por qué nunca alcanzas el número de la caja: la lista completa

Juntemos todas las razones en una sola lista, porque esta es la página que vas a querer releer antes de comprar un router:

1. El número de la caja suma las bandas. Un "AX3000" suma 2.4 GHz + 5 GHz, pero tu dispositivo usa una banda a la vez. Divide el número entre las bandas para tener expectativas sanas.

2. El número de la caja asume el máximo de flujos espaciales del router. Tu celular probablemente tiene 2 flujos; el router anuncia 4 u 8. La conexión usa el mínimo de los dos.
3. El número de la caja asume el canal más ancho posible (160 o 320 MHz). Muchos clientes solo soportan 80 MHz, y además los canales anchos son más vulnerables a la interferencia: si un vecino ocupa parte de tu canal de 160 MHz, tu equipo baja a 80 MHz automáticamente.
4. El número de la caja asume la modulación máxima (1024-QAM o más). Solo se logra con señal excelente, o sea, a pocos metros del router sin obstáculos.
5. El protocolo desperdicia tiempo. Entre encabezados, confirmaciones, turnos de espera para no chocar con vecinos y pausas de cortesía, solo el 50 a 70 por ciento del tiempo de aire lleva datos útiles. Esto es física del protocolo, no defecto de tu equipo.
6. El ambiente manda. Paredes, distancia, microondas, Bluetooth, las 15 redes de tus vecinos: todo resta. El 5 GHz y el 6 GHz son rápidos pero se frenan con cada pared.
7. Tu internet también es un límite. Si tu proveedor te da 200 Mbps, ningún WiFi del mundo te va a dar 500 en un speedtest hacia internet. El WiFi solo puede repartir lo que le llega por el cable. Mucha gente cambia de router cuando debería cambiar de plan de internet, o al revés.

Regla práctica de este libro: para estimar tu velocidad realista con un equipo moderno, toma la velocidad de enlace que reporta tu dispositivo (te enseñamos a verla en los ejemplos), multiplícala por 0.6, y ese es tu throughput real en condiciones buenas. Si la velocidad de enlace dice 866 Mbps, espera unos 500 Mbps reales. Si dice 1200 Mbps, espera unos 700. Funciona sorprendentemente bien.

Errores comunes que debes evitar

Error 1: "Compré router WiFi 6 y mi internet sigue igual". El WiFi 6 no aumenta la velocidad que te da tu proveedor. Si tu plan es de 100 Mbps, con WiFi 5 ya los exprimías todos. El WiFi 6 mejora la experiencia con MUCHOS dispositivos y reduce la latencia, pero no crea megabits de la nada. Antes de actualizar el router, mide tu velocidad con cable: si el cable ya te da lo contratado, el router no era el problema.

Error 2: "Mi router es WiFi 6 pero mi celular es de 2019". La conexión negocia lo mejor que AMBOS soportan. Router AX con cliente AC = conexión AC. Para aprovechar WiFi 6 necesitas clientes WiFi 6. Actualizar solo un extremo es como comprar llantas de carreras para un carro viejo: algo mejora, pero no lo que esperabas.

Error 3: "El AX5400 es mejor que el AX3000 porque el número es más grande". No necesariamente para ti. Esos números son sumas de máximos por banda con distintos anchos de canal. Un AX3000 con canal de 160 MHz puede darle MÁS velocidad real a tu celular que un AX5400 sin 160 MHz, dependiendo de las configuraciones. Lee las especificaciones finas (flujos, ancho de canal, bandas), no solo el número grande de la caja.

Error 4: "Pongo el router en 160 MHz para que vaya más rápido". Los canales de 160 MHz son más rápidos pero más frágiles: ocupan tanto espectro que es fácil que choquen con redes vecinas, y cuando hay interferencia el equipo baja a 80 MHz de todos modos, a veces con cortes. En departamentos con muchos vecinos, 80 MHz suele dar mejor experiencia estable que 160 MHz inestables. Más ancho no siempre es mejor; es mejor cuando el aire está limpio.

Error 5: "La banda de 6 GHz me va a llegar a toda la casa". No. A mayor frecuencia, menor alcance. Los 6 GHz son para el mismo cuarto o el cuarto contiguo. Si tu casa es grande, la banda de 6 GHz será un lujo de corta distancia, no la solución para el cuarto del fondo. Para alcance, 2.4 GHz sigue siendo el rey.

Buenas prácticas al elegir y configurar

Primera: compra la generación de tus clientes. Haz inventario de tus dispositivos (en los ejemplos aprenderás a ver qué WiFi soporta cada uno) y compra un router de esa generación o una arriba. Comprar dos generaciones arriba es pagar por capacidad que no vas a usar en años.

Segunda: prioriza el ancho de canal y los flujos sobre el número de la caja. Entre dos routers del mismo precio, el que tenga 160 MHz y 4 flujos útiles te sirve más que el que tenga un número de caja más grande logrado con trucos de suma.

Tercera: ubica bien el router. En alto, al centro de la casa, lejos de microondas y espejos grandes, sin encerrarlo en un mueble. Ningún estándar arregla una mala ubicación. El beamforming ayuda, pero no hace milagros a través de tres paredes de concreto.

Cuarta: separa las bandas solo si sabes lo que haces. Los routers modernos unen 2.4 y 5 GHz bajo un solo nombre (band steering) y el dispositivo elige. Separarlas te da control, pero también te da la responsabilidad de conectar cada aparato a la banda correcta. Para principiantes, déjalo unido.

Quinta: actualiza el firmware del router. Las mejoras de estabilidad, los parches de seguridad y a veces hasta mejoras de velocidad llegan por firmware. Un router de 2021 con firmware de 2021 es un router viejo; con firmware de 2026 es un router vigente.

Sexta: mide antes de gastar. Haz un speedtest por cable para saber lo que te da tu proveedor, y luego por WiFi pegado al router y en tu cuarto. Si el WiFi pegado al router ya te da casi lo del cable, tu red local está bien y el límite es tu plan de internet. Si el WiFi pegado al router da mucho menos que el cable, ahí sí hay un problema de WiFi que vale la pena investigar (o un router que sí conviene cambiar).

Ejemplos paso a paso

La teoría ya quedó. Ahora vas a ponerle las manos encima a tu propia conexión y a leer qué estándar está usando, con comandos reales en cada sistema operativo. Haz los ejemplos en tu computadora o tu celular mientras lees: no hay mejor forma de fijar estos conceptos que viendo tus propios números.

Ejemplo 1: Ver el estándar de tu conexión en Windows

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

```
netsh wlan show interfaces
```

Vas a ver una salida parecida a esta (los valores cambian según tu equipo):

```
Nombre                : Wi-Fi
Descripción           : Intel(R) Wi-Fi 6 AX201 160MHz
GUID                  : 3f2a1b4c-9d8e-4f7a-b123-456789abcdef
Estado                : conectado
SSID                  : MiCasa_5G
BSSID                 : a4:2b:8c:1d:3e:5f
Tipo de red           : Infraestructura
Tipo de radio         : 802.11ax
Autenticación         : WPA2-Personal
Cifrado               : CCMP
Canal                 : 44
Velocidad de recepción : 1201 Mbps
Velocidad de transmisión : 1201 Mbps
Señal                 : 82%
```

Línea por línea:

- Nombre y Descripción: el nombre de la interfaz y el modelo de tu tarjeta WiFi. Aquí dice "Wi-Fi 6 AX201": la tarjeta es WiFi 6 (802.11ax) y soporta canales de 160 MHz. Este es tu CLIENTE: ya sabes que tu laptop puede negociar hasta WiFi 6.

- Estado: conectado. Si dijera desconectado, lo demás no aplica.
- SSID: el nombre de la red a la que estás conectado.
- BSSID: la dirección MAC del punto de acceso (el radio específico del router al que te conectaste).
- Tipo de red: Infraestructura significa que te conectaste a un router o punto de acceso (lo normal). "Ad hoc" sería conexión directa entre dispositivos.
- Tipo de radio: 802.11ax. ESTA es la línea de oro: te dice el estándar que se negoció en esta conexión. Si tu tarjeta es ax y aquí dice 802.11n, significa que el ROUTER es el que limita (es n o está configurado así).
- Autenticación y Cifrado: WPA2-Personal con CCMP (AES). Es la seguridad de la conexión; la veremos a fondo en la unidad de seguridad, pero por ahora verifica que no diga WEP ni "Abierta".
- Canal: 44. Los canales del 36 al 64 viven en la banda de 5 GHz (los de 2.4 GHz son del 1 al 13 o 14). Con solo ver el canal ya sabes en qué banda estás.
- Velocidad de recepción y transmisión: 1201 Mbps. Esta es la VELOCIDAD DE ENLACE, el máximo teórico de ESTA conexión negociada, no tu velocidad real. Con 1201 Mbps de enlace, tu throughput real estará por los 600 a 700 Mbps en el mejor caso (recuerda la regla del 60 por ciento).
- Señal: 82 por ciento. Buena señal. Arriba del 70 por ciento puedes esperar modulaciones altas; abajo del 50 por ciento, la adaptación de tasa ya bajó la velocidad.

¿Cómo sacas 1201 de la teoría? 802.11ax, canal de 80 MHz, 2 flujos espaciales, 1024-QAM: la tabla del estándar da 1201 Mbps. Si tu tarjeta soporta 160 MHz pero el router no lo tiene activado (o hay interferencia), negocian 80 MHz y obtienes 1201 en lugar de 2402. Todo cuadra.

Para ver además las redes disponibles y sus datos, usa:

```
netsh wlan show networks mode=bssid
```

Te muestra cada red con su SSID, tipo de radio (el estándar que anuncia el router), canal y señal. Es la forma rápida de espiar qué estándares usan tus vecinos.

Ejemplo 2: Ver el estándar de tu conexión en Linux

Abre una terminal y ejecuta (cambia wlan0 por el nombre de tu interfaz si es distinto; averígualo con `iw dev``):

```
iw dev wlan0 link
```

Salida típica:

```
Connected to a4:2b:8c:1d:3e:5f (on wlan0)
    SSID: MiCasa_5G
    freq: 5220
    RX: 1200.9 MBit/s
    TX: 1200.9 MBit/s
    signal: -58 dBm
    tx bitrate: 1200.9 MBit/s
```

Línea por línea:

- Connected to: la MAC del punto de acceso. Estás conectado.
- SSID: el nombre de la red.
- freq: 5220. La frecuencia en MHz. 5220 MHz = 5.22 GHz, o sea, banda de 5 GHz (canal 44). Si vieras 2412, sería 2.4 GHz (canal 1). Si vieras 5955 o similar, sería 6 GHz.
- RX y TX: velocidades de enlace de bajada y subida en Mbps. Aquí ~1201 Mbps, igual que en el ejemplo de Windows: conexión WiFi 6, 80 MHz, 2 flujos.
- signal: -58 dBm. La señal en decibelios-milivatio, donde MENOS negativo es MEJOR. La escala práctica: -30 a -50 dBm es excelente (pegado al router), -50 a -65 es bueno, -65 a -75 es regular, y abajo de -75 es malo. Con -58 dBm tienes buena señal, consistente con la modulación alta que da 1201 Mbps.

Este comando no te dice el estándar con letras (no dice "802.11ax"), pero la velocidad de enlace lo delata: 1201 Mbps con esas características solo existe en 802.11ax. Para ver qué estándares SOPORTA tu tarjeta, usa:

```
iw list
```

En la salida busca las secciones "Bands" y "Capabilities": verás las frecuencias soportadas, los anchos de canal (HT20/HT40 para n, VHT80/VHT160 para ac, HE para ax) y el número de flujos. Si ves "HE" (High Efficiency), tu tarjeta es WiFi 6. Si ves "EHT" (Extremely High Throughput), es WiFi 7.

Ejemplo 3: Ver el estándar de tu conexión en macOS

En Mac no necesitas la terminal para lo básico: mantén presionada la tecla Opción (Alt) y haz clic en el icono de WiFi en la barra de menú. Se abre un panel con datos técnicos de tu conexión actual:

```
MiCasa_5G
Dirección IP: 192.168.1.25
Seguridad: WPA2 Personal
BSSID: a4:2b:8c:1d:3e:5f
Canal: 44 (5 GHz, 80 MHz)
RSSI: -58 dBm
Ruido: -92 dBm
Velocidad de transmisión: 1200 Mbps
Modo PHY: 802.11ax
MCS: 11
NSS: 2
```

Línea por línea:

- Canal: 44 (5 GHz, 80 MHz). macOS te dice directamente la banda Y el ancho de canal. Aquí confirmas: 5 GHz, 80 MHz.
- RSSI: -58 dBm. La intensidad de la señal recibida, misma escala que en Linux.
- Ruido: -92 dBm. El nivel de ruido de fondo. Lo que importa es la diferencia entre RSSI y ruido (la relación señal a ruido): $-58 \text{ menos } -92 = 34 \text{ dB}$ de margen. Arriba de 25 dB es bueno; abajo de 20 dB, la conexión sufre.
- Velocidad de transmisión: 1200 Mbps. La velocidad de enlace, igual que en Windows.
- Modo PHY: 802.11ax. El estándar negociado, dicho sin rodeos.
- MCS: 11. El índice del esquema de modulación y codificación. En 802.11ax, MCS 11 significa 1024-QAM, la modulación máxima. Si vieras MCS 7, sería 64-QAM; MCS 9, 256-QAM. Cuando te alejas del router, verás este número bajar: es la adaptación de tasa mostrada en vivo.
- NSS: 2. Number of Spatial Streams, el número de flujos espaciales: 2. Aquí están tus 2 carriles.

Con estos tres datos (Modo PHY, MCS y NSS) puedes reconstruir toda la negociación: 802.11ax, 1024-QAM, 2 flujos, 80 MHz = 1201 Mbps. Ya no necesitas que nadie te explique tu conexión: la lees tú.

Ejemplo 4: Ver el estándar de tu conexión en Android

En Android los pasos varían un poco según la marca, pero la ruta general es: Ajustes > Red e Internet > WiFi, toca la red a la que estás conectado (o el icono de engrane junto a su nombre). Verás una pantalla con detalles parecidos a estos:

```
MiCasa_5G
Intensidad de señal: Excelente
Velocidad de enlace: 1201 Mbps
Frecuencia: 5 GHz
Seguridad: WPA2-Personal
Dirección IP: 192.168.1.30
```

Android te da menos detalle técnico que los sistemas de escritorio: no siempre muestra el estándar con letras ni el ancho de canal. Pero con dos datos te las arreglas: la frecuencia (5 GHz) y la velocidad de enlace (1201 Mbps). Esa combinación, como ya sabes, corresponde a 802.11ax con 80 MHz y 2 flujos. Si la velocidad de enlace dijera 866 Mbps en 5 GHz, sería 802.11ac (80 MHz, 2 flujos, 256-QAM). Si dijera 150 Mbps en 2.4 GHz, sería 802.11n (40 MHz, 1 flujo) o 802.11g con buena suerte. La velocidad de enlace es tu huella digital del estándar.

En algunos teléfonos (Samsung, Xiaomi, Pixel con opciones de desarrollador), puedes ver más detalle activando las opciones de desarrollador y buscando la información de WiFi, donde a veces aparece el estándar. Y hay apps gratuitas de análisis WiFi que muestran el estándar anunciado por cada red cercana, útil para el ejercicio de espiar a tus vecinos que viene en la práctica.

Ejemplo 5: Interpretar la velocidad de enlace y estimar la real

Ya sabes leer la velocidad de enlace en todos los sistemas. Ahora conviértela en una expectativa realista con la regla del 60 por ciento, paso a paso:

1. Anota la velocidad de enlace. Ejemplo: 866 Mbps (una conexión 802.11ac típica: 80 MHz, 2 flujos, 256-QAM).
2. Multiplica por 0.6 para estimar el throughput máximo en condiciones buenas: $866 \times 0.6 = 520$ Mbps. Ese es tu techo realista pegado al router.
3. Ajusta por distancia y obstáculos: a un cuarto de distancia con una pared, resta un 20 a 30 por ciento más: unos 360 a 400 Mbps esperados.

4. Compara con tu plan de internet: si tu proveedor te da 200 Mbps, tu WiFi (400+) no es el límite; el límite es el plan. Si tu proveedor te da 500 Mbps y tu WiFi te da 360 en tu cuarto, el WiFi SÍ es el cuello de botella en ese punto de la casa.
5. Verifica con un speedtest: haz la prueba pegado al router y en tu cuarto. Si los números se parecen a tu estimación, tu red está sana. Si están muy por debajo, hay un problema que investigar (interferencia, mala ubicación, firmware viejo, o un vecino en tu mismo canal).

Haz este ejercicio una vez con tus números reales y jamás volverás a discutir con un vendedor sobre el número de la caja: tendrás tus propios números, medidos por ti.

Ejemplo 6: Identificar el estándar que anuncia tu router

Hasta ahora hemos visto el estándar NEGOCIADO en tus dispositivos. Pero también puedes ver lo que tu ROUTER ofrece, que a veces es más de lo que tus clientes aprovechan. Entra a la página de administración de tu router (normalmente <http://192.168.1.1> o <http://192.168.0.1> en tu navegador; el usuario y contraseña suelen venir en una etiqueta debajo del router) y busca la sección de configuración inalámbrica. Verás opciones como:

```
Modo inalámbrico: 802.11b/g/n/ax mixto
Ancho de canal 2.4 GHz: 20/40 MHz
Ancho de canal 5 GHz: 20/40/80/160 MHz
```

El "modo mixto" significa que el router acepta clientes de todas esas generaciones: es la compatibilidad hacia atrás en acción. Si cambias el modo a "solo ax", los clientes viejos (n, g) ya no podrán conectarse: más eficiencia para los nuevos, pero los abuelos se quedan fuera. En una casa normal, deja el modo mixto.

El ancho de canal es donde puedes experimentar: si vives en casa sola sin vecinos cercanos, prueba 160 MHz en 5 GHz y mide si mejora. Si vives en departamento con 20 redes vecinas, quédate en 80 MHz para estabilidad. Cambia, mide con speedtest, y quédate con lo que dé mejor resultado REAL, no con lo que suene más grande. Esa es la mentalidad de esta unidad: medir, no suponer.

Práctica

Ejercicio 1: Identifica el estándar de cada dispositivo de tu casa

Toma tu celular, tu computadora y, si puedes, tu televisor o tablet. En cada uno, averigua con qué estándar WiFi está conectado usando los comandos de los ejemplos (netsh en Windows, iw en Linux, opción-clic en macOS, ajustes de red en Android). Anota para cada dispositivo: estándar negociado, banda, velocidad de enlace y señal. Luego responde: ¿cuál es el dispositivo más viejo de tu casa? ¿cuál negocia la velocidad de enlace más alta?

Solución paso a paso:

1. En tu computadora Windows ejecutas `netsh wlan show interfaces` y lees la línea "Tipo de radio". Supongamos que dice 802.11ax, velocidad de enlace 1201 Mbps, canal 44 (5 GHz), señal 75 por ciento.
2. En tu celular Android vas a Ajustes > WiFi > tu red y lees: frecuencia 5 GHz, velocidad de enlace 866 Mbps, señal excelente.
3. Interpretas: la computadora negocia WiFi 6 (ax) a 1201 Mbps: es un cliente moderno con 2 flujos y 80 MHz. El celular negocia 866 Mbps en 5 GHz: esa huella digital corresponde a WiFi 5 (ac) con 80 MHz y 2 flujos. Tu celular es de una generación anterior a tu laptop.
4. El dispositivo más viejo es el celular (WiFi 5). La velocidad de enlace más alta la negocia la computadora (1201 Mbps).
5. Conclusión útil: si tu router es WiFi 6, la computadora lo aprovecha y el celular no. Si algún día cambias el celular por uno WiFi 6, su velocidad de enlace subiría a ~1201 Mbps sin tocar el router. Este inventario es exactamente el que necesitas antes de decidir si actualizas equipos: ahora sabes DÓNDE está el eslabón débil.

Ejercicio 2: ¿Vale la pena cambiar tu router?

Tu situación: tienes un router 802.11n de doble banda (2.4 y 5 GHz) de hace 10 años. Tu plan de internet es de 200 Mbps. Tus dispositivos: una laptop WiFi 6, un celular WiFi 5 y una tele WiFi 4. Por cable, el speedtest te da 195 Mbps. Por WiFi pegado al router te da 90 Mbps, y en tu cuarto te da 45 Mbps. Un router WiFi 6 (AX3000) cuesta 1,500 pesos. ¿Conviene comprarlo? Justifica con números.

Solución paso a paso:

1. Primero descarta al proveedor: por cable llegan 195 Mbps de 200 contratados. El internet está bien; el problema es el WiFi.
2. Analiza el límite actual: el router es 802.11n. En 5 GHz con 40 MHz y 2 flujos, el máximo teórico es 300 Mbps, y el throughput realista (60 por ciento) es ~180 Mbps en el mejor

caso. Pero estás midiendo 90 Mbps pegado al router: muy por debajo, probablemente por interferencia, firmware viejo o saturación de la banda. En tu cuarto, 45 Mbps confirman que el router ya no da más.

3. Calcula lo que daría el router nuevo: un AX3000 con tus clientes daría, para la laptop WiFi 6, unos 1201 Mbps de enlace (80 MHz, 2 flujos) = ~700 Mbps reales pegado al router. Para el celular WiFi 5, ~866 Mbps de enlace = ~500 Mbps reales. Ambos muy por encima de tus 200 Mbps contratados, así que el WiFi dejaría de ser el cuello de botella en toda la casa.
4. Verifica la regla del eslabón más débil: la tele es WiFi 4 (n) y seguirá negociando n con el router nuevo, pero como el router nuevo tiene mejor radio, mejor beamforming y menos saturación, hasta la tele mejoraría algo. Y cuando renueves tus dispositivos, ya tienes la infraestructura.
5. Decisión: Sí conviene. El router actual es el cuello de botella (90 Mbps medidos contra 195 disponibles), el nuevo lo elimina por completo para tus tres dispositivos, y el precio es razonable para el salto generacional (de WiFi 4 a WiFi 6). Nota lo que NO harías: comprar un router WiFi 7 de 5,000 pesos, porque ninguno de tus dispositivos es WiFi 7 y estarías pagando capacidad vacía.

Ejercicio 3: Calcula la velocidad real esperada de un router "AX5400"

Ves una oferta: router AX5400. Sus especificaciones finas dicen: 2.4 GHz hasta 574 Mbps (40 MHz, 2 flujos, 1024-QAM) y 5 GHz hasta 4804 Mbps (160 MHz, 4 flujos, 1024-QAM). Tu celular es WiFi 6 con 2 flujos y soporte de 80 MHz (no 160). Estás a una distancia media del router con una pared de por medio. ¿Qué velocidad realista esperas en un speedtest? Muestra cada descuento que aplicas.

Solución paso a paso:

1. Descarta la suma: $5400 = 574 + 4804$. Tu celular usa una banda a la vez, así que el techo es 4804 Mbps (banda de 5 GHz), no 5400.
2. Ajusta los flujos: el router ofrece 4 flujos, tu celular tiene 2. La conexión negocia 2 flujos. En 160 MHz y 2 flujos, el máximo sería 2402 Mbps. Pero...
3. Ajusta el ancho de canal: tu celular solo soporta 80 MHz, no 160. Así que el máximo teórico de TU conexión es 1201 Mbps (ax, 80 MHz, 2 flujos, 1024-QAM).
4. Aplica la eficiencia del protocolo: $1201 \times 0.6 = \sim 720$ Mbps en condiciones ideales pegado al router.

5. Ajusta por distancia y pared: a distancia media con una pared, descuenta un 25 por ciento adicional: $720 \times 0.75 = \sim 540$ Mbps.
6. Considera la modulación: con una pared de por medio, es posible que la adaptación de tasa baje de 1024-QAM (MCS 11) a 256-QAM (MCS 9), lo que recorta otro ~20 por ciento: unos 430 Mbps.
7. Resultado: espera entre 400 y 550 Mbps reales en tu cuarto. Si tu plan de internet es de 500 Mbps o menos, este router te sobra; si es de 1 Gbps, en tu cuarto no lo vas a exprimir con ese celular (pegado al router sí, ~700 Mbps). El número de la caja decía 5400; tu realidad dice ~500. Y con 500 Mbps haces TODO lo doméstico sin despeinarte.

Ejercicio 4: ¿80 MHz o 160 MHz en tu departamento?

Vives en un departamento con 18 redes WiFi vecinas visibles. Tu router WiFi 6 permite elegir el ancho de canal en 5 GHz: 80 MHz o 160 MHz. Tu laptop soporta 160 MHz. ¿Qué eliges y cómo lo verificas?

Solución paso a paso:

1. Teoría: 160 MHz duplica el máximo teórico (2402 vs 1201 Mbps con 2 flujos). Suena a que 160 es mejor.
2. Realidad del ambiente: con 18 redes vecinas, el espectro de 5 GHz está peleado. Un canal de 160 MHz ocupa la mitad de la banda disponible; es casi seguro que se traslape con redes vecinas, lo que obliga a tu router a mecanismos de cortesía que desperdician tiempo, o a que tu equipo baje a 80 MHz solo cuando detecta interferencia, con microcortes.
3. Decisión inicial: elige 80 MHz. Es más angosto pero más estable: cabe en los huecos libres entre redes vecinas y mantiene la conexión sólida.
4. Verificación empírica (la parte importante): configura 80 MHz, haz 3 speedtests en distintos momentos del día y anota el promedio y la estabilidad (¿varía mucho entre pruebas?). Luego cambia a 160 MHz, repite los 3 speedtests en horarios similares y compara. Quédate con el que dé mejor promedio Y menor variación.
5. Conclusión esperada: en un departamento saturado, 80 MHz casi siempre gana en estabilidad y a veces hasta en promedio, porque 160 MHz pasa más tiempo negociando interferencia que transmitiendo. En una casa sola sin vecinos, el resultado sería el opuesto. La moraleja: el ancho de canal correcto depende de TU aire, no de la teoría. Medir le gana a suponer, siempre.

Ejercicio 5: ¿WiFi 6, 6E o 7? Decisión de compra con inventario

Tienes 2,500 pesos de presupuesto. Tus dispositivos: celular gama media de 2023 (WiFi 6, sin 6 GHz), laptop de 2022 (WiFi 6E), tele de 2021 (WiFi 5), y 12 dispositivos inteligentes (focos, bocinas, cámaras: todos WiFi 4 o 5 en 2.4 GHz). Opciones: router WiFi 6 de 1,600 pesos, router WiFi 6E de 2,400 pesos, o router WiFi 7 de 4,500 pesos (fuera de presupuesto, pero lo consideras). ¿Cuál compras?

Solución paso a paso:

1. Haz el inventario por generación: ningún dispositivo es WiFi 7. Solo la laptop es 6E (tiene radio de 6 GHz). El celular, que es tu dispositivo más usado, es WiFi 6 sin 6 GHz.
2. Evalúa WiFi 7: descartado por presupuesto y por falta de clientes. Sería pagar 4,500 por una red del futuro vacía.
3. Evalúa WiFi 6E: la banda de 6 GHz solo la usaría tu laptop. El celular, la tele y los 12 dispositivos inteligentes seguirían en 2.4 y 5 GHz como con un router WiFi 6 normal. Pagarías 800 pesos extra (2,400 vs 1,600) por beneficiar a UN dispositivo, y solo cuando esté cerca del router (los 6 GHz no atraviesan bien las paredes).
4. Evalúa WiFi 6: cubre a todos tus dispositivos actuales en su mejor generación posible (el celular y los aparatos negocia rían lo máximo que soportan), te sobran 900 pesos del presupuesto, y cuando en unos años cambies el celular por uno 6E o WiFi 7, podrás reevaluar.
5. Decisión: compra el WiFi 6 de 1,600 pesos. Es la generación de tus clientes, que es la regla de oro de esta unidad. Los 800 pesos de diferencia con el 6E no se justifican para un solo dispositivo beneficiado. Guarda el resto: la tecnología baja de precio cada año, y cuando TUS dispositivos sean 6E o 7, los routers también serán más baratos.

Ejercicio 6: Diagnostica un caso de "mi WiFi está lento"

Un familiar te dice: "mi WiFi está lentísimo, quiero comprar otro router". Vas a su casa y mides: por cable al router, el speedtest da 100 Mbps (su plan es de 100). Por WiFi pegado al router da 95 Mbps. En su cuarto da 25 Mbps. Su router es WiFi 5 (AC1200) y su celular es WiFi 5. ¿Qué le recomiendas? ¿Comprar un router nuevo?

Solución paso a paso:

1. Por cable llegan 100 de 100: el proveedor cumple. Pegado al router el WiFi da 95: el router FUNCIONA BIEN, exprime casi todo el plan. El router no es el problema.

2. En el cuarto da 25 Mbps: el problema es de ALCANCE, no de generación. La señal de 5 GHz se degrada con la distancia y las paredes hasta ese cuarto.
3. Verifica la hipótesis: en su cuarto, revisa en el celular la banda usada. Si está en 5 GHz con señal débil, la solución puede ser tan simple como forzar o permitir que use 2.4 GHz ahí (más lento en teoría, pero llega más lejos y sería más estable que un 5 GHz moribundo).
4. Recomendación: NO comprar otro router igual de potente. Las opciones ordenadas por costo: (a) reubicar el router a un punto más central y elevado de la casa (gratis); (b) si el cuarto está muy lejos, agregar un punto de acceso cableado o un sistema mesh (resuelve el alcance de verdad); (c) solo si el router actual fuera WiFi 4 o más viejo valdría la pena renovarlo, pero siendo AC1200 con clientes WiFi 5, ya están en equilibrio.
5. Moraleja del caso: el 80 por ciento de los "mi WiFi está lento" son problemas de ubicación o alcance, no de generación del estándar. Medir en tres puntos (cable, junto al router, en el cuarto problemático) te dice en 5 minutos si el problema es el proveedor, el router o la distancia. En este caso fue la distancia, y ningún router nuevo del mismo tipo la habría arreglado.

Resumen de la unidad

- El IEEE es el organismo que escribe las reglas del WiFi; 802 es el comité de redes locales y 802.11 es el grupo de redes inalámbricas. Cada letra (b, g, n, ac, ax, be) es una enmienda, una nueva edición del estándar.
- La WiFi Alliance creó los nombres generacionales (WiFi 4, 5, 6, 6E, 7) porque "802.11ax" no lo dice nadie en una conversación normal. Son el mismo estándar con nombre comercial amable.
- 802.11b/g llevaron el WiFi a los hogares (11 y 54 Mbps en 2.4 GHz). 802.11n (WiFi 4) introdujo MIMO y los 40 MHz, llegando a 600 Mbps teóricos. 802.11ac (WiFi 5) apostó todo a 5 GHz con 256-QAM y 80/160 MHz, hasta 6.93 Gbps teóricos.
- WiFi 6 (802.11ax) se diseñó para muchos dispositivos: OFDMA reparte un canal entre varios clientes, 1024-QAM mete 10 bits por símbolo, TWT ahorra batería en dispositivos pequeños, BSS Coloring ignora a los vecinos lejanos y el MU-MIMO ya funciona en ambas direcciones. Máximo teórico: 9.6 Gbps.
- WiFi 6E es el mismo WiFi 6 con acceso a la banda de 6 GHz: espectro limpio y enorme, pero con menos alcance y menor capacidad de atravesar paredes. Solo sirve si tus dispositivos tienen radio de 6 GHz.

- WiFi 7 (802.11be) trae canales de 320 MHz, 4096-QAM (12 bits por símbolo), hasta 16 flujos espaciales y su gran novedad: MLO, que usa varias bandas al mismo tiempo para más velocidad y menos latencia. Máximo teórico: 46 Gbps.
- Todo estándar nuevo es compatible hacia atrás con los anteriores, pero la conexión siempre negocia lo mejor que AMBOS extremos soportan: el eslabón más débil manda.
- La velocidad teórica depende de cuatro factores: ancho de canal, modulación QAM, número de flujos espaciales y eficiencia del protocolo. El número de la caja usa los tres primeros al máximo y supone el cuarto perfecto.
- Por eso nunca alcanzas el número de la caja: suma las bandas (que no se usan a la vez), asume más flujos de los que tiene tu celular, asume el canal más ancho y la modulación máxima (que solo existe con señal excelente), e ignora que el protocolo desperdicia del 30 al 50 por ciento del tiempo de aire.
- Regla práctica: velocidad de enlace x 0.6 = throughput realista en buenas condiciones. Si el enlace dice 866 Mbps, espera unos 500 Mbps reales.
- MIMO son los carriles (flujos espaciales por antenas); MU-MIMO reparte esos carriles entre varios clientes a la vez, pero no acelera a uno solo. Más antenas en el router = atiende mejor a muchos, no = más velocidad para ti.
- QAM es cuántos bits mete cada transmisión: 64-QAM = 6 bits, 256-QAM = 8, 1024-QAM = 10, 4096-QAM = 12. Más bits = más velocidad pero menos resistencia al ruido; el equipo ajusta la modulación solo según la señal (adaptación de tasa).
- Errores que ya no vas a cometer: creer que el WiFi 6 aumenta la velocidad de tu proveedor; actualizar solo el router sin clientes compatibles; elegir por el número grande de la caja; forzar 160 MHz en un departamento saturado; esperar que los 6 GHz lleguen lejos.
- Buenas prácticas: compra la generación de tus clientes, mide con speedtest antes de gastar (cable, junto al router y en el cuarto), ubica el router en alto y al centro, y actualiza su firmware.
- Comandos que ya dominas: `netsh wlan show interfaces` en Windows, `iw dev wlan0 link` en Linux, opción-clic en el icono WiFi en macOS, y los ajustes de red en Android. Con ellos lees el estándar, la banda, la velocidad de enlace y la señal de cualquier conexión.

UNIDAD 4: Tu router, pieza por pieza (Clases 10 a 12)

Introducción

Imaginate que estas en una cocina enorme, como las de un restaurante grande en hora pico. Hay chefs por todos lados pidiendo ingredientes, hay repartidores entrando y saliendo, y alguien tiene que decidir quién pasa primero, a dónde va cada cosa y que no se haga un desmadre. Esa persona es el corazón de la cocina. En tu casa, ese corazón se llama router.

Hasta esta unidad ya viste que es una red inalámbrica, cómo viaja la señal y qué papel juegan las frecuencias. Pero hasta ahora todo fue teoría sobre el aire: las ondas, las bandas, los canales. Esta unidad baja los pies a la tierra y te pone frente al aparato físico que hace todo eso posible: el router, esa cajita con antenas y foquitos parpadeando que probablemente tienes escondida atrás del televisor o en un rincón de la sala.

Y aquí viene la verdad que casi nadie te dice: la mayoría de los problemas de internet en los hogares no son del proveedor, no son del plan que pagas ni de la "señal que esta mala hoy". Son del router mal configurado. Un router con la contraseña de fábrica que nunca se cambio, un canal saturado porque veinte vecinos usan el mismo, la potencia de transmisión al máximo cuando vives en un departamento de cincuenta metros cuadrados, o el aparato encerrado dentro de un mueble de madera como si fuera un secreto vergonzoso. Todo eso tiene arreglo, y todo eso lo vas a aprender aquí.

Esta unidad agrupa las clases 10, 11 y 12 del curso, y con ellas vas a lograr algo muy concreto: dejar de ver tu router como una caja misteriosa y empezar a verlo como lo que es, una computadora pequeña que TU puedes controlar.

En la clase 10 abriremos el router por dentro, sin destornillador. Vas a conocer sus partes como si fuera el motor de un carro: la CPU, que es el cerebro; la memoria RAM, que es su mesa de trabajo; la memoria flash, donde guarda la configuración; los puertos WAN y LAN, las puertas de entrada y salida del cableado; y las luces del panel frontal, que no están de adorno: cada foquito te esta contando una historia sobre lo que pasa dentro. Al terminar esta clase vas a poder mirar tu router y entender que hace cada pieza y cada luz.

En la clase 11 hacemos el primer encendido de verdad. Vas a aprender a entrar al panel de administración, esa página web secreta que vive en tu propio router y desde donde se controla todo. Aprenderas las direcciones típicas, 192.168.1.1 y 192.168.0.1, que significan, por qué

existen y que hacer si tu router usa otra. Y haremos lo primero que todo el mundo debería hacer y casi nadie hace: cambiar la contraseña de administrador de fábrica. Te voy a explicar por qué dejar "admin/admin" es como dejar la llave de tu casa pegada en la puerta con un letrero que dice "pasale".

En la clase 12 configuramos tu WiFi de principio a fin. Le pondremos nombre a tu red, el famoso SSID, y veremos porque el nombre que elijas importa más de lo que crees. Configuraremos la seguridad para que ningún vecino se cuelgue de tu internet. Hablaremos de la banda dual, eso de 2.4 GHz y 5 GHz que aparece en tu teléfono, y de cómo decidir cuál usar. Elegiremos el canal correcto para que tu red no pelee con la de los vecinos, ajustaremos el ancho de canal y la potencia de transmision, que es como el volumen de tu router: a veces hay que subirlo, pero muchas veces hay que bajarlo.

Cuando termines esta unidad vas a haber hecho tres cosas reales, no teoricas: vas a haber entrado al panel de tu router, cambiado la contraseña de administrador y configurado tu red WiFi con nombre, contraseña, canal y potencia adecuados. Eso, por si solo, te pone por delante del noventa por ciento de los usuarios de internet en el mundo. La mayoría nunca entra al panel de su router. Tú si.

Un aviso honesto antes de empezar: cada marca de router tiene su panel un poco distinto. Los menus se llaman diferente, los colores cambian, los botones están en otro lado. TP-Link, Tenda, Huawei, Cisco, Netgear, los que da tu compañía de internet... todos hacen lo mismo pero con otra cara. Por eso en esta unidad hablo de un "router generico": los conceptos, los nombres tecnicos y los pasos son los mismos en todos, y te voy a dar las pistas para encontrar cada opcion aunque tu panel se vea distinto. Lo importante es que entiendas QUE estas configurando y Por qué, no memorizar en que renglón de que menú esta. Si entiendes el porqué, el dónde lo encuentras en dos minutos.

Así que agarra una silla, ponte comodo cerca de tu router y ten a la mano tu teléfono o tu computadora. Esta unidad se lee mejor con el aparato enfrente, porque vas a ir comprobando cada cosa en vivo. Vamos a abrir esa caja, a entrar a su cerebro y a dejar tu red funcionando como debe ser. Empezamos por dentro.

Explicacion detallada

El router como director de orquesta

Imagina una orquesta sinfonica. Hay violines, trompetas, tambores, flautas: docenas de musicos, cada uno con su instrumento, cada uno tocando su parte. Si cada quien tocara lo que

quisiera cuando quisiera, sería ruido. El director de orquesta no toca ningún instrumento, pero sin el no hay música: el marca el tiempo, decide quién entra y cuándo, equilibra el volumen de cada sección y se asegura de que todos juntos suenen como una sola cosa.

Tu router es el director de orquesta de tu red. No genera el internet, igual que el director no compone la sinfonia, pero decide cómo se reparte entre todos los músicos: tu teléfono, tu computadora, la television, la tablet de los niños, el foco inteligente, la cámara de la entrada, el videojuego. Cada aparato pide datos, el router decide a quién le toca, cuánto le toca y por dónde se va, todo en milésimas de segundo, cientos de veces por segundo, sin que tú notes nada.

Otra analogía que funciona muy bien es la central telefónica de antes. Hace décadas, cuando querías llamar a alguien, una operadora en una central conectaba tu línea con la línea de la otra persona, clavija en mano. Tu router hace eso mismo pero con datos: recibe un paquete de información que dice "esto va para la laptop", y lo conecta con la laptop; recibe otro que dice "esto viene de internet para el teléfono", y lo manda al teléfono. Millones de clavijas invisibles, conectadas y desconectadas a velocidad imposible.

Y hay una tercera analogía, más mexicana: el router es como el encargado de la taquilla en una central de autobuses chiquita. Hay un solo camión que llega de la ciudad, el internet, y hay muchos pasajeros que quieren subir, tus aparatos. El encargado decide quién sube primero, revisa boletos, les dice a dónde va cada quien y se asegura de que nadie se quede dormido en el pasillo estorbando. Si el encargado es malo, hay pleito en la fila. Si es bueno, todo fluye.

Módem, router y punto de acceso: no son lo mismo

Aquí hay una confusión que tiene a medio mundo perdido, y vale la pena aclararla de una vez porque vas a ver estas palabras en todas partes.

El Módem es el traductor. Su trabajo es hablar con tu proveedor de internet. El proveedor manda la señal por cable coaxial, fibra óptica o línea telefónica, y tu computadora no entiende esa señal directamente. El módem la traduce a datos digitales que tu red sí entiende. Piénsalo así: el módem es el intérprete que habla con el extranjero, el proveedor. Sin módem, no hay internet en tu casa, punto.

El ROUTER es el repartidor. Toma el internet que le entrega el módem y lo reparte entre todos tus aparatos, por cable y por WiFi. Crea tu red local, les asigna direcciones a tus aparatos y decide cómo viaja la información. Es el director de orquesta del que hablamos.

El PUNTO DE ACCESO es el que crea la señal WiFi. Es básicamente una antena con cerebro que permite que tus aparatos se conecten sin cables. Aquí viene el detalle importante: casi

todos los routers caseros modernos TRAEN un punto de acceso integrado. Por eso cuando compras "un router WiFi", en realidad estas comprando un aparato que hace las tres cosas: módem aparte, router y punto de acceso juntos en una sola caja.

Entonces, por qué importa la diferencia? Por tres razones prácticas. Primera: cuando tu compañía de internet te "regala" o te renta un aparato, muchas veces es un módem-router combinado, y eso limita lo que puedes configurar. Segunda: si tu casa es grande y el WiFi no llega a los cuartos de atrás, la solución suele ser agregar PUNTOS DE ACCESO adicionales, no cambiar todo el router. Tercera: cuando algo falla, saber cuál de las tres funciones está fallando te ahorra horas. Si no hay internet en ningún aparato ni por cable, probablemente es el módem o el proveedor. Si hay internet por cable pero no hay WiFi, el problema es el punto de acceso del router. Si el WiFi funciona pero un aparato no se conecta, el problema es ese aparato. Verdad que con esta logica ya puedes diagnosticar mejor que el técnico que te dice "reinicielo y me marca mañana"?

Un caso especial: el modo puente, o "bridge". A veces conviene usar el módem-router de la compañía SOLO como módem, apagando su funcion de router, y conectar tu propio router bueno detras. Esto se llama ponerlo en modo puente. Es como decirle al aparato de la compañía: "tu solo traduce, del reparto me encargo yo". Lo veremos más adelante cuando hablemos de redes avanzadas, pero que sepas que existe.

El router por dentro: CPU, memoria y puertos

Vamos a abrir el router sin destornillador, con la imaginacion. Por dentro, tu router es una computadora completa, chiquita y especializada. Tiene los mismos componentes basicos que tu teléfono o tu laptop, solo que más modestos y dedicados a una sola tarea: mover datos.

La CPU es el cerebro. Es un procesador pequeño, mucho menos potente que el de tu computadora, pero no lo necesita ser: su único trabajo es decidir a dónde va cada paquete de datos. Cuando tienes dos o tres aparatos conectados, cualquier CPU se la lleva tranquila. Pero cuando tienes quince aparatos, alguien viendo peliculas en 4K, otro en videollamada, los ninos jugando en línea y la cámara de seguridad subiendo video, la CPU empieza a sudar. Por eso un router barato se "traba" con muchos aparatos: no es que el internet sea lento, es que el cerebro del router no alcanza a repartir tan rápido. Regla práctica: si tu casa tiene más de diez aparatos conectados al mismo tiempo de forma habitual, necesitas un router de gama media, no el más barato del estante.

La memoria RAM es la mesa de trabajo. Ahí el router guarda temporalmente las listas de que aparato pidio que, las conexiones activas y las tablas de reparto. Más RAM significa que puede atender más conexiones simultaneas sin olvidar nada. Cuando la RAM se llena, el

router empieza a tirar conexiones viejas para hacer espacio, y eso se siente como "el internet se corta a cada rato". Típico de routers muy basicos con muchos aparatos.

La memoria FLASH es el cuaderno donde anota todo lo permanente: tu configuración, el nombre de tu red, las contraseñas, y el FIRMWARE, que es el programa que hace funcionar al router. La flash no se borra cuando apagas el aparato, por eso tu configuración sobrevive a un apagon. El firmware es como el sistema operativo del router, y actualizarlo es importante: los fabricantes sacan actualizaciones que tapan agujeros de seguridad y a veces mejoran el rendimiento. Más adelante te enseño como hacerlo paso a paso.

Los puertos son las puertas físicas. En la parte de atrás de tu router vas a ver varios conectores que parecen de teléfono pero más grandes: esos son puertos Ethernet, para cable de red. Uno de ellos, normalmente separado de los demás, de otro color o marcado como WAN o INTERNET, es el puerto WAN. WAN significa Wide Area Network, red de área amplia: es la puerta por donde ENTRA el internet, el cable que viene del módem o directo del proveedor. Los demás puertos, normalmente cuatro juntos y marcados como LAN, son la red local: ahí conectas por cable tu computadora, tu televisión, tu consola de videojuegos. LAN significa Local Area Network, tu red de la casa.

Memoriza esto porque te va a servir toda la vida: WAN es la puerta del internet que entra, LAN son las puertas de tu casa hacia tus aparatos. Si conectas el cable del módem en un puerto LAN por error, nada va a funcionar, y es un error más común de lo que crees. Cuando algo no jala, lo primero que se revisa es: el cable del módem, está en el WAN? Si o no.

Además de los puertos Ethernet, muchos routers traen un puerto USB. Sirve para conectar un disco duro y compartir archivos en la red, o una impresora para que todos impriman sin cables. No todos lo traen, y si el tuyo lo trae, es un extra bonito pero no esencial.

Y las antenas: esas varitas que sobresalen. Son las que emiten y reciben la señal WiFi. Si tu router tiene antenas externas que se pueden mover, la posición sí importa: lo ideal es ponerlas verticales, paradas derechitas, porque así la señal se reparte mejor en horizontal, que es como están distribuidos tus aparatos en la casa. Antenas acostadas o todas chuecas reparten la señal al techo y al piso. Detalle pequeño, diferencia notable.

Que significan las luces del router

Esas lucecitas que parpadean en el frente no son decoración navideña. Son el tablero del carro: te dicen que está pasando sin necesidad de entrar a ningún menú. Aprende a leerlas y podrás diagnosticar problemas en segundos. Los símbolos varían un poco por marca, pero casi todos usan estos:

POWER o encendido: luz fija significa que el router tiene corriente y prendio bien. Si parpadea sin parar o esta apagada con el aparato conectado, hay problema de corriente o el router no termino de arrancar. Espera un minuto después de conectarlo: los routers tardan en "despertar".

INTERNET o WAN o un globito terrqueo: esta es la importante. Luz fija, normalmente verde o blanca, significa que hay conexión con el proveedor y hay internet. Si está en rojo o naranja, o parpadea en rojo, NO hay internet: el problema está entre tu router y tu proveedor, o sea, revisa el cable del módem, reinicia el módem, y si sigue igual, habla a tu compañía. Si esta apagada, no hay ni siquiera señal fisica: revisa que el cable este bien conectado al puerto WAN.

WIFI o 2.4G y 5G: indica que la red inalámbrica está activa. Normalmente parpadea cuando hay aparatos transmitiendo datos, y eso es bueno: parpadeo significa vida, significa que hay trafico. Si esta apagada, el WiFi está desactivado, ya sea porque alguien apago el boton fisico de WiFi del router o porque se desactivo en la configuración. Ojo: muchos routers traen un botoncito fisico para prender y apagar el WiFi; si tu WiFi "desaparecio" de la nada, revisa que no lo hayas apagado sin querer al mover el aparato.

LAN 1, 2, 3, 4: una lucecita por cada puerto cableado. Se prende cuando hay un aparato conectado por cable en ese puerto, y parpadea cuando hay trafico. Si conectaste tu computadora por cable y su lucecita no prende, el cable está mal, el puerto está mal, o la tarjeta de red de la compu está desactivada. Diagnostico en tres segundos.

WPS: se prende durante el proceso de conexión rapida WPS y luego se apaga. Si la ves prendida fija sin que estes conectando nada, alguien podría estar intentando conectarse: revisalo.

USB: indica que hay un dispositivo USB conectado, si tu router tiene ese puerto.

Regla de oro para leer las luces: verde o blanco fijo es bueno, rojo o naranja es malo, parpadeo rápido en la de internet puede ser actividad normal, pero parpadeo lento y constante en POWER después de varios minutos puede indicar que el firmware se dano. Cuando llames a soporte técnico y te pregunten "que luces tiene prendidas", ya no vas a decir "este... todas parpadean". Vas a decir exactamente cuáles, y te van a atender más rápido.

NAT, DHCP y puerta de enlace: las tres magias invisibles

Tu router hace tres trucos de magia todos los días sin que te des cuenta. Entenderlos te va a dar una ventaja enorme cuando algo falle, porque vas a saber en que capa del truco se rompio la magia.

El primer truco se llama NAT, que significa Network Address Translation, traducción de direcciones de red. Aquí va el problema que resuelve: tu proveedor de internet te da UNA sola dirección IP publica, una sola "dirección" para toda tu casa. Pero tú tienes diez, quince, veinte aparatos que quieren salir a internet. Cómo le hacen? El NAT es el truco: el router les pone a tus aparatos direcciones IP privadas, internas, que solo existen dentro de tu casa, como 192.168.1.5 o 192.168.1.6. Cuando un aparato quiere salir a internet, el router toma su petición, le pega su única dirección publica como remitente, la manda, recibe la respuesta y se la entrega al aparato correcto. Es como un edificio de departamentos con una sola dirección en la calle: el cartero deja todo en recepción con el número de departamento, y el portero, el NAT, reparte cada carta al departamento que le toca. Gracias al NAT, cientos de aparatos comparten una sola IP publica sin pisarse.

El segundo truco es el DHCP, Dynamic Host Configuration Protocol, protocolo de configuración dinámica. Su trabajo es repartir direcciones IP privadas a tus aparatos automáticamente. Cuando tu teléfono se conecta al WiFi, le pregunta al router "oye, que dirección me toca?", y el servidor DHCP del router le responde "te toca la 192.168.1.7, y tu puerta de salida es la 192.168.1.1". Todo automatico, en un segundo, sin que tu hagas nada. Antes había que configurar cada aparato a mano, dirección por dirección, y era un infierno. El DHCP lo hace solo. El rango de direcciones que reparte se puede configurar, y también se pueden "apartar" direcciones fijas para aparatos que siempre deben tener la misma, como una impresora o una cámara: eso se llama reserva DHCP, y es útil cuando quieras.

El tercer concepto es la PUERTA DE ENLACE, o gateway. Es la dirección IP de tu router dentro de tu red local, normalmente 192.168.1.1 o 192.168.0.1. Es "la puerta" por donde tus aparatos salen hacia internet. Por eso cuando entras al panel de administración escribes esa dirección en el navegador: porque le estas hablando directamente a la puerta. Si algun día tu aparato dice "conectado sin internet", muchas veces significa que no esta llegando a la puerta de enlace: o no recibio bien su configuración del DHCP, o la puerta cambio de dirección.

Estos tres trabajan juntos así: tu teléfono se conecta, el DHCP le da su dirección privada y le dice cuál es la puerta de enlace, el teléfono manda sus peticiones a la puerta, y el NAT las traduce para salir a internet con la IP publica. Tres pasos, un segundo, invisible. Cuando entiendes esto, los mensajes de error dejan de ser jeroglíficos.

Firmware: el cerebro que si se puede actualizar

El firmware es el programa interno que hace funcionar a tu router. Es su sistema operativo, más sencillo que el de tu teléfono, pero igual de importante. El fabricante lo va mejorando con el tiempo: tapa agujeros de seguridad que descubren los hackers, corrige errores que hacen que el router se trabe, y a veces agrega funciones nuevas o mejora la velocidad.

Actualizar el firmware es una de las tareas de mantenimiento más importantes y más ignoradas. Un router con firmware de hace cinco años es como una casa con la chapa de hace cinco años después de que ya salió en las noticias como forzarla: los atacantes conocen las vulnerabilidades viejas y las buscan automáticamente por internet. La buena noticia es que actualizar es fácil, y en la sección de ejemplos te doy el paso a paso.

Hay dos formas de actualizar: automática y manual. Algunos routers modernos revisan solos si hay actualización y te avisan, o hasta la instalan de noche. Otros requieren que entres al panel, vayas a la sección de administración o sistema, y le piques a "buscar actualización". Si tu router es de los que da tu compañía de internet, muchas veces ellos actualizan el firmware remotamente sin avisarte.

Dos advertencias serias. Una: NUNCA apagues ni desconectes el router mientras se está actualizando el firmware. Si se interrumpe a la mitad, el cerebro queda a medias y el router puede quedar inservible, lo que los técnicos llaman "brickeado", convertido en ladrillo. Dos: descarga el firmware SOLO de la página oficial del fabricante. Hay sitios pirata con firmwares modificados que traen regalos no deseados. Si vas a actualizar manual, entra a la página oficial, busca tu modelo exacto y descarga de ahí.

Errores comunes que debes evitar desde hoy

Vamos con la sección que más dinero y corajes te va a ahorrar: los errores que comete casi todo el mundo con su router. Leelos, reconoce cuáles estás cometiendo tú, y corrígelos en cuanto termines esta unidad.

Error número uno: dejar la contraseña de administrador de fábrica. Casi todos los routers salen de fábrica con usuario "admin" y contraseña "admin", o "password", o "1234". Esas contraseñas están publicadas en internet, en listas que cualquier persona puede buscar en diez segundos. Si alguien se conecta a tu red, o si tu router tiene activada la administración remota, entrar a tu panel con esas credenciales es trámite. Y desde el panel se puede hacer TODO: cambiar tu WiFi, ver tus aparatos, abrir puertas. Cambiarla es el paso más importante de esta unidad, y lo hacemos juntos en la clase 11.

Error número dos: poner el router en el piso, dentro de un mueble, o escondido atrás de la television. La señal WiFi se comporta como la luz de un foco: si metes el foco dentro de un cajón, alumbró el cajón, no el cuarto. La madera, el metal y sobre todo los espejos y el agua bloquean o rebotan la señal. El lugar ideal para el router es alto, como a la altura de tu pecho o más, en un lugar abierto y lo más centrado posible en tu casa. Arriba de un librero en la sala funciona mil veces mejor que en el piso detrás del sillón. Si tu router está dentro del mueble de la television "para que no se vea", sacalo hoy mismo. Tu internet te lo va a agradecer esta misma noche.

Error número tres: dejar el WiFi abierto o con contraseña fácil. "Mi vecino ni sabe de computadoras" no es estrategia de seguridad. Hay aplicaciones que encuentran redes débiles en segundos, y un vecino colgado no solo te roba velocidad: todo lo que hace en internet sale con TU dirección IP. Si hace algo ilegal, la que aparece eres tu. Contraseña larga y WPA2 o WPA3, siempre. Lo configuramos en la clase 12.

Error número cuatro: nunca reiniciar el router. Los routers son computadoras, y como toda computadora, acumulan basura en la memoria con el tiempo. Un reinicio cada mes, o cuando notes lentitud, les hace bien. Desconéctalo de la corriente, espera treinta segundos y vuélvelo a conectar. Treinta segundos, no cinco: los capacitores internos necesitan descargarse por completo. No es mito, es electrónica.

Error número cinco: comprar repetidores baratos para "ampliar la señal" sin entender que hacen. Un repetidor barato toma tu señal WiFi débil y la repite, pero a la mitad de velocidad, porque usa la misma antena para recibir y transmitir. Es como el juego del teléfono descompuesto: el mensaje llega, pero deformado y lento. A veces la solución no es un repetidor, sino mover el router a mejor lugar o ajustar el canal. Si de plano necesitas más cobertura, un punto de acceso cableado o un sistema mesh es mejor inversión.

Error número seis: ignorar las actualizaciones de firmware. Ya hablamos de esto: es dejar la puerta con la chapa vieja.

Error número siete: usar el mismo nombre y contraseña de WiFi que trae de fábrica, como "TP-LINK_3F2A" o "IZZI-XXXX". No es un problema de seguridad grave si la contraseña es larga y aleatoria, pero es un problema práctico: cuando necesites dictarle la contraseña a una visita, o cuando tengas que reconectar todos tus aparatos, vas a odiar esos códigos. Ponle un nombre que reconozcas y una contraseña que puedas dictar sin deletrear cada letra tres veces.

Buenas prácticas: tu rutina de dueño responsable

Así como un carro necesita sus servicios, tu router necesita una rutina mínima. No es complicada, y te la resumo en una lista que puedes pegar con un imán en el refrigerador:

Primero, cambia la contraseña de administrador en cuanto estrenes router, o hoy mismo si nunca lo hiciste. Segundo, ponle a tu WiFi un nombre reconocible y una contraseña larga con WPA2 o WPA3. Tercero, coloca el router en alto, centrado y despejado. Cuarto, elige un canal poco saturado, te enseño como en la clase 12. Quinto, revisa actualizaciones de firmware cada tres o cuatro meses. Sexto, reinicia el router una vez al mes. Séptimo, haz un respaldo de tu configuración después de dejar todo bien, para restaurarlo en minutos si algo se descompone. Octavo, desactiva lo que no uses: si no usas WPS, apágalo; si no necesitas administración remota, déjala apagada.

Con eso tienes un router sano, rápido y seguro. No necesitas ser técnico, necesitas ser constante. Vamos ahora a la práctica guiada.

El panel de administración: la cabina de control

Todo router trae una página web escondida que es su centro de mando. No está en internet, vive DENTRO del router, y solo puedes entrar si estás conectado a su red, por WiFi o por cable. Ahí se configura absolutamente todo: el nombre del WiFi, la contraseña, los canales, las actualizaciones, los aparatos bloqueados, los horarios. Si el router es el carro, el panel de administración es el tablero con todos los botones.

Para entrar escribes su dirección IP en el navegador, como si fuera una página web. Las dos más comunes son 192.168.1.1 y 192.168.0.1. Por qué esas? Porque pertenecen a un rango de direcciones IP privadas reservado para redes locales, y los fabricantes se pusieron de acuerdo, más o menos, en usarlas. Piensa en ellas como la dirección de la caseta de vigilancia de tu fraccionamiento: no sale en Google Maps, pero todos los vecinos saben dónde está.

Que significa cada número? Una dirección IP tiene cuatro grupos. En 192.168.1.1, los primeros tres grupos, 192.168.1, identifican TU red, tu casa; el último número, el 1, identifica al aparato dentro de la red, y por convención el router se queda con el 1. Tus aparatos reciben los números siguientes: 2, 3, 4, y así. En 192.168.0.1 es lo mismo pero la red es 192.168.0. Son como dos fraccionamientos distintos con la misma lógica de numeración.

Cómo saber cuál usa tu router? Hay tres formas. La fácil: busca la etiqueta pegada abajo o atrás del router; ahí el fabricante imprime la dirección del panel, el usuario y la contraseña de fábrica. La segunda: en Windows abre el símbolo del sistema y escribe ipconfig, y busca dónde dice "puerta de enlace predeterminada": esa es la dirección de tu router. En el teléfono,

entra a los detalles de tu conexión WiFi y busca "puerta de enlace" o "router". La tercera: prueba las dos comunes en el navegador, una te va a abrir la página de login.

Al entrar te pide usuario y contraseña. Los de fábrica típicos son admin/admin, admin/password, o a veces vienen impresos en la etiqueta con una clave única. Si alguien ya los cambio y no te acuerdas, la única salida es resetear el router al estado de fábrica con el botoncito de reset, pero ojo: eso borra TODA tu configuración y hay que empezar de cero. Por eso el respaldo de configuración que veremos en los ejemplos es tan valioso.

Dentro del panel vas a encontrar secciones con nombres parecidos a estos: Estado o Status, dónde ves si hay internet y qué aparatos están conectados; Red inalámbrica o Wireless, donde se configura el WiFi; Red o Network, para lo de WAN, LAN y DHCP; Administracion o System, para la contraseña del panel, firmware y respaldos; y Seguridad o Firewall. No te asustes por la cantidad de opciones: en esta unidad solo necesitas unas diez, y te voy a decir exactamente cuáles.

Cambiar la contraseña de administrador: tu primera mision

Vamos a dimensionar bien por qué esto es tan importante, porque "cambia tu contraseña" suena a consejo de abuelita y la gente lo ignora. Tu panel de administracion es la llave maestra de tu red. Quien entra ahí puede ver todos tus aparatos conectados, puede bloquearte tu propio internet, puede redirigir tu trafico, puede abrir puertos hacia adentro. Y las credenciales de fábrica son publicas: hay paginas web que listan, por marca y modelo, cuál es el usuario y contraseña con los que sale cada router de la tienda. Un atacante no necesita adivinar nada, solo necesita buscar.

"Pero para entrar al panel hay que estar conectado a mi red". Cierto, y por eso el riesgo se combina con el siguiente eslabon: si tu WiFi tiene contraseña débil, o si tienes activada la administracion remota, que permite entrar al panel DESDE internet, la puerta queda abierta de par en par. Hay robots en internet que todo el dia están tocando puertas: prueban direcciones IP al azar buscando routers con administracion remota prendida y credenciales de fábrica. Es automatico, no es personal, y le pasa a miles de personas al dia.

La solución es simple y te toma dos minutos: entra al panel, ve a la sección de Administracion o Sistema, busca "contraseña" o "password", escribe una contraseña nueva, larga, que no uses en ningún otro lado, guardala en un lugar seguro, y guarda los cambios. En los ejemplos te doy el paso a paso con los valores exactos. Hazlo hoy. Si solo haces una cosa de toda esta unidad, que sea esta.

Y ya que andas por ahí, revisa dos ajustes vecinos: la administracion remota debe estar APAGADA, a menos que sepas exactamente por qué la necesitas; y el acceso al panel por

WiFi, si tu router lo permite, dejalo solo por cable o con la contraseña nueva bien puesta. Capas de seguridad, como las capas de una cebolla.

Configurar tu WiFi: el SSID y por qué importa

SSID significa Service Set Identifier, pero olvidate del nombre técnico: es simplemente EL NOMBRE DE TU RED WIFI, el que ves en la lista cuando buscas redes en tu teléfono. "CASA_GARCIA", "IZZI-4F2A", "TP-LINK_XXXX". Ese nombre lo defines tú en el panel, y aunque parezca un detalle estético, tiene implicaciones prácticas y de seguridad.

Primero, lo practico: un nombre claro te ayuda a identificar tu red entre las veinte del edificio. Si vives en un departamento y hay quince redes que se llaman "IZZI-XXXX" o "Telmex-XXXX", vas a estar adivinando cuál es la tuya cada vez que conectes algo nuevo. Ponle algo reconocible para ti.

Segundo, la seguridad: el nombre de tu red NO debe contener informacion personal. Nada de "CASA_DE_JUAN_PEREZ_123", ni tu dirección, ni tu número de teléfono. El SSID se anda gritando por el aire todo el día, lo ve cualquiera que pase por la calle. Un nombre neutro como "RED_CASA" o "FAMILIA_GARCIA_WIFI" está bien; tu nombre completo y tu dirección, no.

Tercero, hay un detalle técnico curioso: no le pongas al SSID caracteres raros, emojis o acentos. Algunos aparatos viejitos, impresoras y focos inteligentes sobre todo, se hacen bolas con nombres raros y luego no se conectan. Letras, números y guion bajo: con eso no falla nada.

El SSID broadcast es la opcion que hace que tu router ande anunciando su nombre a cada rato, como un pregonero: "aquí estoy, soy RED_CASA, conectense". Si lo apagas, tu red se vuelve "oculta": no aparece en las listas y hay que escribir el nombre a mano para conectarse. Suena más seguro, verdad? Pues es una falsa sensacion de seguridad: el nombre sigue viajando por el aire cada vez que tus aparatos se conectan, y hay herramientas gratuitas que lo descubren en segundos. Peor aun: con el broadcast apagado, tus aparatos andan preguntando a gritos "oye, RED_CASA, andas por ahí?" donde quiera que van, y eso SI se puede interceptar. Conclusion de los expertos: deja el broadcast encendido y ponle una buena contraseña. Ocultar el SSID no te protege y te complica la vida.

Seguridad del WiFi: WPA2, WPA3 y la contraseña que si sirve

En la configuración inalámbrica vas a ver un campo que dice "seguridad", "autenticacion" o "cifrado", con opciones como Abierta, WEP, WPA, WPA2 y WPA3. Aquí va la guia rapida:

Abierta significa sin contraseña: cualquiera se conecta. Solo para invitados temporales y con red separada, nunca para tu red principal. WEP es un sistema viejísimo, roto desde hace años: se puede crackear en minutos con programas gratuitos. Si tu router solo ofrece WEP, tu router es un fósil y necesitas cambiarlo. WPA es el intermedio, mejor que WEP pero ya superado. WPA2 es el estándar actual que funciona en todo: úsalo. WPA3 es el nuevo, más seguro, úsalo si tu router y tus aparatos lo soportan; si algún aparato viejito no se conecta con WPA3, baja a WPA2.

La contraseña del WiFi, la que le dictas a las visitas, debe ser larga: mínimo doce caracteres, ideal veinte. No tiene que ser un jeroglífico imposible: cuatro palabras comunes pegadas con un número funcionan muy bien, tipo "casa-perro-foco-1987-mesa". Lo importante es la LONGITUD, no los símbolos raros. Una contraseña de veinte caracteres sencillos es millones de veces más difícil de romper que una de ocho con símbolos. Y no uses la misma que la del panel de administrador: son dos puertas distintas, con dos llaves distintas.

Banda dual: 2.4 GHz y 5 GHz, cuando usar cada una

Los routers modernos son de "banda dual": emiten en dos frecuencias, 2.4 GHz y 5 GHz. No son dos internet distintos, es el mismo internet saliendo por dos "carriles" con características diferentes. Ya viste la teoría de las bandas en la unidad 2; ahora viene la parte práctica de como usarlas.

La banda de 2.4 GHz es el carril largo y lento: llega lejos, atraviesa paredes mejor, pero va más despacio y está muy congestionada porque TODO la usa: tus vecinos, el microondas, los audífonos bluetooth, el control del portón. La banda de 5 GHz es el carril corto y rápido: vuela, hay menos tráfico, pero no llega tan lejos ni atraviesa paredes tan bien.

Regla práctica para tu casa: los aparatos que están cerca del router y necesitan velocidad, televisión viendo 4K, computadora, consola de videojuegos, van en 5 GHz. Los aparatos lejos, o los sencillos que no necesitan velocidad, focos inteligentes, impresora, cámara del patio, van en 2.4 GHz. Así repartes la carga y cada quien usa el carril que le conviene.

Muchos routers ofrecen "band steering", que es una función que une las dos bandas bajo UN solo nombre de red y el router decide solito en cuál pone cada aparato. Suena mágico, y cuando funciona bien es comodísimo: te conectas a "CASA" y ya. Pero a veces se equivoca y pone tu televisión en 2.4 cuando debería estar en 5, o algún aparato viejito se confunde. Mi recomendación para principiantes: empieza con nombres SEPARADOS, por ejemplo "CASA_2G" y "CASA_5G", así TU decides dónde va cada aparato y aprendes cómo se comporta cada banda. Cuando ya domines eso, prueba el band steering si tu router lo trae.

Canales: la autopista invisible

Dentro de cada banda, el WiFi se divide en canales, como carriles de una autopista. En 2.4 GHz hay 13 o 14 canales segun el pais, pero solo tres no se enciman entre si: el 1, el 6 y el 11. Los demas se traslapan y se estorban mutuamente. Es como si en una carretera de tres carriles pintaran catorce líneas: los carros terminarian chocando.

El problema: la mayoría de los routers salen de fábrica en "canal automatico", y el automatico de muchos routers baratos es... el 6, siempre el 6. Resultado: en un edificio de departamentos, veinte routers peleando en el mismo canal 6, todos lentos, todos echandole la culpa al proveedor. La solución es elegir a mano un canal poco usado: el 1, el 6 o el 11, el que tenga menos vecinos.

Cómo saber cuál está libre? Con una aplicacion gratuita de analisis WiFi en tu teléfono, como "WiFi Analyzer" en Android. La abres, ves una grafica con todos los canales y las redes de tus vecinos, y eliges el 1, 6 u 11 más despejado. En iPhone las opciones son más limitadas por restricciones del sistema, pero hay aplicaciones similares. Haces el analisis una vez cada varios meses, porque los vecinos cambian sus routers y los canales se vuelven a llenar.

En 5 GHz la historia es más facil: hay muchos más canales y casi no se enciman, así que la congestion es rara. Ahí puedes dejar el canal en automatico sin remordimiento, o elegir uno libre si quieres afinar.

Ancho de canal: más ancho no siempre es mejor

El ancho de canal es que tan "ancho" es el carril por donde viajan tus datos: 20 MHz, 40 MHz, 80 MHz o hasta 160 MHz. Más ancho significa más velocidad potencial, como una avenida más ancha donde caben más carros. Entonces, por qué no poner siempre el máximo?

Porque un canal más ancho ocupa más espacio en el espectro y tiene más probabilidad de chocar con los vecinos. En 2.4 GHz, poner 40 MHz es como estacionar un trailer en diagonal ocupando dos carriles: si, tú vas rápido, pero estorbas a todos y todos te estorban a ti. En zonas con muchos vecinos, 20 MHz en 2.4 GHz es la eleccion sabia: menos velocidad máxima teorica, pero conexión estable y sin peleas. En 5 GHz, donde hay espacio de sobra, 40 u 80 MHz funcionan de maravilla y si te dan la velocidad prometida.

Regla de bolsillo: 2.4 GHz en 20 MHz siempre, salvo que vivas en el campo sin vecinos. 5 GHz en 40 u 80 MHz sin miedo. Si tu router tiene la opcion en "automatico", en 5 GHz dejalo así; en 2.4 GHz fijalo en 20 MHz a mano.

Potencia de transmision: el volumen de tu router

La potencia de transmision es con cuanta fuerza grita tu router, y se mide en miliwatts (mW) o en decibeles relativos al miliwatt (dBm). Un router casero típico transmite entre 50 y 100 mW, que equivale a unos 17 a 20 dBm. No necesitas memorizar los números, pero si entender la idea: más potencia es más volumen, más alcance.

Y aquí viene lo contraintuitivo: el máximo NO siempre es lo mejor. Si vives en un departamento de 60 metros cuadrados y tu router grita al máximo, tu señal llega hasta la calle, hasta el departamento del vecino de arriba y hasta el de enfrente. Eso tiene dos problemas: uno, le regalas interferencia a tus vecinos y ellos te la devuelven, todos peor; dos, tu teléfono escucha al router perfecto, pero el router no escucha bien a tu teléfono, porque tu teléfono grita bajito. El WiFi es conversacion de dos vias: de nada sirve que tu escuches perfecto si el otro no te oye. Es como hablar con alguien que trae megafono: el te oye gritar y tu a el ni lo escuchas.

Cuando BAJAR la potencia: si tu casa es chica o mediana y el router esta centrado, baja la potencia a media o al 50-75 por ciento. Vas a tener la misma velocidad dentro de tu casa, menos interferencia con vecinos y, de paso, un poquito más de privacidad porque tu señal no sale a la calle. Cuando SUBIRLA al máximo: casas grandes, router en un extremo porque ahí llega el cable del proveedor, o necesidad de llegar al patio o a la planta alta. Ahí si, todo el volumen.

Algunos routers permiten ajustar la potencia en porcentaje, otros en niveles como Bajo, Medio y Alto, otros en dBm. No importa la unidad: la logica es la misma. Empieza en Alto, prueba cómo te va una semana, y si todo funciona bien y vives pegado a vecinos, baja a Medio y compara. El mejor ajuste es el que te da buena velocidad DENTRO de tu casa con la menor potencia posible.

Un detalle de salud que preguntan mucho: la potencia de un router WiFi es bajisima comparada con la de un teléfono celular pegado a tu oreja. Bajar la potencia por "las radiaciones" no es necesario por salud; se baja por rendimiento y buena vecindad, que son razones tecnicas de verdad.

Firmware y actualizaciones: el mantenimiento que nadie hace

Ya lo mencione en la clase 10 y lo repito porque es importante: el firmware desactualizado es una de las causas más comunes de routers hackeados. Los fabricantes publican actualizaciones que corrigen vulnerabilidades, y los atacantes automatizan la busqueda de routers viejos. Es una carrera, y tú quieres estar del lado actualizado.

Cada tres o cuatro meses entra al panel, ve a Administracion o Sistema, busca "actualizacion de firmware" y revisa si hay version nueva. Si tu router tiene actualizacion automatica, activala: es lo más comodo. Y recuerda las dos reglas de oro: nunca lo apagues a media actualizacion, y descarga solo de la página oficial del fabricante.

Ejemplos paso a paso

Antes de empezar los tutoriales, tres preparativos que te van a ahorrar dolores de cabeza. Primero, conecta tu computadora al router POR CABLE si puedes: es más estable y si algo sale mal con el WiFi no te quedas incomunicado a media configuración. Si no tienes cable, por WiFi también se puede, solo ten paciencia. Segundo, ten a la mano la etiqueta del router, donde vienen la dirección del panel y las claves de fábrica, y un papel donde anotar tus nuevas contraseñas. Tercero, hazlo con calma y sin prisas: una configuración bien hecha a la primera dura años.

Ejemplo 1: Configuración inicial completa de un router generico

Este es el tutorial principal de la unidad. Sigue estos pasos en orden y al final tendrás un router seguro, con tu red nombrada y optimizada. Los nombres de los menus cambian segun la marca, pero te doy las variantes más comunes entre parentesis.

Paso 1: Conecta todo físicamente. El cable que viene del módem o de la pared del proveedor va al puerto WAN del router, el que esta separado o marcado como INTERNET. Tu computadora, si la vas a conectar por cable, va a cualquier puerto LAN, los numerados del 1 al 4. Conecta el eliminador de corriente del router y espera un minuto a que terminen de prender las luces. Verifica: la luz de POWER fija, y si el módem ya tiene internet, la luz de INTERNET o WAN también fija o en verde.

Paso 2: Entra al panel de administracion. Abre tu navegador y en la barra de direcciones escribe la IP de tu router. Prueba primero con:

```
http://192.168.1.1
```

Si no abre nada, prueba con:

```
http://192.168.0.1
```

Si ninguna funciona, revisa la etiqueta del router o busca tu puerta de enlace cómo te explique en la teoría. Te debe aparecer una pantalla pidiendo usuario y contraseña.

Paso 3: Inicia sesión con las credenciales de fábrica. Las más comunes son:

```
Usuario: admin
Contraseña: admin
```

Otras combinaciones típicas: admin/password, admin/1234, o las impresas en la etiqueta del equipo. Si entras, perfecto. Si te dice que son incorrectas y nadie las cambió, haz un reset de fábrica: con el router prendido, mete un clip en el orificio de RESET, mantenlo presionado diez segundos y espera a que reinicie. Ojo: el reset borra todo, así que solo úsalo si de plano no puedes entrar.

Paso 4: Corre el asistente de instalación si tu router lo ofrece. Muchos routers muestran un "Quick Setup", "Asistente rápido" o "Configuración inicial" al entrar por primera vez. Úsalo: te pregunta el tipo de conexión a internet, normalmente la opción correcta es "IP dinámica" o "DHCP", que significa que tu proveedor te asigna todo automáticamente. Si tu proveedor te dio datos de PPPoE, que es un usuario y contraseña para conectarse, eliges PPPoE y los escribes. Si no sabes cuál es, elige IP dinámica: funciona en la mayoría de los casos con cable e internet por fibra.

Paso 5: Cambia la contraseña del administrador. Ve a la sección Administración, Sistema o Management, y busca "Contraseña", "Password" o "Cambiar contraseña de acceso". Escribe una contraseña nueva y guárdala. Ejemplo de formato, inventa la tuya:

```
Contraseña nueva de admin: RouterCasa-2026-Seguro-41
```

Reglas: mínimo doce caracteres, que no sea la misma del WiFi, y anótala en papel. Guarda los cambios. Es probable que el panel te saque y te pida entrar de nuevo con la contraseña nueva: es normal, hazlo.

Paso 6: Configura la red de 2.4 GHz. Ve a la sección Inalámbrico, Wireless o WiFi. Busca los ajustes de la banda 2.4G y configura así:

```
Nombre de red (SSID): CASA_2G
Seguridad: WPA2-PSK (o WPA2/WPA3 si lo ofrece)
Contraseña: tu-contrasena-larga-aqui-minimo-12-caracteres
Canal: 1, 6 u 11 (el mas libre segun tu analisis; si no analizaste, deja Auto por ahora)
Ancho de canal: 20 MHz
Potencia de transmision: Alta (la ajustaremos despues de probar)
SSID Broadcast: Activado
```

Sustituye "CASA_2G" por el nombre que quieras y la contraseña por una tuya, larga. Guarda.

Paso 7: Configura la red de 5 GHz. En la misma sección, busca los ajustes de la banda 5G:

```
Nombre de red (SSID): CASA_5G
Seguridad: WPA2-PSK (o WPA3 si tus aparatos lo soportan)
Contraseña: la-misma-larga-del-2G-o-otra-igual-de-larga
Canal: Auto (o uno libre si quieres afinar)
Ancho de canal: 40 MHz u 80 MHz
Potencia de transmision: Alta
SSID Broadcast: Activado
```

Puedes usar la misma contraseña en ambas bandas sin problema. Guarda los cambios.

Paso 8: Revisa el DHCP. Ve a la sección Red, LAN o DHCP. Verifica que el servidor DHCP este ACTIVADO y fijate en el rango de direcciones que reparte, algo como:

```
DHCP: Activado
Rango: 192.168.1.100 a 192.168.1.199
Puerta de enlace: 192.168.1.1
```

No necesitas cambiar nada aquí normalmente; solo confirma que esta prendido. Si estuviera apagado, tus aparatos no recibirían dirección IP automáticamente y nada se conectaría.

Paso 9: Apaga lo que no necesitas. En la sección de WiFi avanzado o WPS, desactiva WPS si no lo usas, es ese sistema de conexión con boton o PIN de ocho digitos que tiene vulnerabilidades conocidas. En Administracion o Acceso remoto, verifica que la administracion remota, "Remote Management", este DESACTIVADA. Guarda.

Paso 10: Guarda todo y reinicia. Busca el boton Guardar o Apply en cada sección donde cambiaste algo, y al final ve a Sistema o Herramientas y elige "Reiniciar", Reboot. Espera dos o tres minutos a que el router vuelva. Vuelve a entrar al panel con tu NUEVA contraseña de admin para confirmar que todo quedo.

Paso 11: Reconecta tus aparatos. En tu teléfono y tus demas aparatos, busca tus nuevas redes CASA_2G y CASA_5G, conéctalos con la nueva contraseña y reparte: television, compu y consola a la 5G; focos, impresora y aparatos lejanos a la 2G. Prueba la velocidad con una página de test en un aparato de cada banda para comparar.

Felicidades: acabas de hacer lo que el noventa por ciento de la gente nunca hace. Tu router ya no tiene claves de fábrica, tu WiFi tiene nombre propio y contraseña decente, y cada banda esta configurada con criterio.

Ejemplo 2: Como actualizar el firmware paso a paso

Paso 1: Identifica tu modelo exacto. Está en la etiqueta del router, algo como "Archer C6 v3" o "DIR-615 T1". El "v3" o "T1" es la version de hardware y SI importa: el firmware de la version 2 no sirve para la version 3.

Paso 2: Entra al panel de administracion con tu nueva contraseña y ve a la sección Sistema, Administracion o Herramientas. Busca "Actualizacion de firmware", "Firmware Upgrade" o similar. Anota la version actual que muestra, por ejemplo:

```
Version actual de firmware: 1.0.4 Build 20240315
```

Paso 3: Revisa si hay actualizacion. Si el router tiene boton de "Buscar actualizacion" o "Check for updates", picalo y espera. Si encuentra una nueva, sigue las instrucciones en pantalla y salta al paso 6.

Paso 4: Si no hay busqueda automatica, ve a la página OFICIAL del fabricante en tu navegador. Busca tu modelo exacto más la palabra "firmware" o "descargas". Descarga el archivo correspondiente a tu version de hardware. Normalmente es un archivo .zip o .bin. Descomprime el zip si es necesario hasta tener el archivo .bin.

Paso 5: En el panel, en la sección de actualizacion de firmware, usa el boton "Examinar" o "Browse", selecciona el archivo .bin que descargaste y pica "Actualizar" o "Upgrade".

Paso 6: Espera sin tocar nada. El proceso tarda de dos a cinco minutos. El router se va a reiniciar solo. REGLA DE ORO: no lo apagues, no lo desconectes, no cierres el navegador, no toques nada. Ponte a hacer otra cosa y regresa en cinco minutos.

Paso 7: Verifica. Vuelve a entrar al panel y confirma que la version cambio:

```
Version nueva de firmware: 1.0.7 Build 20260620
```

Si la version es la nueva, listo. Si algo salio mal y el router no responde después de diez minutos, haz un reset de fábrica con el boton de RESET y vuelve a configurarlo; en casos raros habra que reinstalar el firmware por el modo de recuperacion del fabricante.

Ejemplo 3: Como hacer respaldo de tu configuración

El respaldo es una fotografia de todos tus ajustes guardada en un archivo. Si algun dia tienes que resetear el router, en vez de configurar todo de nuevo a mano, restauras el archivo y en dos minutos queda igual. Hazlo SIEMPRE después de dejar tu configuración perfecta.

Paso 1: Entra al panel de administracion y ve a Sistema, Herramientas o Administracion. Busca "Respaldo", "Backup", "Guardar configuración" o "Backup and Restore".

Paso 2: Pica el boton "Respaldar", "Backup" o "Guardar". El router va a descargar un archivo a tu computadora, normalmente con extension .bin o .cfg, algo como:

```
config-router-2026-09-19.bin
```

Paso 3: Guarda ese archivo en un lugar seguro y con nombre claro. No lo dejes en la carpeta de descargas olvidado: muevelo a una carpeta de respaldos, a una USB o a tu correo. Renombralo si quieres, por ejemplo "respaldo-router-casa-septiembre-2026.bin".

Paso 4: Para restaurarlo algun dia, en la misma sección usa el boton "Examinar", selecciona tu archivo de respaldo y pica "Restaurar" o "Restore". El router reiniciara con toda tu configuración de vuelta: SSID, contraseñas, canales, todo.

Haz un respaldo nuevo cada vez que cambies algo importante en la configuración. Te toma treinta segundos y te ahorra horas.

Práctica

Ejercicio 1: Audita la configuración actual de tu router

Objetivo: descubrir en que estado está tu router hoy, antes de cambiar nada, usando una lista de verificación.

Instrucciones: entra al panel de administracion de tu router y revisa punto por punto esta lista. Marca cada renglón como BIEN o MAL.

- [] 1. La contraseña de administrador NO es la de fábrica (admin/admin, password, 1234)
- [] 2. La administracion remota está DESACTIVADA
- [] 3. El WiFi tiene contraseña con WPA2 o WPA3 (no Abierta, no WEP)
- [] 4. La contraseña del WiFi tiene 12 caracteres o más
- [] 5. El SSID no revela datos personales (nombre completo, dirección, teléfono)
- [] 6. WPS está desactivado (si no lo usas)
- [] 7. El firmware tiene menos de un año de antigüedad
- [] 8. El canal de 2.4 GHz es 1, 6 u 11 y no esta saturado de vecinos
- [] 9. El ancho de canal en 2.4 GHz es 20 MHz
- [] 10. El router está en un lugar alto, centrado y despejado (no en el piso ni dentro de un mueble)

Solución explicada: no hay una "solución" única porque cada casa es distinta, pero así se califica. Si marcaste MAL en los puntos 1, 2 o 3, tienes un problema de SEGURIDAD urgente: corrígelo hoy mismo siguiendo el Ejemplo 1 de esta unidad, pasos 5 y 6. Si fallaste en 4 o 5, es seguridad media: cambia la contraseña y el nombre cuando puedas esta semana. Si fallaste en 7, programa la actualización de firmware del Ejemplo 2 para el fin de semana. Si fallaste en 8, 9 o 10, es rendimiento: elige canal con una app analizadora, fija el ancho en 20 MHz y mueve el router a mejor lugar; notarás la diferencia la misma noche. Cuenta tus BIEN: 9 o 10 significa router sano, 7 u 8 significa ajustes pendientes, 6 o menos significa que tu router necesita el tratamiento completo del Ejemplo 1.

Ejercicio 2: Elige un SSID adecuado para tu red

Objetivo: practicar las reglas de un buen nombre de red.

Instrucciones: estos son nombres de red reales que alguien podría poner. Clasifícalos como BUENO o MALO y explica por qué.

- a) "CASA_GARCIA_5G"
- b) "Juan Perez 555-123-4567"
- c) "TP-LINK_3F2A"
- d) "xX_DarkNet_Xx"
- e) "Calle Falsa 123 - Depto 4"
- f) "RED_FAMILIA"

Solución explicada: a) BUENO: claro, identificable, sin datos sensibles, indica la banda. b) MALO: nombre completo y teléfono gritados al aire para todo el barrio. c) MALO, pero no por seguridad sino por practicidad: es el nombre de fábrica, no sabes cuál es tu red entre las demás y la contraseña de fábrica suele ser igual de genérica. d) MALO: funciona técnicamente, pero algunos aparatos viejos se atorán con guiones bajos múltiples y mayúsculas raras; además no dice nada útil. e) MALO: tu dirección exacta anunciada a quien pase por la calle. f) BUENO: neutro, simple, sin datos personales, fácil de dictar a una visita. Regla de oro que debes memorizar: el SSID debe responder "cuál es mi red" sin responder "quién soy ni dónde vivo".

Ejercicio 3: Plan de canales para tu edificio

Objetivo: elegir el mejor canal de 2.4 GHz usando datos reales de tu entorno.

Instrucciones: instala en tu teléfono una aplicación gratuita de análisis WiFi, como WiFi Analyzer en Android. Parate en el centro de tu casa, abre la app y anota cuántas redes ves en

cada canal del 1 al 11. Luego responde: cuál de los canales 1, 6 u 11 tiene menos redes encima? Ese es tu canal ideal.

Ejemplo de anotacion:

```
Canal 1: 2 redes vecinas  
Canal 6: 7 redes vecinas  
Canal 11: 3 redes vecinas
```

Solución explicada: con esos datos de ejemplo, el canal ideal es el 1, porque es uno de los tres que no se enciman, 1, 6 y 11, y es el que menos vecinos tiene. El 6 esta saturadisimo con siete redes: ahí ni te pares. El 11 es segunda opcion aceptable. Ojo con la trampa: si ves que el canal 3 tiene solo una red, NO lo elijas, porque el canal 3 se enciman con el 1 y con el 6, así que en realidad pelea con las redes de ambos. Solo 1, 6 y 11 son seguros en 2.4 GHz. Una vez elegido, entra al panel, ve a la configuración inalámbrica de 2.4 GHz y fija el canal a mano. Repite este analisis cada tres o cuatro meses, porque los vecinos cambian equipos y encienden redes nuevas.

Ejercicio 4: Decide la potencia de transmision ideal para tu casa

Objetivo: aplicar el criterio de "la menor potencia que funcione bien".

Instrucciones: responde estas preguntas sobre tu casa y deduce el ajuste.

1. Cuantos metros cuadrados tiene tu casa o departamento? (chico: menos de 70, mediano: 70-150, grande: mas de 150)
2. Donde esta el router? (centrado / en un extremo / en el piso dentro de un mueble)
3. Tienes vecinos pegados con sus propios WiFi? (si / no)
4. Necesitas que el WiFi llegue al patio, al jardín o a la planta alta? (si / no)

Solución explicada: caso típico A, departamento chico, router centrado, vecinos pegados, sin patio: pon la potencia en MEDIA o al 60 por ciento. Tu casa se cubre perfecto, generas menos interferencia y tu señal no sale a la calle. Caso típico B, casa grande, router en un extremo porque ahí entra el cable, necesitas llegar a la planta alta: potencia ALTA, al cien por ciento, y considera mover el router a un lugar más centrado si el cable lo permite. Caso típico C, casa mediana, router en un extremo, vecinos pegados: primero intenta MEDIA y haz pruebas de velocidad en el cuarto más lejano; si la velocidad es buena, dejalo en MEDIA; si se cae, sube a ALTA. El metodo científico casero: prueba una semana en cada nivel y quedate con el más bajo que te de buena velocidad en todos tus rincones. Recuerda: más potencia no es más velocidad, es más alcance con más interferencia.

Ejercicio 5: Simula una emergencia: restauracion desde el respaldo

Objetivo: comprobar que tu respaldo de configuración realmente sirve, antes de necesitarlo de verdad.

Instrucciones: este ejercicio es de pensamiento, no toques nada todavía. Imagina que mañana tu router amanece loco: se reinicio solo y perdio toda la configuración. Responde por escrito: dónde está guardado tu archivo de respaldo? Cómo se llama? Cuáles son los pasos para restaurarlo? Cuánto tiempo te tomaría?

Solución explicada: si no tienes archivo de respaldo, tu respuesta honesta es "no tengo", y la accion es ir HOY al Ejemplo 3 y crear uno: te toma dos minutos. Si si tienes, verifica estos tres puntos. Uno: el archivo existe y sabes dónde está, no en "descargas" entre cien archivos, sino en una carpeta de respaldos o una USB con nombre claro como "respaldo-router-casa-2026.bin". Dos: el respaldo es reciente, de después de tu última configuración buena; un respaldo de hace dos años con la contraseña vieja te va a confundir más que ayudar. Tres: sabes los pasos de memoria: entrar al panel, ir a Sistema o Herramientas, sección Respaldo, Examinar, seleccionar el archivo, Restaurar, esperar el reinicio. Si puedes recitar eso sin leer, estas preparado. Una emergencia ensayada en la cabeza es una emergencia resuelta en cinco minutos en la vida real.

Ejercicio 6: Detecta al intruso con la lista de aparatos conectados

Objetivo: aprender a revisar quién está usando tu red.

Instrucciones: entra al panel de tu router y busca la sección "Clientes", "Dispositivos conectados", "Attached Devices" o "DHCP Clients". Ahí veras una lista con los nombres y direcciones IP de todo lo conectado. Cuenta cuántos aparatos reconoces y comparalos con los que deberían estar: tus teléfonos, tu compu, tu tele, tus focos inteligentes. Anota cualquier aparato que no reconozcas.

Solución explicada: primero, no entres en panico si ves nombres raros: muchos aparatos se anuncian con nombres de fábrica crípticos como "Espressif" que es un foco inteligente, o "Amazon" que es una bocina. Apaga tus aparatos uno por uno y ve cuál desaparece de la lista para identificarlos, o busca la dirección MAC del aparato en sus ajustes y comparala. Si después de identificar todo sigue habiendo un aparato desconocido conectado, haz esto en orden: uno, cambia INMEDIATAMENTE la contraseña del WiFi por una larga nueva; dos, cambia la contraseña del administrador si no lo hiciste; tres, revisa que la seguridad sea WPA2 o WPA3 y no WEP; cuatro, desactiva WPS. Al cambiar la contraseña del WiFi, el intruso queda fuera y tendrás que reconectar tus aparatos con la nueva clave, es molesto pero necesario. Haz esta revision una vez al mes: te toma tres minutos y es la mejor alarma contra vecinos colgados.

Resumen de la unidad

- El router es el director de orquesta de tu red: no crea el internet, lo reparte entre tus aparatos cientos de veces por segundo.
- Módem traduce la señal del proveedor, router reparte el internet en tu casa, punto de acceso crea el WiFi; tu "router WiFi" casero hace las tres cosas.
- Por dentro el router es una computadora: CPU que decide rutas, RAM que es su mesa de trabajo, flash que guarda configuración y firmware, puertos WAN para la entrada de internet y LAN para tus aparatos cableados.
- Las luces del panel frontal son tu tablero: POWER, INTERNET/WAN, WIFI, LAN y WPS te dicen en segundos dónde está un problema.
- NAT permite que todos tus aparatos compartan una sola IP publica; DHCP les reparte direcciones privadas automaticamente; la puerta de enlace, 192.168.1.1 o 192.168.0.1, es la dirección de tu router y del panel de administracion.
- El firmware es el sistema operativo del router: revisa actualizaciones cada tres o cuatro meses, nunca lo apagues a media actualizacion y descarga solo del sitio oficial.
- La primera tarea de seguridad es cambiar la contraseña de administrador de fábrica: las credenciales por defecto son publicas y cualquiera las encuentra en internet.
- El SSID es el nombre de tu red: que sea reconocible, sin datos personales y sin caracteres raros; deja el broadcast encendido y protege con contraseña fuerte.
- Usa WPA2 o WPA3, nunca WEP ni red abierta para tu red principal; la contraseña del WiFi debe tener mínimo doce caracteres, ideal veinte.

- Banda dual: 5 GHz para aparatos cercanos que necesitan velocidad, 2.4 GHz para aparatos lejanos o sencillos; empieza con nombres separados y prueba el band steering después.
- En 2.4 GHz usa solo los canales 1, 6 u 11, el más libre segun un analisis con app; en 5 GHz hay espacio de sobra y el automatico funciona bien.
- Ancho de canal: 20 MHz en 2.4 GHz para estabilidad, 40 u 80 MHz en 5 GHz para velocidad.
- Potencia de transmision: usa la menor que cubra bien tu casa; en departamentos chicos con vecinos pegados, bajala a media en vez de gritar al máximo.
- Errores que ya no vas a cometer: claves de fábrica, router en el piso dentro del mueble, WiFi abierto o débil, nunca reiniciar, repetidores baratos sin criterio, firmware abandonado.
- Rutina de dueño responsable: claves cambiadas, buen lugar fisico, canal elegido, firmware al dia, reinicio mensual y respaldo de configuración guardado.

UNIDAD 5: Seguridad inalámbrica (Clases 13 a 15)

Tu red WiFi es la puerta de tu casa digital. Y aquí viene el problema que casi nadie entiende al principio: esa puerta no está en tu pared, está en el aire. Las ondas de tu router atraviesan muros, ventanas y techos, y llegan a la casa del vecino, a la banqueta de enfrente y a veces hasta dos o tres cuerdas más allá. Todo lo que viaja por esas ondas - tus contraseñas, tus fotos, tus mensajes, los datos de tu tarjeta cuando compras en línea - flota en el aire a tu alrededor. La única cosa que separa a un desconocido de todo eso es la seguridad inalámbrica: el candado, la chapa y la alarma de tu casa digital.

Piensa en esto con calma. Cuando conectas tu celular a tu WiFi y entras a tu banco, esa información no viaja por un cable escondido bajo la tierra que solo tú puedes tocar. Viaja por radio, como la señal de una estación de música, y cualquier persona con una laptop y el programa adecuado puede "escuchar" esas ondas desde la calle. Si tu red no está bien protegida, es como si tuvieras una conversación privada a gritos en la banqueta: cualquiera que pase puede oírlo. Y no estamos hablando de espías de película. Estamos hablando del vecino que no quiere pagar internet, del muchacho curioso de la cuadra que vio un tutorial en YouTube, o del desconocido que se sienta en un café con una laptop y se dedica a robar contraseñas de las redes abiertas de la zona.

Los riesgos son muy reales y muy cercanos. El primero es el más común: el vecino colgado. Alguien adivina o rompe tu contraseña débil y se conecta a tu red. Al principio parece inofensivo - "total, nomás me roba un poquito de internet" - pero no es así. Esa persona está dentro de tu red, que es lo mismo que estar dentro de tu casa. Puede ver tus dispositivos, puede intentar entrar a tu computadora, puede ver qué páginas visitas. Y hay algo peor: todo lo que esa persona haga en internet usando tu conexión queda registrado con tu dirección IP, que es como la placa de tu casa en internet. Si esa persona descarga contenido ilegal, hace fraude o acosa a alguien desde tu red, la primera puerta que van a tocar las autoridades es la tuya. Tú tendrás que demostrar que no fuiste tú. ¿De verdad quieres ese problema por no haber puesto una buena contraseña?

El segundo riesgo es el robo de datos. En una red mal protegida, un atacante puede interceptar la información que viaja sin cifrar: nombres de usuario, contraseñas de redes sociales, mensajes, correos. Hoy muchas páginas usan cifrado propio (el candadito del navegador), pero no todas las aplicaciones lo hacen bien, y hay técnicas para engañar a tu dispositivo y quitarle esa protección. Un atacante paciente en una red abierta de un café puede recolectar datos de decenas de personas en una tarde.

El tercer riesgo es para los negocios. Si tienes una tiendita, un café, una barbería o cualquier negocio y ofreces WiFi a tus clientes sin separarlo de tu red privada, estás regalando la llave de tu caja registradora digital. Un cliente malintencionado podría espiar la computadora donde llevas tus cuentas, o usar tu red para actividades ilegales que te meterían en problemas a ti. Por eso en esta unidad vas a aprender también sobre redes de invitados y aislamiento: cómo darle internet a tus clientes sin darles acceso a tus cosas.

Ahora, la buena noticia: proteger tu red WiFi no es difícil ni caro. No necesitas ser hacker ni comprar aparatos especiales. El 95 por ciento de la seguridad de una red casera se logra con cinco acciones que cualquiera puede hacer en una tarde: usar el tipo de seguridad correcto (WPA2 o WPA3), poner una contraseña larga y fuerte, desactivar una función peligrosa llamada WPS, mantener actualizado el router y revisar de vez en cuando quién está conectado. Eso es todo. Esta unidad te va a enseñar exactamente cómo hacer cada una de esas cosas, pero más importante: te va a enseñar por qué funcionan, para que nadie te pueda chamear con mitos como "esconde el nombre de tu red y ya estás seguro" o "el filtrado MAC es suficiente".

Al terminar esta unidad vas a lograr varias cosas concretas. Primero, vas a entender qué es el cifrado y cómo protege tus datos, con analogías tan claras que podrás explicárselo a tu familia. Segundo, vas a conocer la historia completa de la seguridad WiFi: qué fue WEP y por qué está muerto, qué aportó WPA, por qué WPA2 fue el estándar durante más de una década y qué trae de nuevo WPA3. Tercero, vas a saber crear contraseñas fuertes que sí puedas recordar, sin anotarlas en un papel pegado al monitor. Cuarto, vas a saber configurar tu router paso a paso: activar el mejor modo de seguridad, apagar WPS, crear una red de invitados y revisar los dispositivos conectados. Y quinto, vas a tener una lista de verificación de seguridad que podrás aplicar a tu casa, a la casa de tus papás y a tu negocio.

La unidad está organizada en tres clases, igual que en el curso en video de la academia. La Clase 13 es la historia: WEP, WPA y WPA2. Vas a ver cómo nació la seguridad WiFi, por qué el primer intento (WEP) fue un fracaso total y qué aprendió la industria de ese fracaso. Entender esta historia no es curiosidad: es lo que te permite reconocer cuándo un router viejo o una mala configuración te está dejando con la seguridad de hace veinte años. La Clase 14 es el presente y el futuro: WPA3, el cifrado AES, el nuevo método de conexión llamado SAE y las redes abiertas mejoradas (OWE) que protegen hasta el WiFi gratis del café. Y la Clase 15 es la práctica pura: contraseñas fuertes de verdad, WPS y por qué debes desactivarlo, la verdad sobre el filtrado MAC y tu lista de verificación final.

Un aviso importante sobre el enfoque de esta unidad: aquí aprendemos a proteger, no a atacar. Vas a leer sobre cómo funcionan algunos ataques - diccionario, fuerza bruta, KRACK - pero siempre desde el lado defensivo: para que entiendas qué estás evitando y por qué cada

medida de protección existe. No vas a encontrar instrucciones para romper redes ajenas, porque además de ser ilegal, no es lo que necesita un principiante que quiere cuidar su casa y su negocio. El conocimiento de esta unidad es para que seas el dueño responsable de tu red, no el dolor de cabeza del vecino.

Antes de entrar a la teoría, hagamos un trato. Cuando termines de leer la explicación detallada, no te quedes solo con la teoría: haz los ejemplos paso a paso con tu router a la mano. Abre la configuración de tu router mientras lees, revisa qué modo de seguridad tienes activado hoy y anota qué vas a cambiar. La seguridad se aprende haciendo. Y cuando llegues a la práctica, tómate los ejercicios en serio: la auditoría de tu propia red, que es el primer ejercicio, vale más que diez capítulos leídos sin aplicar.

Empecemos por lo más importante: entender qué significa realmente "proteger" una red inalámbrica. Porque hay una diferencia enorme entre sentirte seguro y estar seguro, y esta unidad existe para que nunca más confundas una cosa con la otra.

Explicación detallada

Tu red WiFi es tu casa: la analogía que lo explica todo

Imagina tu casa. Tiene paredes, tiene una puerta y esa puerta tiene una chapa. La chapa no hace que tu casa sea imposible de robar - un ladrón profesional con herramientas podría forzarla - pero cumple dos funciones importantísimas: le dice al vecino honesto "aquí no entres sin permiso" y le pone el trabajo tan difícil al ladrón oportunista que mejor se va a buscar otra casa más fácil. Tu contraseña WiFi es exactamente esa chapa.

Ahora imagina que tu casa, en lugar de paredes de ladrillo, tuviera paredes de vidrio transparente, y que todo lo que hablas adentro se escuchara en la calle. Esa es una red WiFi sin cifrado: todo el mundo ve y oye. El cifrado es como convertir esas paredes de vidrio en paredes de ladrillo y como hablar en un idioma secreto que solo tu familia entiende. Aunque alguien pegue el oído a la pared, solo escucha ruido sin sentido.

Vamos a desarmar esta analogía porque te va a servir para todo el resto de la unidad. La contraseña WiFi es la chapa de la puerta: controla quién entra a tu red. El tipo de seguridad (WEP, WPA, WPA2, WPA3) es la calidad de esa chapa: una chapa de juguete se abre con un clip, una chapa buena necesita taladro y mucho tiempo. El cifrado es el idioma secreto: aunque alguien escuche desde afuera, no entiende nada. Y el router es la casa misma: si no le das mantenimiento (actualizaciones), se le caen las paredes solas.

Hay una pregunta que todo principiante se hace y que vale la pena responder desde ahorita: si pongo una contraseña larguísima, ¿ya estoy 100 por ciento seguro? La respuesta honesta es no, nadie está 100 por ciento seguro en nada que tenga que ver con computadoras. Pero la seguridad no se trata de ser invencible, se trata de ser un objetivo caro. Los atacantes, igual que los ladrones de casas, buscan lo fácil. Una red con WPA3 y contraseña fuerte es como una casa con buena chapa, rejas y alarma en una calle donde hay casas con la puerta abierta: el ladrón ni siquiera la voltea a ver. Tu meta en esta unidad no es la perfección imposible, es dejar de ser el objetivo fácil.

Qué es el cifrado: hablar en clave

De niños, muchos jugamos a hablar en clave: cambiar cada letra por la siguiente del abecedario, de modo que "HOLA" se vuelve "IPMB". Quien no conoce la regla solo ve letras sin sentido; quien sí la conoce, descifra el mensaje en segundos. El cifrado moderno es la versión profesional y matemática de ese juego.

Cuando tu celular se conecta a tu router con WPA2 o WPA3, los dos aparatos acuerdan una clave secreta y a partir de ese momento todo lo que se mandan va "hablado en clave". Si alguien intercepta esas ondas con una antena desde la calle, lo único que captura es un montón de datos revueltos que parecen ruido. Sin la clave, esos datos no sirven para nada. Con la clave correcta, tu celular y tu router los ordenan al instante y todo funciona normal, sin que tú notes nada.

Fíjate en algo importante: el cifrado no esconde que estás transmitiendo. Un atacante con el equipo adecuado puede ver que hay una red WiFi en tu casa, puede ver cuántos datos mandas y a qué horas, más o menos como un espía que ve pasar camiones cerrados frente a tu casa: sabe que algo se mueve, pero no sabe qué llevan adentro. Lo que el cifrado sí protege es el contenido: tus contraseñas, tus mensajes, tus fotos. Por eso el cifrado es la base de todo lo demás en esta unidad.

Hay dos palabras que vas a ver muchísimo cuando hables de cifrado WiFi: algoritmo y clave. El algoritmo es la receta, el método matemático para revolver los datos. La clave es el ingrediente secreto que hace que tu revoltura sea única. Un algoritmo puede ser público - de hecho, los mejores algoritmos son públicos, porque miles de expertos los han revisado buscando fallas - y aun así ser seguro, porque la seguridad está en la clave, no en esconder la receta. Tu contraseña WiFi sirve, entre otras cosas, para generar esas claves de cifrado. Por eso una contraseña débil arruina hasta el mejor algoritmo: es como tener una caja fuerte carísima y dejarle puesta la combinación "1-2-3-4".

Otro concepto que necesitas desde ya: autenticación. Autenticar es comprobar identidad: cuando escribes tu contraseña WiFi en tu celular, le estás demostrando al router "soy alguien autorizado a entrar". El router, a su vez, le demuestra a tu celular "soy tu router de verdad, no un impostor". Esa comprobación mutua es parte de lo que hacen los protocolos modernos, y es lo que evita que te conectes sin darte cuenta a una red falsa creada por un atacante para robarte datos. Autenticación responde "¿quién eres?", cifrado responde "que nadie más entienda lo que decimos". Necesitas las dos cosas.

Clase 13: WEP, el candado de papel

La historia de la seguridad WiFi empieza en 1997, cuando se creó el primer estándar de redes inalámbricas. La gente ya intuía el problema: si los datos viajan por el aire, cualquiera los puede escuchar. Así que al estándar le agregaron un sistema de protección llamado WEP, siglas de Wired Equivalent Privacy, que en español sería algo así como "privacidad equivalente a la del cable". La idea sonaba bien: hacer que una red inalámbrica fuera tan privada como una red con cables, donde para espiar tendrías que cortar físicamente el cable.

WEP usaba un algoritmo de cifrado llamado RC4 con una clave que podía ser de 64 o de 128 bits. En 1997 eso sonaba razonable. El problema es que WEP tenía errores de diseño tan graves que hoy los libros lo ponen como ejemplo de cómo NO diseñar seguridad. El más famoso fue el manejo de algo llamado vector de inicialización, o IV. Sin meternos a matemáticas, la idea es esta: para que el cifrado sea seguro, cada paquete de datos debe revolverse de forma ligeramente distinta, y el IV era el ingrediente que cambiaba en cada paquete. Pero en WEP el IV era muy cortito - solo 24 bits - lo que significa que se repetía rapidísimo, cada pocos miles de paquetes. En una red con tráfico normal, los IV se empezaban a repetir en minutos.

¿Por qué es grave que se repita? Vuelve al juego de hablar en clave de la infancia. Imagina que usas la misma regla para cifrar dos mensajes distintos y un espía intercepta los dos mensajes cifrados. Comparándolos, el espía puede deducir la regla sin conocerla. Con WEP pasaba exactamente eso: un atacante solo tenía que quedarse escuchando tu red unos minutos, juntar suficientes paquetes con IV repetidos y con matemáticas relativamente simples recuperaba tu clave. A principios de los 2000 salieron programas gratuitos que automatizaban todo el ataque: los ejecutabas, esperabas entre 5 y 15 minutos, y el programa te escupía la contraseña de la red WEP. Así de roto estaba.

Para 2001, investigadores ya habían publicado los ataques. Para 2004, romper WEP era un ejercicio de tarea en cursos de seguridad. Y sin embargo - y esto es lo increíble - durante años hubo millones de routers con WEP activado por defecto, y todavía hoy, en 2026, te puedes encontrar algún router viejísimo o alguna impresora antigua configurada con WEP. La lección

de WEP es brutal y clara: un sistema de seguridad con errores de diseño no te protege aunque uses la contraseña más larga del mundo. La chapa puede ser gruesa, pero si está instalada al revés, se abre con un empujón.

WEP está muerto. No "un poco inseguro", no "mejor que nada": muerto. Si en tu router ves una opción que dice WEP, ni la voltees a ver. Si tienes un aparato tan viejo que solo soporta WEP, ese aparato es un riesgo para tu red y deberías pensar en reemplazarlo o aislarlo. En esta unidad lo estudiamos por historia y para que entiendas de dónde vienen los protocolos modernos, no porque vayas a usarlo jamás.

WPA: el parche de emergencia

Cuando WEP se vino abajo, la industria entró en pánico. Había millones de routers y tarjetas WiFi vendidos que solo sabían hablar WEP, y no se podía esperar años a diseñar un estándar nuevo desde cero. Así que en 2003 se sacó un remedio temporal: WPA, WiFi Protected Access. La palabra clave aquí es "temporal": WPA nació como un parche para aguantar mientras se terminaba el estándar definitivo.

El cambio más importante de WPA fue reemplazar la forma de cifrar. En lugar del RC4 mal usado de WEP, WPA introdujo TKIP, siglas de Temporal Key Integrity Protocol. TKIP seguía usando RC4 por dentro - porque tenía que funcionar en los aparatos viejos que no podían con matemáticas más pesadas - pero lo usaba de forma mucho más inteligente: generaba una clave distinta para cada paquete de datos, mezclaba mejor los ingredientes y agregaba una verificación de integridad, es decir, una forma de detectar si alguien había modificado un paquete en el camino. Era como seguir usando el mismo candado barato pero cambiar la combinación cada cinco segundos y ponerle un sello que se rompe si alguien lo manipula.

WPA también introdujo algo que usamos hasta hoy: los dos modos de autenticación. El modo personal, llamado WPA-PSK (Pre-Shared Key, clave precompartida), es el de las casas y negocios pequeños: todos los dispositivos usan la misma contraseña, la que tú configuras en el router. El modo empresarial, WPA-Enterprise, usa un servidor especial (un servidor RADIUS) donde cada usuario tiene su propio nombre de usuario y contraseña, y es lo que usan las empresas grandes y las universidades. En esta unidad nos enfocamos en el modo personal, que es el que vas a configurar en tu casa, pero es bueno que sepas que existe el otro.

WPA cumplió su misión: fue mucho mejor que WEP y le dio a la industria el respiro que necesitaba. Pero como todo parche, tenía fecha de caducidad. Al estar construido sobre RC4, heredó algunas debilidades, y con los años los investigadores encontraron ataques que, aunque más difíciles que los de WEP, demostraban que TKIP tampoco era el futuro. WPA fue el puente, no el destino.

WPA2: el estándar serio (y el cifrado AES)

En 2004 llegó el estándar definitivo que WPA había estado esperando: WPA2. Y con él llegó el cambio más importante en la historia de la seguridad WiFi: el cifrado AES con el modo CCMP. Si WEP era un candado de papel y WPA un parche, WPA2 fue la primera chapa de verdad.

AES son las siglas de Advanced Encryption Standard, Estándar de Cifrado Avanzado. Es un algoritmo adoptado por el gobierno de Estados Unidos después de un concurso público donde los mejores criptógrafos del mundo intentaron romper a los candidatos durante años. AES ganó porque es rápido, elegante y, hasta hoy, nadie ha encontrado una forma práctica de romperlo cuando se usa bien. Lo usan los bancos, los ejércitos y las agencias de gobierno para proteger secretos de estado. Y desde 2004, también lo usa tu router para proteger tus fotos de vacaciones. CCMP es el "modo de operación", es decir, la forma específica en que WPA2 aplica AES a los paquetes WiFi, incluyendo verificación de integridad para detectar manipulaciones.

Aquí conviene detenerse en la comparación que más vas a necesitar: TKIP contra AES/CCMP. TKIP fue el parche temporal de WPA, construido sobre el viejo RC4, diseñado para funcionar en hardware viejo y con debilidades conocidas que se fueron acumulando con los años. AES/CCMP es el cifrado moderno, rápido incluso en aparatos modestos actuales, sin debilidades prácticas conocidas, y el recomendado por todos los expertos desde hace casi veinte años. La regla es simple y no tiene excepciones: en tu router, siempre elige la opción que diga AES (o "WPA2-AES", o "WPA2-PSK AES"), nunca la que diga TKIP. Muchos routers ofrecen una opción mixta "WPA/WPA2" o "TKIP+AES" para compatibilidad con aparatos viejísimos; evítala si puedes, porque esa compatibilidad baja la seguridad de toda tu red al nivel del eslabón más débil. Si tienes un aparato tan viejo que solo funciona con TKIP, el problema no es la configuración: el problema es el aparato.

WPA2 reinó durante más de una década como el estándar de seguridad WiFi en todo el mundo. Y funcionó muy bien. Pero en 2017 la comunidad de seguridad se llevó un susto mayúsculo con un ataque llamado KRACK, que demostró que hasta los buenos diseños pueden tener detalles mal implementados.

El apretón de manos de 4 vías (4-way handshake)

Antes de entender KRACK, necesitas entender una de las piezas más elegantes de WPA2: el apretón de manos de 4 vías, o 4-way handshake. Es el ritual que hacen tu celular y tu router cada vez que te conectas, y dura una fracción de segundo.

Imagina que llegas a una fiesta donde solo entran invitados, y en la puerta hay un guardia. Tú no le gritas tu contraseña a todo el salón - eso la oiría cualquiera. En su lugar, hacen un jueguito de preguntas y respuestas con el que ambos demuestran que conocen el secreto sin decirlo en voz alta. Eso, en esencia, es el handshake.

Técnicamente funciona así, en cuatro mensajes. Primer mensaje: el router le manda a tu celular un número aleatorio, como un reto. Segundo mensaje: tu celular responde con su propio número aleatorio más una prueba matemática de que conoce la contraseña, sin revelar la contraseña. Tercer mensaje: el router confirma que todo cuadra y le entrega a tu celular la clave que se usará para cifrar el tráfico, protegida para que solo tu celular la pueda leer. Cuarto mensaje: tu celular confirma "recibido, ya puedo hablar en clave". A partir de ahí, todo el tráfico va cifrado con claves de sesión únicas que se generan en ese momento.

Fíjate en lo inteligente del diseño: tu contraseña WiFi nunca viaja por el aire, ni siquiera cifrada. Lo que viaja son retos, respuestas y pruebas matemáticas. Un espía que grabe todo el handshake no obtiene tu contraseña directamente. Esa es la teoría, y es buena teoría. El problema vino por un detalle de implementación que nadie había notado en trece años.

El ataque KRACK explicado simple

KRACK son las siglas de Key Reinstallation Attack, ataque de reinstalación de clave. Lo descubrió el investigador Mathy Vanhoef en 2017 y afectaba en teoría a casi todos los dispositivos WiFi del planeta. Pero ojo: entender KRACK te va a servir para entender por qué las actualizaciones importan tanto.

El truco de KRACK aprovechaba el tercer mensaje del handshake. En algunas situaciones - por ejemplo, si el mensaje se perdía por interferencia - el router reenviaba ese tercer mensaje, y el dispositivo, al recibirlo de nuevo, reinstalaba la misma clave de cifrado que ya había instalado. ¿Y cuál es el problema de reinstalar la misma clave? Que al hacerlo se reiniciaba también un contador interno que garantiza que cada paquete se cifre de forma única. Es como si en el juego de hablar en clave empezaras a reusar la misma página del libro de códigos: un espía que junta suficientes mensajes puede empezar a descifrarlos.

En la práctica, KRACK permitía a un atacante cercano interceptar y descifrar parte del tráfico de la víctima, sobre todo en dispositivos que no habían sido actualizados. Fue un escándalo porque no era culpa de los usuarios: era un defecto del estándar mismo, presente desde 2004.

Pero aquí viene la parte que te toca a ti como dueño de tu red. KRACK se arregló con actualizaciones de software. Los fabricantes sacaron parches en semanas. Trece años de WPA2 sólido contra un defecto que se corrigió actualizando. La moraleja no es "WPA2 no sirve" - la moraleja es "actualiza tus aparatos". Un router con el firmware de 2016, sin parches, es vulnerable a KRACK; el mismo router actualizado, no. Por eso en la lista de verificación de esta unidad vas a ver "mantén actualizado el firmware del router" como una de las medidas principales. La seguridad no es algo que configuras una vez y olvidas: es un mantenimiento, como cambiarle el aceite al carro.

KRACK también aceleró la llegada de WPA3, porque demostró que incluso un buen protocolo envejece y que hacía falta un diseño nuevo con protecciones adicionales. Y eso nos lleva a la Clase 14.

Clase 14: WPA3, el nuevo estándar

WPA3 se anunció en 2018 como el sucesor de WPA2. No fue una revolución que volviera obsoleto todo lo anterior de la noche a la mañana - WPA2 bien configurado y actualizado sigue siendo seguro - sino una evolución que cierra las debilidades conocidas y agrega protecciones que antes no existían. Piensa en WPA3 como la chapa nueva con features que la chapa anterior no tenía: protege contra ganzúas modernas, avisa si alguien la manipula y es más cómoda de usar.

El cambio más importante de WPA3 tiene un nombre técnico: SAE, Simultaneous Authentication of Equals, autenticación simultánea de iguales. SAE reemplaza al apretón de manos de 4 vías de WPA2 en el modo personal. ¿Y qué tiene de especial? Dos cosas enormes.

La primera se llama secreto hacia adelante, o forward secrecy. En WPA2, si un atacante graba todo tu tráfico cifrado hoy y dentro de dos años logra adivinar tu contraseña, puede descifrar retroactivamente todo lo que grabó. Es como si alguien grabara tus conversaciones en clave y años después consiguiera el libro de códigos: de pronto entiende todo el pasado. Con SAE, cada conexión genera claves únicas e independientes: aunque el atacante consiga tu contraseña después, no puede descifrar el tráfico viejo. El pasado queda protegido para siempre. Esta es una mejora gigantesca que casi nadie nota, pero que a los expertos les encanta.

La segunda mejora de SAE es la protección contra ataques de diccionario. Para entenderla necesitas saber primero qué son esos ataques, así que hagamos una pausa para eso.

Ataques de diccionario y fuerza bruta: cómo se adivinan las contraseñas

Hay dos formas básicas de adivinar una contraseña sin saberla. La fuerza bruta es probar todas las combinaciones posibles: a, b, c... aa, ab, ac... hasta dar con la correcta. Es como intentar abrir una combinación probando todos los números: garantizado que funciona, pero puede tardar siglos si la contraseña es larga. El ataque de diccionario es más listo: en lugar de probar todo, prueba primero las contraseñas que la gente realmente usa. Existe una lista tristemente famosa de las contraseñas más comunes del mundo: "12345678", "password", "qwerty", el nombre de la compañía de internet, el nombre del equipo de fútbol favorito. Un atacante prueba esa lista - que puede tener millones de entradas - a toda velocidad con un programa.

Aquí está el dato que te tiene que quedar grabado: con WPA2, un atacante puede capturar el handshake de tu red (esos cuatro mensajitos de los que hablamos) y luego irse a su casa a probar contraseñas contra esa captura a toda velocidad, sin que tú te enteres, sin límite de intentos, usando computadoras potentes. Si tu contraseña es "12345678" o el nombre de tu perro, cae en segundos o minutos. Si es una contraseña fuerte y larga, el atacante puede intentarlo hasta el fin de los tiempos sin éxito.

SAE, el sistema nuevo de WPA3, cambia las reglas: obliga a que cada intento de adivinanza sea una conversación en vivo con el router, y el router puede detectar y frenar los intentos repetidos. Es la diferencia entre un ladrón que se lleva una foto de tu chapa a su casa para fabricar una llave con calma, y un ladrón que tiene que estar físicamente en tu puerta probando llaves mientras tú lo ves por la mirilla. Por eso WPA3 protege mucho mejor las contraseñas débiles que WPA2: aunque tu contraseña no sea perfecta, SAE le pone el trabajo muchísimo más difícil al atacante.

Ojo, que esto no significa que con WPA3 puedas poner "12345678" y dormir tranquilo. Significa que tienes un mejor colchón de seguridad, no que puedas tirarte del techo. La contraseña fuerte sigue siendo obligatoria, y en la Clase 15 vas a aprender a crearlas.

SAE contra PSK: ¿qué cambia para ti?

En la práctica, cuando configures un router moderno vas a ver opciones como "WPA2-PSK", "WPA3-SAE" o "WPA2/WPA3 transicional". El modo transicional es un modo de compatibilidad: acepta dispositivos nuevos con WPA3 y dispositivos viejos con WPA2 al mismo tiempo. Es útil durante la transición, porque todavía hay aparatos - impresoras viejas, focos inteligentes baratos, consolas de hace años - que no saben hablar WPA3.

La recomendación práctica es esta. Si todos tus dispositivos son más o menos recientes (de los últimos seis o siete años), usa WPA3 puro. Si tienes algún aparato viejo que lo necesita, usa el modo transicional WPA2/WPA3, pero con AES en ambos. Y nunca, por ningún motivo, bajes a WPA o a modos mixtos con TKIP solo para revivir un aparato del 2008: mejor reemplaza el aparato. Tu red es tan segura como su configuración más débil.

Otra mejora de WPA3 que vale la pena conocer se llama PMF, Protected Management Frames, tramas de gestión protegidas. Suena técnico, pero la idea es simple: antes, ciertos mensajes de control de la red - como los que le dicen a tu celular "desconéctate" - viajaban sin protección, y un atacante podía falsificarlos para sacarte de tu red a cada rato (un ataque de denegación de servicio casero y molesto). PMF cifra también esos mensajes de control. En WPA3, PMF es obligatorio; en WPA2 era opcional y casi nadie lo activaba. Es un detalle, pero es el tipo de detalle que separa a un protocolo moderno de uno viejo.

OWE: seguridad hasta en el WiFi gratis

Hay un problema que ni WPA2 ni WPA3 podían resolver: las redes abiertas. El WiFi gratis del café, del aeropuerto, del parque. Esas redes no tienen contraseña, así que no hay nada que cifrar con una clave compartida: todo viaja abierto y cualquiera puede espiar. Durante años la recomendación fue "no hagas nada importante en redes abiertas", y seguía siendo un problema enorme porque la gente las usa igual.

OWE, Opportunistic Wireless Encryption (cifrado inalámbrico oportunista), es la respuesta de WPA3 a ese problema. Con OWE, aunque la red no tenga contraseña, tu dispositivo y el punto de acceso negocian automáticamente un cifrado único para tu conexión, sin que tengas que hacer nada. Cada usuario tiene su propio "idioma secreto" con el router, aunque todos estén en la misma red abierta. Un espía en el café ya no puede leer tu tráfico tan fácil como antes.

¿OWE hace que el WiFi del café sea totalmente seguro? No. Sigue siendo una red pública: otros usuarios están en la misma red y hay ataques posibles, y siempre es buena idea usar una VPN en redes públicas si manejas cosas delicadas. Pero OWE convierte una red abierta de "todo el mundo puede leer todo" a "cada conexión va cifrada por separado", que es un salto gigantesco. Cuando veas en tu celular una red abierta que dice algo como "segura" o con un candadito, probablemente está usando OWE. Úsala con más confianza que una red abierta tradicional, pero mantén la prudencia de siempre en lugares públicos.

Clase 15: la contraseña es la chapa (y cómo poner una buena)

Volvamos a la analogía de la casa, porque aquí es donde más duele. Puedes tener la mejor chapa del mundo - WPA3, AES, SAE, todo lo moderno - pero si la combinación es "1234", da igual. La contraseña WiFi es lo único que se interpone entre tu red y el vecino curioso con un programa de diccionario. Y aquí viene una verdad incómoda: la mayoría de las redes que son vulneradas no caen por ataques sofisticados de película, caen por contraseñas malas. "12345678". El nombre de la compañía de internet. La dirección de la casa. El nombre del perro más el año de nacimiento.

¿Por qué la gente pone contraseñas malas? Por la misma razón por la que deja la llave bajo el tapete: comodidad y miedo a olvidar. "Es que si la pongo difícil luego no me acuerdo". "Es que cada que viene visita tengo que dictársela". Son preocupaciones reales, y por eso en los ejemplos paso a paso de esta unidad vas a aprender un método para crear contraseñas fuertes que sí se pueden recordar. Pero primero entiende qué hace fuerte a una contraseña, porque hay muchos mitos.

Mito uno: "con ocho caracteres basta". El mínimo técnico de WPA2/WPA3 es 8 caracteres, pero 8 caracteres ya no son suficientes contra un atacante moderno con una buena computadora. Cada carácter extra multiplica el trabajo del atacante de forma exponencial. Una contraseña de 8 caracteres se puede romper por fuerza bruta en horas o días con hardware dedicado; una de 16, en tiempos que superan la edad del universo. La longitud es el factor más importante. Más que los símbolos raros, más que los números: longitud.

Mito dos: "tengo que usar símbolos raros como # \$ %". Ayudan, pero no son obligatorios ni son lo principal. Una frase larga de palabras comunes es muchísimo más segura que una contraseña corta llena de símbolos, y además es más fácil de recordar. Compara "P@ssw0rd!" (9 caracteres, cae en un diccionario con sustituciones comunes en minutos) contra "mi perro toby ladra a las palomas" (33 caracteres contando espacios, prácticamente irrompible y fácil de recordar). La segunda le gana por goleada. Los atacantes ya conocen todos los trucos de "cambiar la a por @" y "la o por 0": esas sustituciones no te protegen.

Mito tres: "la contraseña que trae el router de fábrica está bien". Las contraseñas de fábrica suelen ser razonablemente largas y aleatorias, así que son mejores que "12345678". Pero tienen dos problemas: a veces siguen un patrón predecible según el modelo del router (y los atacantes conocen esos patrones), y si alguien alguna vez vio la etiqueta de tu router, ya la conoce. Cámbiala por una tuya.

Entonces, ¿cómo es una contraseña fuerte de verdad? Larga (mínimo 16 caracteres, ideal 20 o más), única (no la uses también en tu correo o tu banco) y memorable para ti pero impredecible para otros. El método que recomendamos en la academia es el de la frase: elige una frase personal que nadie más diría igual, de preferencia con alguna imagen mental chistosa, y úsala tal cual, con espacios si tu router los acepta. En los ejemplos paso a paso lo practicamos con detalle.

Y una regla de oro: tu contraseña WiFi debe ser distinta de la contraseña de administrador de tu router. Son dos puertas distintas. La contraseña WiFi deja entrar a la red; la contraseña de administrador permite cambiar la configuración del router. Muchos routers traen de fábrica usuario "admin" y contraseña "admin" o "password" para entrar a la configuración, y muchísima gente nunca la cambia. Si un atacante entra a tu red (o si visitas una página maliciosa estando conectado), con esas credenciales de fábrica puede tomar control total de tu router. Cambia las dos contraseñas. Hoy.

WPS: la puerta trasera que debes cerrar

WPS son las siglas de WiFi Protected Setup, y nació con una buena intención: hacer más fácil conectar aparatos a la red sin tener que escribir la contraseña larga. ¿Te acuerdas del botón que tienen algunos routers, que lo aprietas y luego aprietas un botón en la impresora y se conectan solos? Eso es WPS. También existe una versión con un PIN de 8 dígitos que viene impreso en la etiqueta del router.

Suena cómodo. El problema es que el PIN de WPS es una puerta trasera gravísima. Ese PIN de 8 dígitos, por un error de diseño, en realidad se verifica en dos mitades de 4 dígitos por separado, y además el último dígito es de verificación, así que efectivamente solo hay que adivinar 7 dígitos en dos bloques. Eso reduce las combinaciones posibles de cien millones a unas once mil. Un atacante puede probarlas todas en cuestión de horas, a veces minutos, y al final el router le entrega la contraseña WiFi real en bandeja de plata. Da igual que tu contraseña sea perfecta: WPS la regala por la puerta de atrás.

Este ataque se conoce desde 2011 y nunca se ha arreglado del todo, porque el problema está en el diseño del PIN. La única solución real es desactivar WPS por completo en tu router. No "usarlo con cuidado", no "solo activarlo cuando lo necesito": desactivarlo. La comodidad de no

escribir la contraseña una vez no vale el riesgo de tener una puerta trasera abierta permanentemente. En los ejemplos paso a paso te mostramos exactamente dónde se apaga en la configuración típica de un router.

Hay una confusión común que vale la pena aclarar: el botón WPS físico del router no es lo mismo que el PIN WPS, pero ambos son parte del mismo sistema. Al desactivar WPS en la configuración, desactivas las dos cosas. Y no te preocupes por tus aparatos: todos se pueden conectar escribiendo la contraseña normal, cómo se ha hecho toda la vida. Si algún aparato viejo solo se conecta por WPS y no acepta contraseña escrita, ese aparato es un problema de seguridad andante y deberías reemplazarlo.

Filtrado MAC: el mito más persistente

La dirección MAC es el identificador único de hardware de cada dispositivo de red, como su número de serie para el WiFi. Algunos routers ofrecen una función llamada "filtrado MAC": haces una lista de las direcciones MAC de tus dispositivos y el router solo deja entrar a los que están en la lista. Suena seguro, ¿verdad? Es uno de los mitos más persistentes en seguridad WiFi, y es hora de desarmarlo.

El filtrado MAC no es seguridad real por una razón muy simple: la dirección MAC se puede falsificar en segundos. Cuando tu dispositivo habla por WiFi, anuncia su dirección MAC abiertamente, sin cifrar, porque la necesita para comunicarse. Un atacante que esté escuchando tu red puede ver las direcciones MAC de tus dispositivos autorizados y configurar su propio equipo para usar una de esas direcciones - eso se llama suplantación o spoofing de MAC - y el router lo dejará pasar como si fuera tu celular. Es como un antro con un cadenero que solo deja entrar a los que dicen un nombre de la lista, pero cualquiera en la fila puede oír los nombres y repetirlos. El cadenero no pide identificación, solo el nombre en voz alta.

¿Significa que el filtrado MAC no sirve para nada? Tiene un uso legítimo menor: como control parental básico o para llevar un inventario de qué aparatos tienen permiso, puede agregar una capita de molestia para el intruso casual. Pero nunca debe ser tu única protección ni debes confiar en él como medida de seguridad. Si alguien te dice "mi red está segura porque tengo filtrado MAC", esa persona tiene una falsa sensación de seguridad, que es peor que no tener nada porque te hace descuidar las medidas que sí importan. WPA2/WPA3 con contraseña fuerte: eso sí es seguridad. Filtrado MAC: un adorno opcional.

Ya que estamos desarmando mitos, desarmemos otro igual de popular: ocultar el nombre de la red (el SSID). Algunos tutoriales recomiendan desactivar la difusión del nombre de tu red para que "nadie la vea". El problema es que ocultarla no la hace invisible: el nombre viaja en varias partes de la comunicación y cualquier programa básico de análisis WiFi lo muestra. Peor aún,

cuando ocultas el SSID, tus propios dispositivos tienen que andar preguntando a gritos "¿dónde está mi red oculta?" cada vez que se conectan, lo cual de hecho facilita que un atacante capture el nombre. Es como esconderte tapándote los ojos: tú no ves a nadie, pero todos te ven a ti. No ocultes tu SSID esperando seguridad; mejor ponle un nombre que no revele información personal (nada de "Familia Hernández Casa 2" ni tu dirección) y concéntrate en WPA3 y buena contraseña.

Red de invitados y aislamiento: el cuarto de visitas

Cuando recibes visitas en tu casa, no les das la llave de tu recámara ni les enseñas dónde guardas tus documentos importantes. Les das acceso a la sala y al baño. Con tu red WiFi debería pasar lo mismo, y para eso existe la red de invitados.

Casi todos los routers modernos permiten crear una segunda red WiFi, separada de la principal, pensada para visitas, y muchos permiten también una tercera para tus aparatos inteligentes (focos, cámaras, bocinas, televisiones). La gracia está en el aislamiento: los dispositivos de la red de invitados pueden salir a internet, pero no pueden ver ni tocar los dispositivos de tu red principal. Tu visita puede ver videos en su celular, pero no puede asomarse a tu computadora ni a tu disco duro compartido.

Esto es doblemente importante si tienes un negocio. Imagina tu café: quieres ofrecer WiFi gratis a los clientes porque eso atrae gente, pero no quieres que un cliente curioso - o malicioso - pueda ver la computadora donde llevas la contabilidad o la terminal donde cobras con tarjeta. La solución es una red de invitados aislada, con su propio nombre y su propia contraseña (más simple que la principal, porque la vas a compartir y cambiar seguido), y tu red privada con otro nombre, oculta si quieres, con la contraseña fuerte que nadie más conoce. Algunos routers incluso permiten ponerle límite de velocidad a la red de invitados para que nadie abuse, y un portal donde el cliente acepta condiciones antes de conectarse.

Para la casa, la regla práctica es: visitas y aparatos inteligentes van a la red de invitados (o a una red IoT separada si tu router la ofrece); tus celulares, computadoras y tabletas personales van a la red principal. Así, si un foco inteligente barato trae una vulnerabilidad de seguridad - y créeme, muchos la traen - el atacante que lo controle queda atrapado en la red de invitados sin acceso a tus cosas importantes. Es compartimentar el riesgo: que un aparato débil no hunda toda la red.

Un detalle que mucha gente olvida: cambia la contraseña de la red de invitados de vez en cuando, sobre todo en negocios. Si la tienes escrita en un cartel en la pared desde hace dos años, ya la conoce medio barrio. En un negocio, cámbiala cada mes o cada pocos meses; en casa, cada que tengas visitas que ya no van a volver en un buen tiempo, o simplemente cada seis meses.

Errores comunes que debes evitar

Vamos a juntar en una lista los errores que más vemos, para que los reconozcas al instante. El primero ya lo conoces: contraseña débil o de fábrica sin cambiar. "12345678", "password", el nombre de la red igual que la contraseña, la contraseña en la etiqueta del router sin cambiar. Todo eso cae en minutos frente a un ataque de diccionario.

El segundo: WPS activado. Ya viste por qué es una puerta trasera. Mucha gente ni sabe que lo tiene activado porque viene activado de fábrica en muchísimos routers. Revísalo hoy.

El tercero: usar WEP o WPA/TKIP "porque un aparato viejo no se conecta de otra forma". Ya sabes el costo: bajas la seguridad de toda la red al nivel de hace veinte años. La solución correcta es actualizar o reemplazar el aparato viejo, no degradar la red.

El cuarto: nunca actualizar el firmware del router. El router es una computadora chiquita corriendo software, y ese software tiene errores que se descubren y se corrigen, como pasó con KRACK. Si nunca lo actualizas, te quedas con los errores para siempre. Revisa cada pocos meses si hay actualizaciones, o activa las actualizaciones automáticas si tu router las ofrece.

El quinto: red abierta en el negocio sin aislamiento. Dar WiFi gratis está bien; dar WiFi gratis desde la misma red donde está tu computadora de administración es regalar las llaves del negocio. Red de invitados aislada, siempre.

El sexto: compartir la contraseña principal con todo el mundo. Cada persona que conoce tu contraseña principal es un punto de fuga: la puede compartir, la puede anotar en un lugar visible, su celular se puede infectar. Visitas e invitados van a la red de invitados. Punto.

El séptimo: creer que el filtrado MAC o el SSID oculto te protegen. Ya desarmamos esos mitos. Son placebos, no medicina.

El octavo: no revisar nunca quién está conectado. La mayoría de los robos de WiFi se descubren por accidente, meses después. Una revisión de cinco minutos cada mes te ahorra disgustos.

Buenas prácticas: tu rutina de seguridad

Cierra la teoría con la lista de hábitos que separan a una red cuidada de una descuidada. Primero, configura una vez y bien: WPA3 (o WPA2/WPA3 transicional con AES si tienes aparatos viejos), contraseña larga y fuerte creada con el método de la frase, WPS desactivado, contraseña de administrador cambiada. Esa es la base y se hace una sola vez.

Segundo, separa tus redes: principal para tus dispositivos personales, invitados para visitas y aparatos inteligentes. Nombres de red que no revelen datos personales.

Tercero, mantén actualizado el firmware del router. Pon un recordatorio en tu celular cada tres meses para revisar si hay actualizaciones, o activa las automáticas.

Cuarto, revisa periódicamente los dispositivos conectados. Una vez al mes, entra a la configuración del router y mira la lista. Si ves algo que no reconoces, investiga: puede ser un aparato tuyo con un nombre raro (muchos aparatos se anuncian con nombres genéricos), o puede ser un intruso.

Quinto, cambia las contraseñas con criterio. La principal, cuando sospeches algo raro o una vez al año como mantenimiento. La de invitados, más seguido. Y nunca reutilices la contraseña WiFi en otros servicios.

Sexto, cuida el acceso físico al router. El botón de reset de fábrica borra toda tu configuración y la deja como nueva, con las contraseñas de fábrica. Si el router está en un lugar público de tu negocio al alcance de cualquiera, alguien con dos dedos y un clip puede resetearlo. Ponlo en un lugar razonablemente resguardado.

Séptimo, en redes públicas (café, aeropuerto, hotel), asume que la red es hostil: prefiere redes con OWE, evita hacer operaciones bancarias si puedes evitarlo, y considera usar una VPN, que es como un túnel cifrado dentro de la red pública. De VPNs hablaremos en otra unidad; por ahora quédate con la idea.

Con esto tienes la teoría completa. Ahora vamos a la parte donde ensucias las manos: los ejemplos paso a paso con tu router de verdad.

Ejemplos paso a paso

Antes de empezar, un consejo práctico: haz estos ejemplos con tu router a la mano y una computadora o celular conectado a tu red. Los menús cambian un poco entre marcas (TP-Link, Huawei, ZTE, Cisco, Telmex, Totalplay, Izzzi), pero los conceptos y los nombres de las opciones son los mismos en todos. Si algún nombre no coincide exactamente con lo que

ves en tu pantalla, busca el más parecido: "Wireless Security", "Seguridad inalámbrica", "WiFi Settings". Y no tengas miedo de moverle: mientras no guardes cambios que no entiendas, explorar los menús no rompe nada.

Ejemplo 1: activar WPA2/WPA3 en tu router paso a paso

Este es el ejemplo más importante de la unidad. Vas a entrar a la configuración de tu router y verificar (o corregir) el modo de seguridad. Tómate tu tiempo.

PASO 1: Entra a la configuración del router.

- Conéctate a tu red WiFi (o mejor, con cable si puedes).
- Abre el navegador y escribe la dirección del router.
Las más comunes son: 192.168.1.1 | 192.168.0.1 | 192.168.1.254
- Si no sabes cuál es la tuya, en Windows abre CMD y escribe: ipconfig
Busca "Puerta de enlace predeterminada": esa es la dirección.
- En Mac o Linux, abre la terminal y escribe: ip route | grep default

PASO 2: Inicia sesión como administrador.

- Usa el usuario y contraseña de la etiqueta del router
(común: admin/admin, admin/password, o una clave impresa).
- Si nunca la cambiaste, este es el momento de anotar en tu lista de pendientes: "cambiar contraseña de administrador".

PASO 3: Busca la sección de seguridad inalámbrica.

- Menús típicos: "Wireless" > "Wireless Security"
"WiFi" > "Seguridad" | "Red inalámbrica" > "Seguridad"
- Verás una opción como "Authentication", "Security Mode",
"Modo de seguridad" o "Tipo de cifrado".

PASO 4: Elige el mejor modo disponible, en este orden de preferencia:

- 1) WPA3-SAE (o WPA3-Personal): lo mejor, si todos tus aparatos son recientes.
 - 2) WPA2/WPA3 Transicional (o WPA2-PSK [AES] + WPA3): lo mejor si tienes algún aparato viejo que no habla WPA3.
 - 3) WPA2-PSK con AES (puede decir "WPA2-Personal AES"):
muy seguro si tu router no tiene WPA3.
- NUNCA elijas: WEP, WPA-PSK con TKIP, ni modos "Mixto TKIP+AES" si puedes evitarlos.

PASO 5: Escribe tu contraseña nueva (fuerte, del Ejemplo 2).

- Campo "Password", "Pre-Shared Key", "Contraseña" o "Clave".
- Guárdala en un lugar seguro (un gestor de contraseñas o anotada en papel guardado, no pegada al monitor).

PASO 6: Guarda y reconecta.

- Pulsa "Save" / "Guardar" / "Aplicar".
- El router puede reiniciarse (tarda 1-2 minutos).
- Todos tus dispositivos se desconectarán: vuelve a conectarlos con la contraseña nueva, uno por uno.

Verificación: después de guardar, vuelve a entrar al menú de seguridad y confirma que el modo quedó como lo elegiste. En tu celular, al ver la red, debería seguir apareciendo el candadito. Si algún aparato viejo ya no se conecta, no bajes la seguridad de toda la red: revisa

si ese aparato tiene actualización de software, y si no, considera reemplazarlo o conectarlo por cable.

Ejemplo 2: crear una contraseña fuerte que sí puedas recordar

Olvida las contraseñas tipo "x7#kL9!qZ" que nadie recuerda y todo el mundo termina anotando en un post-it. El método de la frase es mejor: más seguro y memorable.

PASO 1: Piensa en una escena personal, chistosa y específica.

- Debe ser algo que solo tú dirías así.
- Ejemplo: recordar a tu abuela regañando al perro porque se comió las tortillas de la canasta.

PASO 2: Convierte la escena en una frase de 6 a 8 palabras.

- Ejemplo: "la abuela regaña al perro tragon de tortillas"
- Cuenta los caracteres: esta frase tiene 45. Perfecto.

PASO 3: Agrega un toque personal impredecible.

- Un número que signifique algo para ti (no tu año de nacimiento ni tu dirección): "la abuela regaña al perro tragon de tortillas 77"
- Opcional: una mayúscula en una palabra inesperada: "la Abuela regaña al perro tragon de tortillas 77"

PASO 4: Verifica la fortaleza con estas 4 preguntas:

- 1) ¿Tiene 20 caracteres o más? (mientras más, mejor)
 - 2) ¿No es una frase famosa, de canción o de película?
 - 3) ¿No contiene tu nombre, dirección, fecha de nacimiento ni el nombre de tu mascota a secas?
 - 4) ¿La puedes recordar sin anotarla después de repetirla 3 veces en voz alta?
- Si las 4 son "sí", tienes una contraseña excelente.

PASO 5: Úsala solo para el WiFi.

- No la uses también en tu correo, tu banco o tus redes sociales. Cada servicio importante merece su propia contraseña (un gestor de contraseñas te ayuda con eso).

Practica el método creando dos o tres frases distintas antes de elegir la definitiva. Dila en voz alta un par de veces, escríbela una vez para verificar que la tecleas bien, y luego confía en tu memoria: las frases con imagen mental chistosa se quedan grabadas mucho mejor que las combinaciones aleatorias.

Ejemplo 3: desactivar WPS en tu router

Recuerda: WPS es la puerta trasera. Viene activado de fábrica en muchísimos routers. Apagarlo toma dos minutos.

PASO 1: Entra a la configuración del router (como en el Ejemplo 1, pasos 1 y 2).

PASO 2: Busca la opción WPS.

- Lugares típicos: "Wireless" > "WPS", "WiFi" > "WPS", "Avanzado" > "WPS" o dentro de "Seguridad inalámbrica".
- Puede aparecer como "WiFi Protected Setup", "WPS" o "Configuración protegida WiFi".

PASO 3: Desactívalo por completo.

- Pon el interruptor en "Disable" / "Desactivado" / "Off".
- Si hay opciones separadas para "PIN" y "Botón", desactiva las dos.
- Algunos routers lo tienen dentro de cada banda (2.4 GHz y 5 GHz): desactívalo en las dos.

PASO 4: Guarda los cambios ("Save" / "Aplicar").

PASO 5: Verifica que quedó apagado.

- Sal de la configuración, vuelve a entrar y confirma que sigue en "Desactivado".
- El botón físico WPS del router (si tiene) ya no debería hacer nada al presionarlo.

Nota: después de desactivar WPS, todos tus aparatos siguen funcionando igual; la única diferencia es que para conectar un aparato nuevo tendrás que escribir la contraseña manualmente. Esa pequeña molestia es el precio de cerrar la puerta trasera, y vale cada centavo.

Ejemplo 4: ver quién está conectado a tu red y expulsar intrusos

Tu router sabe exactamente qué dispositivos están conectados en este momento. Revisar esa lista es como asomarte por la mirilla: rápido y revelador.

PASO 1: Entra a la configuración del router.

PASO 2: Busca la lista de clientes o dispositivos.

- Nombres típicos: "Client List", "Dispositivos conectados", "DHCP Client List", "Attached Devices", "LAN Status".
- Suele estar en "Estado", "Status", "Red local" o "Avanzado".

PASO 3: Lee la lista con calma.

- Verás nombres de dispositivo, direcciones IP y direcciones MAC. Anota cuántos aparatos reconoces.
- Nombres como "android-xyz" o "DESKTOP-ABC" son tus propios aparatos con nombres genéricos: verifícalos comparando con lo que tienes en casa.

PASO 4: Identifica a cada uno.

- Apaga el WiFi de tu celular un momento y mira si desaparece un renglón de la lista: así identificas cuál eres tú.
- Repite con cada aparato de la casa hasta que cada renglón tenga dueño. Los focos, cámaras y televisiones inteligentes también aparecen: no los olvides.

PASO 5: Si encuentras un intruso (un renglón sin dueño):

- a) Cambia INMEDIATAMENTE tu contraseña WiFi (Ejemplo 1) por una fuerte nueva (Ejemplo 2).
- b) Cambia también la contraseña de administrador del router.
- c) Verifica que WPS esté desactivado (Ejemplo 3).
- d) Al cambiar la contraseña, TODOS los dispositivos se desconectan, incluido el intruso, y solo se reconectan los que conozcan la clave nueva.
- e) Revisa la lista de nuevo en unos días para confirmar que no volvió.

PASO 6 (opcional, avanzado): si tu router permite bloquear por MAC, puedes bloquear la dirección MAC del intruso como medida extra. Recuerda que el filtrado MAC no es seguridad real por sí solo: úsalo solo como complemento después de haber cambiado las contraseñas.

Un consejo: haz esta revisión una vez al mes. Pon un recordatorio en tu celular: "revisar quién está en mi WiFi". Cinco minutos al mes te ahorran meses de un vecino colgado en silencio.

Ejemplo 5: qué hacer si sospechas que te están robando el WiFi

Señales de alerta: el internet se pone lento sin explicación (sobre todo de noche), el foco de actividad del router parpadea como loco cuando nadie está usando nada, o ves dispositivos desconocidos en la lista del Ejemplo 4. No entres en pánico: sigue este plan.

PASO 1: Confirma la sospecha.

- Haz la revisión de dispositivos del Ejemplo 4 en un momento en que sepas qué aparatos deberían estar conectados (por ejemplo, de madrugada con todo apagado menos el router).
- Si hay renglones sin dueño, la sospecha se confirma.

PASO 2: Corta el acceso de inmediato.

- Cambia la contraseña WiFi por una fuerte nueva.
- Cambia la contraseña de administrador del router.
- Desactiva WPS si estaba activado.

PASO 3: Reconecta solo tus aparatos.

- Conecta uno por uno tus dispositivos con la clave nueva.
- No compartas la clave nueva con nadie fuera de tu casa.

PASO 4: Refuerza la configuración.

- Verifica que el modo de seguridad sea WPA2-AES o WPA3 (nada de WEP ni TKIP).
- Si no la tienes, crea la red de invitados para visitas y aparatos inteligentes, separada de tu red principal.

PASO 5: Actualiza el firmware del router.

- En el menú de "Administración", "Sistema" o "Avanzado" busca "Firmware Update" o "Actualización".
- Si hay una versión nueva, instálala (no apagues el router durante la actualización).

PASO 6: Vigila durante una semana.

- Revisa la lista de dispositivos cada dos o tres días.
- Si el intruso vuelve a pesar de todo, es posible que alguien de tu casa esté compartiendo la clave, o que el router tenga una vulnerabilidad grave: considera restablecerlo a valores de fábrica y configurarlo desde cero, o reemplazarlo por un modelo actual.

Y un recordatorio legal importante: si descubres que alguien usó tu red para actividades ilegales, guarda evidencia (capturas de la lista de dispositivos, fechas) y considera reportarlo a las autoridades. Tú eres la víctima, y actuar rápido y con evidencia te protege.

Práctica

Haz estos ejercicios de verdad, con tu router y tus dispositivos a la mano. La seguridad se aprende haciendo, y tu propia red es el mejor laboratorio. Cada ejercicio trae su solución explicada: intenta resolverlo primero por tu cuenta y luego compara.

Ejercicio 1: auditoría de seguridad de tu red con checklist

Objetivo: evaluar el estado actual de tu red WiFi usando una lista de verificación, y anotar qué necesitas corregir.

Instrucciones: entra a la configuración de tu router y responde cada pregunta con SÍ o NO. Anota tus respuestas en papel o en tu celular.

1. ¿Mi modo de seguridad es WPA2-AES, WPA3 o WPA2/WPA3 transicional?
2. ¿Mi contraseña WiFi tiene 16 caracteres o más y no es la de fábrica?
3. ¿La contraseña de administrador del router es distinta de la de fábrica?
4. ¿WPS está desactivado?
5. ¿El firmware del router está actualizado (revisado en los últimos 3 meses)?
6. ¿Tengo red de invitados separada para visitas y aparatos inteligentes?
7. ¿El nombre de mi red (SSID) no revela mi nombre, dirección ni datos personales?
8. ¿Revisé la lista de dispositivos conectados en el último mes?

Solución explicada: cada "NO" es una tarea pendiente, y el orden de prioridad es el de la lista. Si respondiste NO a la pregunta 1, esa es tu emergencia número uno: cambia el modo de seguridad hoy mismo siguiendo el Ejemplo 1, porque todo lo demás protege poco si la base es WEP o TKIP. Si el NO está en la 2, crea una contraseña fuerte con el método de la frase del Ejemplo 2; recuerda que la longitud manda. El NO en la 3 es peligroso porque con las credenciales de fábrica cualquiera dentro de tu red puede tomar control del router: cámbiala por una contraseña distinta a la del WiFi. El NO en la 4 se arregla en dos minutos con el Ejemplo 3. Para la 5, busca la opción de actualización de firmware en el menú de administración; si tu router ya no recibe actualizaciones del fabricante desde hace años, anota "evaluar reemplazo" porque un router abandonado es una vulnerabilidad permanente. La 6 se configura en el menú de red inalámbrica buscando "Guest Network" o "Red de invitados": actívala, ponle nombre distinto y contraseña propia. La 7 se arregla cambiando el SSID por algo neutro como "CasaNet" en vez de "FamiliaHernandez_48". Y la 8 se vuelve hábito con el recordatorio mensual del Ejemplo 4. Si sacaste 8 de 8, felicidades: tu red está mejor protegida que el 90 por ciento de las redes caseras.

Ejercicio 2: crea 3 contraseñas fuertes con el método de la frase

Objetivo: dominar la creación de contraseñas largas, memorables y seguras.

Instrucciones: usando el método del Ejemplo 2, crea tres contraseñas distintas: una para tu WiFi principal, una para tu red de invitados y una para la administración del router. No uses la misma dos veces.

Solución explicada: vamos a construir tres ejemplos para que veas el patrón (tú debes crear las tuyas propias, estas son solo ilustración). Para el WiFi principal, piensa en una escena familiar chistosa: "el gato gordo ronca sobre la lavadora 33". Tiene 40 caracteres, imagen mental clara, un número personal al final. Para la red de invitados, algo más corto pero igual válido, porque la cambiarás seguido: "visitas toman cafe en la sala 12". Para la administración del router, la más sería de las tres, que casi nunca escribirás: "el router guarda silencio bajo el escritorio 99". Verifica cada una con las 4 preguntas del Ejemplo 2: ¿20+ caracteres? ¿no es frase famosa? ¿sin datos personales obvios? ¿memorable? Fíjate en que ninguna usa sustituciones obvias como "@" por "a", porque ya vimos que eso no engaña a nadie. El punto clave del ejercicio: después de crearlas, repítelas en voz alta tres veces y escríbelas una vez para practicar el tecleo. Si al día siguiente las recuerdas sin mirar, el método funcionó contigo.

Ejercicio 3: simula (en concepto) un ataque de diccionario contra contraseñas débiles

Objetivo: entender por qué las contraseñas comunes caen tan rápido, para no volver a usarlas jamás. Este ejercicio es 100 por ciento defensivo y conceptual: no vas a atacar nada ni a nadie, solo vas a razonar como lo haría un atacante para entender qué debes evitar.

Instrucciones: escribe en papel una lista de 10 contraseñas que creas que la gente usa comúnmente para su WiFi. Luego, para cada una, estima cuánto tardaría en caer frente a un programa de diccionario: segundos, minutos, horas o "prácticamente nunca".

Solución explicada: casi seguro tu lista incluye joyas como "12345678", "password", "qwerty123", el nombre de tu compañía de internet, "familia2024" o tu equipo de fútbol favorito. La respuesta para todas esas es "segundos o minutos": están en los primeros lugares de todas las listas de diccionario del mundo, y un atacante ni siquiera necesita ser hábil, solo ejecutar el programa. Las variantes con un año al final ("...2024", "...2025") tampoco se salvan: los programas prueban automáticamente los años y las sustituciones comunes. Las únicas que llegan a "prácticamente nunca" son las frases largas y personales del Ejercicio 2, porque no aparecen en ningún diccionario: un atacante tendría que adivinarlas por fuerza bruta pura, y con 30+ caracteres eso toma más tiempo que la edad del universo. La lección del ejercicio: si

tu contraseña se te ocurrió en dos segundos y "se oye normal", probablemente está en un diccionario. Si te tomó un minuto inventar una escena chistosa y personal, probablemente no.

Ejercicio 4: inventario de dispositivos conectados a tu red

Objetivo: saber exactamente qué aparatos viven en tu red, para detectar intrusos al instante en el futuro.

Instrucciones: siguiendo los pasos 1 a 4 del Ejemplo 4, haz una lista completa de todos los dispositivos conectados a tu red en este momento. Para cada uno anota: nombre como aparece en el router, tipo de aparato y dueño.

Solución explicada: una lista típica de una casa podría verse así: "android-9f3a2c" = mi celular; "DESKTOP-MARTA" = la laptop de mi esposa; "Smart-TV-Sala" = la tele; "ESP_84F3A2" = el foco inteligente del cuarto (los aparatos baratos suelen anunciarse con nombres crípticos: ese es normal); "HP-Printer" = la impresora. El truco del ejercicio está en el método de identificación: apaga el WiFi de un aparato y mira qué renglón desaparece de la lista; así confirmas cada identidad sin adivinar. Si al final te queda un renglón sin dueño, no lo ignores: aplica el plan del Ejemplo 5. Guarda esta lista en papel o en una nota de tu celular con la fecha de hoy. La próxima vez que revises, comparar te tomará dos minutos en vez de veinte, porque ya sabes qué es normal en tu red. Y aquí va el detalle profesional: repite el inventario una vez con la red de invitados activa, para verificar que los aparatos de invitados efectivamente no pueden ver los de tu red principal (desde un celular en la red de invitados, intenta abrir una carpeta compartida o la página del router: no deberías poder).

Ejercicio 5: diseña la configuración segura de un pequeño negocio

Objetivo: aplicar todo lo aprendido a un caso realista: un café que quiere ofrecer WiFi gratis a sus clientes sin poner en riesgo su computadora de administración y su terminal de cobro.

Instrucciones: en papel, diseña la configuración completa: nombres de red, modos de seguridad, contraseñas (inventadas para el ejercicio), red de invitados, y reglas de mantenimiento. El café tiene: 1 computadora de administración, 1 terminal de cobro con tarjeta, y quiere WiFi gratis para clientes.

Solución explicada: el diseño correcto tiene dos redes separadas. Red principal (privada): nombre neutro que no diga el nombre del negocio, por ejemplo "OficinaNet"; modo WPA3 o WPA2-AES; contraseña larga con el método de la frase que solo conocen el dueño y el encargado, por ejemplo "el inventario cierra los viernes 41"; aquí se conectan la computadora de administración y la terminal de cobro, y nada más. Red de invitados: nombre visible y

atractivo como "Cafe WiFi Gratis"; modo WPA2-AES como mínimo (si el router lo permite, WPA3); contraseña más simple pero no trivial, por ejemplo "cafe invita la casa 2026", escrita en un cartel y cambiada cada mes; con aislamiento de clientes activado (opción "AP isolation" (AP = access point, punto de acceso) o "aislamiento" en el router) para que ni siquiera los clientes se vean entre sí; con límite de velocidad si el router lo permite, para que un cliente no acapare todo el ancho de banda. Además: WPS desactivado, contraseña de administrador del router cambiada, firmware actualizado, y el router físicamente fuera del alcance de los clientes (nada de dejarlo sobre el mostrador donde cualquiera puede apretar el botón de reset). Regla de mantenimiento: cambio mensual de la clave de invitados, revisión trimestral de firmware y de la lista de dispositivos. Si el dueño quiere un portal de bienvenida donde el cliente acepta condiciones, mejor, pero lo esencial es el aislamiento. Este diseño le da al negocio lo mejor de los dos mundos: clientes contentos con WiFi gratis y administración blindada.

Ejercicio 6: plan de respuesta ante sospecha de intruso

Objetivo: tener por escrito, antes de que pase, exactamente qué harás si sospechas que alguien se metió a tu red. En una emergencia no se improvisa.

Instrucciones: escribe tu plan personal en una hoja, con los pasos numerados y adaptados a tu router y tu casa. Incluye qué harás en la primera hora, en la primera semana y como prevención permanente.

Solución explicada: un buen plan se ve así. Primera hora: 1) confirmo con la lista de dispositivos del Ejemplo 4 en un momento de poco tráfico; 2) cambio la contraseña WiFi por una frase nueva fuerte; 3) cambio la contraseña de administrador del router; 4) verifico que WPS siga desactivado y que el modo sea WPA2-AES o WPA3; 5) reconecto solo mis aparatos, uno por uno. Primera semana: 6) actualizo el firmware del router; 7) reviso la lista de dispositivos cada dos días; 8) si tengo negocio, cambio también la clave de invitados y reviso que el aislamiento siga activo; 9) pienso quién pudo compartir mi clave (visitas recientes, familiares) y ajusto a quién se la doy en adelante. Prevención permanente: 10) recordatorio mensual para revisar dispositivos; 11) recordatorio trimestral para revisar firmware; 12) red de invitados activa para visitas y aparatos inteligentes; 13) contraseñas anotadas solo en lugar seguro, nunca en papelitos pegados al router. Guarda esta hoja dónde la encuentres rápido. Y recuerda el principio de esta unidad: la seguridad es mantenimiento, no un evento de una sola vez. El plan no sirve guardado en un cajón: sírvelo repasándolo cada seis meses, aunque no haya pasado nada.

Resumen de la unidad

- Tu red WiFi viaja por el aire y atraviesa paredes: sin seguridad, cualquiera cercano puede escuchar tu tráfico. La seguridad inalámbrica es la chapa, las paredes de ladrillo y la alarma de tu casa digital.
- El cifrado es "hablar en clave": aunque alguien intercepte tus ondas, sin la clave solo ve ruido sin sentido. La autenticación comprueba quién eres; el cifrado protege lo que dices. Necesitas ambas.
- WEP está muerto: su diseño tenía errores graves (vectores de inicialización cortos que se repetían) y se rompe en minutos con programas gratuitos. Si lo ves en tu router, ni lo consideres.
- WPA fue un parche temporal con TKIP: mejor que WEP, pero construido sobre el viejo RC4 y con fecha de caducidad. Cumplió su misión como puente hacia WPA2.
- WPA2 trajo el cifrado AES con CCMP, el estándar serio que protegió al mundo por más de una década. Regla de oro: siempre AES, nunca TKIP ni modos mixtos por compatibilidad.
- El apretón de manos de 4 vías permite que tu dispositivo y el router acuerden claves sin que tu contraseña viaje nunca por el aire.
- KRACK (2017) demostró que hasta los buenos protocolos envejecen: se arregló actualizando. Moraleja: mantén actualizado el firmware de tu router, siempre.
- WPA3 es el estándar actual: SAE reemplaza al handshake con secreto hacia adelante (el tráfico viejo no se puede descifrar aunque caiga tu contraseña después) y frena los ataques de diccionario.
- Los ataques de diccionario prueban las contraseñas comunes a toda velocidad; la fuerza bruta prueba todas las combinaciones. La defensa es una contraseña larga: la longitud es el factor más importante.
- PMF protege los mensajes de control de la red; en WPA3 es obligatorio.
- OWE cifra incluso las redes abiertas sin contraseña: cada usuario negocia su propio cifrado. Mejor que una red abierta tradicional, pero en sitios públicos mantén la prudencia.
- Contraseña fuerte = larga (20+ caracteres ideal), única y memorable con el método de la frase. Olvida "12345678" y las sustituciones obvias como "@" por "a": los atacantes ya las conocen.
- Tu contraseña WiFi y tu contraseña de administrador del router deben ser distintas, y la de administrador nunca debe quedarse como la de fábrica.

- WPS es una puerta trasera por diseño (el PIN se rompe en horas): desactívalo por completo, PIN y botón, en ambas bandas.
- El filtrado MAC no es seguridad real: las direcciones MAC se anuncian abiertamente y se falsifican en segundos. Úsalo como complemento, nunca como protección principal.
- Ocultar el SSID no te protege: el nombre se descubre fácil y tus dispositivos terminan anunciándolo a gritos. Pon un nombre neutro y concéntrate en lo que sí importa.
- Red de invitados con aislamiento: visitas y aparatos inteligentes en una red separada que solo sale a internet, sin acceso a tus dispositivos personales. Obligatoria en negocios que ofrecen WiFi gratis.
- Los 8 errores comunes: contraseña débil o de fábrica, WPS activado, WEP/TKIP por aparatos viejos, firmware sin actualizar, red abierta en el negocio sin aislamiento, compartir la clave principal con todos, confiar en filtrado MAC o SSID oculto, y nunca revisar quién está conectado.
- Tu rutina de seguridad: configura una vez y bien (WPA3/WPA2-AES, contraseña fuerte, WPS apagado, admin cambiado), separa redes, actualiza firmware cada tres meses, revisa dispositivos cada mes y cambia claves con criterio.
- La seguridad no es un evento de una sola vez: es mantenimiento, como cambiarle el aceite al carro. El objetivo no es ser invencible, es dejar de ser el objetivo fácil.

Con esta unidad completas el cuadro: ya sabes cómo viajan tus datos por el aire y ahora sabes cómo protegerlos. En la siguiente unidad del libro seguiremos construyendo sobre esta base. Por lo pronto, haz tu auditoría del Ejercicio 1 hoy mismo: tu red te lo va a agradecer.

UNIDAD 6: Antenas y cobertura (Clases 16 a 18)

Introducción

Hay una escena que se repite en millones de casas todos los días: una familia paga por un servicio de internet rápido, el técnico instala el módem, todos prueban el WiFi junto al router y funciona de maravilla. Pero unas horas después, alguien intenta ver una película en la recámara del fondo y la imagen se congela. Otro quiere hacer videollamada desde la cocina y la voz llega cortada. El adolescente se encierra en su cuarto y grita: "¡el internet está horrible!". Y nadie entiende por qué, si "pagan por internet de alta velocidad".

Aquí está la primera gran verdad de esta unidad: el problema casi nunca es el internet. El problema es la cobertura. El internet es el agua que llega a tu casa por la tubería principal; la cobertura WiFi es la forma en que esa agua se reparte por cada llave de la casa. Puedes tener la mejor presión de agua del mundo, pero si la tubería está doblada, si hay una llave tapada o si el tinaco está en el peor lugar posible, no vas a poder regar el jardín. Con el WiFi pasa exactamente lo mismo: el cable de fibra o cobre trae los datos hasta tu módem, pero de ahí en adelante todo depende de las antenas, de dónde pusiste el router y de cómo está distribuida tu casa.

Y aquí viene la buena noticia: la cobertura es una de las cosas que más puedes mejorar sin gastar dinero. No necesitas comprar otro router, ni contratar más velocidad, ni cambiar de compañía. En la mayoría de los casos, basta con entender qué hacen las antenas, mover el router a un mejor lugar y orientar correctamente las antenas que ya tienes. Este es el conocimiento que separa a la persona que dice "el WiFi de esta casa no sirve" de la persona que dice "ya sé qué le pasa y cómo se arregla". Al terminar esta unidad, vas a ser la segunda persona.

Pero ojo: esta unidad también tiene una trampa para principiantes. Cuando la gente escucha la palabra "antena", piensa en algo complicado, en fórmulas de física, en torres de telecomunicaciones. Nada de eso. Las antenas de tu casa son piezas sencillas de metal o de plástico que reparten la señal en formas muy predecibles, y una vez que entiendes la forma en que reparten la señal, todo lo demás se vuelve obvio. Vamos a usar analogías de la vida diaria: la antena como bocina, la ganancia como embudo, la señal como luz de un foco. No necesitas saber física. Necesitas saber imaginar.

Esta unidad agrupa tres clases que avanzan paso a paso. La Clase 16 te presenta la familia de las antenas: las omnidireccionales (las que vienen con tu router y reparten señal en todas

direcciones), las direccionales (las que apuntan la señal como un reflector), las de panel, las Yagi y las parabólicas. Vas a aprender qué aspecto tiene cada una, en qué situación se usa y por qué no todas sirven para todo.

La Clase 17 se mete con los números y las palabras raras que aparecen en las cajas y en las especificaciones: ganancia en dBi, polarización, MIMO, EIRP y los límites legales de potencia. Esto suena técnico, pero te lo vamos a explicar de forma que un niño de diez años lo entendería: qué significa realmente que una antena tenga "5 dBi", por qué importa si la antena está vertical u horizontal, y qué es ese MIMO que todos los routers modernos anuncian en grande.

La Clase 18 es la más práctica de las tres: dónde poner el router en tu casa y cómo orientar las antenas para tener la mejor cobertura posible. Aquí vas a aprender las reglas de ubicación (el centro, lo alto, lejos de obstáculos), cómo orientar las antenas si tu casa es de una planta o de dos, y cuándo vale la pena considerar una antena direccional para llevar internet a otra construcción, como un cuarto al fondo del terreno o el taller del patio.

Al terminar esta unidad vas a poder hacer algo que muy poca gente sabe hacer: entrar a una casa, mirar dónde está el router, mirar cómo están puestas las antenas, y diagnosticar en dos minutos por qué el WiFi falla en ciertos cuartos. Y lo más importante: vas a saber cómo arreglarlo. Ese conocimiento, créeme, te va a convertir en la persona a la que toda la familia y todos los vecinos le piden ayuda con el internet.

Un aviso importante antes de empezar: en esta unidad vas a ver muchos números con unidades como dBm y dBi. No te asustes. No vamos a hacer cálculos complicados. Esos números son solo una forma de medir qué tan fuerte llega la señal, como cuando dices que un ruido está "fuerte" o "quedito", pero con números exactos. Te vamos a enseñar a leerlos sin dolor y sin fórmulas. Si sabes sumar y restar, es más que suficiente.

También vas a notar que esta unidad conecta con todo lo que ya aprendiste. En las unidades anteriores viste qué es el WiFi, las bandas de 2.4 y 5 GHz, los canales y la interferencia. Ahora todo eso cobra sentido práctico: vas a entender por qué la banda de 2.4 GHz atraviesa paredes mejor que la de 5 GHz (y por qué eso importa al colocar antenas), por qué los canales importan menos si tu antena no reparte bien la señal, y por qué a veces el mejor "amplificador de WiFi" no cuesta nada: es mover el router treinta centímetros hacia arriba.

Así que ponte cómodo, agarra tu celular (lo vas a necesitar para varios ejercicios de medición) y prepárate. Esta unidad es larga porque el tema lo merece: las antenas y la cobertura son, sin exagerar, el ochenta por ciento de los problemas de WiFi en las casas. Domina esto y dominas el WiFi doméstico.

Explicación detallada

La antena es una bocina: cómo reparte la señal

Empecemos con la analogía más importante de toda la unidad. Imagina que tienes una bocina (un altavoz) en el centro de una fiesta. Si la bocina es de esas redondas que suenan hacia todos lados, la música se escucha igual en todas direcciones, pero no muy lejos. Si en cambio usas una bocina de trompeta, como las de los anuncios de las camionetas, el sonido llega lejísimo... pero solo en la dirección a la que apunta la trompeta. Atrás de la camioneta no se escucha nada.

Las antenas funcionan exactamente igual. Una antena no "crea" más señal de la nada; lo que hace es decidir hacia dónde va la energía que ya tiene. Es como la diferencia entre un foco normal y una lámpara de mano (linterna). El foco ilumina toda la habitación pero no alumbra lejos. La lámpara de mano alumbra lejísimo, pero solo el pedacito al que apunta. Misma cantidad de luz, diferente reparto.

Esto es fundamental y vale la pena repetirlo: la antena no aumenta la energía total. La energía que sale del router es la misma; la antena solo decide si esa energía se reparte en todas direcciones o se concentra en una. Por eso, cuando alguien te venda una antena "más potente", ya vas a saber la verdad: no es más potente, es más concentradora. Y concentrar no siempre es mejor, como vamos a ver.

Esta forma en que la antena reparte la energía se llama patrón de radiación. Es un término elegante para algo muy simple: el dibujo invisible que hace la señal alrededor de la antena. Hay dos patrones básicos que debes conocer, y con esos dos entiendes el noventa por ciento del tema.

El primer patrón es el de la antena omnidireccional: imagina una dona (una rosquilla) acostada alrededor de la antena. La antena está parada en el centro del hoyo de la dona, y la señal sale en forma de dona hacia todos lados, a la misma distancia en todas direcciones. Arriba y abajo de la antena, en cambio, casi no hay señal: es como el hoyo de la dona, ahí no llega nada. Por eso las antenas de los routers se ponen verticales: la dona queda acostada a la altura de los cuartos, cubriendo todo el piso de la casa en círculo.

El segundo patrón es el de la antena direccional: imagina el haz de una lámpara de mano. La señal sale en un cono hacia adelante, llega mucho más lejos, pero a los lados y atrás casi no hay nada. Este patrón sirve cuando quieres llevar la señal a un punto específico lejano, como de tu casa al cuarto del fondo del terreno, o de un edificio a otro.

Con solo estos dos dibujos mentales (la dona y el haz de lámpara) ya puedes razonar casi cualquier situación de cobertura. ¿Tu router está en una esquina de la casa y la señal no llega al otro extremo? Claro: la mitad de la dona se está desperdiciando fuera de la casa, hacia la calle o hacia el vecino. ¿Pusiste el router en el piso detrás del sillón? La dona está a la altura del piso, chocando con muebles, y arriba casi no sube señal. ¿Quieres mandar internet a la casa de tu mamá que está a cincuenta metros? Una dona no llega tan lejos; necesitas el haz de lámpara de una antena direccional.

La familia de las antenas: quién es quién

Ahora que entiendes los dos patrones básicos, conozcamos a los miembros de la familia. Cada tipo de antena tiene su forma, su patrón y su trabajo ideal.

Las antenas omnidireccionales son las que ya conoces: los palitos que traen los routers en la parte de atrás. Son varillas delgadas, normalmente de plástico negro, que se pueden doblar en la base. Su patrón es la dona. Son las reinas de las casas porque una casa necesita señal en todas direcciones: recámaras a un lado, sala al otro, cocina atrás, patio adelante. Si solo tienes un router y una casa normal, las omnidireccionales son lo correcto. Su alcance típico en interiores anda entre los diez y los treinta metros, dependiendo de las paredes.

Las antenas direccionales de panel parecen una cajita plana o un cuadrado, como un libro delgado colgado en la pared. Por dentro tienen una placa metálica que refleja la señal hacia adelante, como el reflector de una lámpara. Su patrón es un haz ancho: cubre un ángulo de unos sesenta a noventa grados hacia adelante y llega bastante más lejos que una omnidireccional. Se usan mucho para cubrir un patio largo, un pasillo de oficinas, o para mandar señal de un punto a otro dentro de un terreno. Si las ves en una pared apuntando hacia el jardín, ya sabes qué están haciendo ahí.

Las antenas Yagi son las que parecen "espinas de pescado": una varilla larga con varias varillitas cruzadas cada vez más cortas. Las has visto en los techos de las casas viejas para la televisión, y las antenas WiFi Yagi son la versión pequeña de esas. Su patrón es un haz angosto y largo: apuntan la señal como un rifle hacia un punto lejano. Se usan para enlaces punto a punto, por ejemplo para llevar internet de tu casa a la casa de un familiar que está a unos cientos de metros, siempre que haya línea de vista (que se vean entre sí sin edificios en medio). Son baratas y muy efectivas para ese trabajo específico, pero inútiles para cubrir una casa por dentro porque todo lo que no esté enfrente se queda sin señal.

Las antenas parabólicas son los platos, como las antenas de televisión satelital pero más pequeñas. Su patrón es el haz más angosto y concentrado de todos: como un rayo láser de radio. Con ellas se hacen enlaces de varios kilómetros entre torres o edificios. Para una casa

normal son excesivas, pero es bueno que sepas que existen porque cuando veas un plato apuntando a lo lejos, vas a entender que ahí hay un enlace direccional serio, no un WiFi para celulares.

Hay un detalle curioso que vale la pena mencionar: el tamaño de la antena tiene que ver con la frecuencia. Las antenas para 2.4 GHz son más largas que las de 5 GHz, porque las ondas de 2.4 GHz son más largas (unos doce centímetros) y la antena necesita medir una fracción de esa longitud para funcionar bien. Por eso los palitos de tu router miden unos diez centímetros: están sintonizados para 2.4 GHz. No es decoración; es física trabajando a tu favor.

La ganancia (dBi): el embudo que concentra

En las cajas de las antenas y de los routers vas a ver un número seguido de "dBi": 3 dBi, 5 dBi, 7 dBi, 9 dBi. Ese número se llama ganancia, y es la medida de qué tanto concentra la antena la señal en su dirección favorita, comparada con una antena teórica perfecta que reparte igual en todas direcciones (incluso arriba y abajo, como una esfera).

La analogía del embudo lo explica perfecto. Imagina que tienes un litro de agua y lo vacías: si lo vacías en el piso, se extiende en un charco grande pero poco profundo. Si lo vacías a través de un embudo, sale un chorro delgado pero con mucha fuerza y llega lejos. Misma agua, diferente concentración. La ganancia en dBi mide qué tan "embudo" es tu antena: mientras más dBi, más concentra la señal en su dirección favorita y más lejos llega... pero más estrecha es la zona cubierta.

Aquí está el truco que los vendedores no te explican: más dBi NO siempre es mejor. Una antena de 9 dBi llega más lejos que una de 3 dBi, pero su dona es más delgada, más aplastada, como una tortilla en vez de una dona esponjada. Si tu casa es de dos pisos y pones antenas de 9 dBi en la planta baja, la señal va a volar horizontalmente muy lejos, pero al piso de arriba casi no va a subir nada porque la dona está muy aplastada. Para una casa de dos pisos, unas antenas de 3 a 5 dBi (dona más gordita, que también sube y baja un poco) funcionan mejor que las de 9 dBi.

Piénsalo así: la ganancia alta es como la lámpara de mano potente, y la ganancia baja es como el foco de la sala. Si quieres iluminar toda tu casa, no compras diez lámparas de mano; prendes los focos. Las antenas de ganancia moderada (3 a 5 dBi) son los focos de tu casa: cubren bien en todas direcciones. Las de ganancia alta son para casos especiales: mandar señal lejos en una dirección.

Otro punto importante: la ganancia se mide en una escala logarítmica, no lineal. Eso significa que 3 dBi más no es "un poquito más", es el doble de concentración de energía en la dirección favorita. Cada 3 dBi aproximadamente duplican la intensidad en la dirección del haz. No

necesitas memorizar esto ni hacer cuentas; solo quédate con la idea de que los dBi crecen más rápido de lo que parece, y que pasar de 3 a 9 dBi es un salto enorme en concentración (y en estrechez de la zona cubierta).

Las antenas que traen los routers caseros de fábrica suelen ser de 3 a 5 dBi, y está bien: están diseñadas para una casa normal. Si alguna vez compras antenas de repuesto, busca que sean de 5 dBi como máximo para uso dentro de casa, a menos que tengas un caso especial (como mandar señal al fondo de un terreno largo, donde una direccional de panel tiene más sentido que una omnidireccional de 9 dBi).

EIRP y los límites legales: no todo se vale

Hay un concepto que suena muy técnico pero que en realidad es sentido común con nombre elegante: la EIRP (potencia isotrópica radiada equivalente). Traducido a cristiano: es la potencia total que efectivamente sale disparada en la dirección favorita de la antena, combinando la potencia del router más la concentración de la antena.

¿Por qué importa? Porque la ley pone un límite. Las señales de radio comparten el aire con todos, y si cada quien transmitiera con la potencia que quisiera, sería un caos: tu router taparía al del vecino, y el del vecino taparía al tuyo. Por eso cada país tiene una autoridad que dice cuánta potencia máxima puedes radiar en las bandas de WiFi. En México, como en la mayoría del mundo, los límites para WiFi andan alrededor de los 30 dBm de EIRP en 2.4 GHz (eso es como 1 watt efectivo en la dirección del haz), con reglas un poco distintas para 5 GHz según el canal.

¿Qué significa esto para ti en la práctica? Dos cosas. Primera: no tiene caso comprar una antena monstruosa de 15 dBi para tu router casero esperando llegar a kilómetros, porque para no violar el límite legal tendrías que bajarle la potencia al router, y al final quedas igual o peor. La ley te pone un techo, y ese techo está pensado para que el WiFi sea de corto alcance. Segunda: desconfía de los productos que prometen "alcance de 5 kilómetros" con un router casero y una antenita. O mienten, o te están invitando a operar fuera de la ley y a interferir a tus vecinos.

La buena noticia es que los routers que se venden legalmente ya vienen ajustados para respetar estos límites. Tú no tienes que calcular nada. Solo quédate con la idea: la potencia tiene un techo legal, y por eso la cobertura se mejora con ubicación, orientación y elección correcta de antena, no con "más potencia a lo loco".

Polarización: las antenas tienen que "mirarse" igual

Este es uno de esos detalles invisibles que explican misterios. Las ondas de radio vibran en una dirección: si la antena está vertical, la onda sale vibrando de arriba a abajo (polarización vertical). Si la antena está horizontal, la onda vibra de lado a lado (polarización horizontal). Y aquí viene lo importante: la antena receptora capta mejor la señal cuando vibra en la misma dirección. Es como tratar de meter una carta por una rendija: si la carta va vertical y la rendija es vertical, entra perfecto; si la carta va horizontal y la rendija es vertical, no entra.

En la práctica, esto significa que si todas las antenas de tu router están verticales, los aparatos que también tienen sus antenas verticales (la mayoría de los celulares cuando los sostienes normal, muchas laptops) reciben mejor. Si acuestas todas las antenas del router en horizontal, esos mismos aparatos reciben peor. La diferencia puede ser de varios dB, que en señal es bastante.

Pero hay un matiz interesante: en una casa real, la señal rebota en paredes, pisos y muebles, y al rebotar la polarización se revuelve un poco. Por eso el WiFi sigue funcionando aunque no todo esté perfectamente alineado. Aun así, la regla de oro es simple: en una casa de una planta, pon las antenas verticales (todas paraditas). En una casa de dos plantas, pon algunas verticales y otras a cuarenta y cinco grados o una horizontal, para que la señal también "vibre" en direcciones que les sirvan a los aparatos del otro piso. Más adelante, en los ejemplos paso a paso, te damos la receta exacta según tu casa.

Un error clásico: la gente acuesta las antenas del router "para que se vea más bonito" o porque el mueble es bajito. Al acostarlas todas, la dona de señal queda parada como una rueda de la fortuna, y la cobertura horizontal de la casa se desploma. Si tu mueble es bajito, mejor cambia el router de lugar antes que acostar las antenas.

Diversidad y MIMO: por qué los routers traen varias antenas

Si tu router tiene dos, tres o cuatro antenas, no es para que se vea más impresionante (bueno, un poco sí). Es porque usa dos trucos muy inteligentes: diversidad y MIMO.

La diversidad es el truco viejo y sencillo. La señal de radio en una casa llega por muchos caminos: directa, rebotada en la pared, rebotada en el techo. Esos caminos se combinan y a veces se cancelan entre sí en puntos específicos, creando "zonas muertas" pequeñitas donde la señal se cae aunque estés cerca del router. Con dos antenas separadas unos centímetros, es muy raro que las dos caigan en una zona muerta al mismo tiempo. El router simplemente usa la que recibe mejor en cada momento. Es como tener dos oídos: si uno te queda tapado, el otro sigue escuchando.

MIMO (que significa múltiples entradas y múltiples salidas) es el truco moderno y poderoso. En vez de usar las antenas solo como respaldo unas de otras, el router las usa para mandar varios chorros de datos al mismo tiempo por caminos diferentes, como abrir varios carriles en una carretera en vez de uno solo. Un router "2x2 MIMO" puede mandar dos chorros simultáneos; uno "4x4 MIMO" puede mandar cuatro. Esto multiplica la velocidad real sin necesidad de más espectro ni más potencia. Por eso los routers modernos anuncian el MIMO en grande: es una de las formas más efectivas de ser más rápidos.

Aquí viene la conexión con las antenas: para que MIMO funcione bien, las antenas deben "ver" caminos de señal diferentes. Por eso en los routers modernos a veces ves antenas en posiciones distintas (una vertical, otra inclinada): no es desorden, es diseño. Cada antena inclinada de forma diferente capta un "sabor" distinto de la señal rebotada, y eso le da al MIMO más caminos independientes para trabajar.

La lección práctica: no quites antenas de tu router "porque se ve mejor con menos", y no las pongas todas pegaditas en la misma posición. Cada antena está ahí por una razón. Si tu router trae antenas desmontables y quieres experimentar, hazlo, pero deja al menos las que traía y en posiciones variadas.

Antenas internas vs externas: las que se ven y las que no

No todos los routers tienen palitos visibles. Muchos routers modernos, sobre todo los que venden las compañías de internet y los sistemas de malla (mesh), traen las antenas por dentro, escondidas en la carcasa. ¿Son peores? No necesariamente.

Las antenas externas (los palitos) tienen dos ventajas: las puedes orientar (doblar, girar, inclinar) y las puedes cambiar por otras de más ganancia o direccionales si tu caso lo necesita. Son las favoritas de los entusiastas porque dan control.

Las antenas internas están diseñadas con mucho cuidado por ingenieros que simulan el patrón de radiación para que cubra bien en todas direcciones sin necesidad de orientar nada. Su ventaja es la estética y la simplicidad: las pones y listo, no hay que mover nada. Su desventaja es que no las puedes orientar ni cambiar; si la cobertura no te alcanza, tienes que mover el aparato completo o agregar otro punto de acceso.

Ninguna es "mejor" en abstracto. Si te gusta ajustar y experimentar, busca un router con antenas externas. Si quieres algo que se vea bonito en la sala y no piensas moverle nada, uno con antenas internas bien diseñadas te sirve igual. Lo que sí debes saber: con antenas internas, la ubicación del router se vuelve aún más importante, porque no tienes el truco de reorientar antenas para compensar una mala ubicación.

Conectores: el RP-SMA y por qué importa

Si tu router tiene antenas desmontables (se desenroscan), casi seguro usan un conector llamado RP-SMA. Es un conector redondo, chiquito, que se enrosca. La "RP" significa polaridad reversa: es una medida para que la gente no conecte cualquier antena de radioaficionado a un equipo WiFi sin saber lo que hace.

¿Por qué te importa esto? Porque si algún día compras una antena de repuesto o una direccional para un proyecto (como llevar internet al cuarto del fondo), tienes que comprar una con conector RP-SMA macho (normalmente) compatible con tu router. Si compras una antena con conector SMA normal (sin la R), no va a embonar. Es un detalle tonto pero es la causa número uno de "compré la antena y no le quedó a mi router". Cuando compres, busca que diga "RP-SMA" y "para WiFi 2.4/5 GHz".

Otro detalle: existen adaptadores y cables extensores (pigtailes) que te permiten poner la antena separada del router, por ejemplo en un lugar alto mientras el router está abajo. Funcionan, pero cada cable mete una pequeña pérdida de señal. Un cable corto de buena calidad pierde poco; un cable largo y barato puede comerse toda la ventaja de la antena nueva. Regla práctica: si vas a separar la antena del router, usa el cable más corto posible y de buena calidad.

2.4 GHz atraviesa, 5 GHz corre: la física que manda

Este concepto ya lo viste en unidades anteriores, pero aquí se vuelve protagonista porque decide dónde pones el router y qué esperas de cada banda. Las ondas de 2.4 GHz son más largas y atraviesan paredes, puertas y muebles con menos pérdida. Las de 5 GHz son más cortas, llevan más datos (más velocidad), pero se debilitan mucho más con cada pared que cruzan.

Traducido a tu casa: si el cuarto del fondo está a dos paredes del router, probablemente ahí solo llegue bien la señal de 2.4 GHz. La de 5 GHz se va a ver débil o no va a llegar. Esto no es un defecto; es física. Por eso muchos aparatos se conectan solos a 2.4 GHz cuando están lejos: es la banda que sobrevive al viaje.

¿Qué implica para las antenas y la ubicación? Que no puedes pedirle a la banda de 5 GHz que haga el trabajo de la de 2.4. Si necesitas cobertura en un cuarto lejano y solo te importa que funcione (no que vuele), asegúrate de que la red de 2.4 GHz esté activa y con buen nombre. Y cuando orientes antenas para cubrir dos pisos, recuerda que la señal que realmente va a subir al otro piso a través del techo es sobre todo la de 2.4 GHz.

Un error común: apagar la red de 2.4 GHz "porque es lenta" y dejar solo 5 GHz. Resultado: cuartos sin señal en toda la casa. Las dos bandas son un equipo: 5 GHz para velocidad cerca del router, 2.4 GHz para alcance lejos del router. No desactives a tu jugador de alcance.

Errores comunes que arruinan la cobertura

Vamos a juntar los errores más frecuentes, esos que vemos en casa tras casa. Revísalos y dime cuántos estás cometiendo tú (sin pena, todos cometimos varios).

Error uno: el router escondido. Meter el router dentro de un mueble cerrado, detrás del televisor, dentro de un cajón o en el clóset "para que no se vea". Cada pared del mueble es una pared más que la señal tiene que atravesar, y además el router se calienta encerrado. El WiFi necesita aire libre alrededor. Si te molesta verlo, ponlo en un lugar discreto pero abierto, no encerrado.

Error dos: el router en el piso. La señal se reparte mejor cuando el router está a una altura media-alta, como a la altura de una mesa o un librero (un metro a metro y medio del piso). En el piso, la mitad de la dona choca con muebles, y la señal tiene que subir atravesando todo. Súbelo y notarás la diferencia.

Error tres: el router en la esquina de la casa. Si lo pones en la esquina del cuarto de la entrada, la mitad de tu dona de señal se va a la calle y al vecino, y el fondo de la casa queda lejos. El router debe ir lo más céntrico posible. Ya sé que el cable del internet entra por donde entra, pero a veces mover el router dos metros hacia el centro (con un cable más largo) cambia todo.

Error cuatro: todas las antenas en la misma posición. Si tu router tiene tres antenas y las tres están verticales y pegaditas, estás desperdiciando la diversidad y el MIMO. Varíalas: una vertical, una a cuarenta y cinco grados, y si tu casa es de dos pisos, una horizontal. Cada posición distinta es un camino de señal distinto.

Error cinco: antenas apuntando al techo o al piso sin querer. Recuerda la dona: la señal sale por los lados de la antena, no por la punta. Si doblas la antena para que apunte hacia dónde estás sentado, en realidad le estás apuntando con el hoyo de la dona (donde no hay señal). Las antenas se ponen verticales para cubrir el piso; la punta no apunta a nadie.

Error seis: comprar un repetidor antes de optimizar lo gratis. Mucha gente compra repetidores o extensores cuando el problema era el router en el piso dentro del mueble. Optimiza primero lo gratis (ubicación, altura, orientación de antenas) y solo si eso no basta, considera agregar equipos.

Error siete: ignorar los obstáculos grandes de metal y agua. Un refrigerador, un espejo grande, un tanque de agua o una pared con mucho metal bloquean muchísimo la señal. Si tu router está justo detrás del refrigerador, ya encontraste tu problema. Los espejos son traicioneros porque parecen inofensivos y son casi una pared para el WiFi.

Buenas prácticas: la receta de oro

Y ahora la parte bonita: lo que sí funciona, resumido en hábitos simples.

Primera: centro y alto. Router cerca del centro de la casa, a un metro o más del piso, en espacio abierto. Esta sola regla arregla la mayoría de los casos.

Segunda: antenas verticales en casas de una planta. Todas paraditas, dona acostada cubriendo el piso. En casas de dos pisos, combina: verticales y una o dos inclinadas u horizontales para que la señal también viaje hacia arriba.

Tercera: lejos de obstáculos. Al menos un metro de distancia de refrigeradores, espejos grandes, tanques de agua y hornos de microondas (el microondas además interfiere en 2.4 GHz cuando está prendido).

Cuarta: las dos bandas activas. 2.4 GHz para alcance, 5 GHz para velocidad. Nombres de red claros para que sepas a cuál te conectas.

Quinta: mide antes de comprar. Usa tu celular para medir la señal cuarto por cuarto (en la sección de ejemplos te enseñamos cómo). Muchas veces el mapa de mediciones te muestra que el problema es un solo cuarto, y la solución es mover el router un metro, no comprar nada.

Sexta: para distancias largas entre construcciones, antena direccional. Si necesitas llevar internet a otra construcción en el mismo terreno, una antena de panel o Yagi bien apuntada hace el trabajo que ninguna omnidireccional puede hacer.

Con esto cierras la explicación. Ya sabes qué hacen las antenas, qué significan los números, y cuáles son los errores y los aciertos. Ahora vamos a la práctica: ejemplos paso a paso para tu casa real.

El mito de las antenas "rompemuros" y los amplificadores milagrosos

En las tiendas en línea vas a encontrar antenas que prometen "atravesar 5 paredes de concreto" o "triplicar tu cobertura", y amplificadores que juran convertir tu router humilde en una torre de telecomunicaciones. Ya tienes el conocimiento para desmontar estas promesas en diez segundos.

Primera verdad: ninguna antena pasiva (una que no lleva electricidad propia) puede crear energía. Solo la concentra. Si una antena promete "más señal en todas direcciones y más lejos al mismo tiempo", está prometiendo algo físicamente imposible: sería como una bocina que suena más fuerte en todas direcciones sin subirle el volumen. Lo que sí puede hacer es concentrar: más lejos en una dirección, a costa de las demás. Cuando un anuncio no te dice en qué dirección concentra, sospecha.

Segunda verdad: los amplificadores (boosters) sí aumentan la potencia, pero chocan con dos muros: el límite legal de EIRP y el hecho de que el WiFi es de dos vías. Este segundo punto es sutil y muy importante: aunque tu router grite más fuerte con un amplificador y tu celular "escuche" la señal desde lejos, tu celular tiene que responder gritando de vuelta... y el celular no tiene amplificador. El router no lo escucha. Es como si alguien te gritara desde la otra cuadra con un megáfono: tú lo oyes perfecto, pero cuando le gritas de vuelta sin megáfono, él no te oye. El enlace se rompe en la dirección de regreso. Por eso los amplificadores de una sola vía casi nunca resuelven nada en la práctica.

Tercera verdad: el "rompemuros" real se llama 2.4 GHz bien ubicada. Ninguna antena mágica atraviesa mejor las paredes que la física permite. Lo que sí atraviesa paredes es usar la banda correcta (2.4 GHz), poner el router en buen lugar y, si de plano hay una pared imposible, poner otro punto de acceso del otro lado conectado por cable. Esa es la solución de los profesionales, y no lleva milagros: lleva cable.

Entonces, ¿cuándo sí conviene comprar una antena? Cuando necesitas concentrar, no cuando necesitas magia: una direccional para el taller del fondo, una de panel para el pasillo largo. Y cuando compres, desconfía de cifras redondas y espectaculares ("¡12 dBi, alcance 3 km!") sin contexto de uso. Una antena honesta dice su ganancia, su patrón (cuántos grados cubre) y para qué banda sirve. Si el anuncio solo dice "potente", no dice nada.

Cómo leer la etiqueta de especificaciones como un profesional

Vamos a practicar con una etiqueta típica de un router o una antena, para que esos números dejen de ser jeroglíficos. Imagina que lees: "Router WiFi 6, 2.4 GHz / 5 GHz, 4 antenas externas de 5 dBi, 2x2 MU-MIMO, potencia de transmisión 20 dBm".

"WiFi 6" es la generación de la tecnología (ya la conoces de unidades anteriores): más eficiente con muchos aparatos. "2.4 GHz / 5 GHz" te dice que es de doble banda: alcance y velocidad, el equipo completo. "4 antenas externas de 5 dBi": cuatro palitos que puedes orientar, con ganancia moderada, o sea donas gorditas ideales para una casa. Perfecto para uso doméstico.

"2x2 MU-MIMO": puede manejar dos chorros de datos simultáneos por aparato (el "MU" significa multi-usuario: reparte esos chorros entre varios aparatos a la vez). Para una familia normal, 2x2 es más que suficiente; el 4x4 se nota en oficinas con mucha gente.

"Potencia de transmisión 20 dBm": el router transmite con 100 miliwatts, que es lo normal y legal para equipos caseros. Si ves "30 dBm", es un equipo más potente (1 watt), típico de exteriores o profesional, y ahí sí debes verificar que respete los límites de tu país.

Ahora una etiqueta de antena suelta: "Antena direccional de panel, 2.4 GHz, 9 dBi, ancho de haz 60 grados, conector RP-SMA". Traducción: cajita plana que concentra la señal en un haz de 60 grados hacia adelante, con buena ganancia para decenas de metros, y conector compatible con tu router. Ideal para el taller del fondo o el pasillo largo. Si en vez de "60 grados" dijera "360 grados" con 9 dBi, sospecha: eso es físicamente contradictorio (no se puede concentrar mucho y cubrir todo a la vez).

Y una más, de antena omnidireccional: "Antena omnidireccional dual band 2.4/5 GHz, 5 dBi, RP-SMA". Traducción: palito de repuesto que sirve para las dos bandas, con dona gordita. Es lo que comprarías si se te rompe una antena del router o quieres un repuesto. Fíjate que diga "dual band": una antena solo de 2.4 GHz en un router de doble banda desperdicia la banda de 5 GHz.

Con esto ya lees etiquetas como técnico: banda, ganancia, patrón, MIMO y conector. Cinco datos y sabes exactamente qué tienes enfrente.

Las antenas y la salud: lo que sí se sabe

Es una pregunta que sale tarde o temprano, y merece una respuesta directa y honesta: ¿hacen daño las ondas del WiFi? La respuesta corta es que, con los niveles de potencia de un router casero, las agencias de salud del mundo no han encontrado evidencia de daño, y los límites legales existen precisamente para mantener un margen de seguridad enorme.

Vamos por partes. El WiFi usa radiación no ionizante: sus ondas no tienen energía suficiente para romper moléculas ni dañar el ADN, a diferencia de los rayos X. Su único efecto conocido a potencias altas es calentar tejidos (como el microondas calienta la comida, que por cierto usa la misma banda de 2.4 GHz pero con cientos de watts encerrados en una caja metálica). Tu router transmite con 0.1 watts, o sea miles de veces menos potencia que el microondas, y además repartida en todas direcciones, no concentrada.

Para ponerlo en perspectiva: la señal de WiFi que te llega al sillón es muchísimo más débil que la luz del sol que te da en la cara cuando sales al patio, y también más débil que las señales de radio y televisión que te atraviesan todo el día desde hace décadas. Los límites de EIRP

que vimos antes no solo evitan interferencia: están calculados con márgenes de seguridad amplios.

Dicho esto, hay dos recomendaciones de puro sentido común que no tienen que ver con miedo sino con buenas prácticas: no duermas con el router pegado a la almohada (no por peligro, sino porque no es su lugar: va al centro y en alto), y si te da tranquilidad, puedes programar tu router para que apague el WiFi de madrugada, que además ahorra luz. Pero no compres "protectores anti-radiación" ni metas el router en cajas metálicas "para bloquear ondas": lo único que logran es arruinar tu cobertura (¿recuerdas el error del router escondido?) sin ningún beneficio real.

Cuándo sí vale la pena cambiar o agregar antenas

Después de todo lo aprendido, esta es la pregunta del millón: ¿compro antenas nuevas o no? La respuesta honesta es que en el ochenta por ciento de los casos, no necesitas comprar nada: con reubicar el router, subirlo y orientar bien las antenas se resuelve. Pero hay casos donde una antena nueva sí es la herramienta correcta.

Caso uno: se te rompió una antena. Compra un repuesto omnidireccional dual band de 3 a 5 dBi con conector RP-SMA. Barato y queda como nuevo.

Caso dos: necesitas llevar señal a otra construcción en tu terreno. Antena de panel direccional, como vimos en el ejemplo 4. Es el caso estrella de las antenas direccionales.

Caso tres: tu router tiene antenas internas y vives en una casa grande de dos pisos donde no puedes mover el router al centro (porque el cable entra en una esquina). Aquí a veces conviene más un segundo punto de acceso o un sistema mesh que cambiar antenas, porque con antenas internas no hay nada que orientar.

Caso cuatro: quieres experimentar y aprender. Comprar una antena de panel barata para jugar a apuntarla y medir con tu celular es una excelente práctica: aprendes más en una tarde de experimentos que en una semana de teoría. Solo verifica el conector RP-SMA y que sea para la banda que vas a usar.

Y un caso donde NO conviene: cuando el problema es interferencia de veinte vecinos o paredes de concreto armado. Ahí ninguna antena hace milagros; la solución es cable de red hasta otro punto de acceso, o un sistema mesh bien planeado. La antena correcta para el problema correcto: esa es la mentalidad de técnico que esta unidad te deja.

La regla de los 30 segundos: diagnóstico exprés

Para cerrar la explicación, te dejo el truco que usan los técnicos cuando entran a una casa ajena: en treinta segundos, con solo mirar, ya saben dónde está el problema. Tú también vas a poder hacerlo. Son cuatro miradas.

Mirada uno: ¿dónde está el router? Si está en el piso, dentro de un mueble o en la esquina de la casa, ya tienes el diagnóstico principal. El ochenta por ciento de los casos se resuelve aquí.

Mirada dos: ¿cómo están las antenas? Todas acostadas, todas pegadas en la misma posición, o apuntando con la punta hacia la sala: diagnóstico secundario. En una casa de una planta deben estar verticales; en dos plantas, mezcladas.

Mirada tres: ¿qué hay alrededor del router? Refrigerador al lado, espejo grande enfrente, microondas encima: enemigos localizados. Un metro de distancia mínima es la receta.

Mirada cuatro: ¿cuántas paredes hay entre el router y dónde se quejan? Si el cuarto del fondo está a tres paredes y solo hay señal de 5 GHz, el diagnóstico es de física, no de falla: hay que activar bien la 2.4 GHz o acercar un punto de acceso.

Con esas cuatro miradas ya puedes entrar a casa de tu mamá, de tu tío o de tu vecino, y decirle exactamente qué le pasa a su WiFi y cómo se arregla, antes de tocar nada. Esa es la diferencia entre alguien que "le sabe al internet" y alguien que adivina. Tú ya no adivinas: diagnosticas.

Ejemplos paso a paso

Ejemplo 1: Orientar las antenas en una casa de una planta

Supongamos que vives en una casa de una planta con tres recámaras, sala, cocina y un patio. Tu router tiene tres antenas externas. Esta es la receta paso a paso.

Paso 1: Coloca el router en el punto más céntrico posible de la casa, a una altura de 1 a 1.5 metros (sobre un librero o mesa alta), en un espacio abierto, no dentro de muebles.

Paso 2: Pon las tres antenas en posición vertical (paraditas, rectas hacia arriba). En una casa de una planta, la dona de señal acostada cubre todo el piso de forma pareja.

Paso 3: Separa ligeramente las antenas entre sí si la base lo permite: una recta, una inclinada unos 45 grados a la izquierda y otra 45 grados a la derecha. Esto mejora la diversidad y el MIMO sin perder la cobertura horizontal.

Paso 4: Verifica que ninguna antena quede apuntando su punta hacia una zona importante (recuerda: por la punta casi no sale señal).

Paso 5: Camina por la casa con tu celular y anota dónde la señal se ve débil. Si un cuarto lejano falla, no toques las antenas: primero prueba mover el router medio metro hacia ese cuarto.

Ejemplo 2: Orientar las antenas en una casa de dos plantas

Ahora la casa tiene planta baja y planta alta. El router está en la planta baja (donde llega el cable del internet). La receta cambia porque necesitas que la señal también suba.

Paso 1: Coloca el router en la planta baja, lo más céntrico posible y lo más alto que puedas (encima de un librero alto, por ejemplo). Mientras más alto esté, menos techo tiene que atravesar la señal para llegar arriba.

Paso 2: Si el router tiene 3 antenas: deja una vertical (cubre la planta baja en dona), inclina la segunda a 45 grados y pon la tercera horizontal (acostada). La antena horizontal genera una dona parada que manda señal hacia arriba y hacia abajo, ideal para el piso de arriba.

Paso 3: Si el router tiene 2 antenas: una vertical y una horizontal. La vertical cubre tu piso, la horizontal ayuda al otro piso.

Paso 4: Si el router tiene 4 antenas: dos verticales, una a 45 grados y una horizontal. Repartes cobertura pareja en tu piso y mandas señal hacia arriba.

Paso 5: Sube a la planta alta con tu celular y mide la señal en cada cuarto. Si arriba llega débil en todos lados, el problema puede ser el techo (los techos de concreto son duros). Considera subir el router aún más o, si no basta, agregar un punto de acceso en la planta alta conectado por cable.

Paso 6: No caigas en la trampa de comprar antenas de 9 dBi para "que suba la señal": la dona aplastada de alta ganancia sube menos, no más. Para dos pisos, ganancia moderada (3 a 5 dBi) con una antena horizontal funciona mejor.

Ejemplo 3: Mapa de calor casero midiendo cuarto por cuarto

Un mapa de calor es un dibujo de tu casa donde marcas qué tan fuerte llega la señal en cada cuarto. Los profesionales usan software caro; tú vas a usar tu celular y una hoja de papel. Es el diagnóstico más útil que existe.

Paso 1: Dibuja en una hoja el plano de tu casa: cada cuarto como un rectángulo, marca puertas y ventanas de forma aproximada. No tiene que ser bonito, tiene que ser útil. Marca con una X dónde está el router.

Paso 2: En tu celular, busca la intensidad de la señal WiFi en dBm. En Android, ve a Ajustes > Acerca del teléfono > Estado > WiFi (la ruta varía por marca; también hay apps gratis como "WiFi Analyzer" que muestran los dBm en grande). En iPhone, marca *3001#12345#* y entra al modo de campo para ver los dBm.

Paso 3: Párate en el centro de cada cuarto, espera 10 segundos a que el número se estabilice y anota el valor en dBm sobre tu plano. Mide también el patio, el baño y los pasillos.

Paso 4: Interpreta tus números con esta escala:

- 30 a -50 dBm: excelente (junto al router).
- 50 a -60 dBm: muy bueno (navegas y ves video sin problema).
- 60 a -70 dBm: aceptable (funciona, pero el video pesado puede fallar).
- 70 a -80 dBm: débil (páginas lentas, videollamadas cortadas).
- Menos de -80 dBm: zona muerta (casi no sirve).

Paso 5: Colorea tu plano: verde donde haya -60 o mejor, amarillo de -60 a -70, rojo donde haya peor de -70. Ahí tienes tu mapa de calor.

Paso 6: Mira el mapa y busca el patrón: ¿los rojos están todos del mismo lado? El router está descentrado. ¿Hay un cuarto rojo rodeado de verdes? Hay un obstáculo (refrigerador, espejo, pared de concreto). ¿Todo está amarillo-rojo menos junto al router? El router está muy bajo o encerrado.

Paso 7: Haz UN cambio (mover el router, subirlo, reorientar antenas) y vuelve a medir solo los puntos rojos y amarillos. Compara. Así sabes si tu cambio sirvió, con números, no con "se siente mejor".

Ejemplo 4: Llevar internet a otra construcción del terreno

Tienes tu casa y, al fondo del terreno (a treinta o cuarenta metros), un cuarto, un taller o la casa de un familiar. La señal omnidireccional no llega. Aquí es donde una antena direccional brilla.

Paso 1: Confirma que hay línea de vista: párate donde pondrías la antena y fíjate si ves la otra construcción. Árboles con mucho follaje y paredes en medio arruinan el enlace. Si no hay línea de vista, la antena direccional no es la solución (considera cable).

Paso 2: Elige una antena de panel direccional para WiFi (2.4 GHz si quieres atravesar mejor, o dual 2.4/5 GHz). Verifica que el conector sea RP-SMA compatible con tu router. Una de panel de 8 a 12 dBi es suficiente para decenas de metros.

Paso 3: Desenrosca UNA de las antenas omnidireccionales de tu router y enrosca la direccional en su lugar. Deja las demás omnidireccionales para que tu casa siga cubierta en dona.

Paso 4: Monta la antena de panel en un lugar alto (un poste, la pared exterior) apuntando directamente hacia la otra construcción. Mientras más alto y despejado, mejor.

Paso 5: En la otra construcción, coloca el aparato receptor (un celular, una laptop o un repetidor configurado como cliente) en el punto más cercano a tu casa, del lado que da hacia tu antena.

Paso 6: Ajusta el apuntamiento poco a poco: mueve la antena unos grados, mide la señal en el otro extremo, repite. El haz es angosto: unos grados de diferencia pueden ser la diferencia entre -65 dBm (funciona) y -80 dBm (no funciona).

Paso 7: Una vez que el enlace funciona, fíjalo bien (que el viento no lo mueva) y protéjelo de la lluvia si está a la intemperie.

Ejemplo 5: Las reglas de ubicación del router, en orden

Si no quieres leer toda la unidad, estas son las reglas en el orden en que debes aplicarlas. Es la lista de verificación que usan los técnicos.

Regla 1: Al centro. El router va lo más cerca posible del centro geométrico de la zona que quieres cubrir. Cada metro que lo alejas del centro es cobertura regalada a la calle.

Regla 2: En alto. Entre 1 y 1.5 metros del piso como mínimo. Arriba de un librero es mejor que debajo de la mesa.

Regla 3: Al aire libre. Nada de muebles cerrados, cajones ni clósets. Alrededor del router debe circular aire (también se calienta menos y dura más).

Regla 4: Lejos de enemigos. Mínimo un metro de distancia de refrigeradores, espejos grandes, tanques de agua, hornos de microondas y bocinas grandes con imanes.

Regla 5: Antenas según tu casa. Una planta: todas verticales. Dos plantas: mezcla verticales con inclinadas y al menos una horizontal.

Regla 6: Las dos bandas prendidas. 2.4 GHz para llegar lejos, 5 GHz para volar cerca. No apagues la de 2.4 "porque es lenta".

Regla 7: Mide, no adivines. Haz tu mapa de calor antes de comprar cualquier aparato. El mapa te dice si el problema es ubicación, obstáculo o distancia real.

Regla 8: Solo entonces, compra. Si después de optimizar todo lo gratis sigue habiendo zonas muertas reales, ahí sí considera un punto de acceso extra, un sistema mesh o una antena direccional según el caso.

Ejemplo 6: Qué hacer cuando el vecino interfiere

A veces el problema no es tu casa, es que vives en un edificio o fraccionamiento donde hay veinte redes WiFi peleando por el aire. Las antenas también ayudan aquí.

Paso 1: Con una app analizadora de WiFi (como WiFi Analyzer en Android), mira cuántas redes hay y en qué canales están. Si tu red está en el mismo canal que tres vecinos, ahí hay interferencia.

Paso 2: Cambia tu router a un canal libre (en 2.4 GHz, los canales 1, 6 y 11 son los que no se enciman; elige el menos ocupado).

Paso 3: Si el problema es un vecino con un router muy potente justo al lado de tu pared, orientar tus antenas no lo arregla, pero SÍ ayuda no empeorarlo: no subas tu potencia al máximo "para ganarle", porque solo crean más ruido los dos. Mejor cambia de canal y, si puedes, usa más la banda de 5 GHz, que tiene más canales y atraviesa menos paredes (la interferencia del vecino también llega menos).

Paso 4: Si vives en casa propia y el vecino de al lado te invade con su señal, una antena direccional de panel apuntando hacia el interior de TU casa (lejos de la pared del vecino) concentra tu señal donde la necesitas y "escucha" menos al vecino.

Paso 5: Como último recurso en edificios muy saturados, un sistema mesh bien colocado supera a un solo router peleando contra veinte redes, porque reparte la cobertura con varios puntos cercanos a tus aparatos en vez de un solo grito desde lejos.

Práctica

Ejercicio 1: Dibuja el plano de tu casa y marca las zonas muertas

Instrucciones: En una hoja de papel (o en una app de dibujo), dibuja el plano aproximado de tu casa: cada cuarto como un rectángulo, con puertas y ventanas marcadas de forma sencilla. Marca con una X el lugar donde está tu router y dibuja con flechas hacia dónde apuntan sus antenas. Después, camina por la casa usando tu celular, tu laptop o tu tableta y marca con color rojo los lugares donde el WiFi se pone lento o se desconecta (la sala de la tele, el baño, el cuarto del fondo, el patio). Esas son tus zonas muertas.

Solución paso a paso: Primero, no te preocupes porque el plano quede bonito; lo importante es que cada cuarto esté representado y que las distancias sean más o menos proporcionales. Segundo, la X del router te va a revelar el primer diagnóstico: si está en una esquina, en el piso o dentro de un mueble, ya encontraste al culpable principal. Tercero, une con una línea cada zona muerta con el router y fíjate qué hay en medio: ¿una pared de concreto? ¿el refrigerador? ¿dos cuartos de distancia? Cuarto, escribe junto a cada zona muerta tu hipótesis

en una frase: "el cuarto del fondo está rojo porque el router está en la esquina opuesta y hay dos paredes en medio". Este ejercicio no tiene una única respuesta correcta: el valor está en que por primera vez VES tu problema dibujado. La mayoría de las personas descubre aquí que su router está en el peor lugar posible, y eso ya es medio problema resuelto.

Ejercicio 2: Mide y registra la señal en dBm cuarto por cuarto

Instrucciones: Usando tu celular, mide la intensidad de la señal WiFi en dBm en el centro de cada cuarto de tu casa (en Android usa una app como WiFi Analyzer; en iPhone marca *3001#12345#* para ver el modo de campo). Anota cada valor en una tabla: cuarto, dBm medido, y qué estabas haciendo ahí (navegar, ver video, nada). Hazlo dos veces: una con las antenas como las tienes ahora, y otra después de ponerlas todas verticales (si tu casa es de una planta).

Solución paso a paso: Primero, asegúrate de medir siempre en el mismo punto de cada cuarto (por ejemplo, el centro) y esperando unos diez segundos a que el número se estabilice; si mides caminando, los números bailan y no sirven. Segundo, interpreta con la escala de la unidad: de -30 a -50 es excelente, de -50 a -60 muy bueno, de -60 a -70 aceptable, de -70 a -80 débil, y peor de -80 es zona muerta. Tercero, compara tus dos rondas de medición: en una casa de una planta, con las antenas verticales deberías ver mejoras de 3 a 10 dB en los cuartos lejanos respecto a tenerlas acostadas o en posiciones raras. Recuerda que la escala es logarítmica: 6 dB de mejora es una gran diferencia, aunque el número parezca pequeño. Cuarto, guarda tu tabla: es tu "antes". Cada cambio que hagas en el futuro (mover el router, subirlo) se compara contra esta tabla. Si un cuarto pasó de -78 a -68 dBm, tu cambio funcionó aunque todavía no sea perfecto. Medir te convierte de "creo que mejoró" a "sé que mejoró 10 dB".

Ejercicio 3: Reorienta las antenas y compara resultados

Instrucciones: Este ejercicio es para casas de dos plantas (o para una planta con un cuarto en un extremo muy lejano). Con tu tabla del ejercicio 2 como base, cambia la orientación de las antenas a la configuración recomendada: una vertical, una a 45 grados y una horizontal (si tienes tres antenas). Vuelve a medir los mismos puntos y compara.

Solución paso a paso: Primero, antes de mover nada, anota la configuración actual de tus antenas (tómale una foto con el celular para poder regresar si algo sale mal). Segundo, aplica la configuración nueva: vertical para tu piso, horizontal para mandar señal hacia arriba (la dona parada), y la de 45 grados como punto medio. Tercero, mide los mismos puntos de siempre, en el mismo orden. Cuarto, analiza: lo normal es que la planta donde está el router se

mantenga igual o mejore un poco, y que la planta de arriba mejore notablemente (de 5 a 12 dB de mejora es un resultado típico y excelente). Quinto, si la planta de arriba sigue en zona muerta (peor de -80 dBm) después del cambio, el problema probablemente es el techo: los techos de concreto con varilla son muy duros para el WiFi, y ahí la solución ya no es orientación sino un segundo punto de acceso arriba conectado por cable. Este ejercicio te enseña la lección más valiosa: hay problemas que se arreglan gratis (orientación) y problemas que requieren equipo (techo de concreto), y medir es lo que te dice cuál es cuál.

Ejercicio 4: Decide la ubicación ideal del router en tu casa

Instrucciones: Con tu plano del ejercicio 1 y tus mediciones del ejercicio 2, propón la ubicación ideal para tu router. Considera: el centro geométrico de la casa, la altura disponible (libreros, repisas), dónde entra el cable del internet, y los obstáculos (refrigerador, espejos, tanque de agua). Escribe tu propuesta en tres líneas: dónde está ahora, dónde debería estar, y qué necesitas para moverlo (un cable más largo, una repisa, etc.).

Solución paso a paso: Primero, marca en tu plano el centro geométrico aproximado: el punto que queda a distancias más parejas de todos los cuartos. Ese es tu objetivo ideal. Segundo, compara con la ubicación real: mide (a pasos) qué tan lejos está el router actual de ese centro. Cada dos o tres metros de descentrado son varios dB perdidos en el extremo lejano. Tercero, revisa la altura: si tu router está en el piso o dentro de un mueble, subirlo a un librero a 1.2 metros puede mejorar la señal entre 5 y 10 dB en los cuartos lejanos, gratis. Cuarto, verifica los enemigos cercanos: si a menos de un metro del router hay un refrigerador, un espejo grande o el microondas, aléjalo. Quinto, escribe tu plan concreto: "Mover el router del piso de la entrada (esquina) al librero de la sala (centro), necesito un cable de red de 5 metros y una extensión de luz". Un plan escrito se ejecuta; una idea vaga se olvida. Si después de moverlo vuelves a medir y los rojos de tu mapa se vuelven amarillos o verdes, acabas de arreglar tu WiFi sin gastar un peso.

Ejercicio 5: Elige la antena correcta para tres casos

Instrucciones: Para cada caso, decide qué tipo de antena conviene y explica por qué. Caso A: familia en un departamento de una planta que quiere buena señal en todos los cuartos. Caso B: señor que quiere llevar internet de su casa a su taller que está a 40 metros al fondo del terreno, con línea de vista despejada. Caso C: oficina pequeña que quiere cubrir un pasillo largo y angosto donde están los escritorios.

Solución paso a paso: Caso A: antenas omnidireccionales de 3 a 5 dBi, todas verticales. ¿Por qué? Porque un departamento necesita señal en todas direcciones (la dona), y la ganancia

moderada mantiene la dona gordita para cubrir parejo. Una direccional dejaría cuartos sin señal, y una de 9 dBi aplastaría la dona sin necesidad. Caso B: antena direccional de panel (o Yagi) de 8 a 12 dBi en la casa, apuntando al taller. ¿Por qué? Porque es un enlace punto a punto a distancia: necesitas el haz concentrado, no la dona. Se reemplaza una sola antena del router y se dejan las demás omnidireccionales para la casa. La línea de vista despejada es la condición que hace viable el enlace. Caso C: antena de panel direccional montada en la pared del extremo del pasillo, apuntando a lo largo del pasillo. ¿Por qué? Porque el pasillo es largo y angosto: la dona desperdiciaría señal en las paredes laterales, mientras que el haz del panel cubre justo el pasillo. Si el pasillo es muy largo, dos paneles (uno en cada extremo apuntándose) cubren todo. La moraleja del ejercicio: no hay antena "mejor", hay antena adecuada para cada forma del espacio. Dona para espacios abiertos en todas direcciones, haz para distancias y pasillos.

Ejercicio 6: Detecta el error en estas fotos mentales

Instrucciones: Lee cada descripción y encuentra qué está mal según lo aprendido en la unidad.

1) "Puse el router dentro del mueble de la tele para que no se vea, y le acosté las antenas para que quepa". 2) "Compré antenas de 12 dBi para mi casa de dos pisos porque quiero que la señal suba". 3) "Apagué la red de 2.4 GHz porque es lenta; solo dejé la de 5 GHz y ahora el cuarto del fondo no tiene señal". 4) "Puse el repetidor junto al router para que agarre buena señal y la repita".

Solución paso a paso: 1) Doble error: el mueble cerrado bloquea y calienta (error uno de la unidad), y las antenas acostadas ponen la dona parada, matando la cobertura horizontal (error cinco). Solución: sacar el router del mueble, subirlo, antenas verticales. 2) Error de concepto: más dBi aplasta la dona y la señal sube MENOS, no más. Para dos pisos se necesita ganancia moderada (3 a 5 dBi) con una antena horizontal, no 12 dBi. Además, probablemente viola el límite de EIRP si no se baja la potencia. 3) Error clásico: la banda de 5 GHz no atraviesa bien las paredes; la de 2.4 es la de alcance. Al apagarla, los cuartos lejanos se quedaron sin su banda. Solución: reactivar la 2.4 GHz. 4) Error de lógica: un repetidor junto al router repite una señal que ya es buena ahí, pero no extiende nada hacia la zona muerta. El repetidor debe ir a la MITAD del camino: donde todavía agarra señal decente del router (-60 a -70 dBm) pero ya está cerca de la zona muerta. Junto al router es un gasto inútil. Si resolviste los cuatro sin dudar, ya piensas como técnico.

Resumen de la unidad

- La antena no crea energía: decide hacia dónde va. Es como una bocina: reparte lo que ya tiene.
- Patrón de radiación: la dona (omnidireccional, señal en todas direcciones) y el haz (direccional, señal concentrada lejos).
- Omnidireccionales: los palitos del router, ideales para casas (señal en todas direcciones).
- Direccionales de panel: cajita plana con haz ancho, para patios, pasillos y enlaces cortos.
- Yagi: espina de pescado con haz angosto, para llevar internet a cientos de metros con línea de vista.
- Parabólicas: platos con haz finísimo, para enlaces de kilómetros entre edificios o torres.
- Ganancia (dBi): qué tanto concentra la antena la señal. Más dBi = más lejos pero zona más estrecha. Para casas, 3 a 5 dBi es lo ideal.
- EIRP: la potencia efectiva radiada; la ley pone un techo. No se arregla la cobertura con "más potencia a lo loco".
- Polarización: las antenas se entienden mejor cuando vibran igual. Verticales para una planta; mezcla con horizontales para dos plantas.
- Diversidad y MIMO: varias antenas evitan zonas muertas y mandan varios chorros de datos a la vez. No las quites ni las pongas todas igual.
- Antenas internas vs externas: las externas se orientan y se cambian; las internas ya vienen optimizadas pero no se ajustan.
- Conector RP-SMA: el estándar de las antenas desmontables WiFi. Verifica compatibilidad antes de comprar.
- 2.4 GHz atraviesa paredes; 5 GHz es más rápido pero se debilita con cada pared. Las dos bandas son un equipo.
- Ubicación de oro: centro de la casa, alto (1 a 1.5 m), al aire libre, lejos de metal, agua y espejos.
- Errores que matan la cobertura: router escondido, en el piso, en la esquina, antenas acostadas o todas iguales, apagar la 2.4 GHz.
- Mide con tu celular en dBm y haz tu mapa de calor: los números te dicen la verdad y te dicen si tus cambios funcionaron.
- Para llevar internet a otra construcción: antena direccional bien apuntada con línea de vista, no más potencia omnidireccional.

UNIDAD 7: Repetidores, puntos de acceso y redes mesh (Clases 19 a 21)

Introduccion

Hay un momento que todo el mundo vive tarde o temprano: estas en tu sala con el celular en la mano, el WiFi marca señal llena, todo jala perfecto, y caminas unos metros hacia el fondo de la casa... y de repente todo se muere. La página se queda cargando, el video se congela, el mensaje de WhatsApp no se envía. Caminas de regreso y como por arte de magia todo vuelve a funcionar. Eso que acabas de vivir se llama zona muerta, y esta unidad existe para que aprendas a eliminarlas para siempre.

Si tu casa es pequeña, probablemente nunca has sufrido este problema de forma seria. Un solo router bien colocado puede cubrir sin broncas un departamento de 60 o 80 metros cuadrados. Pero las casas crecen: de dos recamaras pasas a tres, luego construyes el cuarto de arriba, luego el papá quiere internet en el taller del fondo, luego alguien quiere ver Netflix en la terraza. Y cada pared que se atraviesa en el camino debilita la señal, como ya viste en la Unidad 2 cuando hablamos de atenuación. Tarde o temprano el WiFi llega a su límite, y cuando eso pasa tienes tres caminos: un repetidor, un punto de acceso cableado o un sistema mesh.

Estas tres soluciones suenan parecidas porque las tres hacen algo similar: llevar el WiFi más lejos. Pero por dentro funcionan de maneras muy distintas, cuestan distinto y dan resultados muy distintos. Elegir la equivocada significa tirar dinero y seguir con el mismo problema. Elegir la correcta significa tener internet rápido en cada rincón de tu casa, sin cortes, sin andar cambiando de red manualmente, sin pelear con la familia porque "en mi cuarto no hay internet".

En esta unidad vas a aprender exactamente eso: cuál es la solución correcta para cada situación. Vamos a desarmar las tres tecnologías por dentro para que entiendas cómo funcionan de verdad, no solo lo que dicen las cajas en la tienda. Vas a ver por qué el repetidor barato que venden en todas partes tiene una desventaja que casi nadie te explica: pierdes la mitad de tu velocidad. Vas a entender por qué los profesionales que instalan redes en oficinas y hoteles casi nunca usan repetidores, y en su lugar usan puntos de acceso cableados. Y vas a descubrir que es un sistema mesh, esa tecnología que en los últimos años se volvió la favorita de las casas grandes, con sus nodos que hablan entre sí y te pasan de uno a otro sin que te des cuenta.

Además, esta unidad es muy práctica. No solo vas a entender la teoría: vas a aprender a configurar un repetidor paso a paso, a convertir un router viejo que tengas guardado en un punto de acceso (una forma baratisima de mejorar tu red), y a instalar un sistema mesh de tres nodos desde cero, con la app, la ubicación correcta de cada nodo y las pruebas para comprobar que quedo bien. Y en la sección de práctica vas a resolver escenarios reales: tres casas distintas con tres problemas distintos, dónde tendrás que decidir cuál solución conviene y por qué.

Al terminar esta unidad vas a ser capaz de: explicar cómo funciona un repetidor y por qué pierde velocidad; configurar un repetidor sin ayuda; transformar un router viejo en un punto de acceso funcional; planear dónde colocar los nodos de un sistema mesh; decidir con criterio técnico si una casa necesita repetidor, punto de acceso o mesh; y medir con números reales la mejora que lograste. En pocas palabras: vas a dominar el tema de la cobertura WiFi, que es uno de los problemas más comunes que te van a pedir que resuelvas cuando la gente se entere de que sabes de redes.

Así que ponte comodo. Esta unidad es larga porque el tema lo merece: aquí se juega la diferencia entre una red que apenas sobrevive y una red que de verdad funciona en toda la casa.

El problema de las zonas muertas

Imaginate tu casa como una alberca y la señal WiFi como las ondas que se forman cuando avientas una piedra al centro. Las ondas llegan con fuerza a las orillas cercanas, pero si la alberca es muy grande, al fondo apenas se siente el movimiento. Con el WiFi pasa igual: el router lanza su señal en todas direcciones, pero cada metro que recorre y cada pared que atraviesa le quitan fuerza.

En la Unidad 1 aprendiste que el WiFi usa ondas de radio en las bandas de 2.4 GHz y 5 GHz, y en la Unidad 2 viste que la banda de 5 GHz es más rápida pero se debilita mucho más rápido con la distancia y los obstaculos. Esto es clave para entender las zonas muertas: no es que el router este descompuesto, es fisica pura. Una pared de concreto puede quitarle a la señal entre el 40 y el 60 por ciento de su fuerza. Dos paredes de concreto seguidas y practicamente ya no queda nada. Los espejos, los refrigeradores, las tuberias metalicas y hasta una pecera grande también bloquean la señal.

Las zonas muertas suelen aparecer en los mismos lugares de siempre: el cuarto más alejado del router, la planta de arriba si el router está abajo (o al revés), el patio o la terraza, el sótano, el taller o la oficina que está al fondo del terreno, y el baño de visitas que queda detrás de tres paredes. Si vives en una casa de dos pisos con el router en la sala de abajo, es casi seguro que arriba hay al menos un cuarto con señal débil.

Y aquí viene lo importante: el problema de las zonas muertas no se arregla comprando "más megas" con tu compañía de internet. Mucha gente piensa: "voy a subir mi plan de 100 a 300 megas para que llegue más lejos". No funciona así. La velocidad que contratas es la velocidad que llega a tu módem; la que llega a tu celular en el fondo de la casa depende de tu red WiFi interna. Si la señal llega débil, da igual que tengas 100 o 1000 megas contratados: tu celular solo va a aprovechar una fracción. Es como tener una tubería enorme de agua conectada a una manguerita delgada: el agua que sale depende de la manguerita, no de la tubería.

Tampoco se arregla subiendo el router a lo más alto del closet o pegándolo a la ventana "para que salga mejor". Esos son mitos. Lo que sí funciona es llevar la señal hasta donde se necesita, y para eso existen las tres soluciones de esta unidad.

Panorama: las tres soluciones en una mirada

Antes de entrar en detalle, quedate con esta idea general de cada solución:

El repetidor (o extensor) es el aparato más barato y fácil de instalar. Lo enchufas a la mitad del camino entre el router y la zona muerta, él toma la señal WiFi que recibe, la amplifica y la vuelve a lanzar. Suena perfecto, pero tiene un costo oculto: cómo usa la misma antena para escuchar y para hablar al mismo tiempo, pierde aproximadamente la mitad de la velocidad. Es como el juego del teléfono descompuesto que jugabas de niño: cada vez que el mensaje pasa de una persona a otra, llega un poco más lento y un poco más deformado.

El punto de acceso cableado es la solución profesional. Es un aparato que se conecta al router con un cable de red (Ethernet) y desde ahí crea su propia señal WiFi potente en la zona donde lo colocas. Como recibe internet por cable, no pierde velocidad: entrega el 100 por ciento de lo que le llega por el cable. Es lo que usan las oficinas, los hoteles y las escuelas. Su única desventaja real es que necesitas llevar un cable hasta donde lo vas a poner, y pasar cables por la casa a veces es un rollo.

El sistema mesh es la solución moderna para casas grandes. Son dos o tres aparatos (nodos) que se hablan entre si y forman una sola red inteligente. Tú te conectas una sola vez y el sistema te va pasando del nodo más cercano al siguiente sin que te des cuenta, sin cortes. Algunos sistemas mesh tienen una banda de radio dedicada solo para que los nodos hablen entre ellos (eso se llama backhaul dedicado) y así no pierden velocidad como el repetidor barato. Son más caros, pero dan la mejor experiencia para el usuario: simplemente funciona.

En la explicación detallada vamos a desarmar cada una de estas soluciones pieza por pieza. Vas a ver números reales, vas a entender los términos técnicos sin que te duela la cabeza, y vas a salir de esta unidad sabiendo exactamente que comprar y como instalarlo según tu caso.

Explicación detallada

Clase 19: Repetidores y extensores, cómo funcionan y sus desventajas

Qué es un repetidor y qué promete

Un repetidor WiFi, también llamado extensor de rango o "range extender", es un aparatito que se enchufa directo a la corriente eléctrica, normalmente del tamaño de un cargador grande de celular. Su promesa es simple y por eso se vende tanto: "duplica el alcance de tu WiFi". Lo compras, lo enchufas en un contacto a la mitad del camino entre tu router y la zona muerta, lo configuras en cinco minutos con una app o con un botón, y listo: donde antes no había señal, ahora hay.

Y la verdad es que si cumple lo que promete en cuanto a cobertura: la señal si llega más lejos. El problema está en lo que no te dice la caja: a que velocidad llega. Ahí es donde empieza la historia interesante de esta clase.

Como repite un repetidor: el problema del half-duplex

Para entender la desventaja del repetidor necesitas entender un concepto que ya tocamos de pasada en unidades anteriores: el half-duplex. Recuerda que el WiFi, a diferencia de una llamada telefónica normal, no puede hablar y escuchar al mismo tiempo en el mismo canal. Es como un walkie-talkie: cuando uno habla, el otro tiene que esperar a que termine para responder. Eso se llama half-duplex (medio duplex), y es una característica de cómo funciona el WiFi en general.

Ahora, un repetidor tiene un solo juego de radios trabajando en el mismo canal para hacer dos trabajos: primero tiene que escuchar lo que le manda el router, y después tiene que repetirlo hacia tus aparatos. Como no puede hacer las dos cosas al mismo tiempo, tiene que turnarse:

escucha un momento, luego habla, luego escucha, luego habla. Cada turno toma tiempo, y ese tiempo extra es latencia y velocidad perdida.

El resultado practico es el que dice el titulo de esta clase: un repetidor pierde aproximadamente la mitad de la velocidad. Si tu router manda 100 megas y el repetidor los recibe completos, lo que le entrega a tu celular anda por los 40 o 50 megas. Y ojo: eso es en el mejor de los casos, cuando el repetidor está bien colocado y recibe buena señal del router. Si el repetidor está mal colocado y recibe señal débil, repite señal débil: lento al cuadrado.

Aquí entra la analogía del teléfono descompuesto. De niño jugabas a que alguien susurraba una frase al oído del siguiente, ese se la pasaba al siguiente, y al final la frase llegaba toda cambiada y tardaba un buen rato en recorrer la fila. El repetidor es ese niño en medio de la fila: no inventa nada nuevo, solo repite lo que escucho, y cada repeticion cuesta tiempo. Si pones dos repetidores en cadena (uno repitiendo al otro), es como alargar la fila del teléfono descompuesto: la velocidad se vuelve a partir más o menos a la mitad. Por eso los técnicos dicen que encadenar repetidores es una mala idea: con dos repetidores en serie te puede quedar una cuarta parte de la velocidad original.

SSID extendido vs mismo SSID: el detalle que confunde

Cuando configuras un repetidor, te topas con una decision: que nombre le pones a la red que crea. Aquí hay dos escuelas y cada una tiene sus consecuencias.

La primera opcion es crear un SSID extendido, o sea, un nombre de red distinto. Por ejemplo, si tu red se llama "Casa_Garcia", el repetidor crea "Casa_Garcia_EXT". La ventaja es que siempre sabes a que aparato estas conectado: si ves "_EXT" sabes que estas en el repetidor. La desventaja es que tu celular no cambia solo de una red a otra de forma inteligente. Si caminas de la sala (donde está el router) al fondo (donde está el repetidor), tu celular se queda aferrado a la red del router aunque la señal ya este débil, hasta que la pierde por completo y entonces brinca a la red _EXT. Ese brinco se siente: se corta el video, se traba la llamada. Y al reves igual. Es molesto.

La segunda opcion es usar el mismo SSID y la misma contraseña que el router, de modo que las dos redes se llamen igual. Suena más elegante porque "es una sola red", pero en realidad el celular sigue sin saber cuál aparato le conviene: se conecta al primero que encuentra y se queda ahí pegado hasta que la señal se muere. El resultado es parecido al caso anterior, solo que ahora ni siquiera sabes a cuál estás conectado. A esto los técnicos le llaman "sticky client" (cliente pegajoso): el aparato se pega a un punto y no lo suelta.

Ninguna de las dos opciones le da al repetidor la capacidad de pasarte de un aparato a otro sin cortes. Eso que si existe se llama roaming, y lo tienen los sistemas mesh y los puntos de

acceso bien configurados, como veras en las clases 20 y 21. El repetidor, por barato que sea, no sabe hacer roaming de verdad.

Errores comunes con repetidores (y como evitarlos)

El error número uno, el que comete casi todo el mundo, es poner el repetidor donde ya no hay señal. Suena logico: "no hay internet en mi cuarto, pues pongo el repetidor en mi cuarto". Pero el repetidor no crea internet de la nada: necesita recibir buena señal del router para tener algo que repetir. Si lo pones en la zona muerta, lo único que va a repetir es una señal débil y llena de errores. La regla de oro es: el repetidor va a la MITAD del camino, en un punto donde todavía reciba señal decente del router (unas 3 rayitas de 4, o entre el 50 y 70 por ciento de señal). Desde ahí, su propia señal si alcanza a cubrir la zona muerta.

El error número dos es esperar velocidad completa. Ya sabes por qué: el half-duplex se come la mitad. Si contrataste 200 megas y en el cuarto del fondo te llegan 60 o 70 a traves del repetidor, eso es normal, no es que el aparato este descompuesto. El repetidor sirve para navegar, ver videos en calidad normal y usar redes sociales en zonas donde antes no había nada. No sirve para jugar en línea competitivo ni para videollamadas importantes en 4K desde la zona extendida.

El error número tres es mezclar marcas sin revisar compatibilidad. Un repetidor generico casi siempre funciona con cualquier router porque usa el estandar WiFi normal, pero las funciones extra (como la configuración con un boton WPS o las apps de administracion) a veces solo jalan bien entre aparatos de la misma marca. Si vas a comprar repetidor, no es obligatorio que sea de la misma marca que tu router, pero si compras todo de la misma marca la configuración suele ser más facil.

El error número cuatro es poner el repetidor junto a aparatos que generan interferencia: el microondas, el teléfono inalámbrico viejo, el monitor de bebe o una bocina Bluetooth grande. Ya viste en la Unidad 3 que la banda de 2.4 GHz esta llena de interferencias. Un repetidor colocado al lado del microondas va a repetir una señal llena de ruido cada vez que alguien caliente su comida.

Cuando SI conviene un repetidor

Después de tantas desventajas parece que el repetidor no sirve para nada, pero no es así. El repetidor es la herramienta correcta en casos especificos: cuando necesitas cubrir una zona muerta pequeña y ocasional, cuando el presupuesto es muy ajustado, cuando no puedes o no quieres pasar cables, y cuando la velocidad que necesitas en esa zona es modesta. Ejemplo típico: el cuarto de visitas que se usa dos veces al mes, la cochera donde solo quieres que el celular tenga señal para abrir el porton electrico, o el bano del fondo donde solo vas a ver

videos cortos. Para esos casos, un repetidor de 300 o 500 pesos resuelve el problema sin complicarte la vida. Solo entra con los ojos abiertos: sabes que pierdes la mitad de la velocidad y sabes dónde colocarlo.

Buenas prácticas si vas a usar repetidor

Colocalo a la mitad del camino con buena señal del router, lejos de interferencias y de preferencia en un contacto alto y despejado (no escondido detras del ropero). Si tu repetidor es de doble banda, deja que tus aparatos usen la banda de 5 GHz cerca de el y la de 2.4 GHz para llegar más lejos. Actualiza su firmware cuando la app te lo pida. Y si algun día notas que la zona extendida se puso lenta de repente, reinicialo: como cualquier mini computadora, a veces se atora y un reinicio lo arregla.

Clase 20: Puntos de acceso cableados, la solución profesional

Qué es un punto de acceso y en qué se diferencia de un router

Un punto de acceso (en inglés "access point", abreviado AP) es un aparato cuya única chamba es crear una red WiFi. No reparte direcciones IP, no se conecta a tu compañía de internet, no hace de firewall: solo toma el internet que le llega por un cable de red y lo convierte en señal WiFi. Piensa en el como una bocina: el router es el estéreo completo y el punto de acceso es una bocina extra que conectas con un cable para que la música suene en otro cuarto con toda su calidad.

La diferencia con el router es importante. Un router hace muchas cosas: se conecta al módem de tu compañía de internet, reparte direcciones IP a tus aparatos (eso se llama DHCP y lo viste en la Unidad 4), protege tu red y además crea WiFi. Un punto de acceso solo hace lo último: WiFi. Por eso cuando pones un punto de acceso en tu red, el router sigue siendo el jefe (sigue repartiendo IPs y controlando todo) y el punto de acceso es solo un empleado que extiende la cobertura.

Y aquí viene un concepto que causa mucha confusion: el modo AP. Muchos routers caseros tienen un modo de operación llamado "modo punto de acceso" o "modo AP". Cuando activas ese modo, el router apaga sus funciones de jefe (el DHCP, el firewall, la conexión al módem) y se comporta como un simple punto de acceso. Esto es buenísimo porque significa que no necesitas comprar un aparato especial: ese router viejo que tienes guardado en un cajón puede revivir como punto de acceso. En la sección de ejemplos paso a paso te enseñé exactamente como hacerlo.

Por qué el cable lo cambia todo

La razón por la que los profesionales prefieren el punto de acceso cableado es una sola palabra: cable. El punto de acceso recibe el internet por un cable Ethernet directo desde el router. El cable no sufre interferencias, no pierde velocidad con la distancia (hasta 100 metros sin broncas) y no tiene el problema del half-duplex del repetidor. Resultado: el punto de acceso entrega por WiFi prácticamente el 100 por ciento de la velocidad que le llega por el cable.

Haz las cuentas con el ejemplo de antes: contratas 200 megas. Con repetidor, en la zona extendida te llegan 60 o 70. Con punto de acceso cableado, te llegan los 200 completos (o lo máximo que tu aparato WiFi pueda aprovechar). La diferencia es brutal, y por eso en oficinas, hoteles, escuelas y empresas no veras repetidores por ningún lado: veras puntos de acceso en el techo, conectados por cable.

Además el cable le da estabilidad al punto de acceso. La señal que crea no depende de que tan bien le llegue el WiFi del router, porque no usa WiFi para conectarse al router: usa cable. No hay teléfono descompuesto aquí. Cada punto de acceso es una fuente de señal nueva, fuerte y limpia, justo donde la necesitas.

Cableado Ethernet y PoE básico

Para instalar un punto de acceso necesitas llevar un cable Ethernet desde tu router (o desde un switch, que es como un multicontacto para cables de red) hasta el lugar donde va el punto de acceso. El cable que se usa normalmente es el famoso cable de red azul o amarillo con conectores que parecen de teléfono pero más grandes (conectores RJ45). Las categorías más comunes hoy son Cat5e y Cat6: las dos aguantan 1 Gbps (1000 megas), más que suficiente para una casa. El Cat6 es un poco mejor contra interferencias y es el recomendado si vas a pasar el cable junto a cables eléctricos.

Un cable Ethernet puede medir hasta 100 metros sin perder velocidad, así que en una casa normal la distancia no es problema. Lo que sí es un tema es pasar el cable físicamente: por el techo falso, por canaletas de plástico pegadas a la pared, por detrás de los muebles o, en el mejor de los casos, aprovechando tubería que ya exista en la pared. No necesitas ser electricista para esto, pero sí da un poco de trabajo. Mucha gente contrata a alguien para pasar dos o tres cables y le sale barato comparado con comprar un sistema mesh caro.

Y aquí entra el PoE, que significa "Power over Ethernet" (energía sobre Ethernet). Es una tecnología que manda electricidad por el mismo cable de red que lleva los datos. Para que sirva: muchos puntos de acceso profesionales no traen eliminador de corriente; en su lugar se alimentan por el cable de red. Esto es una maravilla porque puedes poner el punto de acceso en el techo, en el pasillo de arriba o en el patio, sin necesitar un contacto eléctrico cerca. Solo necesitas que del otro lado del cable haya un aparato que mande energía: un switch con PoE o un inyector PoE (un aparatito barato que se enchufa entre el router y el cable). Si compras

un punto de acceso y dice "PoE", ya sabes que se alimenta por el cable y necesitas switch o inyector PoE. Si dice que trae eliminador, pues lo enchufas normal y listo.

Dónde se colocan y cuántos necesitas

El punto de acceso se coloca donde se necesita la cobertura, no a la mitad del camino como el repetidor. Cómo le llega internet por cable, lo pones justo en la zona muerta o en el centro de la zona que quieres cubrir: en el pasillo de la planta alta, en el techo de la sala de arriba, en la pared del taller del fondo. Los profesionales los ponen en el techo porque desde ahí la señal se reparte parejo hacia todos lados y no hay muebles estorbando.

Cuántos necesitas depende del tamaño y la construcción de tu casa, pero una regla práctica para casas de concreto (que es lo común en México) es: un punto de acceso por cada 70 a 100 metros cuadrados por planta, o uno por planta en casas de dos pisos. Una casa de 150 metros cuadrados en dos plantas normalmente queda perfecta con el WiFi del router abajo y un punto de acceso cableado arriba. Una casa de una sola planta pero muy larga puede necesitar dos puntos bien repartidos.

Roaming con puntos de acceso: que tu celular cambie solo

Un detalle importante: si pones dos o tres puntos de acceso con el mismo nombre de red (SSID) y la misma contraseña, tus aparatos van a ver "una sola red" y van a cambiar de un punto a otro cuando te muevas. Pero ojo: ese cambio lo decide tu celular, no la red, y los celulares son medio flojos para cambiar: se aferran al punto actual hasta que la señal está muy débil. En la práctica funciona aceptable para caminar por la casa viendo un video, pero puede haber un cortecito de un segundo al cambiar. Los sistemas mesh hacen esto mejor porque coordinan el cambio de forma inteligente, como veras en la clase 21. Aun así, varios puntos de acceso bien colocados con el mismo SSID dan una experiencia muy decente y muy estable.

Ventajas y desventajas resumidas

Ventajas del punto de acceso cableado: velocidad completa sin pérdidas, máxima estabilidad, puedes poner tantos como necesites, los equipos son baratos (un punto de acceso básico cuesta parecido a un repetidor bueno), y puedes revivir routers viejos en modo AP sin gastar nada. Desventajas: necesitas pasar cables (es el único pero real), y el roaming entre puntos es bueno pero no tan fino como el de un mesh.

Clase 21: Sistemas mesh, que son, backhaul dedicado, roaming sin cortes y como elegirlos

Qué es un sistema mesh

Un sistema mesh es un conjunto de dos o tres aparatos iguales llamados nodos que trabajan en equipo para crear una sola red WiFi grande e inteligente. Uno de los nodos se conecta al módem o router de tu compañía de internet (ese es el nodo principal) y los demás nodos se colocan repartidos por la casa. Los nodos hablan entre sí por WiFi (o por cable, si quieres) y entre todos cubren toda la casa con una sola red, un solo nombre, una sola contraseña.

La palabra "mesh" significa malla en inglés, y la idea es esa: los nodos forman una malla donde cada uno puede hablar con los demás. Si un nodo se apaga o falla, los otros buscan rutas alternas para seguir conectados. Es una red que se organiza sola.

La analogía del equipo de relevos funciona perfecto aquí. En una carrera de relevos, los corredores están repartidos por la pista y se van pasando la estafeta sin que la carrera se detenga. En un sistema mesh, los nodos son los corredores y tu celular es la estafeta: cuando caminas por la casa, los nodos se van pasando tu conexión del uno al otro sin que se corte nada. Tú no haces nada: no cambias de red, no metes contraseñas, no se traba el video. La carrera sigue.

Esto es lo que más enamora del mesh: la experiencia de usuario. Con repetidores andas batallando con redes _EXT y cortes al cambiar. Con mesh simplemente funciona. Por eso, aunque son más caros, se volvieron la solución favorita para casas grandes en los últimos años.

Mesh vs repetidor: las diferencias que importan

Aunque a simple vista "los dos extienden el WiFi", por dentro son mundos distintos. El repetidor es un aparato tonto que repite lo que escucha, pierde la mitad de la velocidad y no coordina nada con el router. El sistema mesh es un equipo coordinado: los nodos usan el mismo sistema operativo, se hablan entre ellos con un protocolo común, deciden juntos cuál nodo atiende a cada aparato y te pasan de uno a otro de forma inteligente.

Otra diferencia grande: el repetidor crea una red separada (aunque le pongas el mismo nombre, por dentro no hay coordinación). El mesh crea una sola red de verdad, administrada desde una sola app donde ves todos los nodos, todos tus aparatos conectados y hasta puedes pausar el internet de los hijos a la hora de la cena. Esa administración centralizada es parte del encanto.

Y la diferencia técnica más importante es el backhaul, que es el tema de la siguiente sección.

Backhaul: la carretera privada de los nodos

Backhaul es una palabra técnica que vale la pena aprender porque es la clave para elegir un buen sistema mesh. El backhaul es la conexión que usan los nodos para hablar ENTRE

ELLOS. Piénsalo así: los nodos tienen dos chambas: atender a tus aparatos (tu celular, tu tele) y pasar información entre ellos para llevarla hasta el nodo principal que está conectado a internet. Esa segunda chamba, la comunicación entre nodos, es el backhaul.

Hay dos tipos. El backhaul inalámbrico compartido es cuando los nodos usan las mismas bandas de radio para hablar entre ellos y para atenderte a ti. Esto tiene un problema parecido al del repetidor: la radio se tiene que turnar entre atenderte y hablar con el otro nodo, y eso cuesta velocidad. Los sistemas mesh baratos (de dos bandas) usan este esquema, y aunque son mucho mejores que un repetidor por su coordinación inteligente, si pierden algo de velocidad en los nodos lejanos.

El backhaul dedicado es cuando el sistema tiene una banda de radio extra usada SOLO para que los nodos hablen entre ellos. Los sistemas mesh tribanda (tres bandas: 2.4 GHz, 5 GHz y otra de 5 GHz extra, o 6 GHz en los más nuevos) dedican esa tercera banda al backhaul. Es como una carretera privada solo para los camiones de la empresa: mientras tus aparatos usan las bandas normales sin estorbos, los nodos se comunican entre ellos por su carril exclusivo a toda velocidad. Resultado: los nodos lejanos entregan casi la misma velocidad que el nodo principal. Esta es la razón por la que un mesh tribanda cuesta más: literalmente trae más radios por dentro.

Y hay un tercer caso, el mejor de todos: el backhaul por cable. Casi todos los sistemas mesh permiten conectar los nodos entre sí con cable Ethernet. Si puedes pasar cables, un mesh con backhaul cableado es la combinación ganadora: la inteligencia y el roaming del mesh más la velocidad completa y la estabilidad del cable. Es lo que los profesionales instalan cuando el presupuesto lo permite.

En resumen para que no se te olvide: backhaul compartido = bueno pero pierde algo; backhaul dedicado (tribanda) = muy bueno, casi sin pérdidas; backhaul por cable = excelente, lo mejor posible.

Roaming sin cortes: 802.11k, 802.11v y 802.11r explicados simple

El roaming es el arte de pasar tu conexión de un nodo a otro sin que se corte. Los sistemas mesh lo hacen bien gracias a tres estándares WiFi que trabajan en equipo. No necesitas memorizar los números, pero sí entender la idea de cada uno porque a veces los verás mencionados en las cajas y en las apps.

El 802.11k es el "mapa". Le permite a tu celular pedirle a la red una lista de los nodos cercanos con su nivel de señal. Es como cuando llegas a una plaza comercial y ves el mapa que dice "usted está aquí" con todas las tiendas marcadas: tu celular ya no anda a ciegas, sabe que opciones tiene antes de cambiar.

El 802.11v es el "consejero". Le permite a la red sugerirle a tu celular que se cambie a otro nodo mejor. Es como el anfitrión de un restaurante que te dice "oiga, hay una mesa mejor junto a la ventana, quiere que lo cambie". La red ve que estás pegado a un nodo lejano con señal débil y te sugiere el nodo cercano. Tu celular normalmente acepta la sugerencia.

El 802.11r es el "pase rápido". Normalmente, cuando tu celular se cambia de un nodo a otro tiene que volver a autenticarse (volver a presentar sus credenciales), y eso toma unas décimas de segundo que se sienten como un corte. El 802.11r permite que la autenticación se haga por adelantado, así el cambio es casi instantáneo. Es como tener pase VIP en un concierto: no haces fila, pasas directo.

Juntos, estos tres estándares hacen que caminar por la casa hablando por videollamada sea una experiencia sin cortes: el mapa (k) le dice a tu celular a dónde puede ir, el consejero (v) le sugiere cuando cambiar, y el pase rápido (r) hace que el cambio sea instantáneo. Los buenos sistemas mesh traen los tres activados. Los repetidores baratos no traen ninguno, por eso se sienten los cortes.

Un detalle honesto: el roaming también depende de tu celular. Los teléfonos modernos (de los últimos 5 o 6 años) soportan estos estándares sin problema. Un celular muy viejo puede no aprovecharlos y comportarse como cliente pegajoso. Pero incluso así, el mesh le da mejor experiencia que un repetidor.

Cuántos nodos necesitas según los metros cuadrados

Esta es la pregunta del millón antes de comprar. La respuesta depende del tamaño de tu casa, pero también del material de las paredes y de cuántos pisos tienes. Aquí van reglas prácticas para casas de concreto típicas en México:

Casa o departamento de hasta 120 metros cuadrados en una sola planta: normalmente basta con 2 nodos (el principal más uno). Si el departamento es chico y de una planta, hasta un buen router solo puede bastar; el mesh de 2 nodos es para cuando hay zonas muertas puntuales.

Casa de 120 a 250 metros cuadrados, o de dos plantas: 3 nodos es el punto ideal y es el paquete más vendido. Un nodo abajo cerca del módem, uno arriba en el pasillo y uno más cubriendo el fondo o la terraza.

Casa de 250 a 400 metros cuadrados o de tres plantas: 4 nodos, o 3 nodos tribanda bien colocados. Aquí ya vale la pena considerar el backhaul dedicado porque las distancias entre nodos son mayores.

Más de 400 metros cuadrados, terrenos grandes o construcciones con mucho concreto y metal: aquí la cosa se pone seria. Puede convenir una mezcla: mesh con backhaul por cable,

o puntos de acceso cableados profesionales. En estos casos a veces sale más barato y más estable contratar a alguien que pase cables y ponga puntos de acceso que comprar 5 o 6 nodos mesh.

Ojo con la trampa de "más nodos es mejor". Poner nodos de más, muy pegados entre si, causa interferencia entre ellos mismos y puede empeorar la red. Cada nodo debe estar lo suficientemente lejos del anterior para extender la cobertura, pero lo suficientemente cerca para tener buena comunicacion entre ellos. La regla de oro: cada nodo debe colocarse donde todavía reciba señal buena o excelente del nodo anterior (igual que el repetidor, a la mitad del camino, no en la zona muerta). Las apps de los sistemas mesh traen una prueba de ubicacion que te dice si el nodo quedo muy lejos o muy cerca: úsala, para eso esta.

Como elegir un sistema mesh: guia de compra sin marcas

Cuando vayas a comprar, compara estos puntos en lugar de dejarte llevar por la caja más bonita:

Número de bandas: si tu casa es grande o tu plan de internet es de más de 300 megas, busca tribanda (con backhaul dedicado). Si tu casa es mediana y tu plan es modesto, un doble banda bueno puede bastar y cuesta menos.

Estandar WiFi: busca WiFi 6 como mínimo hoy en día (ya lo viste en la Unidad 5). WiFi 6E o WiFi 7 son mejores pero más caros; valen la pena si tus aparatos son nuevos y tu plan de internet es rápido.

Puertos Ethernet: revisa que cada nodo traiga al menos uno o dos puertos de red. Sirven para conectar por cable la tele, la consola de videojuegos o una computadora de escritorio, y también sirven para hacer backhaul por cable entre nodos si algun día pasas cables. Un nodo sin puertos Ethernet te limita mucho.

Compatibilidad con tu módem: el nodo principal se conecta al módem de tu compañía de internet. Casi siempre funciona sin broncas, pero si tu módem también es router (casi todos lo son), vas a tener dos aparatos repartiendo direcciones IP, lo que causa un problema llamado doble NAT. La solución facil: pon el módem de tu compañía en modo puente (bridge) o desactiva su WiFi y deja que el mesh sea el único que reparte. En los ejemplos paso a paso te digo como.

App y funciones: todos los mesh se configuran por app. Revisa que la app te deje ver los aparatos conectados, hacer pruebas de velocidad por nodo, crear red de invitados y poner control parental si lo necesitas. Casi todos lo traen, pero la calidad de la app varia.

Mezclar marcas: en general no se puede. Cada marca usa su propio sistema para que los nodos hablen entre ellos. Si compras un mesh, compra todos los nodos de la misma marca y de preferencia de la misma familia o generacion. Hay un estandar nuevo que promete compatibilidad entre marcas, pero al dia de hoy lo seguro es no mezclar.

Precio realista: un mesh decente de 3 nodos doble banda anda en un rango accesible; uno tribanda cuesta bastante más. No compres el más barato del mercado sin revisar que tenga WiFi 6 y buenos puertos, porque lo barato sale caro cuando a los 6 meses quieres más velocidad.

Analogías para no olvidar

El repetidor es el teléfono descompuesto: repite lo que escucha, cada repeticion cuesta la mitad de la velocidad, y si lo pones donde ya no se escucha nada, no tiene nada que repetir.

El punto de acceso es la bocina con cable: la conectas al estéreo y suena con toda la calidad en otro cuarto, porque el cable le lleva todo sin pérdidas.

El mesh es el equipo de relevos: los corredores se pasan la estafeta sin detener la carrera, cada uno corre su tramo a toda velocidad, y tu ni te das cuenta del cambio.

Ejemplos paso a paso

Ejemplo 1: Como configurar un repetidor paso a paso

Este tutorial sirve para la mayoría de los repetidores genericos. El proceso varia un poco segun la marca, pero los pasos son los mismos.

PASO 1: Elige la ubicacion correcta.

Enchufa el repetidor a la MITAD del camino entre tu router y la zona muerta, en un contacto donde tu celular todavia marque 3 de 4 rayitas de WiFi del router. No lo pongas dentro de la zona muerta. Lejos del microondas y de bocinas grandes.

PASO 2: Enchufa el repetidor y espera.

Conectalo a la corriente y espera 1 o 2 minutos a que encienda por completo. Normalmente una luz parpadea y luego se queda fija cuando esta listo para configurar.

PASO 3: Conectate a la red del repetidor.

En tu celular o computadora busca las redes WiFi disponibles.

Aparecera una red nueva con el nombre del repetidor (algo como "Repetidor_XXXX" o el nombre de la marca). Conectate a ella. No te preocupes si dice "sin internet": es normal en este paso.

PASO 4: Abre la pagina de configuracion.

Casi todos los repetidores te abren solos una pagina al conectarte.

Si no se abre sola, abre el navegador y escribe la direccion que dice el manual (normalmente algo como 192.168.0.1, 192.168.1.1 o una direccion con el nombre de la marca). Si te pide usuario y contrasena, vienen en la etiqueta del aparato o en el manual (tipico: admin / admin).

PASO 5: Elige tu red WiFi en la lista.

El repetidor va a buscar las redes cercanas y te muestra una lista.

Elige la red de tu casa (la del router), escribe su contrasena y dale a conectar o "siguiente".

PASO 6: Decide el nombre de la red extendida.

Te dara la opcion de ponerle un nombre. Puedes dejar el que sugiere (tu red mas "_EXT") o ponerle el mismo nombre de tu red.

Recomendacion para principiantes: usa el nombre con "_EXT" para que siempre sepas a cual red estas conectado.

PASO 7: Espera a que se conecte y verifica.

El repetidor se va a reiniciar (tarda 1 o 2 minutos). Cuando termine, busca en tu celular la red "_EXT", conectate con la misma contrasena de tu WiFi y haz una prueba: abre un video o haz una prueba de velocidad.

PASO 8: Ajusta la ubicacion si hace falta.

Camina hasta la zona muerta con el celular conectado a la red "_EXT".

Si la velocidad es muy baja o se corta, el repetidor quedo muy lejos del router: acercalo un poco hacia el router y vuelve a probar. Si la zona muerta sigue sin cubrirse, aleja el repetidor un poco hacia la zona muerta.

Repíte hasta encontrar el punto medio ideal.

Listo. Ya tienes tu zona extendida. Recuerda: es normal que la velocidad sea como la mitad de la que tienes junto al router. Si necesitas más velocidad ahí, la solución es un punto de acceso o un mesh, no otro repetidor.

Ejemplo 2: Como convertir un router viejo en punto de acceso

Si tienes un router viejo guardado (el que te dio tu compañía de internet antes, o uno que compraste hace años), puedes convertirlo en punto de acceso gratis. Necesitas un cable Ethernet largo que vaya desde tu router actual hasta dónde vas a poner el router viejo.

PASO 1: Resetea el router viejo.

Con el router viejo enchufado, busca el botoncito de reset (un hoyito pequeño). Con un clip o un palillo, presionalo unos 10 segundos hasta que las luces parpadeen. Esto lo deja como nuevo, sin contraseñas viejas.

PASO 2: Conectate al router viejo para configurarlo.

Conecta tu computadora o celular a la red WiFi que crea el router viejo (su nombre viene en su etiqueta) o conéctalo con un cable a tu computadora. Abre el navegador y entra a su página de configuración (la dirección viene en la etiqueta: típico 192.168.0.1 o 192.168.1.1). Entra con el usuario y contraseña de fábrica (vienen en la etiqueta).

PASO 3: Cambia su dirección IP para que no choque con tu router actual.

Busca la sección de "Red LAN" o "Configuración de red local".

Tu router actual probablemente usa 192.168.1.1. Cambia el router viejo a 192.168.1.2 (el mismo inicio, diferente final). Guarda los cambios.

El router viejo se va a reiniciar; vuelve a entrar a su configuración pero ahora usando la nueva dirección (192.168.1.2).

PASO 4: Desactiva el DHCP del router viejo.

Busca la sección "DHCP" o "Servidor DHCP" y APAGALO.

Esto es importantísimo: si hay dos aparatos repartiendo direcciones IP en tu red, todo se vuelve un caos. El único que debe repartir IPs es tu router actual. El router viejo solo va a crear WiFi.

PASO 5: Configura el WiFi con el mismo nombre y contraseña de tu red actual.

Ve a la sección de WiFi o "Wireless". Ponle el MISMO nombre de red (SSID) y la MISMA contraseña que tu red principal. Así tus aparatos lo verán como parte de la misma red.

PASO 6 (opcional pero recomendado): Busca el "modo AP" o "modo punto de acceso". Muchos routers tienen un ajuste llamado "Modo de operación" donde puedes elegir "Modo AP" o "Access Point". Si el tuyo lo tiene, actívalo: hace automáticamente los pasos 3 y 4 por ti. Si no lo tiene, con los pasos 3, 4 y 5 ya quedo bien.

PASO 7: Conecta el cable.

Lleva un cable Ethernet desde un puerto LAN de tu router actual (cualquiera de los puertos amarillos numerados, NO el puerto WAN o "Internet") hasta un puerto LAN del router viejo (tambien un puerto amarillo numerado, NO el puerto WAN). Este es el error mas comun: el cable va de LAN a LAN.

PASO 8: Coloca el router viejo donde se necesita y prueba.

Ponlo en la zona donde quieres cobertura (arriba, al fondo, donde sea), enchufalo y espera 2 minutos. Conectate al WiFi y haz una prueba de velocidad: deberias tener casi la misma velocidad que junto al router principal, porque el internet le llega por cable.

Felicidades: acabas de crear un punto de acceso profesional con un aparato que ibas a tirar. Esta es una de las mejores mejoras calidad-precio que existen en redes caseras.

Nota: si tu router viejo es muy antiguo (solo WiFi 4 o de una sola banda), va a funcionar pero con la velocidad de su epoca. Para navegar y videos está bien; para sacarle jugo a un plan rápido de internet, mejor un punto de acceso moderno.

Ejemplo 3: Como instalar y configurar un sistema mesh de 3 nodos

Este tutorial cubre el proceso general que siguen casi todas las marcas: se hace todo desde una app en tu celular.

PASO 1: Prepara todo antes de empezar.

Ten a la mano: tu celular con la app del sistema mesh ya instalada, tu red WiFi actual y su contraseña, y los 3 nodos enchufados cerca del modem para la configuracion inicial. Apunta en un papel donde piensas poner cada nodo.

PASO 2: Configura el nodo principal.

Conecta el primer nodo con un cable Ethernet al modem de tu compania de internet (al puerto LAN del modem). Enchufalo a la corriente, abre la app y sigue el asistente: la app lo va a detectar, te va a pedir crear el nombre de tu nueva red WiFi y su contraseña. Consejo: usa el mismo nombre y contraseña de tu red anterior para que todos tus aparatos se conecten solos sin que tengas que reconfigurarlos.

PASO 3: Apaga el WiFi del modem de tu compania (recomendado).

Si tu modem tambien crea WiFi, entra a su configuracion y apaga su red inalambrica, o ponlo en modo puente (bridge). Asi evitas que haya dos redes peleando y el mesh queda como el unico jefe de tu WiFi. Si no sabes como, busca en internet "[tu compania] modem modo puente" o "[tu compania] desactivar WiFi del modem".

PASO 4: Agrega el segundo nodo.

En la app, elige "agregar nodo". Enchufa el segundo nodo en la ubicacion planeada: a la mitad del camino hacia la zona que quieres cubrir, donde todavia haya buena senal del nodo principal. La app te va a guiar y te va a decir si la ubicacion es buena, regular o mala. Si te dice que esta muy lejos, acercalo al principal.

PASO 5: Agrega el tercer nodo.

Repite el proceso con el tercer nodo, colocandolo para cubrir la zona restante (por ejemplo, la planta alta o el fondo de la casa). Cada nodo debe quedar a una distancia razonable del nodo mas cercano, no todos amontonados junto al principal.

PASO 6: Espera a que la red se estabilice.

Los nodos tardan unos 10 a 15 minutos en hablar entre ellos, actualizarse y optimizar las rutas. No los muevas ni los apagues en este rato. Aprovecha para tomarte un cafe.

PASO 7: Haz pruebas en cada zona de la casa.

Camina por toda la casa con tu celular conectado a la red mesh y en cada cuarto haz una prueba de velocidad (hay apps gratis de "speed test").

Anota los resultados: sala, cocina, cuartos, bano, terraza, cochera.

Todos los puntos importantes deberian tener velocidad suficiente para lo que se hace ahi (videos, videollamadas, juegos).

PASO 8: Ajusta ubicaciones segun los resultados.

Si un cuarto quedo con velocidad baja, mueve el nodo mas cercano un poco hacia el nodo principal (probablemente quedo muy lejos). Si dos nodos quedaron muy pegados, separa uno hacia la zona que peor quedo. Vuelve a hacer pruebas. Repite hasta que toda la casa quede bien cubierta.

PASO 9: Explora la app y activa lo útil.

Revisa la lista de aparatos conectados (así ves que todo se conecta), activa la red de invitados (para visitas, sin darles tu contraseña principal), y si hay niños en casa, configura el control parental con horarios. Activa las actualizaciones automáticas para que el sistema se mantenga al día.

Con esto tu casa queda cubierta por una sola red inteligente. Camina de un extremo a otro viendo un video: no debería cortarse. Si algún día agregas un cuarto o construyes arriba, casi todos los sistemas te dejan agregar un nodo más sin reconfigurar todo.

Práctica

Ejercicio 1: La casa de Dona Marta, que solución conviene

Dona Marta vive en una casa de una planta de 90 metros cuadrados. El router está en la sala, al centro de la casa. El único problema es el cuarto de visitas al fondo, donde la señal llega débil y a veces se corta el video. Ese cuarto se usa dos veces al mes cuando viene su hija. Su presupuesto es ajustado y no quiere complicarse con cables ni instalaciones.

Pregunta: que solución le recomiendas (repetidor, punto de acceso o mesh) y por qué.

Solución explicada paso a paso:

Paso 1: Identifica el tamaño del problema. Es una zona muerta pequeña y puntual: un solo cuarto al fondo. El resto de la casa funciona bien. No es un problema de toda la casa.

Paso 2: Identifica el uso. El cuarto se usa ocasionalmente (dos veces al mes) para ver videos. No se necesita velocidad máxima ni roaming perfecto.

Paso 3: Identifica las restricciones. Presupuesto ajustado, sin ganas de pasar cables, quiere algo fácil.

Paso 4: Descarta opciones. Un sistema mesh sería gastar de más para un problema chiquito y ocasional. Un punto de acceso cableado daría la mejor velocidad, pero requiere pasar un cable hasta el fondo y Dona Marta no quiere instalaciones.

Paso 5: Conclusion. La solución correcta es un repetidor barato. Cubre exactamente lo que necesita: llevar señal usable al cuarto de visitas de forma facil y economica. Hay que explicarle dos cosas: que lo ponga a la mitad del camino (en el pasillo, no dentro del cuarto de visitas) y que la velocidad ahí sera como la mitad de la sala, suficiente para ver videos. Si algun dia el cuarto se usa diario o necesita más velocidad, entonces si se piensa en punto de acceso o mesh.

Ejercicio 2: La casa de dos pisos de la familia Torres, que solución conviene

La familia Torres vive en una casa de dos pisos, 180 metros cuadrados. El módem con router está en la sala de abajo. Arriba hay tres recamaras y un estudio donde los hijos toman clases en línea y hacen videollamadas todos los días. Arriba la señal llega débil y las clases se traban. Tienen presupuesto medio y el papá esta dispuesto a pasar un cable por la escalera si hace falta.

Pregunta: que solución le recomiendas y por qué.

Solución explicada paso a paso:

Paso 1: Identifica el tamaño del problema. No es un cuarto ocasional: es toda la planta alta, con tres recamaras y un estudio de uso diario e importante (clases en línea).

Paso 2: Identifica el uso. Videollamadas y clases en línea diarias necesitan velocidad estable y baja latencia. Un repetidor que pierde la mitad de la velocidad y mete latencia extra es mala idea para este uso.

Paso 3: Identifica las restricciones. Presupuesto medio, pero hay disposicion a pasar un cable. Eso abre la puerta a la solución profesional.

Paso 4: Compara opciones. Repetidor: barato pero lento e inestable para clases diarias, descartado. Mesh de 3 nodos: funcionaría muy bien y daría roaming sin cortes, pero cuesta más. Punto de acceso cableado: con un solo cable hasta la planta alta y un punto de acceso (o un router viejo en modo AP) se cubre toda la planta de arriba con velocidad completa y máxima estabilidad, a una fraccion del costo del mesh.

Paso 5: Conclusion. La mejor relacion costo-beneficio es un punto de acceso cableado en la planta alta. Un solo cable por la escalera o por un ducto, un punto de acceso en el pasillo de arriba con el mismo nombre de red, y listo: clases sin trabas y velocidad completa. Si el presupuesto lo permitiera y quisieran la máxima comodidad (roaming perfecto y app bonita), el mesh de 3 nodos sería la opcion premium. Pero para este caso, el punto de acceso gana.

Ejercicio 3: El terreno grande de Don Beto, que solución conviene

Don Beto tiene una casa de 300 metros cuadrados en un terreno amplio: la casa principal, un taller al fondo a 25 metros de la casa y una terraza donde hace carnes asadas los fines de semana. Quiere WiFi bueno en los tres lugares. El taller lo usa diario para ver tutoriales en YouTube mientras trabaja. No quiere cables por todo el patio porque "se ven feos", y tiene buen presupuesto.

Pregunta: que solución le recomiendas y por qué.

Solución explicada paso a paso:

Paso 1: Identifica el tamaño del problema. Son tres zonas separadas por distancia considerable, incluyendo un edificio aparte (el taller a 25 metros). Un repetidor no va a cruzar 25 metros de patio con buena señal.

Paso 2: Identifica el uso. YouTube diario en el taller necesita velocidad decente y estable. La terraza es uso de fin de semana. La casa principal necesita cobertura completa.

Paso 3: Identifica las restricciones. No quiere cables visibles por el patio, pero tiene buen presupuesto. Ojo: "no quiere cables" se refiere a cables colgando feos; un cable enterrado o por canaleta podría negociarse, pero partamos de su preferencia.

Paso 4: Compara opciones. Repetidor: descartado por distancia y por pérdida de velocidad. Punto de acceso cableado: técnicamente lo ideal para el taller (un cable enterrado hasta allá y un punto de acceso), y se le puede proponer como opción: el cable va enterrado, no se ve. Mesh: con su buen presupuesto, un sistema mesh tribanda (con backhaul dedicado) de 3 o 4 nodos puede cubrir casa, terraza y taller sin cables, con buena velocidad y roaming sin cortes.

Paso 5: Conclusion. La recomendación principal es un sistema mesh tribanda de 3 a 4 nodos: un nodo en la casa, uno orientado hacia la terraza y uno en el taller o lo más cerca posible de él. El backhaul dedicado es clave aquí por las distancias. Como plan B profesional, ofrecerle el cable enterrado hasta el taller con punto de acceso: más barato a largo plazo y velocidad garantizada, sin que se vea feo. Don Beto decide con esta información clara.

Ejercicio 4: Plan de ubicación de nodos en un plano

Imagina esta casa de dos pisos: planta baja de 120 metros cuadrados con sala al frente (ahí está el módem), cocina al centro y comedor al fondo. Planta alta con tres recamaras: la principal al frente, la de los niños al centro y el estudio al fondo. La familia compra un sistema mesh de 3 nodos. Dibuja en un papel el plano aproximado y marca dónde pondrías cada nodo. Luego compara con esta solución.

Solución explicada paso a paso:

Paso 1: Ubica el nodo principal. Va en la planta baja, junto al módem, en la sala al frente. Es el que se conecta por cable al módem. Desde ahí cubre bien la sala y parte de la cocina.

Paso 2: Ubica el segundo nodo. La trampa sería ponerlo en la recamara del fondo de arriba (la zona muerta). No: va a la MITAD del camino. Buena ubicacion: la cocina-comedor de la planta baja (al fondo de abajo) o el pasillo/centro de la planta alta. La mejor opcion suele ser el centro de la planta alta (pasillo o recamara de los niños), porque desde ahí cubre las tres recamaras y todavía recibe buena señal del nodo principal a través del techo/piso. Si la losa es muy gruesa y la señal entre pisos sufre mucho, mejor opcion: comedor de abajo al fondo, y el tercer nodo arriba.

Paso 3: Ubica el tercer nodo. Cubre lo que falte: si el segundo quedo en la planta alta al centro, el tercero va a la planta baja al fondo (comedor) para cubrir cocina, comedor y terraza trasera. Si el segundo quedo abajo al fondo, el tercero va arriba al fondo (estudio).

Paso 4: Verifica con la regla de oro. Cada nodo debe estar donde reciba buena señal del anterior. Ningún nodo va en la zona muerta: van antes de ella. Usa la prueba de ubicacion de la app para confirmar.

Paso 5: Prueba final. Camina con el celular haciendo pruebas de velocidad en: sala, cocina, comedor, las tres recamaras y el estudio. Ajusta si algo quedo bajo.

La lección del ejercicio: la ubicacion de los nodos se planea desde el nodo principal hacia afuera, por mitades, nunca poniendo el nodo dentro de la zona muerta.

Ejercicio 5: Medir la mejora antes y después

Vas a instalarle un punto de acceso a tu tia en su casa. Antes de instalar nada, quieres medir como está la red para después poder demostrarle con números que la mejora valio la pena. Disena el plan de medicion.

Solución explicada paso a paso:

Paso 1: Elige la herramienta. Usa una app gratuita de prueba de velocidad (speed test) en tu celular. Usa siempre la misma app y el mismo servidor si la app lo permite, para que las mediciones sean comparables.

Paso 2: Define los puntos de medicion. Elige 5 o 6 puntos fijos de la casa: junto al router, la cocina, el cuarto del fondo (la zona muerta), el bano, la terraza y donde se vaya a poner el punto de acceso. Marca los puntos o anotalos para repetir exactamente los mismos después.

Paso 3: Mide el ANTES. En cada punto, con el celular conectado al WiFi, haz 3 pruebas de velocidad y anota el promedio de bajada (descarga). También anota cuantas rayitas de señal marca el celular en cada punto. Hazlo todo el mismo día y a la misma hora en que haras el después (la red varia segun la hora).

Paso 4: Instala el punto de acceso y deja que la red se estabilice unos 15 minutos.

Paso 5: Mide el Después. Repite exactamente las mismas mediciones en los mismos puntos, a la misma hora aproximada.

Paso 6: Compara y presenta. Haz una tablita simple: punto, velocidad antes, velocidad después, mejora. Por ejemplo: "Cuarto del fondo: antes 8 megas (se trababa el video), después 95 megas (video en HD sin cortes)". Esa tabla es tu comprobante de que el trabajo quedo bien, y es lo que los profesionales entregan a sus clientes.

Paso 7 (extra): Mide también la latencia (el ping que muestra la prueba). En la zona muerta el ping antes suele estar alto e inestable; después del punto de acceso debe bajar y estabilizarse. Menos ping = videollamadas sin cortes.

Con este metodo nunca vas a discutir de "se siente más rápido": vas a tener números.

Ejercicio 6: Detectar el error en una instalacion

Un vecino te dice: "compre un repetidor, lo puse en mi cuarto del fondo donde no había señal, y ahora tengo señal pero esta lentisimo, peor que con datos del celular. El aparato no sirve, verdad". Identifica todos los errores que cometio y explica cómo corregirlo.

Solución explicada paso a paso:

Paso 1: Error de ubicacion. Puso el repetidor DENTRO de la zona muerta, donde ya no había señal. El repetidor no tenía nada bueno que repetir. Correccion: moverlo a la mitad del camino, donde el celular todavía marque 3 rayitas del router.

Paso 2: Error de expectativas. Esperaba velocidad completa y el repetidor por diseno pierde la mitad (y si recibe señal débil, pierde más). Correccion: explicarle que 40 o 50 megas en la zona extendida es lo normal si su plan es de 100, y que eso alcanza para navegar y ver videos.

Paso 3: Posible error de interferencia. Si el cuarto del fondo esta junto a la cocina, el microondas puede estar metiendo ruido. Correccion: alejar el repetidor de aparatos que interfieran.

Paso 4: Verificación. Después de reubicarlo, hacer prueba de velocidad en el cuarto: debería mejorar notablemente. Si aun así la velocidad no le alcanza para lo que necesita (por ejemplo, home office con videollamadas), la corrección de fondo es cambiar de tecnología: punto de acceso cableado o mesh, porque el repetidor ya dio lo que podía dar.

La lección: el 90 por ciento de los "repetidores que no sirven" en realidad están mal ubicados. Antes de declarar muerto al aparato, reubicalo.

Resumen de la unidad

- Las zonas muertas se deben a distancia y obstáculos que debilitan la señal; no se arreglan contratando más megas, sino llevando la cobertura hasta donde se necesita.
- Repetidor: barato y fácil, pero pierde la mitad de la velocidad por el half-duplex (escucha y habla por turnos en el mismo canal). Es el teléfono descompuesto de las redes.
- Regla de oro del repetidor: se coloca a la MITAD del camino con buena señal del router, nunca dentro de la zona muerta.
- SSID extendido (_EXT) vs mismo SSID: en ambos casos el celular no cambia de forma inteligente y se sienten cortes al moverse; el repetidor no hace roaming de verdad.
- No encadenes repetidores en serie: cada salto vuelve a partir la velocidad a la mitad.
- Punto de acceso cableado: recibe internet por cable Ethernet y crea WiFi con velocidad completa y máxima estabilidad. Es la solución profesional (oficinas, hoteles, escuelas).
- Un router viejo en modo AP (o con DHCP apagado y cable de LAN a LAN) revive como punto de acceso gratis.
- PoE (Power over Ethernet) permite alimentar el punto de acceso por el mismo cable de red, sin contacto eléctrico cerca. Necesitas switch o inyector PoE.
- Sistema mesh: nodos que trabajan en equipo, una sola red, una sola app, y te pasan de nodo a nodo sin que te des cuenta. Es el equipo de relevos.
- Backhaul = la conexión entre nodos. Compartido (pierde algo), dedicado/tribanda (carretera privada, casi sin pérdidas), por cable (lo mejor posible).
- Roaming sin cortes gracias a 802.11k (mapa de nodos), 802.11v (la red sugiere el cambio) y 802.11r (autenticación rápida, cambio instantáneo).
- Nodos necesarios (casas de concreto): hasta 120 m² = 2 nodos; 120 a 250 m² o dos plantas = 3 nodos; más de 250 m² = 4 nodos o mezcla con cableado.

- No pongas nodos de más ni muy pegados: se interfieren entre si. Cada nodo va donde reciba buena señal del anterior.
- Para elegir mesh: tribanda si la casa es grande o el plan es rápido, WiFi 6 mínimo, puertos Ethernet en cada nodo, no mezclar marcas.
- Decision rapida: problema chico y ocasional = repetidor; planta completa o uso exigente con posibilidad de cable = punto de acceso; casa grande con varias zonas y sin cables = mesh.
- Mide antes y después con pruebas de velocidad en puntos fijos: los números son tu comprobante de que la mejora funciona.

Sigue aprendiendo en lucasegaacademy.com, donde encontrarás más cursos gratuitos de redes, programacion y tecnología.

UNIDAD 8: Redes de invitados, control parental y QoS (Clases 22 a 24)

Llegas a tu casa con dos bolsas del súper y el teléfono sonando. Es tu jefe: en diez minutos tienes una videollamada importante con un cliente. Enciendes la laptop, te sientas frente a la cámara, la llamada empieza bien, tú hablando, el cliente escuchando... y de pronto tu voz empieza a sonar como robot. La imagen se congela. Tu cara queda atrapada en una mueca ridícula mientras el cliente te mira en silencio desde su oficina. Abajo, en la sala, tu hijo descargó una actualización de su videojuego de 40 gigabytes. En el cuarto de al lado, tu hija está viendo una serie en 4K. Y en la cocina, tu suegra, que vino de visita el fin de semana, está viendo videos de recetas en su tablet con la contraseña de tu WiFi que le diste el viernes sin pensar dos veces.

Esta escena no es ficción. Es el lunes de millones de hogares. Y lo peor es que la mayoría de la gente cree que la solución es "contratar más megas", como si el problema fuera siempre la velocidad contratada. Pero escucha esto: muchas veces el problema no es cuántos megas entran a tu casa, sino cómo se reparten una vez que ya están adentro.

Piensa en tu conexión a internet como una carretera que llega a tu casa. Da igual que sea una autopista de ocho carriles: si todos los carros quieren entrar por la misma caseta al mismo tiempo, se hace un embotellamiento. El tráiler de la descarga del videojuego ocupa tres carriles. La serie en 4K ocupa otros dos. Tu videollamada, que es pequeña pero urgentísima, queda atorada detrás de todos, pitando sin que nadie la deje pasar. El QoS, uno de los temas estrella de esta unidad, es exactamente eso: el agente de tránsito que le abre un carril de emergencias a tu videollamada para que pase primero, aunque haya tráileres en la fila.

Ahora, la otra mitad del drama: tu suegra con tu contraseña del WiFi. Parece inofensivo, ¿verdad? Es familia. Pero esa contraseña que le diste el viernes es la misma que protege tu red principal, la red donde está tu computadora con tus documentos de trabajo, tu impresora, tu disco duro con las fotos familiares, tu cámara de seguridad, tus focos inteligentes y hasta tu cerradura electrónica si tienes una. Darle tu contraseña principal a una visita es como darle la llave maestra de tu casa a alguien que solo vino a tomar café en la sala: técnicamente puede entrar al baño, a tu recámara y a tu oficina. ¿Confías en tu suegra? Claro que sí. Pero su tablet puede traer un virus sin que ella lo sepa, y ese virus, una vez dentro de tu red principal, puede pasearse libremente por todos tus aparatos. La red de invitados, el primer tema de esta unidad, es la solución elegante: es como tener una salita de visitas con su propia puerta. Tus invitados entran, se sientan cómodos, usan el internet, y jamás pisan tu recámara.

Y luego está el tercer frente, el que más dolores de cabeza les da a los papás: los hijos y el internet. No se trata de prohibirles todo, se trata de poner reglas sensatas. Que el internet se apague solo a las diez de la noche en la tablet del niño de ocho años. Que el adolescente no pueda entrar a sitios para adultos ni a páginas de apuestas. Que cada quien tenga su horario y sus límites, configurados una sola vez en el router, sin tener que andar persiguiendo aparatos por toda la casa. Eso es el control parental, el segundo tema de esta unidad, y créeme: bien configurado, te ahorra más discusiones familiares que cualquier regaño.

Al terminar esta unidad vas a lograr tres cosas muy concretas. Primera: vas a crear una red de invitados separada de tu red principal, con su propia contraseña, de modo que cualquier visita, técnico, repartidor o vecino buena onda que necesite internet pueda conectarse sin poner en riesgo tus aparatos ni tus datos. Segunda: vas a configurar el control parental de tu router con perfiles por hijo, horarios de acceso y filtros de contenido por categorías, para que el internet de tu casa tenga reglas claras que se cumplen solas. Tercera: vas a activar y configurar el QoS para que tus videollamadas de trabajo y tus juegos en línea tengan prioridad sobre las descargas pesadas, y nunca más se te trabe una llamada importante porque alguien más en la casa decidió actualizar un juego.

Esta unidad agrupa tres clases. La clase 22 te enseña todo sobre la red de invitados: qué es, por qué jamás debes dar tu contraseña principal a las visitas y cómo configurarla paso a paso en un router común. La clase 23 se mete de lleno al control parental: horarios, filtros de contenido por categorías y límites por dispositivo, explicados para que cualquier papá o mamá los pueda configurar sin ser técnico. La clase 24 desmenuza el QoS: qué es la calidad de servicio, cómo priorizar videollamadas y juegos sobre descargas, qué es el bufferbloat (ese enemigo invisible que arruina tus llamadas aunque tengas buena velocidad) y cómo configurarlo bien sin empeorar las cosas.

Un aviso importante antes de empezar: los menús de los routers cambian según la marca. Un TP-Link no se ve igual que un Huawei, y un router de tu compañía de internet (Telmex, Totalplay, Izzi, Megacable o el que tengas) trae sus propios nombres para cada opción. No te asustes si en tu router la opción se llama distinto: en esta unidad te voy a enseñar los conceptos y los nombres más comunes de cada función, para que la reconozcas aunque venga disfrazada. Lo importante no es memorizar dónde está cada botón, sino entender qué hace cada cosa y por qué la necesitas.

También quiero que sepas algo desde ahorita: nada de lo que vamos a configurar en esta unidad requiere comprar aparatos nuevos. Todo se hace con el router que ya tienes en tu casa, entrando a su panel de configuración desde el navegador. Si llegaste hasta aquí en el curso, ya sabes entrar al panel de tu router (lo vimos en unidades anteriores); si no, repasa rápido la clase donde lo explicamos, porque aquí lo vamos a usar muchísimo.

Así que ponte cómodo. En esta unidad tu red doméstica deja de ser una vecindad donde todos hacen lo que quieren, y se convierte en una casa bien organizada: visitas en la sala, niños con horario, y un carril de emergencias siempre libre para lo importante. Empecemos.

Explicación detallada

Clase 22: La red de invitados, o la sala de visitas de tu casa

Imagina tu casa. Tiene recámaras, baños, la cocina, tu oficina con documentos importantes... y tiene la sala, ese espacio pensado para recibir gente. Cuando llega una visita, la pasas a la sala. Le ofreces algo de tomar, platican a gusto, y cuando se va, tu recámara sigue intacta, tus cajones sin abrir, tus papeles sin tocar. A nadie se le ocurriría meter a un repartidor hasta tu cuarto a esperar. La red de invitados funciona exactamente igual, pero en el mundo digital.

Técnicamente, una red de invitados es una segunda red WiFi que crea tu router, separada de tu red principal. Tiene su propio nombre (por ejemplo, "CasaDeJuan-Invitados") y su propia contraseña. Los aparatos que se conectan a ella pueden salir a internet sin problema, pero NO pueden ver ni tocar los aparatos de tu red principal. Tu computadora, tu impresora, tu disco de respaldo, tus cámaras: todo eso queda del otro lado de una pared invisible.

¿Por qué es tan importante separarla? Déjame ponerte tres escenarios reales. Escenario uno: viene el técnico de la compañía de internet a revisar tu servicio. Le das tu contraseña principal "para que pruebe la conexión". Él se conecta, hace su trabajo y se va. Pero su laptop ya guardó tu contraseña, y esa laptop se conecta a decenas de casas al día. Si algún día esa máquina se infecta, tu red queda expuesta. Escenario dos: tu hijo invita a tres amigos a hacer la tarea. Uno de ellos trae un celular con un virus que ni sabe que tiene. Si están en tu red principal, ese virus puede intentar brincar a tu computadora. Si están en la red de invitados, el virus queda encerrado en la salita, sin acceso a nada más. Escenario tres: rentas un cuarto por Airbnb o tienes un pequeño negocio y los clientes piden el WiFi. ¿De verdad quieres que un desconocido tenga acceso a la misma red donde está tu computadora con tus cuentas de banco? La respuesta es obvia.

Hay un concepto técnico detrás de esto que vale la pena entender: el aislamiento de clientes, que en muchos routers aparece como "AP isolation" o "aislamiento de AP". Normalmente, dos aparatos conectados al mismo WiFi pueden "verse" entre ellos: tu celular puede encontrar tu impresora, tu laptop puede ver tu bocina inteligente. Eso es útil en tu red principal. Pero en la red de invitados no quieres eso: no quieres que el celular de un invitado pueda ver el celular de otro invitado. El aislamiento de clientes crea una regla simple: cada aparato conectado a la red de invitados solo puede hablar con el router y salir a internet, pero no puede hablar con los

demás aparatos de esa misma red. Es como si cada visita tuviera su propia salita privada. Cuando configures tu red de invitados, busca esta opción y actívala siempre.

Otro concepto que vas a ver mencionado es VLAN, que significa "red de área local virtual". No te asustes por el nombre elegante: una VLAN es simplemente una forma de dividir una red física en varias redes lógicas que no se hablan entre ellas. Es como poner muros invisibles dentro de tu casa: el cable es el mismo, el router es el mismo, pero la red de invitados vive en un "cuarto" y tu red principal vive en otro, y no hay puerta entre ellos. La mayoría de los routers caseros hacen esto automáticamente cuando activas la red de invitados, sin que tengas que configurar la VLAN a mano. Pero es bueno que conozcas el término, porque en routers más avanzados o de negocios pequeños verás opciones de VLAN que sirven para lo mismo: separar grupos de aparatos.

Un error común que debes evitar es el doble NAT. NAT significa "traducción de direcciones de red", y es el mecanismo por el que tu router le da direcciones internas a tus aparatos (como 192.168.1.5) mientras presenta una sola dirección hacia internet. Un NAT es normal y necesario. El problema del doble NAT aparece cuando conectas un segundo router detrás del primero (muy común cuando la gente compra un router "más potente" y lo conecta al módem de la compañía sin ponerlo en modo puente). Entonces tienes dos aparatos haciendo NAT uno tras otro, y eso rompe videollamadas, juegos en línea y cámaras de seguridad. La lección para esta unidad: la red de invitados la debe crear tu router principal, el que está conectado directo al internet. No conectes un segundo router solo para los invitados, porque te metes en un lío de doble NAT. Si ya tienes dos aparatos, configura el segundo como punto de acceso (modo AP), no como router.

Las buenas prácticas para tu red de invitados son sencillas pero poderosas. Primera: ponle una contraseña, aunque sea sencilla. Una red de invitados abierta (sin contraseña) invita a que se conecte todo el vecindario y sature tu conexión. Segunda: usa una contraseña DIFERENTE a la de tu red principal, y cámbiala cada cierto tiempo, sobre todo si tuviste muchas visitas o si diste el WiFi en una fiesta. Tercera: si tu router lo permite, ponle un límite de velocidad a la red de invitados (algunos routers lo llaman "ancho de banda para invitados"), para que las visitas no se coman toda tu conexión. Cuarta: en negocios pequeños (una tienda, un consultorio, una cafetería), la red de invitados no es opcional: es obligatoria. Ahí además conviene poner un mensaje de bienvenida o un tiempo límite de sesión si el router lo soporta.

Y un detalle que casi nadie configura: el horario de la red de invitados. Muchos routers permiten programar a qué horas está activa. Si en tu casa las visitas solo llegan en fin de semana, puedes dejarla apagada entre semana. Menos tiempo encendida, menos superficie de ataque. No es indispensable, pero es un buen hábito de seguridad.

Clase 23: Control parental, o las reglas de la casa que se cumplen solas

Ser papá o mamá en la era del internet es agotador. Antes el peligro era que tu hijo se fuera a jugar a la calle; ahora el peligro cabe en su bolsillo y funciona a las tres de la mañana. Y no puedes estar vigilando pantallas todo el día: tienes que trabajar, cocinar, vivir. El control parental del router es como contratar a un vigilante que nunca duerme: una vez que le das las reglas, las aplica solo, sin discusiones y sin que tengas que andar quitando celulares.

Vamos por partes. El control parental moderno tiene tres patas: horarios, filtros de contenido y límites por dispositivo. Las tres se configuran por perfil, es decir, creas un perfil para cada hijo (o para cada aparato de tus hijos) y le pones sus propias reglas. El niño de 8 años no necesita las mismas reglas que el adolescente de 15, y eso el router lo entiende perfecto.

Los horarios de acceso son la pata más fácil y la más efectiva. Consisten en decirle al router: "este aparato solo puede usar internet en estos días y a estas horas". Por ejemplo: la tablet del niño funciona de lunes a viernes de 4 de la tarde a 8 de la noche, y fines de semana de 9 de la mañana a 9 de la noche. Fuera de ese horario, el aparato simplemente no tiene internet. Punto. No hay que regañar, no hay que quitar la tablet: la red sola dice que no. Esto es oro para la hora de dormir. ¿Cuántos papás han peleado porque el hijo se queda hasta la una de la mañana viendo videos? Con el horario configurado, a las 10 de la noche el internet de su tablet muere, y el pleito se acabó para siempre. Algunos routers incluso permiten horarios distintos para días de escuela y fines de semana, lo cual es ideal.

La segunda pata son los filtros de contenido por categorías. Aquí el router bloquea tipos completos de sitios: contenido para adultos, apuestas, violencia, drogas, redes sociales, juegos, etc. Tú marcas las categorías prohibidas y listo. Es importante entender cómo funciona por dentro para no frustrarte: el router mantiene una lista (que se actualiza por internet) de sitios clasificados por categoría, y cuando un aparato con filtro intenta entrar a un sitio prohibido, la conexión se bloquea y suele aparecer una página de aviso. No es perfecto: ningún filtro atrapa el cien por ciento de los sitios malos, y de vez en cuando bloquea alguno bueno por error. Pero como primera barrera es excelente.

Hay una herramienta muy útil relacionada con esto: el DNS familiar. El DNS es el "directorio telefónico" de internet: convierte nombres como www.ejemplo.com en direcciones numéricas. Si cambias el DNS que usan los aparatos de tus hijos por un DNS familiar (como los que ofrecen algunos proveedores gratuitos, por ejemplo los servicios de DNS con filtrado familiar), ese DNS simplemente se niega a resolver las direcciones de sitios para adultos o peligrosos. Es una capa extra de protección que funciona aunque el niño use otro navegador o borre el historial. En la sección de ejemplos te muestro cómo configurarlo.

La tercera pata son los límites por dispositivo. Esto incluye dos cosas: límites de tiempo total (por ejemplo, "máximo 3 horas de internet al día en este celular") y límites de velocidad o de datos. El límite de tiempo es muy útil para adolescentes: no les apagas el internet a una hora fija, pero sí les pones un tope diario. Cuando se acaban sus 3 horas, se acabó. Algunos routers también permiten pausar el internet de un aparato con un botón desde la app del router: "¡a cenar!" y un toque apaga el WiFi de la tablet. Esa función de pausa manual vale oro.

Ahora, hablemos con honestidad de las limitaciones, porque un papá informado configura mejor que un papá ilusionado. Primera limitación: los filtros por categorías no ven dentro de las aplicaciones. Si bloqueas la categoría "redes sociales" en el navegador, el niño igual puede abrir la app de la red social en su celular, porque muchas apps no pasan por el filtro web del router. Para eso sirven los horarios y los límites de tiempo, que cortan TODO el internet del aparato, no solo el navegador. Segunda limitación: un adolescente avisado puede usar una VPN para saltarse los filtros. Si ves que el filtro "no funciona" con tu hijo mayor, revisa si tiene una app de VPN instalada. Tercera: el control parental del router no reemplaza la conversación. La tecnología pone la barda, pero la educación pone el criterio. Úsalo como apoyo, no como niñera.

Errores comunes en control parental: el más frecuente es ponerle las mismas reglas a todos los hijos. El niño de 8 y el de 15 no son iguales; si al de 15 le pones horario de niño chiquito, va a buscar la forma de saltárselo y perderás autoridad. Otro error: bloquear tantas categorías que el internet queda inservible para la tarea escolar, y entonces los hijos te piden que lo quites todo. Empieza con lo esencial (contenido adulto, apuestas, violencia explícita) y ajusta con el tiempo. Y el error más tonto pero más común: dejar la contraseña del panel del router en la que trae de fábrica (admin/admin). Si tu hijo la adivina, puede quitarse él mismo las reglas. Cambia la contraseña del router a algo que solo tú sepas.

Buenas prácticas: crea un perfil por hijo con su nombre, así es fácil administrar. Revisa cada mes si las reglas siguen teniendo sentido (los niños crecen y las reglas deben crecer con ellos). Combina las tres patas: horarios para la hora de dormir, filtros para el contenido, y límites de tiempo para el uso total. Y habla con tus hijos sobre las reglas: "estas son las reglas de internet de esta casa, como hay reglas para la hora de comer". Cuando las reglas son claras y parejas, hay menos berrinche.

Clase 24: QoS, o el carril de emergencias de tu internet

Vamos a entender el QoS desde cero, porque es el tema más técnico de la unidad pero también el que más cambia tu vida diaria. QoS significa "Quality of Service", calidad de servicio. En español simple: es un sistema de prioridades para tu conexión a internet. Le dice al router qué tipo de tráfico es urgente y cuál puede esperar.

¿Por qué hace falta priorizar? Porque no todos los usos de internet son iguales. Hay dos tipos de tráfico: el sensible al tiempo y el que no. Una videollamada es sensible al tiempo: si un pedacito de tu voz llega medio segundo tarde, se escucha cortado, como robot. Un juego en línea también: si tu disparo llega tarde al servidor, ya te mataron. En cambio, una descarga es paciente: si un archivo de 2 gigabytes tarda 10 minutos o 12 minutos en bajar, a nadie le cambia la vida. El problema es que el router, por defecto, trata a todos por igual: atiende en orden de llegada, como una tortillería. Y cuando la fila está llena de descargas pesadas, tu videollamadita urgente se queda esperando atrás. El QoS cambia la regla: le da un gafete VIP al tráfico urgente para que pase primero.

Aquí entra un concepto primo del QoS que debes conocer: WMM, que significa "multimedia WiFi". Es una función que viene activada por defecto en casi todos los routers modernos y es como un mini-QoS automático solo para el WiFi: le da prioridad al tráfico de voz y video sobre el tráfico normal, sin que tú configures nada. Si tu router tiene una opción WMM, déjala activada. Es la base; el QoS que vamos a configurar es el control fino por encima de esa base.

¿Cómo decide el router qué es prioritario? Hay tres formas, y las tres las vas a ver en los menús: priorización por aplicación o servicio, priorización por dispositivo, y priorización por puertos. La priorización por aplicación es la más cómoda: el router trae una lista de servicios conocidos (Zoom, Teams, Meet, WhatsApp, Netflix, juegos populares) y tú les asignas prioridad alta, media o baja. La priorización por dispositivo es asignarle prioridad a un aparato completo: "la laptop del trabajo siempre tiene prioridad alta". Es útil pero es un martillo: si le das prioridad alta al celular de tu hijo gamer, también estás priorizando sus descargas. La priorización por puertos es la más técnica: cada servicio de internet usa "puertos" numéricos (las videollamadas suelen usar ciertos rangos), y puedes crear reglas para esos puertos. Para esta unidad nos quedamos con las dos primeras, que son las que traen los routers caseros.

Ahora, un concepto que MUCHA gente confunde: ancho de banda de subida contra ancho de banda de bajada. La bajada (descarga) es lo que baja de internet a tu casa: videos, páginas, archivos. La subida es lo que sube de tu casa a internet: tu voz en la videollamada, tu cámara, los archivos que envías. Las compañías venden paquetes asimétricos: te dan, por ejemplo, 100 megas de bajada pero solo 10 de subida. Y aquí está el truco: las videollamadas que se traban casi siempre se traban por la SUBIDA, no por la bajada. Tu voz y tu video tienen que subir; si la subida está saturada (porque alguien está subiendo fotos a la nube o haciendo un respaldo), tu llamada se congela aunque tengas 100 megas de bajada libres. Por eso, cuando configures el QoS, presta atención especial a las reglas de subida. Es el error número uno de los principiantes: solo configuran la bajada y el problema sigue igual.

Y ahora el concepto estrella, el que explica por qué tu internet "se siente lento" aunque el test de velocidad marque bien: el bufferbloat. Te lo explico con una analogía. Imagina un embudo:

arriba le echas agua (los datos que quieren salir) y abajo sale un chorrito (tu conexión de subida, que es angosta). Si le echas agua más rápido de lo que sale, el embudo se llena y el agua se queda esperando. En los routers, ese "embudo" es un depósito temporal llamado buffer, y está diseñado para no perder datos: en vez de tirar paquetes cuando hay congestión, los guarda en fila. Suena bien, ¿verdad? El problema es que los buffers modernos son ENORMES. Entonces cuando tu hijo empieza una descarga pesada, el buffer se llena hasta el tope y tu paquetito urgente de videollamada tiene que esperar detrás de miles de paquetes en la fila. Esa espera se llama latencia, y cuando es muy alta, tu llamada se escucha como robot y tu juego tiene lag. Eso es el bufferbloat: la hinchazón del buffer. Tu test de velocidad puede marcar 100 megas perfectos, pero con el buffer lleno, la experiencia es pésima.

¿Cómo se combate el bufferbloat? Con dos armas. La primera es el QoS bien configurado, que le abre el carril de emergencias al tráfico urgente para que no haga fila. La segunda, en routers más avanzados, es una técnica llamada SQM (manejo inteligente de filas), que mantiene el buffer bajo control automáticamente. No todos los routers caseros traen SQM, así que en esta unidad nos concentramos en el QoS clásico, que sí lo traen casi todos.

Vamos a los errores comunes con el QoS, porque un QoS mal configurado puede dejar tu red PEOR que sin QoS. Error uno: activar el QoS pero no decirle cuál es tu velocidad real. El QoS necesita saber de cuánto es tu conexión para repartirla; si le pones un número inventado o lo dejas en automático con un valor equivocado, las prioridades no funcionan. Siempre mide tu velocidad primero (con un test por cable, de preferencia) y escribe los números reales. Error dos: ponerle prioridad alta a TODO. Si todo es prioritario, nada es prioritario: es como si en el hospital todos los pacientes tuvieran la pulsera roja de emergencias. Elige dos o tres cosas importantes (videollamadas y juegos, por ejemplo) y deja lo demás en normal o bajo. Error tres: priorizar por dispositivo en vez de por aplicación cuando hay varias personas. Si le das prioridad máxima a "la laptop de papá" y papá se pone a descargar una película en su laptop, la descarga también sale con prioridad máxima y el QoS no sirvió de nada. Mejor prioriza la aplicación (la videollamada) y no el aparato. Error cuatro: olvidarse de la subida, como ya vimos. Error cinco: activar el QoS en un router viejito con la función mal implementada y notar que el internet se pone más lento. Si al activar el QoS todo empeora, desactívalo: algunos routers baratos hacen el QoS por software y el procesador no se da abasto. No es tu culpa, es el aparato.

Las buenas prácticas del QoS son claras. Primero: mide tu velocidad real antes de configurar nada, y repite la medición cada seis meses o cuando cambies de paquete. Segundo: configura tanto la bajada como la subida, con los números reales. Tercero: prioriza poco pero bien: videollamadas y voz en lo más alto, juegos en línea justo debajo, streaming de video en medio, descargas y actualizaciones al fondo. Cuarto: si tu router permite ponerle un tope a la red de

invitados, hazlo: así las visitas jamás pueden saturar tu conexión. Quinto: después de configurar, prueba con un caso real: haz una videollamada mientras alguien más descarga algo pesado, y comprueba que la llamada ya no se traba. Si se sigue trabando, revisa los números de velocidad que pusiste.

Un último consejo de esta sección: el QoS no hace magia. Si tu conexión es de 10 megas y en tu casa hay cuatro personas viendo video en 4K al mismo tiempo, ningún QoS del mundo va a hacer que quepan. El QoS reparte lo que hay; no inventa megas. Si después de configurarlo bien sigues sufriendo, entonces sí es momento de considerar subir tu paquete contratado. Pero configúralo primero: te vas a sorprender de cuántos "problemas de velocidad" eran en realidad problemas de prioridades.

Cómo se conectan las tres clases entre sí

Antes de pasar a los ejemplos, mira el panorama completo, porque estas tres clases forman un sistema. La red de invitados protege tu red por fuera: nadie de afuera toca tus aparatos. El control parental ordena tu red por dentro: cada miembro de la familia tiene sus reglas. Y el QoS hace que todo funcione bien al mismo tiempo: lo urgente pasa primero. Una casa con las tres cosas configuradas es una casa donde el internet simplemente funciona: las visitas contentas, los niños con horario, y tus videollamadas claras. Esa es la meta de esta unidad, y en la siguiente sección la construimos paso a paso.

Preguntas que siempre hacen los principiantes

Cuando alguien termina de aprender estos tres temas, siempre aparecen las mismas dudas. Las respondo aquí para que no te quedes con ninguna.

¿La red de invitados me quita velocidad? No, por sí sola no. Crear la red de invitados no consume tu internet; solo lo consumen los aparatos conectados a ella cuando están usando datos. Es como abrir la puerta de la sala: la puerta no gasta luz, la gastan las visitas si prenden la tele. Por eso el límite de velocidad para invitados es tan útil: pones el tope una vez y te olvidas.

¿Puedo ver qué hacen mis invitados en internet? Técnicamente algunos routers avanzados muestran estadísticas por red, pero espiar el tráfico de tus visitas es una mala idea ética y, en un negocio, puede meterte en problemas legales. La red de invitados es para dar servicio, no para vigilar. Si te preocupa el mal uso, el límite de velocidad y el DNS familiar son suficientes.

¿El control parental funciona si mi hijo usa sus datos del celular? No. El control parental del router solo controla el WiFi de tu casa. Si tu hijo apaga el WiFi y usa sus datos móviles, las

reglas del router no aplican. Por eso los papás combinan: reglas en el router para la casa, y los controles propios del celular (tiempo en pantalla, filtros de la tienda de apps) para cuando está fuera. Ninguna herramienta sola cubre todo.

¿Y si mi router no trae opción de QoS? Algunos routers muy básicos o muy viejos no la traen, o la traen con otro nombre ("priorización de tráfico", "control de ancho de banda", "traffic shaping"). Si de plano no existe, tienes tres caminos: actualizar el firmware del router (a veces la opción aparece), usar las funciones de priorización de tus aparatos (algunas consolas y PCs permiten limitar su propio uso), o considerar un router nuevo si el home office depende de ello. Pero primero revisa bien todos los menús: el QoS suele esconderse en "Avanzado".

¿El QoS sirve si solo somos dos personas en casa? Sí, y mucho. Basta una sola descarga pesada en segundo plano (una actualización automática del sistema, un respaldo a la nube) para arruinar una videollamada. El QoS no es solo para casas llenas de gente; es para cualquier casa donde algo importante comparta la conexión con algo pesado.

¿La red de invitados y el control parental se pelean? No, porque viven en mundos separados. La red de invitados es para los de afuera y normalmente no lleva control parental (el huésped es un adulto). Los perfiles de control parental viven en la red principal, para tu familia. Cada quien con sus reglas, sin choques.

¿Cada cuánto debo cambiar la contraseña de invitados? Depende del movimiento. En una casa normal, cada dos o tres meses está bien, o cada vez que tuviste una reunión grande. En un negocio con clientes diarios, una vez al mes. Y siempre que un huésped de Airbnb se vaya, ese mismo día. Anota la fecha del último cambio en una nota pegada al router (solo la fecha, nunca la contraseña).

¿Puedo tener más de una red de invitados? Algunos routers permiten varias (por ejemplo, una para visitas y otra para tus aparatos inteligentes). Si el tuyo lo permite, es una gran idea separar tus focos, cámaras y bocinas inteligentes en su propia red: así, si un aparato barato e inseguro se compromete, no arrastra a tu computadora. Es el mismo principio de la sala de visitas, aplicado a tus propios aparatos.

Una última: ¿tengo que configurar todo esto el mismo día? No. Hazlo en el orden de esta unidad y a tu ritmo: primero la red de invitados (es lo más rápido, quince minutos), luego el control parental (una tarde tranquila con la lista de aparatos de tus hijos a la mano), y al final el QoS (cuando puedas medir la velocidad con calma). Cada cosa que configures empieza a ayudarte desde el primer día.

Tu primera tarde: el plan de 30 minutos

Si todo esto te abruma, aquí tienes el plan mínimo para una sola tarde. Treinta minutos, tres victorias.

Minutos 0 a 10: la red de invitados. Entra al panel de tu router, activa la red de invitados en 2.4 GHz con un nombre claro y una contraseña distinta a la principal, activa el aislamiento de clientes y bloquea el acceso a la red local. Guarda. Prueba conectando tu celular: navega bien, pero no veas tus aparatos. Victoria uno: tus visitas ya no tocan tu red.

Minutos 10 a 20: el control parental básico. Crea un perfil por hijo, asigna sus aparatos y pon solo el horario de apagado nocturno (por ejemplo, sin internet de 10:00 pm a 7:00 am para todos). No configures filtros todavía; el horario nocturno solo ya elimina la pelea más común de la casa. Guarda. Victoria dos: las reglas se cumplen solas.

Minutos 20 a 30: el QoS esencial. Haz un test de velocidad por cable, anota bajada y subida, entra al QoS, activa, escribe los números reales y pon las videollamadas en prioridad alta y las descargas en baja. Guarda. Haz una llamada de prueba mientras alguien descarga algo. Victoria tres: tu trabajo protegido.

Los filtros por categorías, el DNS familiar, los límites de invitados y el ajuste fino del QoS pueden esperar al fin de semana. Lo importante es que hoy tu red ya está separada, con horarios y con prioridades. El resto es pulir.

Ejemplos paso a paso

En esta sección vamos a configurar las tres cosas en un router genérico. Los nombres de los menús cambian según la marca (TP-Link, Huawei, Tenda, Mercusys, o el router de tu compañía), pero las funciones son las mismas. Antes de empezar cualquier tutorial, entra al panel de tu router: abre el navegador y escribe la dirección del router (normalmente 192.168.1.1 o 192.168.0.1), e inicia sesión con tu usuario y contraseña. Si nunca cambiaste esa contraseña, hazlo HOY: es la llave maestra de toda tu red.

Ejemplo 1: Crear la red de invitados con aislamiento (Clase 22)

Situación: cada fin de semana recibes visitas y estás cansado de dar tu contraseña principal. Vas a crear una red "Casa-Invitados" separada, con su propia contraseña y con aislamiento de clientes activado.

Paso 1: entra al panel del router y busca la sección de WiFi. Normalmente se llama "Inalámbrico", "Wireless", "WiFi" o "Red inalámbrica". Dentro busca una pestaña o apartado que diga "Red de invitados", "Guest Network", "WiFi de invitados" o "Red para visitas".

1. Abrir el navegador y entrar a `http://192.168.1.1` (o la dirección de tu router)
2. Iniciar sesión con usuario y contraseña del panel
3. Ir a: Inalámbrico > Red de invitados (Guest Network)

Paso 2: activa la red de invitados para la banda de 2.4 GHz. (La de 5 GHz también la puedes activar, pero con la de 2.4 basta para visitas: tiene más alcance.) Ponle un nombre claro, por ejemplo "Casa-Invitados". Que se distinga de tu red principal para que nadie se confunda.

4. Activar la casilla "Habilitar red de invitados" en 2.4 GHz
5. Nombre de red (SSID): Casa-Invitados

Paso 3: ponle seguridad. Elige WPA2-PSK (o WPA2/WPA3 si tu router lo ofrece) y escribe una contraseña DIFERENTE a la de tu red principal. Que sea fácil de dictar: algo como "Visita2026!" funciona bien y se cambia cada pocos meses.

6. Seguridad: WPA2-PSK (o WPA2/WPA3)
7. Contraseña: una diferente a tu red principal (ejemplo: Visita2026!)

Paso 4: activa el aislamiento. Busca las opciones que digan "Aislamiento de AP", "AP isolation", "Aislar clientes", "Permitir que los invitados se vean entre sí" o "Acceso a la red local". Lo que quieres es: aislamiento ACTIVADO (los invitados no se ven entre sí) y acceso a la red local DESACTIVADO (los invitados no ven tu red principal).

8. Activar "Aislamiento de AP" / "Aislar clientes de invitados"
9. DESACTIVAR "Permitir acceso a la red local" / "Los invitados pueden ver mi red"
10. Verificar que la opción "Acceso a internet" quede ACTIVADA

Paso 5: si tu router lo permite, ponle un límite de velocidad a la red de invitados para que nunca te saturen la conexión. Busca "límite de ancho de banda de invitados" o "QoS de invitados". Un valor razonable: 10 megas de bajada y 5 de subida (ajusta según tu paquete).

11. (Opcional) Límite de ancho de banda para invitados: 10 Mbps bajada / 5 Mbps subida
12. Guardar / Aplicar cambios y esperar a que el router reinicie el WiFi

Paso 6: prueba. Con tu celular, conéctate a "Casa-Invitados" con la nueva contraseña. Abre una página de internet: debe funcionar. Ahora intenta algo más: desde ese celular trata de entrar al panel del router (192.168.1.1) o de ver tu impresora o tu computadora en la red. No deberías poder. Si no puedes ver nada de tu red principal, el aislamiento está funcionando.

Resultado esperado: tienes dos redes WiFi. Tu familia sigue en la red principal de siempre; las visitas usan "Casa-Invitados" y jamás tocan tus aparatos. Cuando termine el fin de semana con mucha visita, cambias la contraseña de invitados y listo.

Ejemplo 2: Configurar el control parental con perfiles, horarios y filtros (Clase 23)

Situación: tienes dos hijos. Mariana, de 8 años, usa una tablet para ver videos y hacer tarea. Diego, de 15, usa su celular para todo. Quieres: que la tablet de Mariana se apague sola a las 8:30 de la noche y bloquee contenido para adultos; que el celular de Diego tenga internet hasta las 10:30 de la noche, con bloqueo de contenido adulto y apuestas, y un máximo de 4 horas diarias.

Paso 1: entra al panel del router y busca "Control parental", "Parental Control" o "Perfil familiar". Los routers modernos trabajan con perfiles: primero creas el perfil de cada hijo y luego le asignas sus aparatos.

1. Entrar al panel del router (<http://192.168.1.1> o similar)
2. Ir a: Control parental / Parental Control
3. Crear perfil nuevo: nombre "Mariana"

Paso 2: asigna la tablet de Mariana a su perfil. El router te muestra la lista de aparatos conectados con sus nombres (a veces aparecen como "Android-xyz" o la marca). Identifica la tablet de Mariana (si dudas, apaga y prende su WiFi y mira cuál aparato aparece y desaparece de la lista) y agrégala al perfil.

4. En el perfil "Mariana", agregar dispositivo: seleccionar la tablet de Mariana de la lista de aparatos conectados

Paso 3: configura el horario de Mariana. De lunes a viernes, internet de 4:00 pm a 8:30 pm. Fines de semana, de 9:00 am a 8:30 pm. Fuera de ese horario, la tablet no tiene internet.

5. Horario del perfil "Mariana":
 - Lunes a viernes: 16:00 a 20:30
 - Sábado y domingo: 09:00 a 20:30
6. Guardar el horario

Paso 4: configura el filtro de contenido de Mariana. Activa el bloqueo por categorías y marca: contenido para adultos, apuestas, violencia, drogas. Para una niña de 8, también puedes bloquear redes sociales y juegos en línea si lo consideras necesario.

7. Filtro de contenido del perfil "Mariana": ACTIVADO
8. Categorías bloqueadas: Adultos, Apuestas, Violencia, Drogas
(opcional: Redes sociales, Juegos)

Paso 5: ahora crea el perfil de Diego con reglas para adolescente: horario hasta las 10:30 pm todos los días, filtro de adultos y apuestas, y límite de 4 horas diarias de internet.

9. Crear perfil nuevo: nombre "Diego"
10. Agregar dispositivo: seleccionar el celular de Diego
11. Horario del perfil "Diego":
 - Lunes a domingo: 07:00 a 22:30
12. Filtro de contenido: ACTIVADO
Categorías bloqueadas: Adultos, Apuestas
13. Límite de tiempo diario: 4 horas
14. Guardar / Aplicar cambios

Paso 6 (capa extra): configura el DNS familiar como respaldo. Busca en tu router la sección de DHCP o de DNS (a veces está en "Red LAN" o "Configuración de internet"). Cambia los DNS que reparte el router por un servicio de DNS con filtrado familiar. Así, aunque un aparato se salte el filtro del perfil, el DNS bloquea los sitios peligrosos.

15. Ir a: Red > LAN > DHCP (o Configuración de internet > DNS)
16. DNS primario: usar la dirección del servicio de DNS familiar elegido
DNS secundario: usar la dirección secundaria del mismo servicio
17. Guardar y reiniciar el router si lo pide

Nota: las direcciones exactas del DNS familiar cambian con el tiempo; busca en internet "DNS familiar gratis" y usa las direcciones oficiales del proveedor que elijas. Anota cuáles pusiste.

Paso 7: prueba con cada aparato. En la tablet de Mariana intenta entrar a un sitio bloqueado: debe aparecer un aviso de bloqueo. Revisa que fuera del horario la tablet no navegue. Haz lo mismo con el celular de Diego. Y verifica que TU celular y tu computadora (que no están en ningún perfil) sigan navegando sin restricciones.

Resultado esperado: cada hijo tiene sus reglas automáticas. Mariana con horario de niña y filtros estrictos; Diego con horario de adolescente, filtros básicos y tope diario. Tú no tienes que andar quitando aparatos: el router aplica las reglas solo.

Ejemplo 3: Configurar el QoS para videollamadas y juegos (Clase 24)

Situación: trabajas desde casa con videollamadas (Zoom/Meet/Teams) y tu hijo juega en línea. Cuando alguien descarga algo pesado, tus llamadas se traban y el juego tiene lag. Vas a medir tu velocidad real y configurar prioridades.

Paso 1: mide tu velocidad REAL. Conecta una computadora por cable al router (el WiFi mete variación), cierra todos los programas que usen internet en tu casa, y haz un test de velocidad en un sitio de medición. Anota dos números: bajada y subida. Repite el test dos o tres veces y quédate con el promedio. Ejemplo: 95 Mbps de bajada, 9 Mbps de subida.

1. Conectar una PC por cable al router
2. Cerrar todo lo que use internet en la casa
3. Hacer 2 o 3 tests de velocidad y anotar el promedio
Ejemplo: Bajada = 95 Mbps, Subida = 9 Mbps

Paso 2: entra al panel del router y busca "QoS", "Calidad de servicio", "Priorización de tráfico" o "Bandwidth Control". Activa la función.

4. Entrar al panel del router
5. Ir a: Avanzado > QoS (o Calidad de servicio)
6. Activar QoS

Paso 3: escribe tu velocidad real en los campos de ancho de banda total. Este es el paso que la mayoría se salta y por eso "el QoS no les funciona". Pon los números que mediste en el paso 1. Algunos routers piden la velocidad en Mbps y otros en Kbps (1 Mbps = 1000 Kbps).

7. Ancho de banda total de bajada: 95 Mbps (el valor medido)
8. Ancho de banda total de subida: 9 Mbps (el valor medido)

Paso 4: crea las reglas de prioridad. La idea: videollamadas y voz en prioridad ALTA, juegos en línea en ALTA o MEDIA-ALTA, video por streaming en MEDIA, descargas y actualizaciones

en BAJA. Si tu router prioriza por aplicación, elige las apps de la lista; si prioriza por dispositivo, asigna prioridades a los aparatos clave.

9. Agregar reglas de prioridad (de mayor a menor):
 - Prioridad ALTA: Videollamadas (Zoom, Meet, Teams, WhatsApp llamadas)
 - Prioridad ALTA: Voz / VoIP
 - Prioridad MEDIA-ALTA: Juegos en línea (consola o PC del hijo)
 - Prioridad MEDIA: Streaming de video (Netflix, YouTube)
 - Prioridad BAJA: Descargas, actualizaciones, nube
10. Si el router lo permite por dispositivo:
 - Laptop del trabajo: prioridad ALTA
 - Consola/PC de juegos: prioridad MEDIA-ALTA
11. Guardar / Aplicar cambios

Paso 5: verifica que WMM esté activado en el WiFi (normalmente está en la configuración inalámbrica avanzada). Es la base automática de prioridad para voz y video en el WiFi.

12. Ir a: Inalámbrico > Configuración avanzada
13. Verificar que WMM esté ACTIVADO (normalmente ya lo está)

Paso 6: haz la prueba de fuego. Pide a alguien en tu casa que inicie una descarga pesada (un juego, una actualización grande, un respaldo a la nube). Mientras tanto, haz una videollamada o juega en línea. Antes del QoS, la llamada se trababa; ahora debería mantenerse fluida. Si se sigue trabando, revisa: ¿pusiste bien los números de velocidad? ¿la regla de la videollamada quedó en prioridad alta? ¿configuraste la subida y no solo la bajada?

Resultado esperado: con la red saturada a propósito, tu videollamada sigue clara y el juego sin lag, mientras la descarga simplemente tarda un poco más. Eso es el QoS funcionando: lo urgente pasa primero.

Práctica

Ejercicio 1: Diseña la política de WiFi para invitados de un pequeño negocio

Situación: tienes una cafetería pequeña con 20 mesas. Quieres ofrecer WiFi gratis a los clientes, pero tu computadora de la caja (donde llevas las ventas) y tu impresora de tickets están en la misma red. Diseña la política completa: nombre de la red, seguridad, aislamiento, límites y reglas de uso.

Solución paso a paso:

Primero, separa las redes. La computadora de la caja y la impresora se quedan en la red principal, que NO se comparte con nadie. Para los clientes creas una red de invitados con un nombre atractivo y claro, por ejemplo "CafeWiFi-Clientes". Nunca uses el nombre de tu red principal ni una contraseña parecida.

Segundo, seguridad con contraseña sencilla pero que cambie. Una red abierta en un negocio es un imán de problemas: se conecta gente de la banqueta y hasta el local de enfrente. Pon una contraseña fácil de dictar, como "Cafe2026!", y cámbiala cada mes. Imprímela en un cartelito en la caja o en las mesas; así la controlas tú.

Tercero, activa el aislamiento de clientes (AP isolation) y bloquea el acceso a la red local. Esto es NO negociable en un negocio: un cliente jamás debe poder ver la computadora de la caja ni la impresora, ni tampoco el celular de otro cliente. Verifica en el panel del router que las dos opciones queden bien puestas: aislamiento activado, acceso a red local desactivado.

Cuarto, ponle límite de velocidad a la red de invitados. Si tu paquete es de 100 megas, reserva 60 para tu operación (caja, terminal de pago) y deja 40 para invitados, o usa el límite por red de invitados que traiga tu router. Así, aunque se llene la cafetería, tu terminal de pago nunca se traba.

Quinto, define reglas de uso y horario. Programa la red de invitados para que solo esté activa en tu horario de servicio (por ejemplo, de 8:00 am a 10:00 pm). Si tu router permite tiempo máximo por sesión, pon 2 horas por cliente para que la mesa rote. Y coloca un aviso visible: "WiFi gratuito para clientes, uso moderado".

Sexto, mantenimiento mensual: cambia la contraseña de invitados, revisa que el aislamiento siga activado después de cualquier actualización del router, y verifica que tu red principal siga con contraseña fuerte y distinta. Con esto, tus clientes felices y tu caja blindada.

Ejercicio 2: Configura horarios y filtros para dos hijos de distintas edades

Situación: tienes a Sofía, de 7 años, con una tablet, y a Martín, de 16, con laptop y celular. En tu router ya existe el control parental con perfiles. Define las reglas completas para cada uno y explica por qué son distintas.

Solución paso a paso:

Paso 1: crea el perfil "Sofía" y asigna su tablet. Las reglas para una niña de 7 años son protectoras y simples. Horario: lunes a viernes de 5:00 pm a 8:00 pm (después de la tarea y antes de dormir), fines de semana de 10:00 am a 8:00 pm. Fuera de ese horario, sin internet. Filtros: bloquea las categorías de adultos, apuestas, violencia, drogas y redes sociales (a los 7 años no necesita redes sociales). No le pongas límite de horas diarias dentro de su ventana, porque la ventana ya es corta.

Paso 2: crea el perfil "Martín" y asigna su laptop y su celular (los dos aparatos al mismo perfil). Las reglas para un adolescente de 16 son de confianza con límites. Horario: todos los días de 7:00 am a 11:00 pm (necesita internet para la tarea y su vida social, pero a las 11 se acabó). Filtros: bloquea adultos y apuestas, pero permite redes sociales y juegos (prohibirle todo a un adolescente solo lo empuja a buscar cómo saltárselo). Límite diario: 5 horas de internet al día entre sus dos aparatos, para que administre su propio tiempo.

Paso 3: justifica la diferencia. A Sofía la proteges con horarios cortos y filtros amplios porque aún no tiene criterio para distinguir contenido. A Martín le das más libertad pero con topes (hora de apagado y límite diario) porque ya necesita autonomía, y los topes automáticos evitan la pelea diaria. Si a Martín le pusieras las reglas de Sofía, buscaría una VPN o los datos de su celular para saltárselas; si a Sofía le pusieras las de Martín, quedaría expuesta a contenido inadecuado.

Paso 4: capa de respaldo para ambos. Configura el DNS familiar en el router para que, aunque algún filtro de perfil falle, los sitios peligrosos sigan bloqueados. Y cambia la contraseña del panel del router: Martín tiene 16 años y sabe googlear "contraseña por defecto de mi router".

Paso 5: revisión mensual. Siéntate con cada uno y revisa si las reglas siguen funcionando. ¿Sofía necesita más tiempo para una tarea en línea? Se ajusta. ¿Martín demuestra responsabilidad? Se puede ampliar media hora. Las reglas crecen con ellos, y cuando participan en la revisión, las respetan más.

Ejercicio 3: Plan de QoS para una casa con home office y gamer

Situación: en tu casa hay 4 personas. Tú trabajas desde casa con videollamadas todo el día (laptop). Tu hijo juega en línea en su PC en las tardes. Tu esposa ve series en streaming en la noche. Tu hija sube videos a la nube para la escuela. El paquete contratado es de 120 Mbps de bajada y 12 Mbps de subida (medidos por cable: 115 de bajada, 11 de subida). Diseña el plan de QoS completo.

Solución paso a paso:

Paso 1: escribe los números reales en el QoS. En el panel del router, activa el QoS y pon como ancho de banda total: 115 Mbps de bajada y 11 Mbps de subida (los valores MEDIDOS, no los contratados). Este paso es la base de todo; sin números reales, las prioridades son adorno.

Paso 2: define las prioridades por aplicación, de mayor a menor. Prioridad ALTA: videollamadas (Zoom, Meet, Teams) y voz. Son tu trabajo y son lo más sensible al tiempo: un segundo de retraso arruina una llamada. Prioridad MEDIA-ALTA: juegos en línea. Necesitan respuesta rápida pero consumen poco ancho de banda, así que darles prioridad alta no le quita casi nada a los demás. Prioridad MEDIA: streaming de video (las series de tu esposa). El video trae su propio colchón (buffer), así que aguanta bien una prioridad media. Prioridad BAJA: subidas a la nube y descargas grandes (los videos de tu hija y cualquier actualización). Son pacientes por naturaleza: nadie nota si tardan unos minutos más.

Paso 3: atiende la subida con lupa. Tu subida es de solo 11 Mbps y es el recurso más escaso. Las videollamadas necesitan subir tu voz y tu video; si tu hija está subiendo un video pesado a la nube al mismo tiempo, te va a comer la subida. Por eso la regla de "subidas a la nube en prioridad BAJA" es la más importante de tu plan. Además, si tu router permite reservar un mínimo garantizado, reserva 3 Mbps de subida para videollamadas: así tu llamada siempre tiene su carril libre.

Paso 4: complementa con reglas por horario si tu router lo permite. De 9:00 am a 6:00 pm (tu horario de trabajo), las videollamadas mandan. De 6:00 pm a 11:00 pm, los juegos y el streaming suben de prioridad porque tú ya no trabajas. No todos los routers tienen QoS por horario; si el tuyo no, deja las prioridades fijas del paso 2, que ya resuelven el 90 por ciento del problema.

Paso 5: ponle límite a la red de invitados si la tienes activa, para que las visitas nunca compitan con tu trabajo. Y verifica que WMM esté activado en el WiFi.

Paso 6: prueba de fuego. Un día entre semana, pide a tu hijo que descargue un juego pesado y a tu hija que suba un video a la nube, mientras tú haces una videollamada de prueba. Si tu voz se escucha clara y el video no se congela, el plan funciona. Si algo falla, revisa en este orden: ¿los números de velocidad están bien escritos? ¿la subida también está configurada? ¿las videollamadas quedaron en prioridad alta de verdad?

Ejercicio 4: Diagnostica por qué el QoS "no sirve"

Situación: tu vecino activó el QoS en su router porque sus videollamadas se trababan, pero dice que "no sirvió para nada, todo sigue igual". Le revisas la configuración y encuentras esto: dejó el ancho de banda en los valores de fábrica (1000 Mbps de bajada y 1000 Mbps de

subida), puso TODAS las aplicaciones en prioridad alta, solo configuró la bajada, y además le dio prioridad alta a su Smart TV donde ve películas todo el día. Identifica cada error y explica cómo corregirlo.

Solución paso a paso:

Error 1: números de velocidad inventados. El router cree que tiene 1000 Mbps, así que jamás detecta congestión y nunca aplica las prioridades. Es como ponerle a un semáforo el horario de una ciudad fantasma: nunca cambia. Corrección: medir la velocidad real por cable y escribir esos números en el QoS.

Error 2: todo en prioridad alta. Si las videollamadas, los juegos, el streaming y las descargas tienen la misma prioridad, el router no sabe a quién atender primero y todo sigue igual. Corrección: solo dos o tres cosas en alta (videollamadas y voz), juegos en media-alta, streaming en media, descargas en baja. La prioridad solo funciona si hay algo NO prioritario con qué comparar.

Error 3: solo configuró la bajada. Las videollamadas que se traban casi siempre sufren por la subida saturada, y él no le puso ninguna regla a la subida. Corrección: configurar también el ancho de banda de subida con el valor medido y darle prioridad alta al tráfico de videollamadas en la subida.

Error 4: prioridad alta al Smart TV. La TV solo hace streaming, que ya trae su colchón y no necesita prioridad máxima; además, con prioridad alta, las películas de la TV compiten de igual a igual con sus videollamadas de trabajo. Corrección: bajar el streaming a prioridad media y quitar la regla del Smart TV, o mejor aún, priorizar por aplicación (la app de videollamadas) en lugar de por aparato.

Verificación final: después de corregir los cuatro puntos, hacer la prueba de fuego (descarga pesada + videollamada al mismo tiempo). Si la llamada se mantiene clara, el QoS ya está trabajando. Moraleja del ejercicio: el QoS no es un botón mágico; es un sistema de reglas, y las reglas mal escritas no gobiernan nada.

Ejercicio 5: Casa con cuarto de renta: invitados permanentes y familia

Situación: rentas un cuarto de tu casa por Airbnb. Los huéspedes cambian cada semana. Tienes dos hijos con control parental ya configurado y trabajas desde casa. Diseña la estrategia completa que combine red de invitados, control parental y QoS sin que choquen entre sí.

Solución paso a paso:

Paso 1: red de invitados como base de todo. Crea la red "Casa-Visitas" con contraseña que cambias cada semana (o cada que se va un huésped). Activa aislamiento de clientes y bloquea el acceso a la red local: el huésped jamás debe ver tus cámaras, tu impresora ni las computadoras de tus hijos. Esta red es también la que usarán las visitas de fin de semana; una sola red de invitados para todos los de afuera.

Paso 2: protege tu trabajo con QoS. Los huéspedes ven series y hacen videollamadas; no quieres que saturen tu conexión en tu horario laboral. Ponle a la red de invitados un límite de velocidad (por ejemplo, 15 Mbps de bajada y 4 de subida si tu paquete lo permite) y además configura el QoS general: tus videollamadas de trabajo en prioridad alta, el tráfico de la red de invitados en prioridad media-baja. Así el huésped navega a gusto pero jamás te tumba una llamada importante.

Paso 3: el control parental no toca a los invitados. Los perfiles de tus hijos siguen intactos en la red principal con sus horarios y filtros. La red de invitados NO lleva control parental (el huésped es un adulto que paga por el servicio), pero sí lleva el DNS familiar como cortesía básica: bloquea sitios maliciosos y de contenido extremo sin restringir la navegación normal. Es un punto medio razonable entre hospitalidad y responsabilidad.

Paso 4: horarios inteligentes. Programa la red de invitados para que esté activa siempre (los huéspedes pagan por ella), pero los perfiles de tus hijos mantienen sus horarios de apagado nocturno. No hay choque porque son redes separadas: a las 10 de la noche se apaga el internet de la tablet de tu hijo, pero el huésped sigue navegando en su red. Esa es la magia de separar: las reglas de cada grupo se aplican sin afectarse.

Paso 5: rutina de cambio de huésped. Cada que se va un huésped: cambia la contraseña de la red de invitados, revisa en el panel del router que no haya aparatos desconocidos conectados a tu red principal, y verifica que el aislamiento siga activado. Son tres minutos que te ahorran disgustos.

Paso 6: prueba integral una vez al mes. Conéctate a la red de invitados desde tu celular e intenta ver tus aparatos de la red principal (no deberías poder). Verifica que los horarios de tus hijos sigan aplicándose. Haz una videollamada mientras alguien ve una serie en la red de invitados y comprueba que tu llamada no se traba. Si las tres pruebas pasan, tu sistema está sano: afuera los invitados, adentro las reglas, y tu trabajo siempre con carril libre.

Resumen de la unidad

- La red de invitados es una segunda red WiFi separada de tu red principal: las visitas usan internet sin poder ver ni tocar tus aparatos ni tus datos. Es la sala de visitas de tu casa digital.
- Jamás des tu contraseña principal a visitas, técnicos o clientes: una vez que alguien entra a tu red principal, puede ver tu computadora, tu impresora, tus cámaras y todo lo conectado.
- El aislamiento de clientes (AP isolation) impide que los aparatos de la red de invitados se vean entre sí; y el bloqueo de acceso a la red local impide que vean tu red principal. Activa las dos opciones siempre.
- VLAN es la tecnología que divide una red física en redes lógicas separadas; tu router la usa automáticamente al crear la red de invitados. No necesitas configurarla a mano en un router casero.
- No conectes un segundo router solo para los invitados: eso crea doble NAT y rompe videollamadas, juegos y cámaras. La red de invitados la crea tu router principal.
- Buenas prácticas de invitados: contraseña propia y distinta a la principal, cámbiala seguido, ponle límite de velocidad, y en negocios es obligatoria, no opcional.
- El control parental tiene tres patas: horarios de acceso (el internet se apaga solo), filtros de contenido por categorías (bloquean tipos de sitios) y límites por dispositivo (tope de horas diarias, pausa manual).
- Crea un perfil por hijo con reglas según su edad: protección estricta para los pequeños, confianza con topes para los adolescentes. Las mismas reglas para todos no funcionan.
- El DNS familiar es una capa extra de protección: bloquea sitios peligrosos aunque el filtro del perfil falle. Configúralo como respaldo.
- Limitaciones honestas: los filtros no ven dentro de las apps, un adolescente puede usar VPN para saltárselos, y ningún filtro reemplaza la conversación con tus hijos.
- Cambia la contraseña del panel de tu router: si tu hijo la adivina, se quita las reglas él solo.
- QoS significa calidad de servicio: es el sistema de prioridades que le abre un carril de emergencias al tráfico urgente (videollamadas, juegos) para que pase antes que las descargas.
- WMM es el mini-QoS automático del WiFi que prioriza voz y video; déjalo activado, es la base.

- Prioriza poco pero bien: videollamadas y voz en alta, juegos en media-alta, streaming en media, descargas y nube en baja. Si todo es prioritario, nada lo es.
- La subida es el recurso escaso: las videollamadas que se traban casi siempre sufren por la subida saturada, no por la bajada. Configura el QoS de subida con el mismo cuidado que el de bajada.
- El bufferbloat es el embudo lleno: el buffer del router se satura con descargas y tu tráfico urgente queda haciendo fila, lo que causa voz de robot y lag aunque el test de velocidad marque bien. El QoS bien configurado lo combate.
- El QoS necesita tus números reales: mide la velocidad por cable antes de configurar y escribe esos valores. Sin números reales, las prioridades no funcionan.
- Las tres clases forman un sistema: invitados protegidos por fuera, familia ordenada por dentro con reglas automáticas, y QoS haciendo que todo funcione al mismo tiempo sin atorarse.
- El QoS reparte lo que hay, no inventa megas: si después de configurarlo bien sigues sufriendo con todo saturado, entonces sí considera subir tu paquete contratado.
- En negocios, la red de invitados es obligatoria: protege la caja, la terminal de pago y los datos de clientes; cámbiale la contraseña cada mes y programa su horario de servicio.
- Revisa tu configuración una vez al mes: que el aislamiento siga activo, que los horarios de tus hijos sigan teniendo sentido y que los números del QoS sigan siendo tus velocidades reales.
- Empieza hoy con el plan de 30 minutos: invitados separados, horario nocturno y QoS esencial. Lo demás se pule el fin de semana.

UNIDAD 9: Diagnóstico y solución de problemas (Clases 25 a 27)

INTRODUCCIÓN

Llegaste a la unidad donde todo lo que aprendiste se convierte en poder real. Hasta ahora ya sabes qué es una red inalámbrica, cómo funciona el espectro de frecuencias, qué significan las bandas de 2.4, 5 y 6 GHz, cómo configurar tu router con seguridad y cómo extender tu cobertura. Todo eso es valiosísimo. Pero hay una realidad que todo el mundo enfrenta tarde o temprano, y es esta: el WiFi falla. Se cae. Se pone lento. Un día deja de funcionar sin avisar y sin explicación. Y en ese momento, toda la teoría que acumulaste vale oro únicamente si sabes aplicarla con método, como un técnico profesional.

Piénsalo por un momento. ¿Cuántas veces has escuchado a alguien decir "mi internet está lentísimo" mientras reinicia el router por décima vez sin que nada cambie? ¿Cuántas veces has visto a un familiar gritarle al módem como si el aparato tuviera la culpa de todo? ¿Cuántas veces has llamado al proveedor para quejarte, has esperado una hora en el teléfono, y el técnico te ha dicho "señor, su conexión está perfecta, el problema es su WiFi"? Esa frustración es universal. Y la mayoría de las personas la enfrenta con la misma estrategia: reiniciar todo, esperar, y si no funciona, enojarse. Esa estrategia no es diagnóstico. Es esperanza. Y la esperanza no arregla redes.

En esta unidad vas a aprender algo distinto: a pensar como un técnico de redes. Un técnico no adivina. Un técnico no reinicia y reza. Un técnico observa los síntomas, hace pruebas ordenadas, interpreta los números y llega a un diagnóstico que le dice exactamente qué está mal y qué hay que hacer. Es el mismo proceso que sigue un doctor con un paciente: nadie receta medicina sin antes escuchar los síntomas y pedir análisis. En redes, los "análisis" son mediciones: niveles de señal en dBm, velocidad de enlace, pruebas de velocidad, ping, traceroute. Cuando sabes leer esos números, dejas de ser víctima del WiFi caprichoso y te conviertes en la persona que lo controla.

Esta unidad está organizada en tres clases que forman un arco completo. En la Clase 25 vas a aprender a medir tu red: qué significan los números que tu teléfono, tu laptop o tu router te muestran. ¿Qué es ese -67 dBm que aparece en la configuración avanzada? ¿Por qué tu velocidad de enlace dice 866 Mbps pero tu prueba de velocidad marca apenas 120 Mbps? ¿Qué diferencia hay entre latencia y velocidad, y por qué un ping alto arruina tus videollamadas aunque la velocidad sea buena? Cuando termines esta clase, los números dejarán de ser misteriosos y se convertirán en tus informantes.

En la Clase 26 conocerás las herramientas de diagnóstico: los analizadores WiFi que te muestran qué canales están saturados, los comandos ping y traceroute que te dicen exactamente dónde se rompe el camino entre tu dispositivo e internet, y el panel de administración de tu router, que es como la sala de máquinas donde vive toda la información que necesitas. Vas a practicar con cada herramienta hasta que usarlas se sienta natural.

Y en la Clase 27 llegamos al plato fuerte: los 15 problemas más comunes de las redes WiFi y cómo resolverlos paso a paso. El WiFi que se cae cada noche. La red que va lenta solo en el cuarto del fondo. El celular que no conecta mientras la laptop funciona perfecto. El internet que se desploma cuando todos están en casa. Cada problema con su causa probable, su prueba de confirmación y su solución ordenada. Esta clase es la que vas a consultar una y otra vez cuando algo falle en tu casa, en tu oficina o en casa de tus clientes.

Al final de esta unidad serás capaz de hacer lo siguiente: medir la señal de tu red e interpretar los valores en dBm; distinguir entre un problema de WiFi y un problema de conexión a internet; ejecutar un diagnóstico completo y ordenado con pruebas de velocidad, ping y traceroute; usar un analizador WiFi para elegir el mejor canal; leer el panel de tu router y encontrar la información relevante; y resolver los 15 problemas más frecuentes con una metodología que no depende de la suerte.

Una advertencia honesta antes de empezar: esta unidad es larga y está llena de números, comandos y procedimientos. Es normal sentir al principio que es mucha información. La buena noticia es que el diagnóstico de redes es una habilidad práctica, no un examen de memoria. No necesitas memorizar cada valor de la tabla de dBm para siempre; necesitas saber que la tabla existe y dónde consultarla. No necesitas recitar de memoria la sintaxis de cada comando; necesitas haberlos ejecutado una vez y entender qué te dicen. Así que sigue el orden: lee la explicación, haz los ejemplos paso a paso con tus propios dispositivos, resuelve la práctica, y al final quédate con el resumen y el checklist de diagnóstico rápido. Ese checklist de una página, impreso o guardado en tu teléfono, va a ser tu mejor amigo cada vez que una red falle.

También quiero que tengas claro algo desde ahora: en esta unidad no vamos a culpar al proveedor por todo, ni vamos a suponer que el router siempre es el problema. La mayoría de los problemas de "internet lento" no son del internet. Son del WiFi. Y la mayoría de los problemas del WiFi no requieren comprar equipo nuevo. Requieren entender qué está pasando. Un cambio de canal, mover el router dos metros, o actualizar la configuración de un dispositivo viejo pueden hacer más diferencia que comprar el router más caro de la tienda. El diagnóstico correcto ahorra dinero, tiempo y corajes. Eso es lo que vas a aprender aquí.

Respira hondo. Abre tu laptop o tu teléfono, porque en esta unidad vas a tocar tu red de verdad. Y cuando termines, vas a mirar tu WiFi con otros ojos: ya no como una caja misteriosa

que a veces funciona y a veces no, sino como un sistema que entiendes, que mides y que sabes reparar. Eso, en el mundo de las redes, es la diferencia entre un usuario y un técnico. Bienvenido a tu transformación.

Explicación detallada

El diagnóstico es como ir al doctor: síntomas, pruebas y diagnóstico

Cuando te sientes mal, no llegas con el doctor y le dices "dame medicina". Primero le describes los síntomas: me duele la cabeza desde ayer, tengo fiebre, me duele la garganta. El doctor te escucha, te hace preguntas, y después pide pruebas: análisis de sangre, una radiografía, te toma la presión. Solo con los resultados en la mano emite un diagnóstico y receta el tratamiento. Si el doctor te recetara sin pruebas, estaría adivinando, y adivinar con la salud es peligroso.

Diagnosticar una red WiFi funciona exactamente igual. Los síntomas son lo que el usuario reporta: "se cae el WiFi", "está lento", "no conecta mi celular". Las pruebas son las mediciones que tú haces: nivel de señal, prueba de velocidad, ping, traceroute, revisión del canal. El diagnóstico es tu conclusión fundamentada: "la señal llega débil al cuarto del fondo, -78 dBm, y el canal 6 está saturado; por eso se cae". Y el tratamiento es la solución: cambiar de canal, mover el router, agregar un repetidor.

Este orden importa más de lo que parece. La mayoría de las personas salta directamente al "tratamiento": reinician el router, cambian la contraseña, compran un repetidor, llaman al proveedor. A veces funciona, por pura suerte, porque el reinicio resolvió un bloqueo temporal. Pero cuando no funciona, no saben qué hacer después, porque nunca supieron qué estaba mal. Un técnico, en cambio, sigue el orden siempre: síntomas, pruebas, diagnóstico, solución. Y lo sigue incluso cuando cree que ya sabe qué pasa, porque las redes engañan: dos problemas distintos pueden tener exactamente los mismos síntomas.

Toma nota de este principio porque va a aparecer en toda la unidad: nunca apliques una solución sin antes tener un diagnóstico, y nunca emitas un diagnóstico sin antes tener mediciones. Los números no mienten. Las corazonadas sí.

Otra lección del doctor: un buen diagnóstico empieza por escuchar bien los síntomas. Cuando alguien te diga "el internet no sirve", tu primera tarea es convertir esa queja vaga en datos concretos. ¿Qué significa "no sirve"? ¿No abre ninguna página? ¿Abre pero lento? ¿Se cae cada cierto tiempo? ¿Pasa en todos los dispositivos o solo en uno? ¿Pasa a todas horas o solo en la noche? ¿Empezó de repente o lleva semanas así? ¿Cambió algo recientemente: un

router nuevo, un vecino nuevo, una pared nueva? Cada respuesta elimina sospechosos. Un problema que afecta a todos los dispositivos apunta al router o al proveedor. Un problema en un solo dispositivo apunta a ese dispositivo. Un problema que aparece a las 8 de la noche todos los días apunta a congestión o interferencia con horario. Escuchar bien te ahorra la mitad del trabajo.

dBm: el idioma en el que habla tu señal

Todo dispositivo WiFi mide constantemente la potencia de la señal que recibe del router, y expresa esa medida en una unidad llamada dBm, que significa decibelios referidos a un milivatio. No te asustes con el nombre técnico: lo único que necesitas entender es que el dBm es la forma estándar de decir "qué tan fuerte me llega la señal", y que funciona con una escala de números negativos donde, atención, menos negativo significa más fuerte. Es decir, -40 dBm es una señal mucho más fuerte que -80 dBm. Esto confunde al principio porque estamos acostumbrados a que los números más grandes sean mejores, pero aquí el -40 está "más cerca de cero" y por tanto es mejor que el -80.

¿Por qué números negativos? Porque un milivatio (0 dBm) sería una potencia enorme para una señal WiFi recibida; las señales reales que recibe tu teléfono son fracciones minúsculas de milivatio, y en la escala logarítmica de decibelios eso se expresa con negativos. No necesitas hacer la matemática. Solo necesitas la tabla de referencia, que es el instrumento más consultado por cualquier técnico. Memorízala a grandes rasgos o guárdala dónde la puedas consultar:

- -30 dBm a -50 dBm: EXCELENTE. Estás prácticamente al lado del router. Señal máxima, velocidad máxima, todo funciona perfecto.
- -50 dBm a -60 dBm: MUY BUENA. Calidad alta, ideal para videollamadas, streaming en 4K y juegos en línea. Es el rango objetivo para los lugares donde más usas la red.
- -60 dBm a -67 dBm: BUENA. Funcionamiento confiable para casi todo, incluyendo videollamadas. A partir de aquí empieza la zona donde conviene poner atención.
- -67 dBm a -70 dBm: ACEPTABLE. Es el límite práctico recomendado para voz y video. Navegación y streaming básico funcionan, pero ya no hay margen: cualquier interferencia se nota.
- -70 dBm a -80 dBm: DÉBIL. La conexión se vuelve inestable. Las páginas tardan, el video se traba, las videollamadas se cortan. Aquí ya hay un problema que atender.
- -80 dBm a -90 dBm: MUY DÉBIL. Apenas usable; muchas veces el dispositivo se desconecta solo o no logra mantener la conexión.

- Menos de -90 dBm: INSERVIBLE. En la práctica no hay conexión útil.

Un detalle importante: la escala es logarítmica, no lineal. Eso significa que cada 10 dBm de diferencia representan un cambio de 10 veces en la potencia real. Pasar de -70 a -60 dBm no es "un poquito mejor": es diez veces más potencia de señal. Y pasar de -80 a -60 es cien veces más. Por eso un cambio de apenas unos dBm se puede sentir muchísimo en la práctica, y por eso mover el router un par de metros o cambiar de canal puede transformar una red.

¿Dónde ves este número? En Windows, puedes abrir una terminal y escribir ``netsh wlan show interfaces``; en la información aparece "Señal" como porcentaje, pero hay formas de ver el dBm con aplicaciones. En Android, aplicaciones como analizadores WiFi muestran el dBm directamente. En iPhone, el sistema no lo muestra de forma sencilla al usuario, pero el modo de diagnóstico de campo (marcando un código especial) lo revela. En el panel de administración de tu router, la lista de clientes conectados suele mostrar la intensidad de señal de cada dispositivo. En la Clase 26 veremos cada herramienta con calma; por ahora quédate con la idea: el dBm es tu termómetro. Igual que 37 grados es fiebre y 40 es urgencia, -65 dBm es saludable y -85 dBm es urgencia.

Un error común de principiantes: obsesionarse con conseguir -30 dBm en toda la casa. No es necesario ni realista. Tu objetivo práctico es que los lugares donde realmente usas la red (tu escritorio, tu sala, tu cuarto) estén entre -50 y -67 dBm. Si el baño o el patio quedan en -75, no pasa nada, a menos que hagas videollamadas desde ahí. El diagnóstico siempre se hace pensando en el uso real, no en números perfectos.

RSSI vs dBm: no son lo mismo, aunque lo parezcan

Vas a encontrar dos términos que parecen hablar de lo mismo: RSSI y dBm. RSSI significa Received Signal Strength Indicator, indicador de la intensidad de señal recibida. En la práctica, muchos fabricantes usan "RSSI" como el nombre del valor y "dBm" como la unidad en la que lo expresan. Es decir, cuando tu teléfono dice "RSSI: -65 dBm", te está diciendo la intensidad de la señal recibida medida en dBm. Hasta ahí, son dos nombres para el mismo dato.

La confusión aparece porque algunos dispositivos, en lugar de mostrarte el dBm, te muestran la señal como un porcentaje (0 a 100%) o como las clásicas "barritas" del WiFi. Esos porcentajes y barritas se calculan a partir del RSSI, pero cada fabricante usa su propia fórmula. Para un fabricante, 70% puede significar -60 dBm; para otro, puede significar -65 dBm. Las barritas son todavía peores: no hay un estándar que diga cuántas barritas corresponden a cada dBm, así que tres barritas en un Samsung no significan lo mismo que tres barritas en un iPhone.

Moraleja de técnico: cuando diagnostiques, busca siempre el valor en dBm, no el porcentaje ni las barritas. El dBm es universal y comparable; el porcentaje y las barritas son adornos de cada fabricante. Es como la diferencia entre decir "hace calor" y decir "hay 38 grados": lo primero depende de quién lo diga, lo segundo es un dato.

Otro matiz que vale oro: el RSSI que ves es la señal que TU dispositivo recibe del router, medida por tu dispositivo. El router también mide la señal que recibe de tu dispositivo, y no son necesariamente iguales. Tu router transmite con más potencia que tu teléfono, así que es común que tu teléfono reciba bien al router (-60 dBm) pero el router reciba débil a tu teléfono. Esto explica un misterio clásico: "tengo todas las barritas pero el internet va lento". Las barritas solo te dicen que la descarga llega bien; si tu teléfono no tiene fuerza para que su señal de subida llegue clara al router, la comunicación se traba. Cuando veas este síntoma, sospecha de asimetría: buena señal de bajada, mala de subida, típico en dispositivos alejados o con antenas débiles.

Velocidad de enlace vs velocidad real: por qué los números no cuadran

Esta es una de las confusiones más grandes y más caras en el mundo del WiFi. Tu laptop dice "velocidad de conexión: 866 Mbps" y tú contrataste 200 Mbps de internet, pero la prueba de velocidad marca 90 Mbps. ¿Quién miente? Nadie. Es que están midiendo cosas distintas.

La velocidad de enlace (también llamada tasa de enlace o link rate) es la velocidad teórica máxima a la que tu dispositivo y el router acordaron comunicarse entre ellos, por el aire, en condiciones ideales. Es un número que depende del estándar WiFi (WiFi 5, WiFi 6), del ancho de canal (20, 40, 80 MHz), del número de antenas y de la calidad de la señal en ese momento. Es como el velocímetro de un coche que marca 220 km/h: es lo máximo que el coche puede dar, no lo que vas a alcanzar en el tráfico de la ciudad.

La velocidad real (throughput) es lo que efectivamente logras transferir, medida con una prueba de velocidad. Siempre es menor que la velocidad de enlace, y normalmente mucho menor: entre el 30% y el 60% de la velocidad de enlace en condiciones buenas. ¿Por qué? Porque el WiFi tiene una sobrecarga enorme: por cada paquete de datos útiles viajan encabezados, confirmaciones de recepción, tiempos de espera para evitar colisiones, retransmisiones por interferencia y el cifrado de seguridad. Todo eso consume "aire". Además, el WiFi es un medio compartido: tu dispositivo no transmite todo el tiempo, sino que espera su turno para hablar, como en una conversación donde solo una persona puede hablar a la vez.

Haz la cuenta con un ejemplo típico: velocidad de enlace de 866 Mbps (muy común en WiFi 5 con canal de 80 MHz y buena señal). En la práctica, con un solo dispositivo y buenas condiciones, obtendrás entre 250 y 450 Mbps reales. Si tu internet contratado es de 200 Mbps,

tu WiFi no es el cuello de botella: el límite lo pone tu proveedor. Pero si tu velocidad de enlace es de 72 Mbps (típico de un dispositivo viejo en 2.4 GHz con canal de 20 MHz), tu velocidad real andrà por los 25-40 Mbps, y ahí sí el WiFi es el que te está frenando, aunque hayas contratado 200.

Esta distinción es una herramienta de diagnóstico potentísima. Compara siempre estos tres números en orden: 1) velocidad contratada con tu proveedor, 2) velocidad de enlace de tu dispositivo, 3) velocidad real medida. Si la velocidad real es parecida a la contratada, tu WiFi está bien y no hay nada que arreglar aunque la velocidad de enlace "se vea baja". Si la velocidad real es mucho menor que la contratada pero la velocidad de enlace es alta, el problema puede estar en el proveedor o en la saturación. Si la velocidad de enlace es baja, el problema está en tu red WiFi (señal débil, banda de 2.4 GHz saturada, dispositivo viejo) y ahí es donde debes actuar.

Un caso clásico: alguien contrata 500 Mbps, hace la prueba en su celular y obtiene 95 Mbps, y llama furioso al proveedor. El técnico llega, conecta su laptop por cable al router y mide 480 Mbps: el proveedor cumple. El problema es que el celular estaba conectado a la banda de 2.4 GHz con velocidad de enlace de 144 Mbps. La solución no era pelear con el proveedor, sino pasar el celular a la banda de 5 GHz. Sin entender la diferencia entre velocidad de enlace y velocidad real, ese diagnóstico es imposible.

Otro detalle que debes conocer: la velocidad de enlace cambia sola todo el tiempo. Si te alejas del router, tu dispositivo y el router negocian una velocidad menor para mantener la conexión estable con la señal más débil. Verás el número bajar de 866 a 433 a 216 a 54 Mbps conforme te alejas. Esto es normal y es por diseño: mejor ir lento y estable que rápido y con errores. Pero también es un indicador diagnóstico: si junto al router tu velocidad de enlace es bajísima, algo anda mal (interferencia fuerte, configuración incorrecta o dispositivo limitado).

Latencia, ping y jitter: la velocidad que no se ve en los anuncios

Los anuncios de internet solo hablan de velocidad de descarga: "200 megas, 500 megas, 1 giga". Pero hay otra medida igual o más importante para muchas actividades: la latencia. La latencia es el tiempo que tarda un paquete en ir de tu dispositivo al destino y regresar, y se mide en milisegundos (ms). La herramienta para medirla es el ping, que ya usarás en esta unidad.

Piensa en la diferencia así: la velocidad (ancho de banda) es cuántos carriles tiene la autopista; la latencia es qué tan rápido viajan los coches por ella. Una autopista de 10 carriles con tráfico detenido no te sirve si tienes prisa. Para descargar una película, lo que importa son los carriles (velocidad). Para una videollamada, un juego en línea o una llamada de voz, lo que

importa es que los coches lleguen rápido (latencia). Puedes tener 500 Mbps y aun así tener videollamadas horribles si tu latencia es de 300 ms.

Valores de referencia para latencia (haciendo ping a un servidor cercano o a tu puerta de enlace):

- Menos de 20 ms: excelente. Juegos en línea y videollamadas perfectos.
- 20 a 50 ms: bueno. Todo funciona bien.
- 50 a 100 ms: aceptable. Videollamadas bien, juegos con ligero retraso.
- 100 a 200 ms: malo. Se nota el retraso en llamadas y juegos; el "¿me escuchas? ...sí, te escucho" con pausas incómodas.
- Más de 200 ms: muy malo. Llamadas casi imposibles, juegos injugables.

Ojo con un matiz: la latencia a tu puerta de enlace (tu router, normalmente 192.168.1.1 o 192.168.0.1) debería ser de 1 a 5 ms por WiFi. Si el ping a tu propio router ya marca 80 ms, el problema está en tu WiFi, sin duda: interferencia, saturación o señal débil. Si el ping al router es de 2 ms pero el ping a google.com es de 250 ms, tu WiFi está bien y el problema está más allá: en tu proveedor o en la ruta hacia internet. Esta comparación es una de las pruebas más reveladoras del diagnóstico, y la harás paso a paso en la sección de ejemplos.

El jitter es la variación de la latencia: si tus pings son 20, 22, 19, 21 ms, el jitter es bajo y todo bien; si son 20, 180, 35, 250 ms, el jitter es alto y las llamadas se escuchan entrecortadas aunque la velocidad sea buena. El jitter alto es típico de WiFi con interferencia o saturado: los paquetes llegan, pero llegan a destiempo, como un tamborilero que no lleva el ritmo. Para voz y video, un jitter menor a 30 ms es lo deseable.

Un error común: creer que "más megas" arregla la latencia. No. Si tu problema son videollamadas entrecortadas con 200 Mbps contratados, subir a 500 Mbps no va a cambiar nada, porque tu problema no es de carriles sino de rapidez. Lo que necesitas es bajar la latencia y el jitter: acercarte al router, cambiar de canal, usar 5 GHz o conectar por cable. El diagnóstico correcto te ahorra pagar por velocidad que no necesitas.

Pérdida de paquetes: el enemigo silencioso

Hay un tercer indicador que los principiantes casi nunca miran y que explica muchos misterios: la pérdida de paquetes. Cuando tu dispositivo envía datos por WiFi, algunos paquetes se pierden en el camino por interferencia, señal débil o colisiones, y tienen que reenviarse. Una pérdida pequeña (menos del 1%) es normal y ni la notas. Pero cuando la pérdida sube al 5%, 10% o más, la red se siente "rara": las páginas cargan a medias, los videos se congelan

aunque la velocidad marque bien, las llamadas se cortan por segundos, los juegos se "traban" de golpe.

Lo traicionero de la pérdida de paquetes es que la prueba de velocidad puede salir perfecta mientras el problema existe. La prueba de velocidad mide cuántos datos llegan por segundo en condiciones de esfuerzo sostenido, y el protocolo se adapta; pero una videollamada no puede "esperar" a que lleguen los paquetes perdidos: si no llegan a tiempo, se pierde el audio o el video de ese instante. Por eso el síntoma clásico de pérdida de paquetes es: "la velocidad está bien pero las llamadas se cortan".

¿Cómo se mide? Con el ping extendido: envías muchos pings seguidos (por ejemplo 100) y cuentas cuántos no regresan. En Windows, ``ping google.com -n 100`` te da al final el porcentaje de pérdida. Valores de referencia: 0% a 1% es normal; 2% a 5% ya se nota en llamadas y juegos; más de 5% es un problema serio que hay que atender.

Las causas más comunes de pérdida de paquetes en WiFi son: señal débil (el paquete llega tan deteriorado que se descarta), interferencia (otro dispositivo "pisa" tu transmisión), saturación del canal (demasiados dispositivos hablando a la vez y chocando) y, a veces, un router sobrecargado o con firmware viejo. El procedimiento de diagnóstico que aprenderás te llevará por cada causa en orden, de la más probable a la menos probable.

Guarda esta frase: velocidad, latencia y pérdida de paquetes son las tres patas del diagnóstico. Una red puede estar perfecta en velocidad y fallar en latencia; puede estar bien en latencia y fallar en pérdida. El técnico completo mide las tres, porque cada una apunta a causas distintas y a soluciones distintas.

Problema de WiFi o problema de internet: la pregunta que lo decide todo

Si solo te quedas con una idea de esta unidad, que sea esta: "mi internet está lento" casi nunca significa que el internet esté lento. Significa que algo en el camino entre tu dispositivo y el internet está lento, y ese camino tiene dos tramos muy distintos: el tramo inalámbrico (tu WiFi, de tu dispositivo al router, que es tu responsabilidad) y el tramo del proveedor (del router hacia internet, que es responsabilidad de la compañía). Diagnosticar es, antes que nada, averiguar en cuál de los dos tramos está el problema, porque las soluciones son completamente distintas y porque reclamarle al proveedor un problema de tu WiFi es perder el tiempo.

La prueba reina para separar los tramos es muy simple: conecta un dispositivo por cable Ethernet directamente al router y haz una prueba de velocidad. El cable elimina el WiFi de la ecuación. Si por cable la velocidad es buena (cercana a lo contratado) pero por WiFi es mala, el problema es tu WiFi: señal, interferencia, banda, configuración. Si por cable la velocidad

también es mala, el problema es del proveedor o del router mismo: llama a la compañía con datos en mano.

¿Y si no tienes cable ni adaptador? Hay una segunda prueba casi igual de buena: haz la prueba de velocidad pegado al router (a un metro, sin obstáculos) y compárala con la prueba en el lugar donde tienes el problema. Si junto al router todo vuela y en tu cuarto todo se arrastra, el problema es cobertura o interferencia en el tramo WiFi. Si junto al router también va mal, sospecha del proveedor o del router.

Esta distinción también aplica a las caídas totales. Si ningún dispositivo tiene internet (ni por WiFi ni por cable) y las luces del módem/router muestran falla, es problema del proveedor o del equipo. Si los dispositivos siguen conectados al WiFi (con las barritas llenas) pero "no hay internet", puede ser que el router perdió la conexión con el proveedor: ahí el WiFi funciona perfecto y lo que falló es el otro tramo. Fíjate qué importante es el lenguaje: "no tengo WiFi" y "no tengo internet" son problemas distintos. El WiFi es tu red local; el internet es lo que está más allá de tu router. Puedes tener WiFi perfecto sin internet, e internet perfecto con WiFi pésimo.

Memoriza este árbol de decisión porque lo usarás toda la vida:

1. ¿El problema afecta a todos los dispositivos o solo a uno? Si es uno solo, el problema es ese dispositivo. Si son todos, sigue.
2. ¿Por cable funciona bien? Si sí, el problema es el WiFi. Si no, el problema es el proveedor o el router.
3. ¿Junto al router funciona bien pero lejos no? Si sí, es cobertura o interferencia. Si no, sigue.
4. ¿El ping al router es bajo pero el ping a internet es alto? Si sí, tu WiFi está bien y el problema está más allá.

Con esas cuatro preguntas, sin ninguna herramienta especial, ya diagnosticas como técnico el 80% de los casos. Las herramientas de la Clase 26 sirven para el 20% restante y para confirmar con números lo que las preguntas ya te dijeron.

Cómo leer un analizador WiFi: canales, gráficos y decisiones

Un analizador WiFi es una aplicación (para teléfono o computadora) que "ve" las redes inalámbricas a tu alrededor y te muestra información que normalmente está oculta: qué redes existen, en qué canal transmite cada una, con qué intensidad llega su señal y cuánto se traslapan entre ellas. Es como unas gafas de rayos X para el espectro. Las más conocidas son WiFi Analyzer (Android), NetSpot o inSSIDer (Windows/Mac) y Airport Utility (iPhone). Todas muestran básicamente lo mismo con distinto diseño.

Lo primero que verás es una lista de redes con estos datos por cada una: nombre (SSID), intensidad de señal en dBm, canal y banda (2.4 o 5 GHz). Lo segundo, y más útil, es el gráfico de canales: un dibujo donde el eje horizontal son los canales y cada red aparece como una curva o "joroba" centrada en su canal, con la altura indicando su intensidad. Este gráfico es tu mapa de batalla.

Cómo interpretarlo: en la banda de 2.4 GHz solo hay tres canales que no se traslapan entre sí: el 1, el 6 y el 11. Si tu red está en el canal 6 y el gráfico muestra tres redes vecinas también en el 6 con buena intensidad, están compartiendo el mismo "carril" y se estorban: es como cuatro coches tratando de pasar por un carril al mismo tiempo. La solución es moverte a un canal menos ocupado, típicamente el 1 o el 11, el que tenga menos redes fuertes. En cambio, si pones tu red en el canal 3 "para no usar el mismo que el vecino", es peor: el canal 3 se traslapa parcialmente con el 1 y el 6, así que interferirás con ambos sin compartir bien con ninguno. Regla de oro en 2.4 GHz: usa solo 1, 6 u 11, y elige el menos saturado.

En la banda de 5 GHz la vida es más fácil: hay muchos más canales y casi no se traslapan, así que normalmente basta con elegir uno poco usado. El analizador te lo muestra igual: busca un canal donde no haya jorobas altas de vecinos.

Qué buscar exactamente en el gráfico: 1) ¿Cuántas redes comparten tu canal? Más de 2 o 3 redes fuertes en tu mismo canal es congestión. 2) ¿Hay redes en canales adyacentes que se traslapan con el tuyo? Eso es interferencia y es peor que compartir canal, porque ni siquiera pueden coordinarse. 3) ¿La intensidad de las redes vecinas es alta (más de -70 dBm)? Una red vecina débil (-85 dBm) apenas te afecta; una fuerte (-55 dBm) te afecta mucho.

El analizador también te sirve para medir tu propia cobertura: camina por tu casa viendo el dBm de tu red en cada cuarto y anota los valores. Así construyes un "mapa de calor" casero que te dice exactamente dónde la señal se degrada y dónde necesitas actuar. Hazlo una vez y tendrás el diagnóstico de cobertura más preciso que existe, mejor que cualquier suposición.

Un consejo práctico: haz el análisis de canales en el horario en que tienes el problema. Si tu WiFi falla en las noches, analiza en la noche, porque es cuando los vecinos encienden sus redes y sus dispositivos. Un análisis hecho a las 10 de la mañana puede mostrar canales libres que a las 9 de la noche están saturados.

Errores comunes: reiniciar sin diagnosticar y culpar al proveedor

Hay dos errores que comete casi todo el mundo y que tú, después de esta unidad, no vas a cometer más.

Error uno: reiniciar sin diagnosticar. Reiniciar el router se ha convertido en el "apágalo y préndelo" de las redes, y hay que decirlo con justicia: a veces sí funciona, porque limpia bloqueos temporales de memoria, reconexiones atascadas o tablas saturadas del router. El problema no es reiniciar; el problema es reiniciar como única estrategia, sin medir nada antes ni después. Si reinicias y se arregla pero no sabes por qué falló, el problema va a volver, y volverá en el peor momento. Peor aún: reiniciar borra evidencia. Es como tomar un analgésico sin decirle al doctor dónde te dolía: el dolor se calma, pero la causa sigue ahí. La forma profesional es: mide primero (señal, velocidad, ping), anota los números, reinicia si lo consideras necesario, y mide después. Si los números mejoraron, documenta qué hiciste. Si no mejoraron, ya descartaste una causa y sigues con la siguiente. Reiniciar es una herramienta, no un diagnóstico.

Error dos: culpar al proveedor cuando el problema es el WiFi. Es el error más caro en tiempo y corajes. Funciona así: el usuario nota lentitud, asume que "el internet" falla, llama a la compañía, espera, el técnico revisa y dice "su servicio está bien, el problema es su red interna", y el usuario se queda igual que al principio pero más enojado. Todo eso se evita con la prueba del cable o la prueba "junto al router" que viste arriba. Antes de llamar al proveedor, ten estos datos listos: velocidad por cable (o junto al router), velocidad en el punto del problema, ping a la puerta de enlace y ping a internet, y hora y frecuencia del problema. Con esos datos, la llamada dura cinco minutos: o te confirman la falla de su lado, o te dicen con precisión qué está mal. Llamar sin datos es pedirle al técnico que adivine por teléfono.

Hay un tercer error, más sutil: comprar equipo para un problema que no se ha diagnosticado. Repetidores, routers nuevos, "amplificadores de señal" que venden en internet... Mucha gente gasta dinero antes de saber qué necesita. Un repetidor no arregla un canal saturado; un router nuevo no arregla una mala ubicación; nada comprado arregla un problema del proveedor. La regla es: primero el diagnóstico, después la compra, y solo si el diagnóstico dice que hace falta hardware. El mejor técnico no es el que tiene más aparatos, sino el que compra menos porque diagnostica mejor.

Y un cuarto error clásico: cambiar muchas cosas a la vez. "Cambié el canal, moví el router, actualicé el firmware y reinicié todo, y ya funciona". ¿Qué lo arregló? Nadie lo sabe. Y cuando vuelva a fallar, nadie sabrá por dónde empezar. El método profesional es cambiar una sola cosa a la vez y medir después de cada cambio. Es más lento, pero cada medición te enseña algo y construye un historial. Los técnicos buenos tienen memoria de qué funcionó; los técnicos excelentes tienen notas.

La metodología del técnico: el orden que nunca falla

Vamos a cerrar la explicación con la metodología completa, el procedimiento ordenado que un técnico profesional sigue ante cualquier reporte de falla. No es una receta mágica: es una secuencia lógica donde cada paso descarta causas y el siguiente profundiza. Apréndetela como un mantra: síntomas, mediciones base, separación de tramos, pruebas dirigidas, diagnóstico, solución, verificación.

Paso 1: Escucha los síntomas y conviértelos en datos. ¿Qué falla exactamente? ¿En qué dispositivos? ¿A qué horas? ¿Desde cuándo? ¿Qué cambió recientemente? Anota las respuestas. Este paso toma cinco minutos y ahorra horas.

Paso 2: Toma mediciones base. Junto al router: nivel de señal en dBm, velocidad de enlace, prueba de velocidad, ping a la puerta de enlace. En el punto del problema: lo mismo. Ya con estas dos tandas de números tienes el 80% del diagnóstico.

Paso 3: Separa los tramos. Prueba por cable si puedes; si no, compara "junto al router" contra "punto del problema". Decide: ¿es WiFi o es internet/proveedor? Todo lo que sigue depende de esta decisión.

Paso 4: Si es WiFi, haz pruebas dirigidas. Revisa el canal con el analizador. Mide la señal cuarto por cuarto. Revisa qué banda está usando el dispositivo afectado (2.4 o 5 GHz). Revisa cuántos dispositivos están conectados. Busca interferencias (microondas, vecinos, Bluetooth).

Paso 5: Si es internet/proveedor, haz pruebas dirigidas al otro tramo. Ping a la puerta de enlace (debe ser bajo), ping a un servidor de internet (revela latencia del proveedor), traceroute para ver en qué salto se degrada, prueba de velocidad por cable a distintas horas. Con esos datos llamas al proveedor o revisas tu módem/router.

Paso 6: Emite el diagnóstico en una frase. Por ejemplo: "Señal débil en el cuarto del fondo (-78 dBm) más canal 6 saturado por tres vecinos; el proveedor entrega bien (450 Mbps por cable)". Si no puedes resumirlo en una frase, todavía no tienes el diagnóstico: sigue midiendo.

Paso 7: Aplica la solución de menor costo y menor riesgo primero. Cambiar un canal es gratis y reversible; mover el router cuesta cinco minutos; comprar un repetidor cuesta dinero; llamar al proveedor cuesta tiempo. Siempre en ese orden.

Paso 8: Verifica. Mide de nuevo después de la solución y compara con las mediciones base. ¿Mejoró el dBm? ¿Bajó el ping? ¿Subió la velocidad? Si sí, documenta qué hiciste. Si no, revierte el cambio y prueba la siguiente hipótesis. Un arreglo sin verificación es una suposición con buena suerte.

Dos principios sostienen toda la metodología. El primero: una sola variable a la vez. El segundo: todo se mide antes y después. Con esos dos principios y las herramientas de la siguiente clase, no hay problema de WiFi doméstico que se te resista. En la Clase 25 aprendiste el idioma de los números; en la Clase 26 vas a aprender a manejar los instrumentos; en la Clase 27 aplicarás todo a los 15 problemas más comunes. Vamos a los ejemplos paso a paso, donde harás tu primer diagnóstico completo con tus propias manos.

Ejemplos paso a paso

Ejemplo 1: Diagnóstico completo de una red lenta, de principio a fin

Escenario: en tu casa el WiFi "se siente lento" desde hace dos semanas. Vas a aplicar la metodología completa. Necesitas tu laptop o tu teléfono, y unos 20 minutos. Hazlo de verdad mientras lees: este ejemplo está diseñado para ejecutarse.

Paso 1: Escucha los síntomas (tus propios datos). Pregúntate y anota: ¿qué significa "lento"? (las páginas tardan, el video se traba). ¿En qué dispositivos? (en mi laptop y en mi teléfono). ¿A qué horas? (todo el día, pero peor en la noche). ¿Desde cuándo? (unas dos semanas). ¿Cambió algo? (mi vecino de al lado puso internet hace poco, lo vi cuando vino el técnico). Ya tienes sospechosos: posible saturación de canal por el vecino nuevo, posible problema general.

Paso 2: Mediciones base junto al router. Ponte a un metro del router, sin paredes de por medio. Primero revisa la intensidad de señal y la velocidad de enlace. En Windows abre una terminal (tecla Windows + R, escribe `cmd`, Enter) y ejecuta:

```
netsh wlan show interfaces
```

Verás algo como esto (los valores exactos varían):

```
Nombre          : Wi-Fi
Estado          : conectado
SSID            : MiCasa_WiFi
Señal           : 95%
Velocidad de recepción : 866.7 Mbps
Velocidad de transmisión : 866.7 Mbps
Canal           : 44
```

Anota: señal 95% (excelente, junto al router es lo esperado), velocidad de enlace 866 Mbps (banda de 5 GHz, muy bien), canal 44 (5 GHz, bien). Ahora haz una prueba de velocidad (speedtest.net o la app de tu proveedor). Supongamos que marca: descarga 180 Mbps, subida 20 Mbps, ping 15 ms. Si tienes contratado 200 Mbps, esto está perfecto: junto al router tu red vuela. Conclusión parcial: el router y el proveedor están bien.

Paso 3: Mediciones en el punto del problema. Ve al cuarto donde trabajas, el lugar donde "se siente lento". Repite el comando:

```
netsh wlan show interfaces
```

Supongamos que ahora ves:

```
Señal           : 58%
Velocidad de recepción : 216.7 Mbps
Velocidad de transmisión : 216.7 Mbps
Canal           : 6
```

Alerta: el canal cambió de 44 a 6. Tu dispositivo se cambió solo a la banda de 2.4 GHz (los canales bajos como el 6 son de 2.4 GHz) porque la señal de 5 GHz no llega bien hasta aquí. La velocidad de enlace cayó de 866 a 216 Mbps. Ahora la prueba de velocidad: supongamos 28 Mbps de descarga, ping 65 ms. Ahí está tu problema en números: lejos del router, tu dispositivo cae a 2.4 GHz con enlace modesto y la velocidad real se desploma.

Paso 4: Ping a la puerta de enlace. Esta prueba te dice si el tramo WiFi introduce latencia o pérdida. Primero averigua la puerta de enlace con:

```
ipconfig
```

Busca "Puerta de enlace predeterminada", normalmente 192.168.1.1 o 192.168.0.1. Luego haz un ping continuo de un minuto (detenlo con Ctrl + C):

```
ping 192.168.1.1 -t
```

Junto al router verías algo así:

```
Respuesta desde 192.168.1.1: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.1.1: bytes=32 tiempo=3ms TTL=64
Respuesta desde 192.168.1.1: bytes=32 tiempo=2ms TTL=64
```

Tiempos de 1 a 5 ms: WiFi sano. En el cuarto del problema, supongamos que ves:

```
Respuesta desde 192.168.1.1: bytes=32 tiempo=45ms TTL=64
Respuesta desde 192.168.1.1: bytes=32 tiempo=210ms TTL=64
Respuesta desde 192.168.1.1: bytes=32 tiempo=38ms TTL=64
Tiempo de espera agotado para esta solicitud.
Respuesta desde 192.168.1.1: bytes=32 tiempo=150ms TTL=64
```

Latencia alta, irregular (jitter alto) y hasta un paquete perdido ("tiempo de espera agotado"). Diagnóstico confirmado: el tramo WiFi hasta tu cuarto está degradado. No es el proveedor: es tu red inalámbrica.

Paso 5: Ping a internet para comparar. Detén el ping anterior (Ctrl + C) y ejecuta:

```
ping google.com -n 50
```

El ``-n 50`` envía 50 pings y al final te muestra el resumen con el porcentaje de pérdida. Si el ping a tu router era malo y el ping a google también es malo, pero la prueba por cable (o junto al router) sale bien, todo apunta al WiFi. Si el ping al router es bueno (2 ms) pero el ping a google es malo (200 ms con pérdida), entonces tu WiFi está bien y el problema está en el proveedor o en la ruta.

Paso 6: Traceroute para ver dónde se rompe el camino. Ejecuta:

```
tracert google.com
```

Verás una lista de saltos más o menos así:

1	2 ms	3 ms	2 ms	192.168.1.1
2	12 ms	10 ms	11 ms	10.20.30.1
3	14 ms	13 ms	15 ms	servidor.proveedor.com
4	18 ms	17 ms	19 ms	...

El salto 1 es tu router: debe estar en 1-5 ms. Si el salto 1 ya marca 100 ms o más, el problema es tu WiFi, confirmado por tercera vez. Si el salto 1 está bien pero el salto 2 o 3 se disparan, el problema está en la red de tu proveedor: esos datos son los que le llevas cuando llames.

Paso 7: Revisar el canal con el analizador. Abre tu analizador WiFi en el teléfono (en el cuarto del problema) y mira el gráfico de 2.4 GHz. Supongamos que ves tu red en el canal 6 junto con tres redes vecinas fuertes (el vecino nuevo entre ellas). Diagnóstico completo en una frase: "En el cuarto de trabajo el dispositivo cae a 2.4 GHz con señal mediocre, y el canal 6 está saturado por los vecinos; el proveedor entrega bien". Soluciones ordenadas de menor a mayor costo: 1) cambiar tu red 2.4 GHz al canal 1 u 11, el menos ocupado según el analizador; 2) mover el router a un punto más central; 3) si nada basta, agregar un repetidor o un sistema mesh para llevar 5 GHz al cuarto. Mide después de cada cambio y compara con tus números base.

Ejemplo 2: "Se cae el WiFi cada noche a las 8" - diagnóstico con horario

Escenario: todo el día el WiFi funciona bien, pero entre las 8 y las 11 de la noche se cae o se pone imposible. El patrón con horario es una pista de oro: apunta a congestión (todos los vecinos conectándose) o a interferencia con horario (un aparato que se enciende en la noche).

Paso 1: Confirma el patrón. Durante tres noches anota la hora exacta en que empieza y termina el problema. Si es consistente (siempre alrededor de las 8), no es casualidad.

Paso 2: En horario bueno (digamos, 4 de la tarde), haz tus mediciones base: prueba de velocidad, ping a la puerta de enlace con `ping 192.168.1.1 -n 50` y captura del analizador (cuántas redes ves y en qué canales). Anota todo.

Paso 3: En horario malo (9 de la noche), repite exactamente las mismas mediciones. Compara. Si la velocidad cae a la mitad, el ping al router sube de 3 ms a 150 ms y el analizador muestra el doble de redes activas en tu canal, el diagnóstico es congestión nocturna: los vecinos saturan el canal. Solución: cambia a un canal menos ocupado (medido de noche, no de día) o migra tus dispositivos importantes a 5 GHz, que suele estar menos saturada.

Paso 4: Si en cambio el analizador no muestra más redes de noche pero el problema persiste, sospecha interferencia no-WiFi con horario: ¿alguien enciende algo a las 8? Un microondas viejo, un teléfono inalámbrico, un monitor de bebé, luces LED baratas. Prueba: cuando empiece el problema, apaga por turnos los aparatos sospechosos y observa si mejora. La interferencia de microondas, por ejemplo, destroza el canal 6-9 de 2.4 GHz mientras calienta la cena.

Paso 5: Verifica la solución midiendo de noche después del cambio. El diagnóstico con horario solo se confirma en el horario del problema: medir de día no cuenta.

Ejemplo 3: "Mi celular no conecta pero la laptop sí" - problema de un solo dispositivo

Escenario: la laptop navega perfecto, pero el celular no conecta al WiFi o se conecta y no tiene internet. Regla de oro: si un solo dispositivo falla, el problema es ese dispositivo (o su relación con el router), no la red.

Paso 1: En el celular, olvida la red y vuelve a conectarte escribiendo la contraseña con cuidado. Parece obvio, pero una contraseña mal guardada o un cambio de contraseña del router que el celular no actualizó es la causa número uno.

Paso 2: Revisa si el celular se está conectando a la banda correcta. Algunos celulares viejos solo ven 2.4 GHz; si tu red de 2.4 GHz tiene nombre distinto o está apagada, no la verán. En el celular, en los ajustes de WiFi, verifica el nombre exacto de la red y compáralo con el de la laptop.

Paso 3: Reinicia el celular (no el router). Los teléfonos acumulan estados de red corruptos; un reinicio limpia la pila de red.

Paso 4: Si se conecta pero "no tiene internet", revisa la configuración IP del celular: debe estar en DHCP (automático). Una IP manual mal configurada de hace meses es una causa clásica. En Android: ajustes de la red WiFi, opciones avanzadas, "DHCP". En iPhone: ajustes del WiFi, la "i" de la red, "Configurar IP: Automático".

Paso 5: Prueba con otro celular o lleva tu celular a otra red WiFi. Si tu celular falla en todas las redes, el problema es su antena o su software (actualiza el sistema). Si solo falla en tu red, entra al panel del router y revisa: ¿el celular aparece en la lista de clientes? ¿Tiene señal muy débil (menos de -80 dBm)? ¿El router tiene límite de dispositivos o filtrado MAC activado que lo esté bloqueando? ¿Hay una regla de control parental o de horario que lo afecte?

Paso 6: Último recurso del lado del dispositivo: restablece los ajustes de red del celular (esto borra redes guardadas, no tus fotos). Si ni así funciona y otros dispositivos sí, el problema es de hardware del celular.

Ejemplo 4: Lectura guiada de un analizador WiFi y cambio de canal

Escenario: ya sospechas congestión. Vas a usar el analizador para elegir el mejor canal y cambiarlo en el router.

Paso 1: Instala un analizador WiFi en tu teléfono Android (por ejemplo "WiFi Analyzer") o en tu laptop. Párate en el lugar donde usas más la red.

Paso 2: Mira la lista de redes y anota para la banda 2.4 GHz: cuántas redes hay en el canal 1, cuántas en el 6 y cuántas en el 11, y con qué intensidad llegan (dBm). Ejemplo de lo que podrías ver: canal 1: dos redes débiles (-82, -85 dBm); canal 6: tu red más cuatro redes fuertes (-55 a -70 dBm); canal 11: una red media (-72 dBm).

Paso 3: Mira el gráfico de canales. Confirma visualmente: en el canal 6 hay una montaña de jorobas traslapadas; el canal 1 está casi vacío. Decisión: mover tu red de 2.4 GHz al canal 1.

Paso 4: Entra al panel de tu router (normalmente escribiendo 192.168.1.1 o 192.168.0.1 en el navegador; usuario y contraseña suelen estar en la etiqueta del router). Busca la sección de WiFi o Wireless, luego la configuración de la red de 2.4 GHz, y cambia "Canal" de "Automático" o "6" a "1". Guarda y espera a que el router aplique el cambio (se desconectarán los dispositivos unos segundos y se reconectarán solos).

Paso 5: Vuelve al analizador y confirma que tu red ahora aparece en el canal 1. Haz una prueba de velocidad y un ping a la puerta de enlace, y compara con tus mediciones base. Si mejoró, documenta: "canal 6 saturado, cambiado a 1 el 19 de septiembre, velocidad subió de 28 a 65 Mbps".

Nota importante: si tu router tiene la opción de "selección automática de canal", evalúala con escepticismo: muchos routers eligen mal o cambian de canal a cada rato, lo que causa microcortes. Un canal fijo bien elegido suele ser más estable que el automático mal implementado. Mide y decide.

Práctica

Ejercicio 1: "Mi WiFi se cae cada noche a las 8 en punto"

Caso: Marta reporta que su WiFi funciona bien todo el día, pero todos los días entre las 8:00 y las 8:30 de la noche la conexión se cae durante unos minutos, a veces varias veces. Le pasa en todos sus dispositivos. Ya reinició el router tres veces y el problema sigue. Su proveedor dice que la conexión "se ve estable".

Tu tarea: aplica la metodología y llega al diagnóstico y la solución.

Solución paso a paso:

1. Síntomas convertidos en datos: falla todos los dispositivos (descarta problema de un aparato), con horario fijo muy preciso (8:00 a 8:30 pm), se cae por minutos y vuelve solo. Un horario tan exacto rara vez es congestión de vecinos (ellos no se conectan todos a las 8:00 en punto); apunta a algo programado o a un aparato con temporizador.
2. Pregunta clave que hay que hacerle a Marta: ¿qué se enciende en tu casa o cerca de tu casa a las 8 de la noche? Resulta que a las 8:00 en punto se enciende automáticamente el sistema de riego del jardín con su controlador inteligente, y también las luces LED del patio con temporizador.
3. Prueba de confirmación: una noche, a las 7:55, Marta desconecta el controlador de riego y las luces del patio antes de las 8. Las 8:00 pasan sin caída. Repite la prueba dos noches más: con los aparatos encendidos el WiFi se cae; con los aparatos apagados no se cae. Causa confirmada: interferencia electromagnética.
4. Diagnóstico en una frase: "Interferencia en 2.4 GHz provocada por el controlador de riego y/o las luces LED con temporizador que se encienden a las 8:00 pm; el router está cerca del patio y recibe la interferencia de lleno".
5. Solución ordenada: primero, alejar el router de la pared que da al patio o cambiarlo de lugar; segundo, migrar los dispositivos importantes a la banda de 5 GHz, que es menos vulnerable a ese tipo de interferencia; tercero, si se identifica que es un aparato específico, reemplazarlo o ponerle un filtro. Medir de noche después del cambio para verificar.
6. Lección: el patrón con horario exacto casi siempre es un aparato, no los vecinos. Y reiniciar el router jamás iba a arreglar una interferencia con temporizador.

Ejercicio 2: "El celular no conecta pero la laptop sí"

Caso: En casa de Jorge, la laptop navega a 150 Mbps sin problemas, pero su celular se conecta al WiFi y dice "sin acceso a internet". El celular de su esposa funciona perfecto en la misma red. Jorge ya reinició el router y no cambió nada.

Tu tarea: diagnostica sin tocar el router primero.

Solución paso a paso:

1. Un solo dispositivo falla (el de Jorge), otros funcionan (laptop y celular de la esposa). Conclusión inmediata: el problema NO es la red ni el router en general; es el celular de Jorge o su configuración.
2. Prueba 1: olvidar la red en el celular de Jorge y reconectar escribiendo la contraseña. Supongamos que se conecta pero sigue "sin internet". Descartada la contraseña.

3. Prueba 2: revisar la configuración IP del celular. En los ajustes de la red WiFi aparece "IP estática: 192.168.1.50, puerta de enlace: 192.168.1.1". Jorge había configurado una IP manual hace un año para un proyecto y lo olvidó; el router cambió su rango o esa IP ya la usa otro dispositivo, causando conflicto.
4. Solución: cambiar a DHCP (automático) en el celular. Se reconecta, obtiene IP válida y el internet vuelve al instante.
5. Verificación: navegar, hacer una prueba de velocidad en el celular y compararla con la de la laptop. Si son similares, caso cerrado.
6. Lección: "se conecta pero no tiene internet" en un solo dispositivo casi siempre es configuración IP, DNS manual mal puesto, o fecha/hora incorrecta del dispositivo (los certificados de seguridad fallan si la fecha está mal). El router nunca fue el culpable.

Ejercicio 3: "Lento solo en el cuarto del fondo"

Caso: Casa de dos pisos. En la sala (donde está el router) todo vuela: 190 Mbps. En el cuarto del fondo, al final del pasillo, apenas 12 Mbps y las videollamadas se cortan. El proveedor entrega 200 Mbps (verificado por cable).

Tu tarea: mide, diagnostica y propón soluciones en orden de costo.

Solución paso a paso:

1. Mediciones base junto al router: señal -42 dBm (excelente), velocidad de enlace 866 Mbps, velocidad real 190 Mbps, ping a la puerta de enlace 2 ms. Todo perfecto: el proveedor y el router cumplen.
2. Mediciones en el cuarto del fondo: señal -79 dBm (débil, zona roja de la tabla), velocidad de enlace 72 Mbps (el dispositivo bajó a 2.4 GHz para sobrevivir), velocidad real 12 Mbps, ping a la puerta de enlace 90 ms con jitter alto y 4% de pérdida de paquetes.
3. Diagnóstico en una frase: "Cobertura insuficiente: la señal llega débil al cuarto del fondo (-79 dBm) atravesando varias paredes, el dispositivo cae a 2.4 GHz y la latencia y pérdida se disparan; el proveedor entrega bien".

4. Soluciones en orden de menor a mayor costo: a) mover el router a un punto más central y elevado de la casa (gratis; a veces basta con sacarlo del rincón detrás del televisor); b) verificar con el analizador si además hay saturación de canal en el cuarto y cambiar al 1, 6 u 11 menos ocupado (gratis); c) si la casa es grande o de dos pisos con losas gruesas, instalar un repetidor o mejor un sistema mesh con el nodo satélite a medio camino entre el router y el cuarto (costo moderado); d) para el escritorio de trabajo, considerar un adaptador con cable o powerline si hay un enchufe cercano (costo moderado, máxima estabilidad).
5. Verificación: medir de nuevo en el cuarto después de cada cambio. Objetivo: llevar la señal a -67 dBm o mejor y la velocidad real a un nivel que sostenga videollamadas (mínimo 10-20 Mbps estables con ping bajo).
6. Lección: cuando el problema es solo en un lugar lejano y junto al router todo está bien, no llames al proveedor ni compres un router más caro: es física, distancia y obstáculos. Se arregla con ubicación o con cobertura adicional.

Ejercicio 4: Diagnostica con estos números

Caso: Te pasan estas mediciones de la casa de un cliente, tomadas en la sala donde tiene el problema. No puedes ir en persona; debes diagnosticar con los datos.

Datos:

- Velocidad contratada: 300 Mbps.
- Junto al router: velocidad real 285 Mbps, ping a puerta de enlace 3 ms.
- En la sala del problema: señal -58 dBm, velocidad de enlace 433 Mbps, velocidad real 40 Mbps, ping a puerta de enlace 120 ms con jitter alto, pérdida de paquetes 6%.
- Analizador: tu red en canal 6 de 2.4 GHz; hay 5 redes vecinas fuertes en el canal 6 y 2 más en el canal 4 (traslapado).
- El dispositivo afectado está conectado en 2.4 GHz aunque el router tiene 5 GHz disponible.

Tu tarea: escribe el diagnóstico en una frase y el plan de solución ordenado.

Solución paso a paso:

1. Descarta al proveedor: junto al router hay 285 Mbps de 300 contratados. El proveedor cumple.
2. Analiza el punto del problema: la señal de -58 dBm es buena (zona verde), y la velocidad de enlace de 433 Mbps es decente. Con esos dos datos, la velocidad real debería ser

mucho mayor a 40 Mbps. Pero el ping al router es de 120 ms (debería ser 2-5 ms) con jitter alto y 6% de pérdida. Conclusión: la señal llega bien, pero el canal está destruido por congestión e interferencia. Los números lo gritan: buena señal + mal ping + pérdida = canal saturado, no cobertura.

3. Confirma con el analizador: 5 vecinos fuertes en tu mismo canal 6 más 2 en el canal 4 traslapado. Congestión severa confirmada.
4. Diagnóstico en una frase: "Canal 6 de 2.4 GHz saturado por vecinos (5 redes fuertes en el mismo canal y 2 traslapadas), lo que causa alta latencia y 6% de pérdida aunque la señal es buena; el proveedor entrega correctamente".
5. Plan de solución: a) cambiar la red 2.4 GHz al canal 1 u 11, el que tenga menos redes fuertes según el analizador (gratis, inmediato); b) forzar o priorizar que el dispositivo use la banda de 5 GHz, que está libre (en el router, separar los nombres de red de 2.4 y 5 GHz para elegir manualmente, o activar band steering si el router lo soporta bien); c) medir de nuevo: objetivo ping a puerta de enlace menor a 10 ms y pérdida cercana a 0%.
6. Lección: señal buena no significa red buena. Este caso demuestra por qué se miden las tres patas: velocidad, latencia y pérdida. Quien solo mira las barritas jamás encuentra este problema.

Ejercicio 5: "Contraté 500 Mbps y solo me llegan 95"

Caso: Luis contrató 500 Mbps. Hace la prueba en su celular y obtiene 95 Mbps. Llama al proveedor furioso. El técnico va a su casa, conecta su laptop por cable al router y mide 480 Mbps. "Su servicio está bien", dice, y se va. Luis sigue con 95 Mbps en su celular y siente que lo estafaron.

Tu tarea: explica qué pasa y cómo se resuelve, con números.

Solución paso a paso:

1. La prueba por cable (480 Mbps) demuestra que el proveedor entrega lo contratado. El problema está dentro de la casa, en el WiFi o en el dispositivo.
2. Revisar en el celular la velocidad de enlace con el analizador o en ajustes avanzados: supongamos 144 Mbps en 2.4 GHz. Con la regla práctica (velocidad real = 30% a 60% del enlace), 95 Mbps reales desde 144 de enlace es un resultado normal y hasta bueno. El celular no está "fallando": está limitado por su enlace.
3. ¿Por qué el enlace es de solo 144 Mbps? Porque el celular está en 2.4 GHz con canal de 20 MHz, probablemente porque está lejos del router o porque la red de 5 GHz tiene otro nombre y nunca se conectó a ella.

4. Solución: conectar el celular a la red de 5 GHz (verificar el nombre exacto), acercarse al router para la prueba de referencia, y si el router lo permite, activar canal de 40 u 80 MHz en 5 GHz. Con enlace de 866 Mbps en 5 GHz, la velocidad real típica será de 250 a 450 Mbps, muy por encima de los 95 actuales.
5. Expectativa honesta: por WiFi es muy difícil ver los 500 Mbps completos en un celular común; 300-400 Mbps en 5 GHz junto al router es un excelente resultado. Los 500 se ven por cable. Explicarle esto a Luis evita la frustración: no lo estafaron, solo medía en el lugar y la banda equivocados.
6. Lección: antes de pelear con el proveedor, compara velocidad de enlace, banda usada y medición por cable. El 90% de estos casos se resuelven cambiando de banda, no cambiando de compañía.

Ejercicio 6: El misterio del ping perfecto y las llamadas horribles

Caso: Ana tiene 200 Mbps, la prueba de velocidad sale perfecta, el ping a google.com marca 18 ms estables... pero sus llamadas de trabajo se escuchan entrecortadas y a veces se congelan por segundos. Ya cambió de canal una vez y no mejoró.

Tu tarea: encuentra la causa con las herramientas de esta unidad.

Solución paso a paso:

1. La velocidad y el ping promedio están bien, así que la mayoría diría "la red está perfecta". Pero el síntoma (audio entrecortado, congelamientos) apunta a jitter o pérdida de paquetes, que el ping promedio no muestra.
2. Prueba dirigida: ping extendido a la puerta de enlace, `ping 192.168.1.1 -n 100`, y observa no el promedio sino la variación y la pérdida. Supongamos el resultado: promedio 12 ms, pero con picos de 400 ms cada 10-15 segundos y 3% de pérdida. Ahí está: jitter alto y pérdida intermitente.
3. ¿Qué causa picos periódicos? Un dispositivo que transmite en ráfagas: un teléfono inalámbrico DECT, un monitor de bebé, un microondas en uso, o un vecino con un router que cambia de canal automáticamente. Pregunta a Ana: ¿los cortes coinciden con algo? Descubren que su esposo usa un teléfono inalámbrico viejo para llamadas largas justo en su horario de trabajo, y la base está al lado del router.
4. Prueba de confirmación: desenchufan la base del teléfono inalámbrico durante una llamada de prueba. Los picos desaparecen, el ping queda estable en 3 ms, la llamada se escucha perfecta.

5. Solución: mover la base del teléfono lejos del router (varios metros), o reemplazar el teléfono viejo por uno moderno que no interfiera, o migrar la laptop de Ana a 5 GHz donde el teléfono no interfiere. Verificar con otro ping extendido de 100 paquetes.
6. Lección: el ping promedio miente por omisión; lo que importa para voz y video es la estabilidad (jitter) y la pérdida. Y las interferencias no-WiFi no aparecen en el analizador de redes: se descubren con preguntas y pruebas de encendido/apagado. El técnico que solo mira números de velocidad jamás resuelve este caso.

Resumen de la unidad

Puntos clave para repaso rápido:

- Diagnosticar es como ir al doctor: síntomas, pruebas, diagnóstico, solución. Nunca apliques una solución sin diagnóstico, y nunca diagnostiques sin mediciones. Los números no mienten; las corazonadas sí.
- El dBm es el idioma de la señal: escala de negativos donde menos negativo es mejor. -30 a -50 excelente, -50 a -60 muy buena, -60 a -67 buena, -67 a -70 aceptable (límite para voz/video), -70 a -80 débil, -80 a -90 muy débil, menos de -90 inservible. Cada 10 dBm son 10 veces más potencia: pequeños cambios se sienten mucho.
- Busca siempre el valor en dBm, no el porcentaje ni las barritas: cada fabricante calcula esos a su manera y no son comparables.
- Velocidad de enlace no es velocidad real: el enlace es el máximo teórico negociado por el aire; la velocidad real (throughput) suele ser del 30% al 60% del enlace por sobrecarga del WiFi. Compara siempre contratada vs enlace vs real para saber dónde está el cuello de botella.
- La latencia (ping) y el jitter mandan en videollamadas y juegos: menos de 20 ms excelente, 20-50 bueno, 50-100 aceptable, más de 100 malo. El ping a tu propio router debe ser de 1 a 5 ms; si ahí ya es alto, el problema es tu WiFi.
- La pérdida de paquetes es el enemigo silencioso: con 0-1% todo bien, con 2-5% se notan cortes en llamadas, con más de 5% hay problema serio. Se mide con ping extendido (ping -n 100) y la prueba de velocidad no la revela.
- Separa siempre los tramos: prueba por cable o "junto al router" para decidir si el problema es tu WiFi o tu proveedor. Puedes tener WiFi perfecto sin internet, e internet perfecto con WiFi pésimo: son problemas distintos con soluciones distintas.

- En 2.4 GHz usa solo los canales 1, 6 u 11 (los únicos que no se traslapan) y elige el menos ocupado según el analizador, medido en el horario del problema. En 5 GHz hay más canales y menos congestión.
- El analizador WiFi es tu mapa de batalla: lista de redes con dBm y canal, gráfico de canales para ver saturación y traslapes, y medición cuarto por cuarto para tu mapa de cobertura.
- Errores que ya no vas a cometer: reiniciar sin medir antes y después; culpar al proveedor sin la prueba del cable; comprar equipo antes de diagnosticar; cambiar varias cosas a la vez sin saber cuál funcionó.
- La metodología del técnico: 1) convierte síntomas en datos, 2) toma mediciones base junto al router y en el punto del problema, 3) separa WiFi de internet, 4) haz pruebas dirigidas al tramo culpable, 5) resume el diagnóstico en una frase, 6) aplica la solución más barata y reversible primero, 7) verifica midiendo de nuevo, 8) documenta.
- Una sola variable a la vez, y todo se mide antes y después. Ese es el secreto completo.

Checklist de diagnóstico rápido (una página: guárdala en tu teléfono):

1. SÍNTOMAS: ¿Qué falla exactamente? ¿En cuántos dispositivos? ¿A qué horas? ¿Desde cuándo? ¿Qué cambió?
2. BASE JUNTO AL ROUTER: señal dBm, velocidad de enlace, prueba de velocidad, `ping 192.168.1.1 -n 20`.
3. BASE EN EL PUNTO DEL PROBLEMA: lo mismo que en el paso 2. Compara.
4. SEPARA TRAMOS: ¿por cable (o junto al router) funciona bien? SÍ = problema de WiFi. NO = problema de proveedor/router.
5. SI ES UN SOLO DISPOSITIVO: olvida la red y reconecta, revisa IP en DHCP, reinicia el dispositivo, prueba en otra red.
6. SI ES WIFI: revisa canal con el analizador (usa 1, 6 u 11 en 2.4 GHz), verifica banda (¿está en 2.4 pudiendo usar 5?), mide señal cuarto por cuarto (objetivo -67 dBm o mejor donde trabajas).
7. LATENCIA Y PÉRDIDA: `ping 192.168.1.1 -n 100` (busca jitter y % de pérdida) y `tracert google.com` (¿en qué salto se degrada?).
8. INTERFERENCIAS: ¿el problema tiene horario exacto? Busca aparatos con temporizador, microondas, teléfonos inalámbricos, Bluetooth.
9. DIAGNÓSTICO EN UNA FRASE: si no puedes resumirlo, sigue midiendo.

10. SOLUCIÓN (de menor a mayor costo): cambiar canal, cambiar de banda, mover el router, actualizar firmware/configuración, agregar cobertura (repetidor/mesh), llamar al proveedor con datos en mano.
11. VERIFICA: mide de nuevo después del cambio y compara con la base. ¿Mejoró? Documenta qué hiciste y cuándo.
12. ANTES DE LLAMAR AL PROVEEDOR: ten listos velocidad por cable, velocidad por WiFi, ping a la puerta de enlace, ping a internet, traceroute y horario del problema. Sin datos, la llamada es adivinanza.

Con esta unidad cierras el círculo: ya no solo sabes cómo funciona una red inalámbrica, sabes medirla, interrogarla y repararla. Esa es la diferencia entre un usuario y un técnico, y es una habilidad que te va a servir en tu casa, en tu trabajo y con cada persona que te pida ayuda con su WiFi. Nos vemos en la siguiente unidad.

UNIDAD 10: WiFi en el mundo real y lo que viene (Clases 28 a 30)

Llegaste a la última unidad. Felicidades en serio, porque si empezaste este libro sin saber qué era un router y hoy puedes explicar qué es un canal, por qué tu red de 5 GHz no llega al baño y cómo se cifra una contraseña WPA2, entonces ya tienes más conocimientos que la mayoría de la gente que usa internet todos los días. Pero falta una parte importante, y es la que une todo lo que aprendiste con la vida real: el WiFi no vive en tu casa. Vive en el café donde tomas tu latte, en el aeropuerto donde esperas tu vuelo, en la oficina donde trabajas, en la taquería de la esquina, en el hotel donde te hospedas y en el futuro que se está cocinando justo ahora en laboratorios de todo el mundo. Esta unidad cierra el curso llevándote de tu casa al mundo.

Piensa en lo que ya dominas. Aprendiste qué es el WiFi y cómo viajan las ondas, conoces las bandas de 2.4, 5 y 6 GHz, sabes qué son los estándares 802.11a, b, g, n, ac y ax, aprendiste a elegir un router, a colocarlo bien, a cambiar el canal, a poner una contraseña segura, a entender el roaming entre puntos de acceso, las redes mesh, el PoE, la seguridad WPA2 y WPA3 y cómo detectar a los vecinos colgados de tu red. Eso es mucho. Es el noventa por ciento de lo que un usuario necesita saber. Pero hay un diez por ciento que pasa afuera, en la calle, en los negocios y en las redes públicas, y ese diez por ciento es el que más daño puede hacer si lo ignoras. Esta unidad es ese diez por ciento, y al mismo tiempo es una ventana al futuro.

La unidad está organizada en tres clases, igual que todas las del libro. La Clase 28 te lleva al otro lado del mostrador: cómo se arma el WiFi de un negocio. Un café, una oficina pequeña, una taquería. Vas a aprender qué es un portal cautivo (esa página que te pide aceptar términos o dar tu correo antes de navegar), por qué un negocio serio nunca mezcla en la misma red a sus empleados, a sus clientes y a sus cámaras de seguridad, y cuáles son las buenas prácticas que separan al café que llena sus mesas del café que pierde clientes porque su WiFi es un desastre. La Clase 29 te lleva a la silla del cliente: tú, sentado en un aeropuerto con dos horas de espera, viendo en tu teléfono una lista de redes que dicen "WiFi Gratis Aeropuerto". Vas a aprender qué puede salir mal si te conectas sin pensar, qué es un ataque de gemelo malvado explicado de forma que lo entienda hasta tu abuelita, y sobre todo qué puedes hacer para protegerte: qué es una VPN y por qué es tu mejor amiga en redes públicas, qué es el candado del navegador y HTTPS, y qué es OWE, la tecnología que está tratando de hacer el WiFi público menos peligroso. La Clase 30 mira hacia adelante: WiFi 7 con sus trucos nuevos, LiFi que transmite datos con luz, la llegada del 5G y la sombra del 6G, el internet de las cosas con el estándar Matter y cómo todo esto va a cambiar la conectividad en los próximos años.

Al terminar esta unidad vas a lograr varias cosas concretas. Primero, vas a saber diseñar la red WiFi de un negocio pequeño desde cero: qué equipos comprar, cuántas redes crear, cómo configurar el portal cautivo y qué límites ponerle a cada usuario para que un solo cliente viendo videos no tumbé el internet de todos. Segundo, vas a tener una rutina personal de seguridad para redes públicas que te va a acompañar toda la vida, igual que mirar a los lados antes de cruzar la calle. Tercero, vas a entender las noticias de tecnología que están por venir: cuando escuches que "ya salió el WiFi 7" vas a saber qué significa eso de verdad y si te conviene gastar en él o esperar. Y cuarto, y quizás lo más importante: vas a cerrar este curso con una visión completa, de la antena de tu casa a la red del futuro, con criterio para tomar decisiones y no solo para seguir instructivos.

Una advertencia de tono antes de empezar, porque es importante. En esta unidad vamos a hablar de ataques: el gemelo malvado, el hombre en el medio, el espionaje en redes abiertas. Lo vamos a hacer con un enfoque totalmente defensivo. Te voy a enseñar cómo funcionan estos ataques de forma sencilla no para que los hagas, sino para que los reconozcas y te protejas. Saber que existe el veneno no te convierte en envenenador: te convierte en alguien que no se toma lo que le ofrece un desconocido. Todo lo que sigue está escrito para que protejas tu información, la de tu familia y, si pones un negocio, la de tus clientes. Con eso claro, vamos a la última parada de este viaje.

Explicación detallada

El WiFi salió de tu casa

Hay una frase que se escucha mucho en el mundo de la tecnología: el WiFi es como el agua, nadie lo nota hasta que falta. En tu casa ya aprendiste a dominarlo, pero el WiFi moderno se usa mucho más fuera que dentro. Piensa en un día normal: te levantas, revisas el teléfono conectado a tu red casera; vas a la oficina y te conectas a la red de la empresa; comes en un restaurante y pides la contraseña del WiFi; esperas en el aeropuerto y te conectas a la red gratuita; llegas al hotel y el recepcionista te da un código. En todos esos lugares hay alguien que tuvo que pensar, diseñar y cuidar esa red. A veces lo hizo bien y ni lo notas. A veces lo hizo mal y lo sufres: la página no carga, el video se congela, te pide la contraseña tres veces, o peor, te conectas a algo que no es lo que parece.

Esta unidad tiene dos mitades bien claras. La primera mitad es para cuando TÚ eres el responsable de la red: tienes un negocio, trabajas en una oficina o ayudas a un familiar con su café. La segunda mitad es para cuando TÚ eres el visitante: el cliente del café, el viajero del aeropuerto, el huésped del hotel. Y la tercera clase, la del futuro, es para los dos, porque lo que viene nos va a tocar a todos. Empecemos por el negocio.

Clase 28: WiFi para negocios

Imagina que abres un café. Local bonito, café de calidad, pan recién hecho. Pones un router casero, el mismo que tienes en tu casa, le pones de contraseña "cafe1234" y la escribes en un pizarrón junto a la caja. Los primeros días todo bien. A la semana, un cliente se queja de que el internet está lentísimo. Al mes, otro dice que le apareció una publicidad rara en su teléfono justo después de conectarse. A los dos meses, tu computadora de la caja (donde registras las ventas) empieza a fallar y descubres que alguien, desde la mesa de la esquina, estaba husmeando en tu red. Suena exagerado, pero pasa más de lo que crees, y casi siempre por los mismos errores de novato. Vamos a evitarlos uno por uno.

El primer concepto clave de esta clase es el portal cautivo. El nombre suena técnico, pero lo conoces de sobra: es esa pantalla que aparece cuando te conectas al WiFi de un hotel, un aeropuerto o un centro comercial y te pide aceptar términos y condiciones, o poner tu correo, o ver un anuncio, antes de dejarte navegar. "Cautivo" significa que estás cautivo, atrapado, hasta que haces lo que te pide. Técnicamente funciona así: te conectas a la red abierta, pero el router no te deja salir a internet de verdad; cualquier página que intentes abrir te redirige a la página del portal. Cuando aceptas los términos (o te registras, o ves el anuncio), el router anota tu dispositivo en una lista de permitidos y te abre la puerta por cierto tiempo.

¿Por qué le conviene esto al negocio? Por varias razones. La primera es legal y de responsabilidad: cuando el cliente acepta los términos, queda registrado que el uso es bajo su

responsabilidad y que ciertas actividades (descargas ilegales, por ejemplo) están prohibidas. Si alguien hace algo indebido desde la red del café, el negocio puede demostrar que tenía reglas claras. La segunda es comercial: el portal puede pedir el correo del cliente, y con eso el café arma su lista para enviar promociones ("martes 2x1 en capuchinos"). La tercera es control: el portal permite poner límite de tiempo (dos horas de navegación por cliente, por ejemplo) para que las mesas roten y no haya alguien ocupando una mesa seis horas con un solo café. Y la cuarta es seguridad básica: aunque el portal no cifra tu tráfico (ojo con esto, lo veremos en la clase 29), al menos separa a los usuarios anónimos de los registrados y permite bloquear a quien abuse.

El segundo concepto clave son los múltiples SSID, es decir, varias redes WiFi saliendo del mismo equipo. Recuerda: el SSID es el nombre de la red, lo que ves en la lista de tu teléfono. Un router de negocio (o un punto de acceso profesional) puede emitir varias redes a la vez, cada una con sus propias reglas. La receta estándar para un negocio pequeño es de tres redes: una para empleados, una para invitados y una para los aparatos del local (lo que se llama IoT: cámaras de seguridad, terminal de pagos, impresora, termostato, bocinas). ¿Por qué separarlas? Porque cada grupo tiene necesidades y riesgos distintos.

La red de empleados lleva la información sensible: la computadora de la caja, el inventario, los correos del negocio, los datos de los proveedores. Debe tener la contraseña más fuerte, cifrado WPA2 o WPA3, y nadie de fuera debe conocerla. La red de invitados es la de los clientes: puede ser abierta con portal cautivo o con una contraseña sencilla que cambie cada cierto tiempo, pero lo importante es que esté AISLADA de la red de empleados. Esa palabra, aislada, es la clave de todo: significa que un cliente conectado al WiFi del café no puede ver ni tocar la computadora de la caja ni las cámaras, aunque estén en el mismo local. Los equipos profesionales tienen una función con nombres como "aislamiento de clientes" o "VLAN" que hace exactamente eso: cada red vive en su propio carril y no se meten entre ellas. La tercera red, la de los aparatos, existe porque las cámaras y los focos inteligentes suelen tener seguridad pobre y rara vez se actualizan; si alguien logra entrar a una cámara barata, no queremos que desde ahí salte a la computadora de las ventas. Separar es proteger.

Vamos con las buenas prácticas concretas, las que separan al negocio profesional del improvisado. Primera: nunca uses el router casero que te regaló tu proveedor de internet como única solución si tienes más de diez clientes simultáneos. Esos equipos están diseñados para una familia, no para treinta teléfonos, diez laptops y cuatro cámaras peleando por el aire al mismo tiempo. Para un café pequeño, un punto de acceso de gama negocio (marcas como Ubiquiti, TP-Link Omada o Aruba Instant On, por mencionar las más comunes) cuesta lo de unas cuantas docenas de cafés y cambia la historia por completo. Segunda: coloca el punto de acceso en alto y al centro del local, no escondido detrás de la caja registradora entre cajas de

cartón. Ya aprendiste en las primeras unidades que la ubicación lo es todo. Tercera: usa la banda de 5 GHz para los clientes siempre que sea posible, porque en un local lleno de teléfonos la banda de 2.4 GHz se satura rapidísimo con las redes vecinas.

Cuarta: pon límites por usuario. Casi todos los sistemas de negocio permiten decir "cada cliente puede usar máximo 10 Mbps de bajada y 2 horas de sesión". Esto evita que un solo cliente viendo videos en 4K se coma todo el internet del local. Es como en un buffet: si uno se sirve todo el guisado, los demás se quedan sin comer. Los límites son cortesía convertida en configuración. Quinta: cambia la contraseña de invitados con regularidad (cada mes, o cada semana en lugares muy concurridos) y no la escribas en un pizarrón gigante visible desde la calle; mejor dila de palabra o ponla en la mesa en tarjetas pequeñas. Sexta: mantén el firmware actualizado. Ya lo viste en este curso: las actualizaciones tapan agujeros de seguridad. En un negocio, un agujero no solo te afecta a ti, afecta a tus clientes. Séptima: si el negocio maneja pagos con tarjeta por internet o datos de clientes, considera contratar a un profesional para la instalación inicial. No es derrota pedir ayuda: es lo que hacen los negocios serios.

Ahora, los errores comunes, porque aprender de errores ajenos es más barato. Error uno: red abierta de negocio sin portal ni contraseña. "Es que así es más fácil para el cliente". Sí, y también es más fácil para el atacante, que no necesita ni contraseña para espiar el tráfico. Una red de negocio sin ningún control es como un local sin puerta: entra quien quiera. Error dos: la misma red y la misma contraseña para empleados y clientes, escrita en el pizarrón. Eso significa que cualquier cliente (o cualquier persona que pase por la banqueta y lea el pizarrón) tiene acceso a la misma red donde está la computadora de las ventas. Error tres: el router con la contraseña de fábrica ("admin/admin") porque "nadie se va a meter a configurarlo". Créeme, hay gente que sí, y hay programas que prueban esas contraseñas automáticamente. Error cuatro: poner el punto de acceso junto al microondas de la cocina o detrás de un refrigerador industrial de metal. El metal y los electrodomésticos son enemigos del WiFi; ya lo sabes de las primeras unidades, pero en los negocios se repite muchísimo porque "ahí había un enchufe libre". Error cinco: no poner límites y luego quejarse de que "el internet es malo" cuando en realidad un par de clientes acaparan todo el ancho de banda.

El caso real que te prometí: el café que pierde clientes por mal WiFi. Pongámosle nombre: "Café El Rincón". Buen café, buena ubicación, pero el dueño puso un router casero detrás del mostrador, contraseña "rincon2020" en un cartel, sin portal, sin límites, sin redes separadas. Los viernes se llena. Treinta clientes conectados al mismo router casero en la banda de 2.4 GHz, tres de ellos viendo videos, uno haciendo videollamada. El resultado: nadie puede cargar ni el menú digital. Los clientes se van al café de enfrente, que tiene un portal bonito, WiFi rápido y enchufes en las mesas. El dueño de El Rincón invierte en mejor café, en decoración,

en publicidad, pero no en la red, porque "el internet no es mi negocio". Error: hoy el internet **SÍ** es parte del negocio. Un estudio tras otro muestra que en cafés, restaurantes y hoteles el WiFi es uno de los factores que más pesan en la decisión de volver. La moraleja no es gastar una fortuna: es que una inversión pequeña y bien pensada (un punto de acceso decente, tres redes separadas, un portal cautivo, límites por usuario) vale más que meses de publicidad.

El portal cautivo bien hecho

Ya que el portal cautivo es la cara visible del WiFi de un negocio, vale la pena detallar cómo debe ser uno bueno. Primero, debe aparecer solo y rápido: el cliente se conecta y en segundos ve la página, sin tener que abrir el navegador manualmente (los teléfonos modernos lo hacen solos, pero el portal debe estar bien configurado para que funcione). Segundo, debe ser corto: nombre del negocio, una frase de bienvenida, los términos en lenguaje humano (no un pergamino legal de diez páginas) y un botón grande de "Conectar". Cada campo extra que pidas (nombre, teléfono, fecha de nacimiento, signo zodiacal) es un cliente que se rinde y no se conecta. Tercero, debe funcionar en español y verse bien en el teléfono, porque el noventa por ciento de tus clientes se conectará desde el celular. Cuarto, si pides correo, explica para qué lo quieres ("para enviarte promociones, puedes darte de baja cuando quieras"); la transparencia genera confianza y además es lo que exige la ley en muchos países. Quinto, el límite de tiempo debe avisarse con amabilidad ("tienes 2 horas de navegación, ¡disfruta tu café!") y no como castigo. Un buen portal es marketing; un mal portal es un muro.

Clase 29: Redes públicas seguras

Cambiamos de silla. Ya no eres el dueño del café: eres el cliente. Estás en el aeropuerto, tu vuelo sale en dos horas, la batería va en 40% y ves en tu teléfono estas redes: "Aeropuerto_WiFi_Gratis", "Aeropuerto WiFi Gratis", "Free Airport WiFi" y "xX_WiFi_Gratis_Xx". ¿A cuál te conectas? Si tu respuesta fue "a la que tenga mejor señal", esta clase es para ti, porque acabas de describir exactamente cómo cae la gente en la trampa más vieja del WiFi público.

El ataque del gemelo malvado (evil twin) es simple de entender con una analogía. Imagina que llegas a un centro comercial y ves un puesto que dice "Café El Rincón" con el mismo logo, pero es un puesto falso puesto por estafadores: te venden "café" que es agua sucia y además te copian la tarjeta cuando pagas. El gemelo malvado digital es igual: un atacante lleva una laptop o un aparatito barato al aeropuerto y crea una red WiFi con el mismo nombre (o casi el mismo) que la red legítima. Tu teléfono, que está buscando redes conocidas o simplemente muestra la lista, no distingue la verdadera de la falsa. Te conectas al gemelo, y a partir de ese momento todo tu tráfico pasa por las manos del atacante. Puede ver las páginas que visitas, y

si entras a un sitio sin protección, puede ver tus contraseñas. Por eso la lista de arriba es una trampa: con cuatro nombres parecidos, al menos uno probablemente sea falso, y el teléfono no te avisa.

Pero ojo, y esto es importante: ni siquiera necesitas un atacante para estar en riesgo en una red pública. En una red WiFi abierta (sin contraseña), el tráfico viaja por el aire sin cifrar, como postales en lugar de cartas cerradas. Cualquiera con un programa gratuito y un poco de conocimiento puede "escuchar" lo que viaja por el aire: qué páginas visitas, qué escribes en sitios sin protección. No es magia ni es cosa de películas: es cómo funciona la radio. Por eso la regla de oro de esta clase es: en una red pública, actúa como si alguien estuviera mirando por encima de tu hombro. Porque técnicamente, alguien podría.

Entonces, ¿cómo te proteges? Con capas, como una cebolla. Ninguna medida es perfecta sola, pero juntas te hacen un objetivo muy poco atractivo. Capa uno: la VPN. VPN significa "red privada virtual". Imagina que en lugar de mandar tus postales al aire, las metes todas en un tubo blindado que va directo desde tu teléfono hasta un servidor seguro de la empresa de VPN, y de ahí salen a internet. Todo lo que viaja por el aire entre tu teléfono y el punto de acceso va cifrado dentro de ese tubo: el atacante del gemelo malvado o el curioso de la mesa de al lado solo ven ruido. Una VPN no te hace invisible ni anónimo por completo (la empresa de VPN sí puede ver tu tráfico, así que elige una de pago con buena reputación, nunca una gratuita que se mantenga con tus datos), pero en redes públicas es la diferencia entre hablar a gritos y hablar en clave. Úsala siempre que te conectes fuera de casa: cafés, aeropuertos, hoteles, centros comerciales.

Capa dos: HTTPS y el candado del navegador. HTTPS es la versión segura de las páginas web: cifra la comunicación entre tu navegador y el sitio. Lo reconoces por el candado junto a la dirección y porque la dirección empieza con `https://`. Con HTTPS, aunque alguien intercepte tu tráfico, no puede leer el contenido (puede ver a qué sitio entraste, pero no qué escribiste ni tu contraseña). La buena noticia es que hoy casi todo internet usa HTTPS: tu banco, tu correo, tus redes sociales. La mala noticia es que no todo, y que un atacante puede intentar engañarte para que uses la versión insegura. Reglas prácticas: nunca escribas contraseñas ni datos de tarjeta en una página sin candado; si el navegador te muestra una advertencia de "conexión no segura" o "certificado inválido", no la ignores ni le des "continuar de todos modos": ciérrala; y en redes públicas, evita hacer operaciones bancarias si puedes esperar a llegar a casa, VPN o no.

Capa tres: OWE. Estas siglas significan "Opportunistic Wireless Encryption", cifrado inalámbrico oportunista. Es un invento relativamente nuevo que resuelve un problema viejo: las redes abiertas no cifran nada porque no hay contraseña con la cual cifrar. OWE permite que tu dispositivo y el punto de acceso negocien un cifrado automáticamente, sin que tengas

que escribir ninguna contraseña. Es como si cada cliente del café recibiera automáticamente un sobre sellado para sus postales, sin tener que pedirlo. No es perfecto (no verifica que el punto de acceso sea legítimo, así que no te protege del gemelo malvado), pero sí evita que el curioso de al lado lea tu tráfico. Lo verás anunciado como "red abierta mejorada" o aparecerá en tu teléfono como una red abierta con un aviso de cifrado. Si tienes la opción entre una red abierta normal y una con OWE, elige la de OWE.

Capa cuatro: tus hábitos, que no cuestan nada. Desactiva la conexión automática a redes abiertas en tu teléfono (esa función que hace que tu teléfono se conecte solo a cualquier red "gratis" que encuentre es una invitación abierta al gemelo malvado). Cuando termines de usar una red pública, olvídale: entra a la configuración WiFi, busca la red y dale "olvidar". ¿Por qué? Porque tu teléfono guarda las redes y las busca después por su nombre; un atacante puede crear una red con ese mismo nombre en otro lugar y tu teléfono se conectará solo, creyendo que es la del café. También desactiva el compartir archivos e impresoras cuando estés en redes públicas, mantén tu sistema actualizado y desconfía de las redes con nombres sospechosos ("xX_WiFi_Gratis_Xx" grita peligro). Y un consejo de oro: si el lugar tiene red oficial, pregunta cuál es. "¿Cuál es su WiFi oficial?" le gana a cualquier tecnología.

Vamos a juntar todo en una escena. Llegas al aeropuerto. Preguntas en el mostrador cuál es la red oficial y te dicen que es "Aeropuerto_WiFi" con portal cautivo. Te conectas a ESA (no a las imitaciones), aceptas los términos, activas tu VPN, verificas el candado antes de entrar a tu correo, no haces transferencias bancarias, y al abordar pones el modo avión y olvidas la red. Eso es todo. No necesitas ser hacker ni experto: necesitas una rutina. La seguridad en redes públicas no es un producto que compras, es un hábito que repites.

Clase 30: El futuro

Si este libro lo hubieras leído hace diez años, hablaría de WiFi 4 como la novedad. Hoy hablamos de WiFi 6 y 6E como lo normal. La tecnología inalámbrica avanza en olas, y vale la pena asomarse a la ola que viene, no para comprar todo lo nuevo el día uno, sino para entender hacia dónde va el mundo y tomar decisiones inteligentes.

Empecemos con WiFi 7, cuyo nombre técnico es 802.11be. Ya conoces el patrón: cada generación trae más velocidad, más capacidad y menos espera. WiFi 7 trae tres trucos principales. El primero se llama MLO, "Multi-Link Operation", operación multi-enlace. Hasta ahora, tu dispositivo se conectaba al router por UNA banda a la vez: o 2.4, o 5, o 6 GHz. Con MLO, el dispositivo puede usar varias bandas AL MISMO TIEMPO, como una persona que habla por teléfono mientras escribe en la computadora: si una banda se satura o tiene interferencia, el tráfico fluye por la otra sin cortes. Esto es oro para videollamadas, juegos en línea y realidad virtual, donde un micro-corte se nota muchísimo. El segundo truco son los

canales de 320 MHz, el doble de anchos que los de WiFi 6E: más ancho es como una carretera más ancha, caben más datos a la vez. El tercer truco es una modulación más eficiente (4096-QAM, si quieres el nombre técnico), que mete más información en cada transmisión.

Ahora la pregunta del millón: ¿vale la pena comprar WiFi 7 hoy? La respuesta honesta es: depende, y para la mayoría de la gente, todavía no. Piensa en esto: para aprovechar WiFi 7 necesitas router WiFi 7 Y dispositivos WiFi 7 (teléfono, laptop). Si tu teléfono es WiFi 6, un router WiFi 7 te dará casi lo mismo que uno WiFi 6 bueno. Además, los primeros equipos de una generación suelen ser caros y a veces traen fallos que se corrigen después. Mi recomendación de siempre: si vas a comprar router hoy y la diferencia de precio no es absurda, un equipo WiFi 6E o WiFi 7 "preparado para el futuro" no es mala idea; pero no corras a cambiar un WiFi 6 que funciona bien solo por el número nuevo. La velocidad que anuncian en la caja casi nunca es la que sientes en el sillón, y tu internet contratado (50, 100, 200 Mbps) es el que manda al final del día.

El segundo invitado del futuro es LiFi. Si WiFi usa ondas de radio, LiFi usa LUZ para transmitir datos: focos LED especiales que parpadean miles de millones de veces por segundo (tan rápido que tu ojo no lo nota) para mandar información. Suena a ciencia ficción, pero ya existen productos reales. ¿Ventajas? La luz no atraviesa paredes, así que es muy difícil espiar desde afuera: ideal para oficinas, hospitales o lugares donde la seguridad es crítica. Además, no interfiere con equipos sensibles (en hospitales o aviones, donde las ondas de radio a veces son problema). ¿Desventajas? Pues las obvias: si algo tapa la luz, se corta la conexión; no sirve para moverte por la casa con el teléfono en el bolsillo. LiFi no va a reemplazar al WiFi: va a ser su compañero en lugares específicos. Es un buen ejemplo de que el futuro no es "una tecnología gana y las demás mueren", sino "cada tecnología encuentra su lugar".

El tercer tema es la convergencia de WiFi con 5G y, más adelante, 6G. Durante años fueron mundos separados: el WiFi era "lo de adentro" (casa, oficina) y la red celular era "lo de afuera" (calle, carretera). Eso se está borrando. El 5G ya ofrece velocidades que compiten con el WiFi en muchos casos, y los teléfonos modernos saltan entre WiFi y datos móviles sin que lo notes. En el futuro cercano verás más lugares donde tu dispositivo elige automáticamente la mejor conexión disponible, y tecnologías que combinan ambas. El 6G todavía está en investigación (se espera hacia 2030), pero apunta a velocidades absurdas y a conectar no solo personas sino millones de sensores por kilómetro cuadrado: ciudades inteligentes de verdad. Para ti como usuario, la lección es simple: no te cases con una sola tecnología. El futuro es mixto.

El cuarto tema es el internet de las cosas, IoT, y el estándar Matter. Ya tienes focos, bocinas, cámaras y termostatos conectados, y cada año habrá más. El problema histórico fue que cada marca hablaba su propio idioma: el foco de una marca no se entendía con el asistente de otra.

Matter es un acuerdo entre los gigantes (Apple, Google, Amazon, Samsung y más) para que los aparatos del hogar inteligente hablen el mismo idioma, funcionen con WiFi y con otro protocolo llamado Thread, y sean más seguros desde el diseño. Si vas a comprar aparatos inteligentes en los próximos años, busca el logo de Matter: es tu garantía de que no quedarás atrapado en la marca equivocada. Y recuerda la lección de la clase 28: todos esos aparatos van en su propia red separada, porque un foco barato con seguridad pobre no debe tener acceso a tu computadora.

Hablemos también de sustentabilidad, porque el futuro no es solo velocidad. Miles de millones de dispositivos conectados consumen energía, y las nuevas generaciones de WiFi incluyen modos de ahorro: los aparatos "duermen" más tiempo y despiertan solo para transmitir, lo que alarga la batería de sensores y reduce el consumo. Como usuario puedes aportar: apaga los equipos que no usas, no cambies el router cada año por moda, y cuando compres, prefiere equipos eficientes. El mejor dispositivo para el planeta es el que no necesitas fabricar.

Cierro la clase del futuro con una idea que une todo el curso. Hace veinte años, conectarse a internet era un ritual: el módem chillaba, ocupaba la línea del teléfono y tu mamá te regañaba si tardabas. Hoy el WiFi es invisible, como la electricidad: está ahí y solo lo notas cuando falta. El futuro va en esa dirección, pero más: conexión en todas partes, cambiando sola entre tecnologías, con tus aparatos hablando entre ellos sin que configures nada. Y sin embargo, los fundamentos que aprendiste en este libro no van a caducar: las ondas siguen siendo ondas, la interferencia sigue siendo interferencia, y la seguridad seguirá dependiendo de que alguien (tú) tome buenas decisiones. La tecnología cambia; el criterio permanece.

El costo real de un WiFi malo (números que duelen)

Hablemos de dinero, porque los negocios entienden de dinero. Un punto de acceso de gama negocio cuesta entre lo que vende un café en dos o tres días buenos. Una tarde de instalación, una hora de configuración. En cambio, un cliente que se va molesto porque el WiFi no sirvió no solo se lleva su consumo de hoy: se lleva sus visitas futuras y, peor, se lleva su reseña. Hoy la gente califica todo en Google Maps, y "el WiFi no sirve" aparece en las reseñas de cafés, hoteles y restaurantes con una frecuencia que asusta. Una estrella menos en tu calificación puede significar decenas de clientes menos al mes. Haz la cuenta: si un cliente promedio gasta 80 pesos y pierdes 20 clientes al mes por malas reseñas del WiFi, son 1,600 pesos mensuales tirados a la basura, mes tras mes, por no haber invertido una vez en una buena red. El WiFi malo no es un gasto que evitas: es un impuesto invisible que pagas todos los días.

Y hay otro costo menos visible: tu tiempo. El dueño que improvisó la red pasa horas a la semana reiniciando el router, dando la contraseña a cada cliente, escuchando quejas. Una red

bien diseñada se administra sola: el portal hace el trabajo de dar acceso, los límites evitan los abusos, y el reporte mensual te dice cuánta gente se conectó sin que muevas un dedo. La tecnología bien puesta no te da trabajo: te lo quita.

Términos y condiciones: qué deben decir (en humano)

El portal cautivo casi siempre incluye términos y condiciones, y casi nadie los lee. Pero como responsable del negocio, tú sí debes saber qué cubren. En lenguaje simple, unos buenos términos dicen cuatro cosas. Uno: el servicio es cortesía del negocio y puede limitarse o suspenderse (así nadie te exige internet perfecto como si fuera un derecho constitucional). Dos: el usuario es responsable de lo que haga en la red (descargas ilegales, fraudes, acoso), no el negocio. Tres: reglas básicas de convivencia digital (no saturar la red, no intentar hackear nada, no hacer nada ilegal). Cuatro: qué datos recoges (por ejemplo, el correo) y para qué los usas, con la opción de darse de baja. No necesitas un abogado para la primera versión, pero si tu negocio crece o manejas datos sensibles, una revisión legal es barata comparada con un problema. Y un consejo de oro: si pides datos personales, tu aviso de privacidad debe estar visible y ser honesto. La confianza del cliente vale más que una base de datos conseguida con engaños.

VPN por dentro: cómo elegir una buena (y huir de las malas)

Ya sabes qué hace una VPN: mete tu tráfico en un túnel cifrado. Pero el mercado está lleno de opciones y de trampas, así que vamos a lo práctico. Una VPN decente se reconoce por esto: es de pago (las VPN cuestan servidores y mantenimiento; si es gratis, el producto eres tú y tus datos), tiene política clara de no guardar registros de tu actividad, usa protocolos modernos (WireGuard o OpenVPN son los nombres que debes ver), tiene aplicaciones fáciles para teléfono y computadora, y permite conectarte con un toque. Las señales de alarma: la app gratuita que te promete "internet gratis ilimitado", la que te pide permisos raros en el teléfono (¿para qué quiere tu lista de contactos una VPN?), la que no dice quién es la empresa detrás ni en qué país opera. Instala la VPN en casa, con calma y buen internet, no en el aeropuerto con prisa: configúrala una vez, prueba que se conecte sola, y actívala como reflejo cada vez que salgas. Piensa en ella como el seguro del coche: lo contratas antes del accidente, no durante.

OWE y WPA3 en redes públicas: lo que está cambiando

Vale la pena detenerse en cómo está evolucionando la seguridad del WiFi público, porque en los próximos años lo vas a ver en tus dispositivos. El problema de fondo es viejo: las redes abiertas no pueden cifrar porque no hay una contraseña compartida. OWE, que ya conociste,

resuelve la mitad: cifra el tráfico de cada usuario por separado sin pedir contraseña. La otra mitad del problema es verificar que el punto de acceso sea legítimo (el gemelo malvado), y eso sigue dependiendo de ti y de tu criterio. Por otro lado, WPA3, el estándar de seguridad moderno que aprendiste en este curso, incluye un modo para redes abiertas mejoradas que combina lo mejor de los dos mundos en equipos nuevos. ¿Qué significa esto en la práctica? Que cuando veas en tu teléfono una red abierta marcada como "segura" o "cifrada", es mejor opción que la red abierta tradicional, pero NO significa que puedas bajar la guardia: la VPN sigue siendo recomendable. La tecnología mejora el piso de seguridad para todos, pero tu criterio sigue siendo el techo.

Los aparatos del negocio también son computadoras

Un detalle que muchos negocios pasan por alto: la cámara de seguridad barata, la bocina inteligente, el termostato, la pantalla del menú digital y la terminal de pagos son computadoras conectadas a tu red, y la mayoría tiene la seguridad de una puerta de cartón. Estos aparatos rara vez reciben actualizaciones, traen contraseñas de fábrica que nadie cambia y a veces tienen accesos ocultos del fabricante. Por eso van en su propia red separada, como ya vimos, pero además merecen estas reglas: cambia todas sus contraseñas de fábrica el día que los instalas; si un aparato no necesita salir a internet (una impresora local, por ejemplo), no le des salida; revisa una vez al año si hay actualizaciones de firmware; y cuando un aparato deje de recibir soporte del fabricante, planea reemplazarlo. El ataque más vergonzoso para un negocio no es que le hackeen la computadora principal: es que le hackeen el foco inteligente y desde ahí lleguen a todo lo demás. La cadena se rompe por el eslabón más débil, y en los negocios modernos el eslabón más débil suele tener forma de cámara de 500 pesos.

Casos reales: cuando sale mal y cuando sale bien

Nada enseña como una historia real, así que aquí van tres, basadas en situaciones que se repiten todos los días.

Caso uno: el hotel del gemelo. Una viajera llega a un hotel de ciudad, cansada, y en el elevador ve un cartelito que dice "WiFi gratis en todo el hotel". En su cuarto aparecen dos redes: "Hotel_GranVía" y "Hotel GranVía Gratis". Se conecta a la segunda porque "es la gratis". A los diez minutos le llega un correo de su banco: "detectamos un inicio de sesión inusual". Por suerte el banco lo bloqueó a tiempo. Lo que pasó: alguien en el cuarto de al lado había montado el gemelo malvado y capturó su contraseña porque entró al banco sin VPN en una red falsa. El hotel sí tenía red oficial, pero ella no preguntó en recepción. Moraleja: treinta segundos preguntando en recepción valen más que cualquier antivirus.

Caso dos: la oficina que mezcló todo. Un despacho pequeño de contadores usaba una sola red para todo: las computadoras con las declaraciones de impuestos de sus clientes, los teléfonos de los empleados y el WiFi que le daban a los clientes en la sala de espera, todo con la misma contraseña escrita en un papelito pegado al monitor. Un "cliente" se sentó tres tardes seguidas en la sala de espera con una laptop. Nadie sospechó nada. Meses después, varios de los clientes del despacho empezaron a recibir fraudes de identidad. Nunca se pudo probar de dónde salió la fuga, pero el despacho tuvo que avisar a todos sus clientes, contratar abogados y cambiar toda su red. El costo de separar las redes desde el día uno habría sido una tarde de trabajo. Moraleja: los datos de tus clientes son tu reputación; la red que los toca debe estar aislada.

Caso tres: el café que sí lo hizo bien. Una cafetería de barrio contrató a un técnico una sola tarde. Resultado: tres redes separadas, portal cautivo con el logo y una promoción ("segundo café a mitad de precio si te registras"), límite de dos horas por cliente. En seis meses reunió 800 correos de clientes reales, y sus promociones por correo empezaron a llenar las tardes flojas de entre semana. El dueño dice que la red se pagó sola en dos meses, no por el WiFi en sí, sino por lo que el portal le permitió hacer: conocer a sus clientes y traerlos de vuelta. Moraleja: el WiFi de un negocio no es un gasto ni un lujo; bien hecho, es una máquina de marketing que trabaja sola.

Fíjate en el patrón de los tres casos: en ninguno hizo falta tecnología exótica ni presupuestos enormes. La diferencia entre el desastre y el éxito fue el criterio: verificar, separar, limitar y pensar en el cliente. Todo lo que aprendiste en esta unidad. Y todo lo que aprendiste en este curso.

Ejemplos paso a paso

Tutorial 1: Diseña la red WiFi de un café pequeño, paso a paso

Vamos a aplicar la Clase 28 completa con un caso concreto: "Café El Rincón" decide hacer las cosas bien. Local de 80 metros cuadrados, unas 30 personas en hora pico, computadora de caja, dos cámaras de seguridad, terminal de pagos con chip. Presupuesto moderado. Sigue estos pasos:

PASO 1: Mide y dibuja.

Dibuja en una hoja el plano del local: mesas, mostrador, cocina, baño.

Marca dónde hay enchufes y dónde está la llegada del internet del proveedor.

Regla: el punto de acceso va alto (2.5 metros o más) y lo más centrado posible, lejos del microondas y de refrigeradores de metal.

PASO 2: Elige el equipo.

- Un punto de acceso de gama negocio con soporte para múltiples SSID, portal cautivo y límites por usuario (ejemplos comunes: Ubiquiti UniFi, TP-Link Omada, Aruba Instant On).
 - Un switch sencillo si necesitas conectar por cable la caja y las cámaras.
 - Contrata con tu proveedor al menos 100 Mbps si esperas 30 clientes (3 Mbps por cliente simultáneo es una base razonable para navegar y video ligero).
- Evita el router casero como equipo principal: no está hecho para 30 clientes.

PASO 3: Crea las tres redes (SSID).

- "RINCON-Empleados": WPA2 o WPA3, contraseña larga y privada. Solo el personal la conoce.
- "RINCON-Clientes": portal cautivo, sin contraseña o con contraseña sencilla que cambias cada mes. Esta es la que usará la mayoría.
- "RINCON-Equipos": WPA2/WPA3, contraseña privada, solo para cámaras, terminal de pagos e impresora. Nadie más la usa.

Activa el aislamiento entre redes (VLAN o "aislamiento de clientes"):
un cliente JAMÁS debe poder ver la computadora de la caja.

PASO 4: Configura el portal cautivo.

- Logo del café y mensaje de bienvenida corto.
- Términos y condiciones en lenguaje simple, una pantalla como máximo.
- Botón grande de "Conectarme".
- Si pides correo, explica para qué ("promociones, date de baja cuando quieras").
- Límite de sesión: 2 horas. Límite de velocidad: 10 Mbps de bajada por cliente.

Prueba el portal con tu propio teléfono antes de abrir: debe aparecer solo en menos de 10 segundos.

PASO 5: Prueba de estrés.

Un viernes a la hora pico, conéctate como cliente y haz lo que haría un cliente: abre videos, haz una videollamada, carga páginas. Camina por todo el local y anota dónde se cae la señal. Ajusta la posición del punto de acceso si hace falta. Si un solo cliente con video tumba a los demás, baja el límite por usuario.

PASO 6: Rutina de mantenimiento (una vez al mes).

- Revisa que el firmware esté actualizado.
- Cambia la contraseña de invitados si usas una.
- Revisa el reporte de uso: ¿cuántos clientes se conectan? ¿a qué horas?
- Limpia la lista de dispositivos bloqueados si el sistema bloqueó a alguien por error.

Anota la contraseña de administración en un lugar seguro (no en un post-it pegado al router).

Con esto, Café El Rincón pasa de "el WiFi no sirve" a "qué buen internet tienen aquí", y eso se traduce en clientes que regresan.

Tutorial 2: Checklist de seguridad para conectarte a una red pública

Imprime esta lista mentalmente y repásala cada vez que te conectes fuera de casa. Es tu rutina de la Clase 29:

ANTES DE CONECTARTE:

- [] Pregunta cuál es la red oficial del lugar. No adivines por el nombre.
- [] Desconfía de nombres con faltas de ortografía, mayúsculas raras o sufijos sospechosos ("Gratis", "Free", "xX_..._Xx").
- [] Desactiva la conexión automática a redes abiertas en tu teléfono (ajustes WiFi: desactiva "conectar automáticamente" a redes abiertas).

AL CONECTARTE:

- [] Si hay portal cautivo, léelo de rápido: ¿es del negocio real? ¿pide datos razonables? Un portal del aeropuerto no necesita tu CURP.
- [] Activa tu VPN antes de abrir cualquier app o página. Sin excepciones.
- [] Verifica el candado (https://) antes de escribir contraseñas.

MIENTRAS LA USAS:

- [] Evita operaciones bancarias y compras con tarjeta si puedes esperar. Si es urgente, hazlo solo con VPN activa y candado verificado.
- [] Si el navegador muestra advertencia de "conexión no segura" o "certificado inválido": cierra la página, no le des "continuar".
- [] No descargues archivos ni actualices programas en redes públicas (un atacante podría ofrecerte una "actualización" falsa).

AL TERMINAR:

- [] Olvida la red: ajustes WiFi > la red > "olvidar esta red". Así tu teléfono no se conectará solo a un gemelo con el mismo nombre después.
- [] Desactiva el WiFi si ya no lo necesitas, o activa el modo avión.
- [] Al llegar a casa, revisa que tu VPN siga configurada y actualizada.

Repite esta lista unas cinco veces y se vuelve automática, como abrocharte el cinturón.

Tutorial 3: Cómo evaluar si un negocio necesita ayuda profesional

No todo lo puede (ni lo debe) hacer el dueño. Esta guía te dice cuándo llamar a un técnico o empresa de redes:

EVALÚA ESTOS PUNTOS:

- [] ¿Más de 30 usuarios simultáneos? Un solo punto de acceso ya no basta: necesitas varios coordinados (roaming) y eso ya es trabajo profesional.
- [] ¿El local tiene varios pisos, muros gruesos o más de 200 m2?
El diseño de cobertura se complica y un plano de calor ayuda mucho.
- [] ¿Manejas datos sensibles (consultorio, despacho, pagos en línea)?
La segmentación y el registro de accesos deben quedar bien desde el día uno.
- [] ¿Necesitas que el portal pida datos y cumpla con leyes de privacidad?
Un profesional configura el aviso de privacidad y el manejo de datos.
- [] ¿Ya intentaste lo básico (buen equipo, tres redes, portal, límites)
y sigue fallando? No es derrota: es el momento de llamar a quien lo hace diario.

QUÉ PEDIRLE AL PROFESIONAL (para que no te vendan humo):

- Un plano de cobertura: dónde va cada punto de acceso y por qué.
- Las tres redes separadas con aislamiento, configuradas y probadas.
- Portal cautivo con tus términos y tu imagen.
- Límites por usuario configurados según tu número de clientes.
- Contraseñas de administración entregadas por escrito y cambio de todas las contraseñas de fábrica.
- Una sesión de 30 minutos donde te enseñe lo básico: cómo reiniciar, cómo ver quién está conectado y a quién llamar si algo falla.

Un buen profesional no te hace dependiente: te deja las llaves y te enseña a usarlas.

Práctica

Ejercicio 1: Propuesta de red para una taquería con 30 clientes

Una taquería quiere ofrecer WiFi a sus clientes. Tiene 30 mesas, hora pico con unos 30 clientes conectados a la vez, una computadora donde llevan las ventas, una cámara de seguridad y una bocina inteligente para la música. El dueño quiere gastar poco pero hacerlo bien. Diseña la propuesta: equipos, redes, portal y límites.

Solución explicada paso a paso:

Paso 1: dimensiona la necesidad. Treinta clientes simultáneos es justo el límite donde un router casero se rinde. La propuesta debe incluir un punto de acceso de gama negocio (no el router del proveedor como equipo principal). Internet contratado: mínimo 100 Mbps para que 30 clientes tengan unos 3 Mbps cada uno en hora pico.

Paso 2: define las tres redes. "TAQUERIA-Empleados" (WPA3, contraseña privada, para la computadora de ventas y el personal), "TAQUERIA-Clientes" (portal cautivo, para los comensales) y "TAQUERIA-Equipos" (para la cámara y la bocina). Las tres aisladas entre sí: el cliente de la mesa 12 no puede ver la computadora de las ventas ni la cámara.

Paso 3: configura el portal cautivo con la identidad de la taquería: logo, "Bienvenido a Taquería El Faro", términos simples de una pantalla, botón de conectar. Límite de sesión de 1.5 horas (la rotación de mesas en una taquería es rápida) y límite de 8 Mbps por cliente, suficiente para redes sociales y video sin que uno solo acapare todo.

Paso 4: ubicación del equipo. Punto de acceso al centro del comedor, a unos 2.5 metros de altura, lejos de la cocina (el microondas y el metal de los refrigeradores interfieren). La computadora de ventas, si se puede, conectada por cable al switch: lo que va por cable no compite por el aire.

Paso 5: mantenimiento mensual. Actualizar firmware, revisar el reporte de conexiones del portal (¿cuántos clientes se conectaron? es información de marketing: esos correos sirven para promociones con aviso de privacidad), y cambiar la contraseña de empleados si alguien del personal se fue. Costo total estimado: el punto de acceso de gama negocio más la instalación, equivalente a unas semanas de venta; el retorno llega en clientes que se quedan más tiempo y regresan.

Ejercicio 2: Auditoría de tus hábitos en redes públicas

Sé honesto y responde: en los últimos tres meses, ¿te conectaste a alguna red WiFi pública (café, aeropuerto, hotel, centro comercial)? ¿Preguntaste cuál era la red oficial o te conectaste a la primera que decía "gratis"? ¿Usaste VPN? ¿Olvidaste la red después? ¿Hiciste alguna operación bancaria? Escribe tus respuestas y califícate del 1 al 10.

Solución explicada paso a paso:

Paso 1: lista cada red pública que recuerdes y anota qué hiciste en cada una. No te juzgues todavía; solo registra. La mayoría de la gente descubre que se conectó a tres o cuatro redes sin pensar.

Paso 2: marca con rojo cada vez que te conectaste sin verificar que fuera la red oficial, cada vez que navegaste sin VPN y cada vez que dejaste la red guardada en tu teléfono. Esos son tus puntos de riesgo.

Paso 3: corrige hoy mismo lo corregible. Entra a los ajustes WiFi de tu teléfono y olvida todas las redes públicas guardadas ("Café_", "Aeropuerto", "Hotel_"). Desactiva la conexión automática a redes abiertas. Si no tienes VPN, instala una de pago con buena reputación (las gratuitas suelen pagarse con tus datos, que es justo lo que quieres proteger).

Paso 4: escribe tu rutina personal en una nota del teléfono, con tus palabras, basada en el checklist del Tutorial 2. Ejemplo: "1) Pregunto la red oficial. 2) Activo VPN. 3) Reviso el candado. 4) Olvido la red al salir." La seguridad que no está escrita se olvida; la escrita se vuelve hábito.

Paso 5: repite la auditoría dentro de un mes. Si tu calificación subió, vas bien. El objetivo no es la perfección del 10, es no regalar tus datos por flojera.

Ejercicio 3: Detecta al gemelo malvado (en papel)

Estás en un hotel. En tu teléfono aparecen estas redes: "Hotel_Paraiso", "Hotel-Paraiso", "Hotel Paraiso WiFi Gratis", "HOTEL_PARAISO_5G" y "Paraiso_Hotel_Invitados". El recepcionista te dijo que la red oficial es "Hotel_Paraiso" con contraseña. ¿A cuál te conectas y por qué? ¿Qué harías con las demás?

Solución explicada paso a paso:

Paso 1: la respuesta es "Hotel_Paraiso", exactamente como la dijo el recepcionista, con la contraseña que te dio. El nombre idéntico más la contraseña que solo el hotel conoce es tu mejor garantía. Las demás, aunque se parezcan, no las verificó nadie.

Paso 2: analiza las sospechosas. "Hotel Paraiso WiFi Gratis" es el clásico anzuelo: agrega "Gratis" para tentar. "HOTEL_PARAISO_5G" finge ser la versión rápida. "Hotel-Paraiso" cambia un guion bajo por un guion medio, diferencia que casi nadie nota. Cualquiera de ellas podría ser el gemelo malvado de un atacante sentado en el lobby.

Paso 3: aunque te conectes a la oficial, activa tu VPN antes de navegar, porque en un hotel nunca sabes quién más está en la red ni si la red oficial está bien configurada.

Paso 4: al hacer check-out, olvida la red "Hotel_Paraiso" de tu teléfono. Si no lo haces, dentro de un mes tu teléfono buscará automáticamente una red llamada "Hotel_Paraiso" y un atacante en otro lugar podría crearla para atraparte.

Paso 5: la lección general. Los atacantes no hackean tu teléfono con magia: hackean tu confianza con un nombre parecido. La defensa es siempre la misma: verifica con una persona real cuál es la red oficial.

Ejercicio 4: Plan de actualización a WiFi 7, ¿vale la pena hoy?

Tienes un router WiFi 6 que funciona bien, internet contratado de 200 Mbps, un teléfono WiFi 6 y una laptop WiFi 6. Ves una oferta de un router WiFi 7 al triple de precio. Decide con argumentos si lo compras hoy o esperas, y escribe tu plan.

Solución explicada paso a paso:

Paso 1: identifica el cuello de botella real. Tu internet es de 200 Mbps y tu router WiFi 6 ya puede entregar eso sin problema a tus dispositivos. Un router WiFi 7 no va a hacer que tu internet contratado sea más rápido: el límite lo pone tu proveedor, no tu router.

Paso 2: revisa tus dispositivos. Ninguno es WiFi 7, así que no aprovecharías el MLO ni los canales de 320 MHz, que son las grandes novedades. Sería como comprar llantas de carreras para un coche que no sale del estacionamiento.

Paso 3: considera el precio y la madurez. Los equipos de primera generación suelen ser caros y a veces traen fallos que se corrigen con el tiempo. Pagar el triple hoy por funciones que no puedes usar es mala inversión.

Paso 4: la decisión recomendada. No lo compres hoy. Tu plan: sigue con tu WiFi 6, que está en su mejor momento de precio y madurez; cuando cambies de teléfono o laptop a modelos WiFi 7 (probablemente en 2 o 3 años), reevalúa; y si para entonces el precio del WiFi 7 bajó, ahí sí será buen momento.

Paso 5: la excepción. Sí convendría si fueras un negocio con muchísimos dispositivos, necesitaras la menor latencia posible (juegos competitivos, realidad virtual) y ya tuvieras dispositivos WiFi 7. Para un hogar normal con 200 Mbps, la respuesta es esperar. El criterio que aprendiste en este curso vale más que la novedad de la caja.

Ejercicio 5: El portal cautivo perfecto para tu negocio imaginario

Inventa un negocio (cafetería, barbería, consultorio, taller) y diseña en papel su portal cautivo: qué dice la pantalla, qué datos pide, qué límites pone y por qué. Luego críticoalo como si fueras el cliente más impaciente del mundo.

Solución explicada paso a paso:

Paso 1: elige el negocio y su cliente típico. Ejemplo: barbería "El Navajazo", clientes que esperan 20 a 40 minutos. El portal debe entretener la espera, no estorbarla.

Paso 2: diseña la pantalla. Logo, "Bienvenido a El Navajazo, tu espera con buen internet", términos de una pantalla en lenguaje simple, botón grande "Conectar". Pide solo el correo, con

la explicación "para avisarte de promociones; date de baja cuando quieras". Nada de nombre, teléfono y fecha de nacimiento: cada campo extra es un cliente que abandona.

Paso 3: define los límites con lógica del negocio. Sesión de 1 hora (nadie espera más en una barbería), 10 Mbps por cliente (suficiente para video mientras esperan). Horario del portal igual al horario del local: de noche, la red de invitados se puede apagar para que nadie se conecte desde la banqueta a las 3 de la mañana.

Paso 4: ponte en los zapatos del cliente impaciente. ¿El portal apareció solo en menos de 10 segundos? ¿Se entiende a la primera? ¿Funciona bien en un teléfono con pantalla chica? ¿El botón se puede tocar con el pulgar sin hacer zoom? Si algo falla aquí, rediseña.

Paso 5: cierra el círculo comercial. Esos correos, con aviso de privacidad, se convierten en la lista de clientes para promociones ("corte + barba 2x1 los martes"). El portal deja de ser un trámite y se vuelve una herramienta del negocio. Eso es lo que separa al portal bien pensado del que solo estorba.

Ejercicio 6: Conversación para convencer al dueño del café

Tu tío tiene un café con WiFi abierto sin contraseña, la misma red para empleados y clientes, y la contraseña del router es "admin123". Quiere cambiarlo pero le da flojera y dice "nunca ha pasado nada". Escribe cómo le explicarías, con calma y sin tecnicismos, por qué debe cambiarlo, usando lo aprendido en esta unidad.

Solución explicada paso a paso:

Paso 1: empieza por lo que a él le duele: los clientes. "Tío, cuando se llena el café el internet se arrastra y la gente se va al café de enfrente. No es que el internet sea malo: es que un router casero no aguanta 30 teléfonos y no tienes límites por cliente. Con un equipo decente y un límite de 10 Mbps por persona, se acaba el problema."

Paso 2: sigue con su dinero. "Tu computadora de las ventas está en la misma red que los clientes. Cualquiera con un programa gratuito puede husmear. Si un día te vacían la cuenta o te roban los datos de tus proveedores, el daño es mucho mayor que lo que cuesta un punto de acceso bueno. Separar empleados de clientes es como tener caja fuerte: no es opcional."

Paso 3: desarma el "nunca ha pasado nada". "Que no te hayas dado cuenta no significa que no pasó. Los ataques a redes abiertas no avisan: no se rompe nada, no sale humo. Solo alguien copiando datos en silencio. Es como dejar la puerta del local abierta de noche porque 'nunca han robado'."

Paso 4: ofrece el camino fácil. "No tienes que hacerlo tú: un técnico te lo deja instalado en una tarde (tres redes, portal con tu logo, límites) y te enseña lo básico. Tú solo cambias la contraseña de invitados cada mes. Es una tarde de trabajo contra años de tranquilidad."

Paso 5: cierra con el beneficio, no con el miedo. "El café de enfrente ya lo hizo y por eso se llena. Tu café es mejor: solo te falta que el WiFi esté a la altura. Los clientes lo notan y regresan." Convencer no es asustar: es mostrar que lo seguro y lo rentable van de la mano.

Resumen de la unidad

- El WiFi vive fuera de tu casa tanto como dentro: cafés, oficinas, aeropuertos, hoteles y taquerías dependen de redes bien diseñadas, y ahora sabes diseñarlas.
- Un negocio serio usa portal cautivo: controla el acceso, protege legalmente al negocio, permite límites de tiempo y velocidad, y sirve como herramienta de marketing.
- Todo negocio debe separar tres redes (SSID): empleados, invitados y equipos (IoT), aisladas entre sí para que un cliente nunca toque los sistemas del negocio.
- Buenas prácticas de negocio: equipo de gama negocio (no router casero) para más de 10 clientes, punto de acceso alto y centrado, banda de 5 GHz, límites por usuario, contraseñas que se cambian y firmware actualizado.
- Errores que cuestan clientes: red abierta sin control, misma red para todos, contraseñas de fábrica, equipo mal ubicado y ningún límite de velocidad.
- El ataque de gemelo malvado (evil twin) es una red falsa con nombre parecido a la legítima: la defensa es preguntar cuál es la red oficial y no conectarte a imitaciones.
- En redes públicas, tu escudo tiene cuatro capas: VPN siempre activa, HTTPS y el candado del navegador, preferir redes con OWE cuando existan, y buenos hábitos (desactivar conexión automática, olvidar la red al terminar).
- Una VPN cifra todo tu tráfico en un túnel seguro: es tu mejor amiga fuera de casa. Elige una de pago con buena reputación, nunca una gratuita dudosa.
- Nunca ignores una advertencia de "conexión no segura" del navegador y evita operaciones bancarias en redes públicas si puedes esperar.
- WiFi 7 trae MLO (usar varias bandas a la vez), canales de 320 MHz y mejor eficiencia, pero para la mayoría conviene esperar: sin dispositivos WiFi 7 y con internet contratado modesto, no lo aprovecharás.
- LiFi transmite datos con luz: no atraviesa paredes (más seguro) pero se corta si algo tapa la luz. Será compañero del WiFi, no su reemplazo.

- El futuro es la convergencia: WiFi, 5G y luego 6G se combinarán y tu dispositivo elegirá solo la mejor conexión. No te cases con una sola tecnología.
- Matter es el idioma común del hogar inteligente (Apple, Google, Amazon, Samsung): busca su logo al comprar aparatos y mantén tus dispositivos IoT en su propia red separada.
- Los fundamentos no caducan: las ondas, la interferencia y el criterio para tomar buenas decisiones seguirán valiendo cuando el WiFi 7 sea historia.

Y aquí se cierra el curso. Empezaste sin saber qué era un SSID y terminas sabiendo diseñar la red de un café, protegerte en un aeropuerto y decidir si te conviene el WiFi 7. Eso no es poco: es criterio, y el criterio es lo único que la tecnología no puede automatizar. El WiFi va a seguir cambiando (ya viste lo que viene), pero tú ya no eres el usuario que se conecta a "xX_WiFi_Gratis_Xx" sin pensar, ni el dueño que pone "admin123" en el router del negocio. Eres alguien que entiende lo invisible: las ondas que cruzan el aire llevando tu vida de un lado a otro. Cuídalas, úsalas bien y comparte lo que aprendiste, porque el internet es de todos y funciona mejor cuando todos sabemos cuidarlo.

¿Y ahora qué? El curso termina pero tu camino sigue, y te dejo un mapa corto. Primero, practica en tu casa: optimiza tu red con todo lo de las primeras unidades, porque la teoría sin práctica se olvida en un mes. Segundo, ayuda a alguien: configura el WiFi de un familiar, explica a un amigo por qué no debe conectarse a la red "gratis" del atacante; enseñar es la forma más rápida de dominar un tema. Tercero, si te picó el gusanito profesional, este curso es una base excelente para certificaciones de redes (como las de CompTIA Network+ o las de Cisco), donde lo que aprendiste aquí te va a sonar familiar desde el día uno. Cuarto, mantente al día con criterio: cuando salga una novedad (WiFi 8, 6G, lo que sea), pregúntate lo que este libro te enseñó a preguntar: ¿qué problema resuelve?, ¿qué necesito para aprovecharlo?, ¿vale lo que cuesta hoy o espero? Esa pregunta vale más que cualquier especificación técnica.

Gracias por llegar hasta aquí. Pocos terminan lo que empiezan, y tú terminaste un curso completo de redes inalámbricas. Lleva ese orgullo a dónde vayas, y cuando alguien te pregunte por qué sabes tanto de WiFi, ya sabes qué responderles: lucasegaacademy.com. Nos vemos en el aire.

EXAMEN FINAL

Instrucciones

Este examen cubre las 10 unidades del libro "Curso Completo de Redes inalámbricas (Wireless)" de Lucas EGA Academy (lucasegaacademy.com). Tiene 50 preguntas de tres tipos: opción múltiple (elige la letra correcta), verdadero o falso (decide si la afirmación es correcta y piensa el porque) y preguntas abiertas (explica con tus palabras, describe pasos de configuración o resuelve un caso práctico).

Hazlo sin ver la sección de respuestas, con papel y pluma a la mano. Si es posible, ten tu computadora y tu router cerca para las preguntas prácticas. Cada pregunta vale 2 puntos, así que el máximo es 100 puntos.

Puntaje sugerido: 90 a 100, excelente, dominas el tema de redes inalámbricas; 70 a 89, bien, repasa las unidades donde fallaste antes de dar el siguiente paso; 60 a 69, pasaste raspando, vuelve a leer las unidades completas donde tuviste errores; menos de 60, repasa el libro completo y vuelve a intentarlo en una o dos semanas. El objetivo no es solo pasar, sino detectar exactamente que unidades necesitas reforzar.

Guía rápida de repaso por unidad

Si fallas preguntas de un tema, aquí tienes a dónde volver: las preguntas 1 a 3, 31 y 41 corresponden a la unidad 1 (fundamentos de ondas: frecuencia, longitud de onda y espectro electromagnético). Las preguntas 4 a 6, 32 y 42 son de la unidad 2 (bandas y canales: 2.4 GHz, 5 GHz, canales que no se traslapan e interferencia). Las preguntas 7 a 9, 33 y 43 cubren la unidad 3 (estándares 802.11: n, ac, ax, MIMO y compatibilidad). Las preguntas 10 a 12, 34 y 44 son de la unidad 4 (el router: puerta de enlace, DHCP, SSID y configuración básica). Las preguntas 13 a 15, 35 y 45 corresponden a la unidad 5 (seguridad: WPA2, WPA3, Personal contra Enterprise y el cifrado). Las preguntas 16 a 18, 36 y 46 son de la unidad 6 (antenas: omnidireccionales, direccionales y ganancia en dBi). Las preguntas 19 a 21, 37 y 46 también tocan la unidad 7 (repetidores y mesh: colocación, velocidad y auto-reparación). Las preguntas 22 a 24, 38 y 47 son de la unidad 8 (red de invitados y QoS: aislamiento y priorización de tráfico). Las preguntas 25 a 27, 39 y 48 cubren la unidad 9 (diagnóstico: pruebas de velocidad, analizadores de WiFi y procedimiento de fallas). Las preguntas 28 a 30, 40 y 49 corresponden a la unidad 10 (redes públicas y futuro: riesgos, VPN y WiFi 7). La pregunta 50 es el caso integrador que junta todo lo aprendido.

Consejo para las preguntas abiertas: no las respondas solo de memoria, escríbelas completas como si se las explicarías a un amigo que no sabe del tema. Si puedes explicar un concepto sin trabarte, es que lo dominas; si te atorras, esa es exactamente la unidad que debes repasar. En las de configuración, si tienes un router a la mano, entra a su panel y verifica cada paso mientras respondes: la práctica fija el conocimiento mejor que la relectura.

Preguntas de opcion multiple

PREGUNTA 1: El WiFi comunica tus dispositivos usando ondas de radio. Qué es lo que viaja por el aire en una red inalámbrica?

a) Pequeños paquetes de datos hechos de materia b) Ondas electromagneticas que transportan informacion codificada c) Corriente electrica transmitida sin cables d) Rayos de luz infrarroja visibles

PREGUNTA 2: La frecuencia de una onda se mide en Hertz (Hz). Si tu router transmite en 2.4 GHz, que significa eso?

a) Que la onda recorre 2.4 kilometros por segundo b) Que la onda oscila 2,400 millones de veces por segundo c) Que la red puede conectar 2.4 dispositivos por segundo d) Que la velocidad máxima es de 2.4 gigabits por segundo

PREGUNTA 3: Una característica de las ondas de mayor frecuencia (como 5 GHz frente a 2.4 GHz) es que:

a) Atraviesan mejor las paredes y llegan más lejos b) Llevan más datos por segundo, pero pierden fuerza más rápido y atraviesan peor los obstaculos c) Son visibles a simple vista en forma de luz azul d) No necesitan antena porque viajan en línea recta perfecta

PREGUNTA 4: Un canal WiFi es:

a) El cable interno con el que el router se conecta a la luz b) Una porcion especifica del espectro de frecuencias por donde viaja la señal inalámbrica c) Un programa que se instala en el celular para tener internet d) El nombre de usuario que usas para entrar al router

PREGUNTA 5: En la banda de 2.4 GHz, que canales se recomiendan usar para evitar que las redes vecinas se interfieran entre si?

a) 1, 2 y 3 b) 1, 6 y 11 c) 3, 7 y 12 d) Todos los canales del 1 al 13 funcionan igual de bien

PREGUNTA 6: Si vives en un departamento y tu WiFi se pone lento justo a las 8 de la noche, una causa muy probable es:

a) Que el internet de todo el pais se apaga a esa hora b) Interferencia por saturacion: muchos vecinos usando los mismos canales al mismo tiempo c) Que tu router se calienta y baja la velocidad por ley d) Que los satelites cambian de orbita por la noche

PREGUNTA 7: El estandar 802.11n (WiFi 4) introdujo una mejora importante frente a los anteriores.Cuál fue?

a) El uso exclusivo de la banda de 60 GHz b) La tecnología MIMO, que usa varias antenas para enviar y recibir datos al mismo tiempo c) La eliminacion total de las contraseñas d) La transmision de datos por medio de cables de fibra óptica

PREGUNTA 8: Que banda de frecuencia agrego el estandar 802.11ac (WiFi 5) como su principal novedad frente a 802.11n?

a) La banda de 900 MHz b) La banda de 5 GHz con canales más anchos y mayor velocidad c) La banda de 2.4 GHz, que antes no existia d) La banda de 60 GHz para uso domestico

PREGUNTA 9: La principal ventaja de WiFi 6 (802.11ax) en una casa llena de dispositivos conectados es:

a) Que ya no necesitas router b) Que maneja mejor muchos dispositivos al mismo tiempo gracias a tecnologías como OFDMA, con menos congestion c) Que la señal atraviesa edificios completos sin perderse d) Que funciona sin electricidad

PREGUNTA 10: La dirección IP privada 192.168.1.1 que aparece en muchos manuales corresponde normalmente a:

a) La página web de tu proveedor de internet b) La puerta de enlace de tu red local, es decir, tu router, desde donde entras a su panel de configuración c) Un servidor de Google d) La dirección publica de tu casa en internet

PREGUNTA 11: El DHCP en un router sirve para:

a) Encriptar la contraseña del WiFi b) Asignar automaticamente direcciones IP a los dispositivos que se conectan a la red c) Aumentar la velocidad contratada con el proveedor d) Bloquear paginas peligrosas

PREGUNTA 12: Si cambias el SSID de tu red WiFi, que estas cambiando exactamente?

a) La contraseña de administrador del router b) El nombre visible de tu red inalámbrica, el que aparece en la lista de redes del celular c) La velocidad de bajada de tu internet d) La dirección fisica del router

PREGUNTA 13: WPA2 es el protocolo de seguridad que protege la mayoría de las redes WiFi domesticas. Que hace exactamente?

a) Oculta el nombre de la red para que nadie la vea b) Cifra los datos que viajan por el aire para que solo los dispositivos con la contraseña puedan leerlos c) Aumenta la velocidad del internet al doble d) Bloquea automaticamente a los vecinos

PREGUNTA 14:Cuál es la diferencia principal entre WPA2-Personal y WPA2-Enterprise?

a) No hay diferencia, son el mismo protocolo con distinto nombre b) Personal usa una sola contraseña compartida para todos, Enterprise usa un servidor que da credenciales individuales a cada usuario c) Enterprise es más lento pero más barato d) Personal solo funciona en celulares y Enterprise solo en computadoras

PREGUNTA 15: La gran mejora de WPA3 frente a WPA2 es:

a) Que las contraseñas ya no son necesarias b) La proteccion contra ataques de diccionario y el cifrado individualizado por dispositivo (SAE), que hace mucho más difícil adivinar la clave c) Que la señal llega al triple de distancia d) Qué es compatible con redes de los años noventa

PREGUNTA 16: Una antena omnidireccional se caracteriza porque:

a) Envía la señal en una sola dirección, como un reflector b) Irradia la señal en todas direcciones a su alrededor, como una dona o rosquilla c) No necesita estar conectada al router d) Solo funciona en exteriores

PREGUNTA 17: La ganancia de una antena se mide en dBi. Si cambias la antena de tu router por una de mayor dBi, que puedes esperar?

a) Más velocidad de internet contratada b) Que la señal llegue más lejos en la dirección a la que apunta, aunque la potencia total de transmisión no cambia c) Que el router consuma menos electricidad d) Que la red quede protegida contra hackers

PREGUNTA 18: Para llevar WiFi a un patio largo y angosto detras de tu casa, la mejor opcion de antena sería:

a) Una omnidireccional en el centro de la casa b) Una antena direccional (tipo panel o yagi) apuntando hacia el patio c) Quitarle las antenas al router para que la señal se concentre d) Poner el router dentro del refrigerador para amplificar la señal

PREGUNTA 19: Un repetidor WiFi tradicional (no mesh) funciona así:

a) Crea una red completamente nueva con otro proveedor de internet b) Recibe la señal del router y la retransmite, extendiendo la cobertura, aunque normalmente a la mitad de la

velocidad c) Cambia la contraseña de tu red automaticamente cada hora d) Convierte la señal WiFi en datos moviles

PREGUNTA 20: La principal ventaja de un sistema mesh frente a un repetidor tradicional es:

a) Qué es más barato siempre b) Que los nodos crean una sola red unificada con transicion suave entre ellos, sin cortes al moverte por la casa c) Que no necesita electricidad d) Que duplica la velocidad contratada con el proveedor

PREGUNTA 21: Cuándo configuras un repetidor, dónde conviene colocarlo físicamente?

a) Lo más lejos posible del router, en el cuarto sin señal b) A la mitad del camino: donde todavía recibe buena señal del router pero ya está cerca de la zona sin cobertura c) Pegado al router para que copie mejor la configuración d) Dentro de un cajón metalico para protegerlo del polvo

PREGUNTA 22: Una red de invitados en tu router sirve para:

a) Darle internet a tus visitas sin darles acceso a tus archivos, impresoras y dispositivos personales b) Aumentar la velocidad de tu red principal c) Conectarte a redes publicas cuando viajas d) Crear una segunda cuenta de Netflix

PREGUNTA 23: El QoS (Quality of Service) en un router te permite:

a) Ver las contraseñas guardadas en tu celular b) Darle prioridad al trafico importante (videollamadas, juegos, trabajo) sobre el menos urgente (descargas, actualizaciones) c) Cambiar de proveedor de internet automaticamente d) Medir la temperatura del router

PREGUNTA 24: Si en tu casa alguien juega en línea y se queja de lag cada vez que otro miembro de la familia ve videos en 4K, que configuración del router ayudaria más?

a) Cambiar el nombre de la red b) Activar QoS y darle prioridad al trafico del juego o a la consola c) Apagar el router cada 10 minutos d) Ponerle contraseña al Netflix

PREGUNTA 25: Haces una prueba de velocidad junto al router y obtienes 200 Mbps, pero en tu cuarto solo llegan 25 Mbps. Lo primero que deberias sospechar es:

a) Que el proveedor te esta robando b) Un problema de cobertura o interferencia en el trayecto: distancia, paredes o canal saturado c) Que tu celular esta descompuesto d) Que el internet se acaba con la distancia como si fuera agua

PREGUNTA 26: Si sospechas que un vecino esta usando tu WiFi sin permiso, qué es lo primero que debes revisar?

a) La lista de dispositivos conectados en el panel del router y cambiar la contraseña por una fuerte con WPA2 o WPA3 b) Desconectar el router para siempre c) Cambiar de casa d) Llamar a la policia antes de revisar nada

PREGUNTA 27: Una herramienta como un analizador de WiFi en tu celular te sirve principalmente para:

a) Hackear redes vecinas b) Ver que canales están saturados a tu alrededor y elegir el más libre para tu router c) Aumentar la velocidad contratada d) Cambiar tu dirección IP publica

PREGUNTA 28: Conectarte a una red WiFi publica (cafe, aeropuerto) sin proteccion es riesgoso porque:

a) El cafe puede cobrarte de más b) Otros usuarios de la misma red podrian interceptar tus datos no cifrados con tecnicas de espionaje c) Tu celular se puede quedar sin bateria más rápido d) Las redes publicas siempre tienen virus instalados

PREGUNTA 29: Si necesitas trabajar con informacion delicada desde una red WiFi publica, la medida de proteccion más efectiva es:

a) Bajar el brillo de la pantalla b) Usar una VPN, que cifra todo tu trafico aunque la red sea insegura c) Conectarte rápido para que no te detecten d) Usar el modo avion con el WiFi encendido

PREGUNTA 30: Sobre el futuro de las redes inalámbricas (WiFi 7 y siguientes), cuál afirmación es correcta?

a) Ya no se necesitaran contrasenas porque todo sera público b) Se esperan velocidades multi-gigabit, menor latencia y mejor manejo de muchos dispositivos, con bandas como 6 GHz c) El WiFi va a desaparecer y todo sera por cable otra vez d) Las ondas de radio seran reemplazadas por señales de humo digitales

Preguntas de verdadero o falso

PREGUNTA 31: Verdadero o falso: Las ondas de radio del WiFi y la luz visible son el mismo tipo de fenomeno fisico (radiacion electromagnetica), solo que vibran a frecuencias distintas.

PREGUNTA 32: Verdadero o falso: En la banda de 2.4 GHz, usar el canal 3 es una buena idea porque así evitas a los vecinos que usan el canal 1 y el canal 6.

PREGUNTA 33: Verdadero o falso: Un router con estandar 802.11ac (WiFi 5) puede comunicarse con un celular viejo que solo soporta 802.11n, aunque a la velocidad del estandar más lento.

PREGUNTA 34: Verdadero o falso: Si desactivas el DHCP de tu router, tus dispositivos seguirán conectándose a internet automáticamente sin que tengas que configurar nada más.

PREGUNTA 35: Verdadero o falso: Ocultar el SSID (que el nombre de tu red no aparezca en la lista) es suficiente para proteger tu WiFi y ya no necesitas contraseña.

PREGUNTA 36: Verdadero o falso: Una antena con más dBi de ganancia concentra mejor la señal en cierta dirección, pero no aumenta la potencia total que transmite el router.

PREGUNTA 37: Verdadero o falso: En un sistema mesh, si se apaga uno de los nodos intermedios, los demás nodos pueden buscar otra ruta para seguir dando servicio.

PREGUNTA 38: Verdadero o falso: La red de invitados aísla a los visitantes de tus dispositivos personales, por eso es más seguro darles esa clave que la clave de tu red principal.

PREGUNTA 39: Verdadero o falso: Reiniciar el router (apagarlo 30 segundos y encenderlo) es un paso válido de diagnóstico cuando el internet falla de repente y antes funcionaba bien.

PREGUNTA 40: Verdadero o falso: Si la red WiFi pública de un hotel pide contraseña para conectarte, eso significa que tus datos viajan cifrados y es totalmente seguro hacer operaciones bancarias.

Preguntas abiertas

PREGUNTA 41: Explica con tus palabras qué es la frecuencia de una onda de radio, qué es la longitud de onda y cómo se relacionan entre sí. Usa el ejemplo de las bandas de 2.4 GHz y 5 GHz para ilustrar por qué una atraviesa mejor las paredes que la otra.

PREGUNTA 42: Tu vecino te dice que su WiFi de 2.4 GHz va muy lento y vive en un edificio con 20 redes visibles. Describe paso a paso que harías para diagnosticar y mejorar su situación usando lo que sabes de bandas y canales.

PREGUNTA 43: Explica la evolución de los estándares WiFi desde 802.11n hasta WiFi 6: qué aporta cada uno y en qué situación real notarías la diferencia entre ellos.

PREGUNTA 44: Describe paso a paso como entrarias al panel de configuración de un router nuevo y que 5 ajustes basicos harias para dejarlo funcionando de forma segura (nombre de red, contraseña, tipo de seguridad, etc.).

PREGUNTA 45: Explica con tus palabras cómo funciona el cifrado WPA2-PSK: qué pasa cuando escribes la contraseña en tu celular y por qué un vecino no puede leer tus datos aunque capture las ondas del aire. Menciona además que mejora WPA3 en este proceso.

PREGUNTA 46: Tienes una casa de dos pisos: el router está en la planta baja y en la planta alta la señal llega muy débil. Compara las tres soluciones (cambiar antenas, poner un repetidor, instalar un sistema mesh) y recomienda una justificando tu elección.

PREGUNTA 47: Explica qué es el QoS y describe un caso practico completo: una familia donde el papá trabaja en videollamadas, la hija ve series en 4K y el hijo juega en línea. Que reglas de QoS configurarías y por qué?

PREGUNTA 48: Tu internet se cayó por completo: ni por WiFi ni por cable hay conexión. Describe el procedimiento de diagnostico paso a paso que seguirías, en orden logico, hasta encontrar la causa.

PREGUNTA 49: Vas a pasar una semana trabajando desde cafeterias con WiFi público y manejas informacion sensible de tu trabajo. Describe tu plan de seguridad completo: que herramientas usarías, que harías y que evitarías.

PREGUNTA 50: Caso practico final: una pequeña oficina con 15 empleados necesita una red inalámbrica. El dueño te pide que propongamos la solución completa. Describe tu propuesta: que estandar WiFi elegirías, que banda(s) usarías, como organizarías las redes (empleados, invitados), que seguridad aplicarías y que consideraciones de cobertura tendrías.

Respuestas y soluciones

RESPUESTA 1: b) Ondas electromagnéticas que transportan información codificada. Lo que viaja por el aire no es materia ni electricidad, sino ondas electromagnéticas: variaciones de campos eléctricos y magnéticos que se propagan por el espacio. El router codifica los datos digitales (unos y ceros) en esas ondas modulando sus propiedades, y el dispositivo receptor las decodifica. La opción a) es incorrecta porque no viajan partículas de materia; la c) es incorrecta porque la corriente eléctrica necesita un conductor, no viaja por el aire en el WiFi; la d) es incorrecta porque las ondas del WiFi son de radio, invisibles, no luz infrarroja visible.

RESPUESTA 2: b) Que la onda oscila 2,400 millones de veces por segundo. El Hertz mide ciclos por segundo: 1 GHz equivale a mil millones de oscilaciones por segundo, así que 2.4 GHz son 2,400 millones. Es una medida de que tan rápido vibra la onda, no de distancia ni de velocidad de datos. La opción a) confunde frecuencia con velocidad de propagación; la c) inventa una relación con dispositivos que no existe; la d) confunde la frecuencia de la portadora con la velocidad de transferencia de datos, que depende del estándar y del ancho de canal, no solo de la frecuencia.

RESPUESTA 3: b) Llevan más datos por segundo, pero pierden fuerza más rápido y atraviesan peor los obstáculos. Las frecuencias altas tienen longitudes de onda más cortas, lo que permite modular más información por segundo, pero esas ondas cortas son absorbidas y reflejadas con más facilidad por paredes, muebles y hasta el aire húmedo. Por eso 5 GHz es más rápido cerca del router pero 2.4 GHz llega más lejos y atraviesa mejor las paredes. La opción a) describe justo lo contrario de lo que ocurre; la c) es falsa porque ninguna de estas frecuencias es visible; la d) es falsa porque toda antena real irradia con algún patrón y las ondas sí se debilitan con obstáculos.

RESPUESTA 4: b) Una porción específica del espectro de frecuencias por donde viaja la señal inalámbrica. El espectro de radio se divide en canales para que varias redes puedan transmitir sin pisarse, igual que las estaciones de radio FM tienen cada una su frecuencia. Tu router transmite en un canal específico dentro de la banda. La opción a) es incorrecta porque el canal no es un cable físico; la c) confunde el concepto con una aplicación; la d) confunde el canal con el SSID, que es el nombre de la red.

RESPUESTA 5: b) 1, 6 y 11. En 2.4 GHz los canales se traslapan entre sí: cada canal ocupa más ancho del que parece y se mete en los vecinos. Los únicos tres canales que no se traslapan en la mayoría de los países son el 1, el 6 y el 11, por eso son los recomendados. La opción a) es incorrecta porque los canales 1, 2 y 3 se interfieren entre sí al estar pegados; la c) es incorrecta porque el 3 se traslapa con el 1 y el 6, y el 7 con el 6; la d) es incorrecta porque usar canales traslapados genera interferencia y baja el rendimiento de todas las redes involucradas.

RESPUESTA 6: b) Interferencia por saturación: muchos vecinos usando los mismos canales al mismo tiempo. En las noches todos llegan a casa, se conectan y saturan los canales disponibles, sobre todo en edificios. Las redes compiten por el mismo "espacio aéreo" y el rendimiento cae. La opción a) es un mito, el internet no se apaga por horario; la c) es incorrecta porque los routers no bajan la velocidad por calentamiento de forma programada; la d) es absurda, los satélites no afectan tu WiFi local de esa manera.

RESPUESTA 7: b) La tecnología MIMO, que usa varias antenas para enviar y recibir datos al mismo tiempo. MIMO (Multiple Input Multiple Output) permite transmitir varios flujos de datos simultáneos por diferentes antenas, multiplicando la velocidad real frente a los estándares anteriores que usaban un solo flujo. La opción a) es incorrecta porque la banda de 60 GHz llegó mucho después con 802.11ad; la c) es falsa, las contraseñas siguieron existiendo; la d) es incorrecta porque el WiFi por definición es inalámbrico y 802.11n no usa fibra.

RESPUESTA 8: b) La banda de 5 GHz con canales más anchos y mayor velocidad. Aunque 802.11n ya podía usar 5 GHz, fue 802.11ac el que la convirtió en su banda principal, con canales de hasta 80 y 160 MHz que permiten velocidades cercanas al gigabit. La opción a) es incorrecta porque 900 MHz no es una banda WiFi comercial relevante; la c) es incorrecta porque 2.4 GHz existía desde los primeros estándares; la d) es incorrecta porque 60 GHz corresponde a 802.11ad/ay, no a 802.11ac.

RESPUESTA 9: b) Que maneja mejor muchos dispositivos al mismo tiempo gracias a tecnologías como OFDMA, con menos congestión. OFDMA divide el canal en pequeñas subporciones que se asignan a distintos dispositivos simultáneamente, así un router WiFi 6 atiende decenas de aparatos sin que se formen cuellos de botella. La opción a) es falsa, el router sigue siendo necesario; la c) es falsa, WiFi 6 no atraviesa mágicamente edificios; la d) es absurda, todo equipo electrónico necesita energía.

RESPUESTA 10: b) La puerta de enlace de tu red local, es decir, tu router, desde donde entras a su panel de configuración. Las direcciones que empiezan con 192.168 son privadas y no existen en internet público; por convención los fabricantes asignan 192.168.1.1 o 192.168.0.1 al router. Al escribirla en el navegador entras a su panel. La opción a) es incorrecta porque el proveedor tiene su propio portal con dirección pública; la c) es incorrecta porque Google usa direcciones públicas; la d) es incorrecta porque tu dirección pública la asigna el proveedor y es distinta.

RESPUESTA 11: b) Asignar automáticamente direcciones IP a los dispositivos que se conectan a la red. DHCP (Dynamic Host Configuration Protocol) reparte direcciones IP privadas, máscara de subred y puerta de enlace a cada dispositivo que se une a la red,

para que no tengas que configurarlos a mano uno por uno. La opción a) es incorrecta porque el cifrado lo hace WPA2/WPA3, no el DHCP; la c) es incorrecta porque la velocidad contratada la define tu plan con el proveedor; la d) es incorrecta porque el bloqueo de páginas es función del control parental o del firewall, no del DHCP.

RESPUESTA 12: b) El nombre visible de tu red inalámbrica, el que aparece en la lista de redes del celular. SSID significa Service Set Identifier y es simplemente cómo se anuncia tu red. Cambiarlo no afecta la seguridad por sí mismo, pero un nombre personalizado evita confundir tu red con la del vecino. La opción a) es incorrecta porque la contraseña de administrador es otro ajuste distinto; la c) es incorrecta porque el nombre no influye en la velocidad; la d) es incorrecta porque el router no tiene "dirección física" configurable de esa forma.

RESPUESTA 13: b) Cifra los datos que viajan por el aire para que solo los dispositivos con la contraseña puedan leerlos. WPA2 usa el cifrado AES para revolver los datos: aunque alguien capture las ondas con una antena, solo verá basura ilegible sin la clave. La opción a) es incorrecta porque ocultar el SSID no cifra nada y es una medida débil por sí sola; la c) es incorrecta porque el cifrado no aumenta la velocidad, de hecho añade una mínima sobrecarga; la d) es incorrecta porque WPA2 no bloquea vecinos, solo impide que lean o usen tu red sin la clave.

RESPUESTA 14: b) Personal usa una sola contraseña compartida para todos, Enterprise usa un servidor que da credenciales individuales a cada usuario. En una casa, todos escriben la misma clave (PSK, Pre-Shared Key). En una empresa, un servidor RADIUS autentica a cada empleado con su propio usuario y contraseña, así si alguien se va se revoca solo su acceso sin cambiar la clave de todos. La opción a) es incorrecta porque la diferencia es real y es justamente el método de autenticación; la c) es incorrecta porque Enterprise no es más lento ni más barato, requiere infraestructura; la d) es incorrecta porque ambos funcionan en cualquier dispositivo compatible.

RESPUESTA 15: b) La protección contra ataques de diccionario y el cifrado individualizado por dispositivo (SAE), que hace mucho más difícil adivinar la clave. WPA3 reemplaza el apretón de manos de WPA2 con SAE (Simultaneous Authentication of Equals): cada intento de adivinar la contraseña obliga al atacante a interactuar con la red, así no puede descargar datos y probar millones de claves en su computadora. Además, cada dispositivo negocia su propia clave de cifrado. La opción a) es falsa, WPA3 sigue usando contraseñas; la c) es falsa, el alcance depende de la banda y la potencia, no del protocolo de seguridad; la d) es falsa porque WPA3 es moderno y de hecho puede no ser compatible con equipos muy viejos.

RESPUESTA 16: b) Irradia la señal en todas direcciones a su alrededor, como una dona o rosquilla. Las antenas tipo "palito" que traen la mayoría de los routers son omnidireccionales: cubren bien en horizontal hacia todos lados, pero con poca ganancia hacia arriba y abajo. La opción a) describe una antena direccional, que es lo opuesto; la c) es falsa porque toda antena necesita conectarse al radio del router; la d) es falsa porque las omnidireccionales se usan tanto dentro como fuera.

RESPUESTA 17: b) Que la señal llegue más lejos en la dirección a la que apunta, aunque la potencia total de transmisión no cambia. Los dBi miden ganancia respecto a una antena ideal: una antena de más dBi no crea más energía, la concentra, como el reflector de una lámpara que no hace más luz pero la dirige. Por eso una antena de alta ganancia sacrifica cobertura en otras direcciones. La opción a) es incorrecta porque la velocidad contratada no depende de la antena; la c) es incorrecta porque el consumo lo define el radio del router; la d) es incorrecta porque la ganancia no tiene nada que ver con la seguridad.

RESPUESTA 18: b) Una antena direccional (tipo panel o yagi) apuntando hacia el patio. Un patio largo y angosto necesita la señal concentrada en una dirección, justo lo que hace una antena direccional. La opción a) desperdiciaría la mitad de la energía hacia el frente de la casa; la c) es un error grave: quitar las antenas deja al router casi sin capacidad de transmitir ni recibir; la d) es un mito peligroso: el metal del refrigerador bloquea las ondas en lugar de amplificarlas y el frío y la humedad danan el equipo.

RESPUESTA 19: b) Recibe la señal del router y la retransmite, extendiendo la cobertura, aunque normalmente a la mitad de la velocidad. El repetidor usa la misma radio para escuchar al router y hablar con tus dispositivos, así que divide su tiempo y el ancho de banda se reduce aproximadamente a la mitad. Además suele crear una red con otro nombre (SSID_EXT). La opción a) es incorrecta porque el repetidor no contrata otro internet, extiende el que ya tienes; la c) es falsa, no cambia contraseñas solo; la d) es falsa porque no convierte nada a datos móviles, sigue siendo WiFi.

RESPUESTA 20: b) Que los nodos crean una sola red unificada con transición suave entre ellos, sin cortes al moverte por la casa. En un sistema mesh todos los nodos comparten el mismo SSID y se coordinan para pasarte de uno a otro (roaming) sin que tu videollamada se corte. La opción a) es incorrecta porque un mesh suele costar más que un repetidor sencillo; la c) es falsa, cada nodo necesita corriente; la d) es falsa porque ningún equipo casero aumenta la velocidad que contrataste con tu proveedor.

RESPUESTA 21: b) A la mitad del camino: donde todavía recibe buena señal del router pero ya está cerca de la zona sin cobertura. Un repetidor solo puede retransmitir la

calidad que recibe: si lo pones en la zona muerta, amplificara una señal débil y el resultado sera malo. El punto ideal es donde la señal aun es fuerte (unas 2 o 3 barras) para que lo que retransmita sea de buena calidad. La opcion a) es el error más común y da el peor resultado; la c) no extiende nada porque queda pegado al origen; la d) es mala idea porque el metal bloquea las ondas de radio.

RESPUESTA 22: a) Darle internet a tus visitas sin darles acceso a tus archivos, impresoras y dispositivos personales. La red de invitados crea un segmento aislado: tus visitas navegan por internet pero no pueden ver tu computadora, tu disco de red ni tus cámaras. La opcion b) es incorrecta porque una red extra no aumenta la velocidad, la comparte; la c) es incorrecta porque la red de invitados es para tu casa, no para conectarte fuera; la d) es incorrecta porque no tiene relacion con cuentas de streaming.

RESPUESTA 23: b) Darle prioridad al trafico importante (videollamadas, juegos, trabajo) sobre el menos urgente (descargas, actualizaciones). QoS clasifica los paquetes y atiende primero los sensibles a la latencia, así tu llamada de trabajo no se entrecorta aunque alguien este descargando. La opcion a) es incorrecta porque ningún router muestra contraseñas ajenas; la c) es incorrecta porque el router no cambia de proveedor solo; la d) es incorrecta porque QoS es gestion de trafico, no un termometro.

RESPUESTA 24: b) Activar QoS y darle prioridad al trafico del juego o a la consola. El lag en juegos no siempre es falta de velocidad, sino competencia: el video en 4K acapara el ancho de banda y los paquetes del juego llegan tarde. Con QoS el router reserva prioridad para la consola y el juego fluye aunque haya streaming. La opcion a) no cambia nada en el trafico; la c) solo interrumpiria todo sin resolver la causa; la d) no existe como funcion: Netflix no se protege con contraseña del router y bloquear el servicio no es la solución elegante.

RESPUESTA 25: b) Un problema de cobertura o interferencia en el trayecto: distancia, paredes o canal saturado. Si junto al router la velocidad es buena, el proveedor y el router están bien; la caída en el cuarto indica que la señal se degrada en el camino. Hay que revisar distancia, obstaculos y saturacion de canales. La opcion a) es una conclusion apresurada sin evidencia; la c) es poco probable si el celular funciona bien cerca del router; la d) usa una analogía enganosa: la señal no "se gasta" como el agua, se atenúa por distancia, obstaculos e interferencia.

RESPUESTA 26: a) La lista de dispositivos conectados en el panel del router y cambiar la contraseña por una fuerte con WPA2 o WPA3. El panel del router muestra que equipos están conectados con su nombre y dirección MAC; si ves desconocidos, alguien entro. La solución es una contraseña nueva, larga y única, con cifrado WPA2 o

WPA3. La opcion b) es una reaccion exagerada que te deja sin servicio; la c) es absurda; la d) es desproporcionada: primero se verifica y se corrige, la via legal es el último recurso y solo con pruebas.

RESPUESTA 27: b) Ver que canales están saturados a tu alrededor y elegir el más libre para tu router. Un analizador muestra las redes vecinas, su intensidad y el canal que usan, con graficas claras. Con esa informacion eliges el canal menos congestionado (en 2.4 GHz, entre 1, 6 y 11). La opcion a) es incorrecta y además ilegal: la herramienta es para diagnostico, no para intrusiones; la c) es incorrecta porque ninguna app aumenta tu velocidad contratada; la d) es incorrecta porque tu IP publica la asigna el proveedor, no una app.

RESPUESTA 28: b) Otros usuarios de la misma red podrian interceptar tus datos no cifrados con tecnicas de espionaje. En una red abierta o compartida, el trafico puede ser capturado del aire por cualquiera con las herramientas adecuadas; si un sitio no usa cifrado (HTTPS), tus datos viajan legibles. La opcion a) es irrelevante para la seguridad; la c) puede ser cierta en la práctica pero no es el riesgo de seguridad; la d) es una exageracion: no todas las redes publicas tienen malware, el riesgo real es la intercepcion de datos.

RESPUESTA 29: b) Usar una VPN, que cifra todo tu trafico aunque la red sea insegura. Una VPN crea un tunel cifrado entre tu dispositivo y un servidor confiable: aunque alguien intercepte las ondas del cafe, solo vera datos ilegibles. Es la proteccion estandar para trabajar fuera de casa. La opcion a) solo evita miradas curiosas sobre tu hombro, no protege los datos; la c) es un mito: la velocidad de conexión no te hace invisible; la d) no tiene sentido técnico como medida de seguridad.

RESPUESTA 30: b) Se esperan velocidades multi-gigabit, menor latencia y mejor manejo de muchos dispositivos, con bandas como 6 GHz. WiFi 7 (802.11be) apunta a canales de hasta 320 MHz, operación multi-banda simultanea y latencias bajisimas para realidad virtual y juegos en la nube; la banda de 6 GHz, estrenada con WiFi 6E, da espectro limpio adicional. La opcion a) es falsa, la seguridad seguira siendo necesaria; la c) va contra toda la tendencia, lo inalámbrico crece; la d) es una broma, no una tecnología real.

RESPUESTA 31: Verdadero. Tanto las ondas de radio del WiFi como la luz visible son radiación electromagnética: la misma naturaleza física, campos eléctricos y magnéticos oscilando y propagándose por el espacio. La única diferencia es la frecuencia a la que vibran: la luz visible oscila muchísimo más rápido (cientos de terahertz) que las ondas del WiFi (2.4 o 5 gigahertz). Esa diferencia de frecuencia es la que hace que unas las vean tus ojos y las otras las capte la antena de tu celular.

RESPUESTA 32: Falso. El canal 3 se traslapa con el canal 1 y con el canal 6, así que usarlo no evita a nadie: interfiere con los vecinos de ambos lados y ellos interfieren contigo. En 2.4 GHz los únicos canales que no se traslapan son 1, 6 y 11, por eso son los recomendados. Usar un canal intermedio como el 3 es peor que sumarse ordenadamente a uno de los tres canales "limpios", porque genera interferencia con dos grupos de redes en lugar de convivir con uno solo.

RESPUESTA 33: Verdadero. Los estándares WiFi están diseñados para ser compatibles hacia atrás: un router 802.11ac habla también 802.11n, 802.11g y 802.11a. Cuando se conecta un dispositivo viejo, ambos negocian el mejor estándar que los dos entiendan, que será el del dispositivo más antiguo. Por eso el celular viejo si se conecta, pero a velocidades 802.11n, mientras tus dispositivos nuevos siguen usando 802.11ac con el mismo router.

RESPUESTA 34: Falso. El DHCP es el que reparte direcciones IP automáticamente; si lo desactivas, los dispositivos nuevos no recibirán dirección y no sabrán cómo salir a internet. Para que la red siga funcionando tendrías que asignar a mano una IP estática, la máscara y la puerta de enlace en cada dispositivo, cosa tediosa y propensa a errores (como asignar dos veces la misma IP). Desactivar el DHCP sin configurar IPs estáticas deja a los equipos conectados al WiFi pero sin acceso real a la red.

RESPUESTA 35: Falso. Ocultar el SSID solo evita que el nombre aparezca en la lista, pero la red sigue transmitiendo y su nombre viaja en las tramas de gestión, así que cualquiera con una herramienta básica la descubre en segundos. Es como quitarle el letrero a una tienda pero dejar la puerta abierta: no impide la entrada. La verdadera protección es el cifrado WPA2 o WPA3 con una contraseña fuerte; el SSID oculto como única medida deja la red completamente expuesta.

RESPUESTA 36: Verdadero. La ganancia en dBi no crea energía de la nada: la potencia de transmisión la fija el radio del router y esta limitada por la ley. Lo que hace una antena de mayor ganancia es concentrar esa misma energía en un patrón más estrecho, igual que una lámpara con reflector ilumina más lejos en una dirección pero menos hacia los lados. Por eso una antena de alta ganancia mejora el alcance en su dirección de apunte a costa de reducir la cobertura en otras direcciones.

RESPUESTA 37: Verdadero. Esa es una de las grandes ventajas del mesh: los nodos forman una malla donde cada uno conoce varias rutas hacia los demás. Si un nodo intermedio se apaga, el sistema recalcula y el tráfico viaja por otro camino, igual que cuando cierran una calle y el navegador te manda por otra. A esto se le llama auto-reparación (self-healing) y es lo que hace a las redes mesh mucho más robustas que un simple repetidor en cadena.

RESPUESTA 38: Verdadero. La red de invitados crea un segmento separado y aislado del resto de tu red local: los visitantes obtienen internet pero el router les bloquea el acceso a tus computadoras, discos compartidos, impresoras y dispositivos inteligentes. Por eso es la forma correcta de compartir internet: das la clave de invitados y tu clave principal, la que protege tus cosas, sigue siendo solo tuya. Dar la clave principal a las visitas expone todos tus dispositivos.

RESPUESTA 39: Verdadero. El reinicio es el primer paso clásico del diagnóstico porque resuelve una gran cantidad de fallas temporales: tablas de memoria corruptas, sesiones atoradas, direcciones IP vencidas o procesos del router trabados. Apagarlo 30 segundos permite que los capacitores se descarguen y el equipo arranque limpio. Si después del reinicio todo vuelve a funcionar, fue una falla transitoria; si no, se sigue con el resto del diagnóstico (cables, proveedor, configuración).

RESPUESTA 40: Falso. La contraseña de una red pública normalmente solo controla quién entra a la red, no cifra tu tráfico de forma individual: todos los conectados comparten el medio y un atacante en la misma red puede interceptar datos no cifrados. Además, nada garantiza que el dueño de la red sea honesto. Para operaciones bancarias en una red pública lo seguro es verificar que el sitio use HTTPS (candado en el navegador) y, mejor aun, usar una VPN que cifre todo tu tráfico.

RESPUESTA 41: La frecuencia es cuantas veces oscila la onda por segundo y se mide en Hertz: 2.4 GHz significa 2,400 millones de oscilaciones por segundo. La longitud de onda es la distancia física que recorre la onda en una oscilación completa. Se relacionan de forma inversa: a mayor frecuencia, menor longitud de onda, porque la onda vibra más rápido y "avanza menos" entre cada ciclo (longitud de onda = velocidad

de la luz / frecuencia). La banda de 2.4 GHz tiene una longitud de onda de unos 12.5 centímetros, mientras que la de 5 GHz anda por los 6 centímetros. Las ondas más largas (2.4 GHz) "rodean" mejor los obstáculos y los atraviesan con menos pérdida, como las olas grandes del mar que pasan por encima de rocas pequeñas; las ondas cortas (5 GHz) chocan más con los obstáculos y pierden energía más rápido, aunque a cambio pueden transportar más datos por segundo. Por eso 5 GHz es más veloz cerca del router y 2.4 GHz llega más lejos y atraviesa mejor las paredes.

RESPUESTA 42: Respuesta modelo paso a paso. Primero, diagnosticar: 1) Preguntarle a que banda está conectado (2.4 o 5 GHz) y hacer una prueba de velocidad junto al router para saber si el problema es del proveedor o del WiFi. 2) Instalar en su celular un analizador de WiFi y ver cuántas redes hay y en que canales están: en un edificio con 20 redes, lo normal es encontrar los canales 1, 6 y 11 saturados. 3) Revisar en que canal está su router y cuántas redes lo comparten. Después, mejorar: 4) Cambiar manualmente su router al canal menos congestionado entre 1, 6 y 11 (nunca a un canal intermedio como 3 o 9, que se traslapa con dos). 5) Si su router y sus dispositivos lo soportan, mover los equipos importantes a la banda de 5 GHz, que tiene más canales y casi no la usan los vecinos. 6) Como medida extra, reducir el ancho de canal a 20 MHz en 2.4 GHz para interferir menos, y colocar el router en un punto alto y centrado del departamento. Con esto, el vecino debería notar una mejora clara sin gastar un peso.

RESPUESTA 43: Respuesta modelo. El 802.11n (WiFi 4) fue el salto a la velocidad moderna: introdujo MIMO con varias antenas y el uso de la banda de 5 GHz, llevando las redes caseras de 54 Mbps teóricos a 300-450 Mbps; en la práctica lo notas cuando por fin puedes ver video en HD sin cortes. El 802.11ac (WiFi 5) se concentró en 5 GHz con canales más anchos (80 y 160 MHz) y más flujos MIMO, acercándose al gigabit; lo notas al copiar archivos grandes en tu red local o al tener varias personas viendo streaming 4K al mismo tiempo sin que nadie se trabe. WiFi 6 (802.11ax) no busca tanto más velocidad pico como eficiencia con muchos dispositivos: con OFDMA y mejor manejo de la congestión, atiende decenas de aparatos (celulares, focos, teles, asistentes) sin degradarse; lo notas en una casa llena de dispositivos inteligentes donde antes todo se ponía lento a ciertas horas. En resumen: n te dio velocidad, ac te dio más velocidad en 5 GHz, y ax te dio orden y eficiencia cuando hay muchos equipos conectados.

RESPUESTA 44: Respuesta modelo. Paso 1: conectar la computadora al router por cable o al WiFi con los datos de fábrica (vienen en una etiqueta debajo del equipo). Paso 2: abrir el navegador y escribir la puerta de enlace, normalmente 192.168.1.1 o 192.168.0.1, e iniciar sesión con el usuario y clave de fábrica (admin/admin es lo típico, y hay que cambiarlos). Los 5 ajustes básicos serían: 1) Cambiar la contraseña de

administrador del router por una fuerte y única, para que nadie más entre al panel. 2) Ponerle un nombre (SSID) personalizado a la red, fácil de reconocer y sin datos personales. 3) Activar WPA2 o WPA3 (nunca WEP ni red abierta) con una contraseña larga de al menos 12 caracteres. 4) Verificar que el DHCP esté activado para que los dispositivos reciban IP automáticamente, y revisar que el firmware esté actualizado. 5) Crear la red de invitados con su propia clave para las visitas. Con esos cinco pasos la red queda funcional y con un nivel de seguridad decente desde el primer día.

RESPUESTA 45: Respuesta modelo. Cuando escribes la contraseña en tu celular, este no la manda tal cual por el aire: la usa para derivar, junto con datos de una negociación con el router (el "apretón de manos" de 4 pasos), las claves temporales de cifrado de la sesión. A partir de ahí, cada paquete de datos se cifra con AES antes de transmitirse. Un vecino que capture las ondas con una antena solo obtendrá datos revueltos e ilegibles, porque no tiene la contraseña para derivar las claves. Además, las claves de sesión cambian y cada paquete lleva protección contra alteraciones, así que tampoco puede modificar los datos sin que se detecte. WPA2 tiene una debilidad conocida: si el atacante captura el apretón de manos inicial, puede llevarse a su computadora e intentar adivinar la contraseña probando millones de combinaciones (ataque de diccionario) sin que el router se entere. WPA3 corrige esto con SAE: cada intento de adivinanza obliga a interactuar con el router, que puede bloquear los intentos repetidos, y además cada dispositivo negocia su propia clave individual, así que ni siquiera dos equipos de la misma red comparten la misma clave de cifrado.

RESPUESTA 46: Respuesta modelo. Opción 1, cambiar antenas: es lo más barato (unas antenas de mayor ganancia cuestan poco), pero solo ayuda si el problema es de alcance en una dirección; entre pisos, la señal debe atravesar la losa y una antena no hace milagros contra el concreto. Opción 2, repetidor: cuesta poco y es fácil de instalar, pero retransmite a la mitad de la velocidad y si se coloca mal (en la zona sin señal) el resultado es pobre; sirve como remedio rápido para un par de cuartos. Opción 3, sistema mesh: es lo más caro, pero crea una red unificada con buena transición entre pisos, se auto-repara si un nodo falla y mantiene mejor velocidad porque los nodos se comunican entre sí de forma inteligente. Recomendación: para una casa de dos pisos de uso diario, el sistema mesh de 2 o 3 nodos (uno por piso más el principal) es la mejor inversión, porque resuelve el problema de raíz y da una experiencia sin cortes al subir y bajar; el repetidor solo lo recomendaría si el presupuesto es muy ajustado y la zona a cubrir es pequeña.

RESPUESTA 47: Respuesta modelo. El QoS (Quality of Service) es la función del router que clasifica el tráfico y decide qué paquetes atiende primero cuando la red se satura,

como un policia de transito que le abre paso a las ambulancias. En esta familia hay tres necesidades distintas: el papá necesita latencia baja y estable para sus videollamadas (poco ancho de banda pero constante), la hija necesita mucho ancho de banda sostenido para el 4K, y el hijo necesita latencia minima y sin picos para el juego en línea. Las reglas que configuraria serían: 1) Prioridad máxima al trafico de videollamadas y juegos (puertos y aplicaciones sensibles a latencia), porque un corte en una llamada de trabajo o un pico de lag arruinan la experiencia aunque duren segundos. 2) Prioridad media-alta a la consola o PC del hijo por dirección MAC o IP, para garantizarle su carril. 3) El streaming de video en prioridad normal: el 4K usa mucho ancho de banda pero los servicios tienen buffer de varios segundos, así que toleran pequeñas variaciones sin que se note. 4) Las descargas, actualizaciones y respaldos en la nube en prioridad baja, para que usen solo el ancho de banda sobrante. Así, cuando todos usan la red a la vez, el trabajo y el juego no se enteran de que alguien esta viendo series.

RESPUESTA 48: Respuesta modelo, en orden logico de lo simple a lo complejo. Paso 1: verificar lo fisico, que el router y el módem esten encendidos, con sus luces normales, y que los cables esten bien conectados (a veces solo se safo el cable del módem). Paso 2: reiniciar módem y router (apagar 30 segundos, encender primero el módem, esperar 2 minutos y luego el router), porque la mayoría de las fallas repentinas son transitorias. Paso 3: probar con cable directo al módem o al router: si por cable si hay internet, el problema es solo el WiFi; si ni por cable hay, el problema está antes. Paso 4: revisar las luces del módem: si la luz de internet o de línea esta apagada o parpadeando en rojo, la falla es del proveedor o de la línea. Paso 5: entrar al panel del router y ver el estado de la conexión WAN y si tiene IP publica; sin IP, el router no esta logrando conectarse. Paso 6: probar con otro dispositivo para descartar que sea un solo equipo. Paso 7: si todo lo anterior falla, llamar al proveedor y reportar con los datos ya verificados (luces, pruebas hechas), lo que acelera el soporte. Este orden evita perder tiempo: se descartan primero las causas más comunes y baratas antes de escalar.

RESPUESTA 49: Respuesta modelo. Plan de seguridad para trabajar con informacion sensible en WiFi público. Herramientas: 1) Una VPN confiable instalada y configurada para conectarse automaticamente, que cifre todo mi trafico. 2) Verificar que todos los sitios de trabajo usen HTTPS (candado en el navegador) y activar la verificacion en dos pasos en mis cuentas. 3) Tener el firewall del sistema operativo activado y el sistema actualizado. Que haria: conectarme siempre con la VPN antes de abrir cualquier aplicacion de trabajo; usar la red del establecimiento solo para navegar y trabajar, nunca para mover archivos ultra sensibles si puedo esperar a una red segura; al terminar, olvidar la red para que mi dispositivo no se reconecte solo después. Que

evitaria: hacer operaciones bancarias o manejar contraseñas maestras en la red pública aunque tenga VPN; conectarme a redes con nombres sospechosos o gemelos ("Cafe_Gratis" junto a "Cafe Oficial"), que pueden ser trampas; dejar el WiFi y el Bluetooth encendidos cuando no los uso; y descargar archivos o actualizaciones desde redes públicas. La regla de oro: en una red pública, actúa como si alguien estuviera mirando todo lo que no va cifrado.

RESPUESTA 50: Respuesta modelo de propuesta. Estandar WiFi: propondría equipos WiFi 6 (802.11ax), porque 15 empleados más sus celulares y visitantes suman fácilmente 40 o más dispositivos, y WiFi 6 maneja esa densidad sin congestionarse; además es compatible con equipos viejos. Bandas: usaría doble banda, 5 GHz como principal para los equipos de trabajo (más velocidad y menos interferencia) y 2.4 GHz para dispositivos de bajo consumo (impresoras, sensores) y como respaldo de cobertura. Organización de redes: tres SSID, la red corporativa solo para equipos de la empresa, una red de invitados aislada para clientes y visitas, y de ser posible una red separada para dispositivos IoT; cada una con su propia contraseña y sin comunicación entre sí. Seguridad: WPA3-Enterprise si hay un servidor para credenciales por empleado, o al menos WPA3-Personal con contraseña larga y cambio periódico; contraseña de administrador del router cambiada y firmware actualizado. Cobertura: un estudio rápido del local para ubicar el o los puntos de acceso en el techo al centro de cada área, considerando que las paredes de concreto atenúan la señal; si la oficina es grande o tiene muros gruesos, un sistema mesh empresarial o dos puntos de acceso cableados. Finalmente, documentaría las claves y la configuración y dejaría un plan básico de mantenimiento: revisión de firmware cada tres meses y cambio de contraseña de invitados cada mes.

Nota final

Si llegaste hasta aquí y revisaste tus respuestas con honestidad, ya hiciste lo más difícil: enfrentarte a lo que no sabías. Un examen no mide tu valor como técnico, mide tu mapa: ahora sabes exactamente qué unidades dominas y cuáles necesitan otra vuelta. Las redes inalámbricas se aprenden haciendo, así que el siguiente paso es práctico: entra al panel de tu router y cambia un canal, instala un analizador de WiFi en tu celular y mira las redes de tus vecinos, activa la red de invitados y el QoS aunque sea para probar. Cada ajuste que hagas con tus propias manos vale más que diez relecturas. Y cuando sientas que ya dominas este libro, vuelve a hacer el examen en un mes: si sacas más de 90 sin dudar, estás listo para el siguiente nivel. Sigue aprendiendo en lucasegaacademy.com.

Curso Completo de Wireless

Bienvenido a "Curso Completo de Redes Inalámbricas (Wireless)", el libro de Lucas EGA Academy para entender de una vez por todas ese mundo invisible que te conecta con todo: el WiFi. 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 para aplicar en tu casa o tu negocio, prácticas con soluciones explicadas y un examen final para medir lo que aprendiste.

lucasegaacademy.com

Colibrí Editorial EGA