

Material de estudio

¿Qué es un servidor?

El término servidor tiene dos significados en el ámbito informático. El primero hace referencia al ordenador que pone recursos a disposición a través de una red, y el segundo se

refiere al programa que funciona en dicho ordenador. En consecuencia aparecen dos definiciones de servidor:

Definición Servidor (hardware): un servidor basado en hardware es una máquina física integrada en una red informática en la que, además del sistema operativo, funcionan uno o varios servidores basados en software. Una denominación alternativa para un servidor basado en hardware es "host" (término inglés para "anfitrión"). En

principio, todo ordenador puede usarse como "host" con el correspondiente software

para servidores.

Definición Servidor (software): un servidor basado en software es un programa que ofrece un servicio especial que otros programas denominados clientes (clients) pueden usar a nivel local o a través de una red. El tipo de servicio depende del tipo de software del servidor. La base de la comunicación es el modelo cliente-servidor y, en lo que concierne al intercambio de datos, entran en acción los protocolos de transmisión específicos del servicio.

¿Cómo funciona un servidor?

La puesta a disposición de los servicios del servidor a través de una red informática se basa

en el modelo cliente-servidor, concepto que hace posible distribuir las tareas entre los diferentes ordenadores y hacerlas accesibles para más de un usuario final de manera independiente. Cada servicio disponible a través de una red será ofrecido por un servidor (software) que está permanentemente en espera. Este es el único modo de asegurar que los

clientes como el navegador web o los clientes de correo electrónico siempre tengan la posibilidad de acceder al servidor activamente y de usar el servicio en función de sus necesidades.

Tipos de servidores

La comunicación entre cliente y servidor depende de cada servicio y se define por medio de

un protocolo de transmisión. Este principio puede aclararse partiendo de los siguientes tipos

de servidores:

Servidor web: la tarea principal de un servidor web es la de guardar y organizar páginas web y entregarlas a clientes como navegadores web o crawlers. La comunicación entre servidor (software) y cliente se basa en HTTP, es decir, en el protocolo de transferencia de hipertexto o en HTTPS, la variante codificada. Por regla general, se transmiten documentos HTML y los elementos integrados en ellos, tales como imágenes, hojas de estilo o scripts. Los servidores web más populares son el servidor HTTP Apache, los servicios de Internet Information Server de Microsoft (ISS) o el servidor Nginx.

2

Servidor de archivos: un servidor de archivos se encarga de almacenar los datos a los que acceden los diferentes clientes a través de una red. Las empresas apuestan por dicha gestión de archivos para que sea mayor el número de grupos de trabajo que tengan acceso a los mismos datos. Un servidor de archivos contrarresta los conflictos originados por las diferentes versiones de archivos locales y hace posible tanto la creación automática de las diferentes versiones de datos como la realización de una copia de seguridad central de la totalidad de datos de la empresa. En el acceso al servidor de archivos por medio de Internet entran en juego protocolos de transmisión como FTP (File Transfer Protocol), SFTP (Secure File Transfer Protocol), FTPS (FTP over SSL) o SCP (Secure Copy). Los protocolos SMB (Server Message Block) y NFS (Network File System) se encuentran habitualmente en las redes de área locales (LAN).

Servidor de correo electrónico: un servidor de correo electrónico consta de varios módulos de software cuya interacción hace posible la recepción, el envío y el reenvío de correos electrónicos, así como su puesta a punto para que estén disponibles. Por


regla general funciona mediante el protocolo de transferencia simple de correo (SMTP). Los usuarios que quieran acceder a un servidor de correo electrónico necesitan un cliente de correo electrónico que recoja los mensajes del servidor y los entregue en la bandeja de entrada, proceso que tiene lugar a través de los protocolos IMAP (Internet Message Access Protocol) o POP (Post Office Protocol).

Servidor de base de datos: un servidor de base de datos es un programa informático que posibilita que otros programas puedan acceder a uno o varios sistemas de bases de datos a través de una red. Las soluciones de software con una elevada cuota de mercado son Oracle, MySQL, Microsoft SQL Server, PostgreSQL y DB2. Los servidores de bases de datos ayudan a los servidores web, por regla general, a la hora de almacenar y entregar datos.

Servidor de juegos: los servidores de juegos son servidores (software) creados específicamente para juegos multijugador online. Estos servidores gestionan los datos del juego online y permiten la interacción sincrónica con el mundo virtual. La base de hardware de un servidor de juegos se encuentra en el centro de datos de los proveedores especializados o está disponible en una red doméstica local.

Servidor proxy: el servidor proxy sirve como interfaz de comunicación en las redes informáticas. En su papel de intermediario, el servidor proxy recibe las solicitudes de red y las transmite a través de su propia dirección IP. Los servidores proxy se usan para filtrar la comunicación, para controlar el ancho de banda, para aumentar la disponibilidad a través del reparto de cargas, así como para guardar datos temporalmente (caching). Además, los servidores proxy permiten una amplia anonimización, ya que la dirección IP del cliente queda oculta en el proxy.

Servidor DNS: el servidor DNS o servidor de nombres permite la resolución de nombres en una red. Los servidores DNS son de vital importancia para la red informática mundial (WWW), ya que traducen los nombres de host como www.example.com en la correspondiente dirección IP. Si quieres saber más sobre los servidores de nombres y sobre el sistema de nombres de dominio (DNS), visita nuestra guía digital.



En teoría, un único dispositivo físico puede alojar diferentes tipos de servidores. Sin embargo,

es habitual alojar cada uno de los servidores en un ordenador independiente o que estos se repartan en más de un ordenador. De esta manera, se evita que la utilización del hardware

de un servicio repercuta en el rendimiento de otros servicios.

2

¿En qué consiste el alojamiento de servidores?

Mientras que a las grandes empresas les sale rentable la adquisición de hardware de servidores, los autónomos y los particulares que quieren desarrollar proyectos en un servidor

propio recurren normalmente al alquiler. Los proveedores especializados ofrecen diferentes

modelos de servidores de alquiler en los que los usuarios no tienen que preocuparse por el

funcionamiento de la máquina física. La gama de productos abarca desde servidores dedicados cuyos componentes de hardware se ponen a disposición de los usuarios de manera exclusiva, hasta servicios de hosting compartido para alojar a varios clientes virtuales en una base de hardware común. Para obtener más información, visita nuestra guía

sobre las ventajas y los inconvenientes de los diferentes modelos de alojamiento.

¿Qué es una RED?

Es la interconexión de 2 o más dispositivos.

En una red se interconectan 2 dispositivos mínimo, los mismos pueden o ser similares, como por ejemplo 2 pc entre sí, o bien pueden ser distintos como una pc con un teléfono celular.

Siempre la intención de esta interconexión es el compartir datos, pero no por eso es que siempre la interconexión entre los dispositivos es la misma o de similar manera.

Podemos encontrar que para interconectarse los 2 dispositivos necesitan de un programa o app, y es necesario de el tener e mismo en ambos sistemas funcionando para que se puedan ver o conectarse entre si.

También encontramos que estas redes conforman distintas topologías para poder funcionar de la forma más óptima, de acuerdo al espacio geográfico y la distribución necesaria para su funcionamiento; así como también es que estas topologías pueden depender de la cantidad de dispositivos que se conecten en nuestra red.

Los tipos de topologías de redes son:

1. Punto a punto.
2. Bus.
3. Estrella
4. Anillo o círculo
5. Malla
6. Árbol
7. Híbrida o mixta

Punto a punto

La topología más simple es un enlace permanente entre dos puntos finales (también conocida como point-to-point, o abreviadamente, PtP). La topología punto a punto conmutado es el modelo básico de la telefonía convencional. El valor de una red permanente de punto a punto la comunicación sin obstáculos entre los dos puntos finales. El valor de una conexión punto-a-punto a demanda es proporcional al número de pares posibles de abonados y se ha expresado como la ley de Metcalfe.

Topología en Bus

Topología de bus En la topología de bus todos los nodos (computadoras) están conectados a un circuito común (bus). La información que se envía de una computadora a otra viaja directamente o indirectamente, si existe un controlador que enruta los datos al destino correcto. La información viaja por el cable en ambos sentidos a una velocidad aproximada de 10/100 Mbps y tiene en sus dos extremos una resistencia (terminador). Se pueden conectar una gran cantidad de computadoras al bus, si un computador falla, la comunicación se mantiene, no sucede lo mismo si el bus es el que falla. El tipo de cableado que se usa puede ser coaxial, par trenzado o fibra óptica. En una topología de bus, cada computadora está conectada a un segmento común de cable de red. El segmento de red se coloca como un bus lineal, es decir un cable largo que va de un extremo a otro de la red, y al cual se conecta cada nodo de ésta. El cable puede ir por el piso, las paredes, el techo o por varios lugares, siempre y cuando sea un segmento continuo.

La topología en estrella

Reduce la posibilidad de fallo de red conectando todos los nodos a un nodo central. Cuando se aplica a una red basada en la topología estrella este concentrador central reenvía todas las transmisiones recibidas de cualquier nodo periférico a todos los nodos periféricos de la red, algunas veces incluso al nodo que lo envió. Todos los nodos periféricos se pueden comunicar con los demás transmitiendo o recibiendo del nodo central solamente. Un fallo en la línea de conexión de cualquier nodo con el nodo central provocaría el aislamiento de ese nodo respecto a los demás, pero el resto de sistemas permanecería intacto. El tipo de concentrador hub se utiliza en esta topología, aunque ya es muy obsoleto; se suele usar comúnmente un switch.

La desventaja radica en la carga que recae sobre el nodo central. La cantidad de tráfico que deberá soportar es grande y aumentará conforme vayamos agregando más nodos periféricos, lo que la hace poco recomendable para redes de gran tamaño. Además, un fallo en el nodo central puede dejar inoperante a toda la red. Esto último conlleva también una mayor vulnerabilidad de la red, en su conjunto, ante ataques.

Topología en Anillo

Si el nodo central es pasivo, el nodo origen debe ser capaz de tolerar un eco de su transmisión. Una red, en estrella activa, tiene un nodo central activo que normalmente tiene los medios para prevenir problemas relacionados con el eco.

Una red en anillo es una topología de red en la que cada estación tiene una única conexión de entrada y otra de salida. Cada estación tiene un receptor y un transmisor que hace la función de traductor, pasando la señal a la siguiente estación. En este tipo de red la comunicación se da por el paso de un token o testigo, que se puede conceptualizar como un cartero que pasa recogiendo y entregando paquetes de información, de esta manera se evitan eventuales pérdidas de información debidas a colisiones. En un anillo doble (Token Ring), dos anillos permiten que los datos se envíen en ambas direcciones (Token passing). Esta configuración crea redundancia (tolerancia a fallos). Evita las colisiones.

La topología en árbol

(También conocida como topología jerárquica) puede ser vista como una colección de redes en estrella ordenadas en una jerarquía. Éste árbol tiene nodos periféricos individuales (por ejemplo hojas) que requieren transmitir a y recibir de otro nodo solamente y no necesitan actuar como repetidores o regeneradores. Al contrario que en las redes en estrella, la función del nodo central se puede distribuir.

Como en las redes en estrella convencionales, los nodos individuales pueden quedar aislados de la red por un fallo puntual en la ruta de conexión del nodo. Si falla un enlace que conecta con un nodo hoja, ese nodo hoja queda aislado; si falla un enlace con un nodo que no sea hoja, la sección entera queda aislada del resto.

Para aliviar la cantidad de tráfico de red que se necesita para retransmitir en su totalidad, a todos los nodos, se desarrollaron nodos centrales más avanzados que permiten mantener un listado de las identidades de los diferentes sistemas conectados a la red. Éstos switches de red “aprenderían” cómo es la estructura de la red transmitiendo paquetes de datos a todos los nodos y luego observando de dónde vienen los paquetes de respuesta también es utilizada como un enchufe u artefacto.

Topología en Malla

La topología de red mallada es una topología de red en la que cada nodo está conectado a todos los nodos. De esta manera es posible llevar los mensajes de un nodo a otro por distintos caminos. Si la red de malla está completamente conectada, no puede existir absolutamente ninguna interrupción en las comunicaciones. Cada servidor tiene sus propias conexiones con todos los demás servidores. Las redes de malla son auto ruteables. La red puede funcionar, incluso cuando un nodo desaparece o la conexión falla, ya que el resto de los nodos evitan el paso por ese punto. En consecuencia, la red malla, se transforma en una red muy confiable.

Topología Híbrida o Mixta

Topología híbrida, las redes pueden utilizar diversas topologías para conectarse, como por ejemplo en estrella. La topología híbrida es una de las más frecuentes y se deriva de la unión de varios tipos de topologías de red, de aquí el nombre de híbridas. Ejemplos de topologías híbridas serían: en árbol, estrella-estrella, bus-estrella, etc.

Su implementación se debe a la complejidad de la solución de red, o bien al aumento en el número de dispositivos, lo que hace necesario establecer una topología de este tipo. Las topologías híbridas tienen un costo muy elevado debido a su administración y mantenimiento, ya que cuentan con segmentos de diferentes tipos, lo que obliga a invertir en equipo adicional para lograr la conectividad deseada.

También encontramos que las redes se dividen de acuerdo a su alcance y esto nos da las siguientes redes:

- Personal Área Networks (PAN) o red de área personal
- Local Área Networks (LAN) o red de área local

- Metropolitan Área Networks (MAN) o red de área metropolitana
- Wide Área Networks (WAN) o red de área amplia
- Global Área Networks (GAN) o red de área global

Personal Area Network (PAN)

Para llevar a cabo un intercambio de datos, los terminales modernos como smartphones, tablets, ordenadores portátiles o equipos de escritorio permiten asociarse *ad hoc* a una red. Esto puede realizarse por cable y adoptar la forma de una Personal Área Network (PAN) o red de área personal, aunque las técnicas de transmisión más habituales son la **memoria USB** o el **conector FireWire**. La variante inalámbrica **Wireless Personal Área Network (WPAN)** se basa en técnicas como Bluetooth, Wireless USB, Insteon, IrDA, ZigBee o Z-Wave. Una Personal Área Network inalámbrica que se lleva a cabo vía Bluetooth recibe el nombre de **Piconet**. El ámbito de acción de las redes PAN y WPAN se limita normalmente a unos pocos metros y, por lo tanto, no son aptas para establecer la conexión con dispositivos que se encuentran en habitaciones o edificios diferentes.

Además de establecer la comunicación entre cada uno de los dispositivos entre sí, las redes de área personal (Personal Área Networks) permiten, asimismo, la conexión con otras redes de mayor tamaño. En este caso se puede hablar de un **uplink** o de un enlace o conexión de subida. Debido al alcance limitado y a una tasa de transmisión de datos relativamente baja, las PAN se utilizan principalmente para conectar periféricos en el ámbito del ocio y de los hobbies. Algunos ejemplos típicos son los auriculares inalámbricos, las videoconsolas y las cámaras digitales. En el marco del **Internet of Things (IoT)** las redes WPAN se utilizan para la comunicación de las aplicaciones de control y monitorización con una frecuencia de transferencia baja. A este respecto, los protocolos como Insteon, Z-Wave y ZigBee han sido diseñados especialmente para la domótica y para la automatización del hogar.

Local Area Network (LAN)

Si una red está formada por más de un ordenador, esta recibe el nombre de Local Área Network (LAN). Una red local de tales características puede incluir a dos ordenadores en una vivienda privada o a varios miles de dispositivos en una empresa. Asimismo, las redes en instituciones públicas como administraciones, colegios o universidades también son redes LAN. Un estándar muy frecuente para redes de área local por cable es **Ethernet**. Otras opciones menos comunes y algo obsoletas son las tecnologías de red ARCNET, FDDI y Token Ring. La transmisión de datos tiene lugar o bien de manera electrónica **a través de cables de cobre** o mediante **fibra óptica de vidrio**.

Si se conectan más de dos ordenadores en una red LAN, se necesitan otros componentes de red como hubs, bridges y switches, es decir, concentradores, puentes de red y conmutadores, los cuales funcionan como elementos de acoplamiento y nodos de distribución. El tipo de red conocido como LAN o red de área local fue desarrollado para posibilitar la **rápida transmisión de cantidades de datos más grandes**. En función de la estructura de la red y del medio de transmisión utilizado se puede hablar de un rendimiento de 10 a 1.000 Mbit/s. Asimismo, las redes LAN permiten un intercambio de información cómodo entre los diversos dispositivos conectados a la red. Por ello, en el entorno empresarial es habitual que varios equipos de trabajo puedan acceder a servidores de archivos comunes, a impresoras de red o a aplicaciones por medio de la red LAN.

Si la red local tiene lugar de manera inalámbrica, se puede hablar en este caso de una **Wireless Local Área Network (WLAN)** o red de área local inalámbrica y los fundamentos básicos de los estándares de la red WLAN quedan definidos por la familia de normas IEEE 802.11. Las redes locales inalámbricas ofrecen la posibilidad de integrar terminales cómodamente en una red doméstica o empresarial y son compatibles con redes LAN Ethernet, aunque el rendimiento es, en este caso, algo menor que el de una conexión Ethernet.

El alcance de una Local Área Network depende tanto del estándar usado como del medio de transmisión y aumenta a través de un amplificador de señal que recibe el nombre de repetidor (**repeater**). En el caso de la ampliación Gigabit Ethernet por medio de fibra de vidrio, se puede llegar a un alcance de señal de varios kilómetros. No resulta muy habitual, sin embargo, que las Local Área Networks estén formadas por más de una estructura. El grupo de redes LAN geográficamente cercanas puede asociarse a una **Metropolitan Área Network (MAN)** o **Wide Área Network (WAN)** superiores.

Metropolitan Area Network (MAN)

La Metropolitan Área Network (MAN) o red de área metropolitana es una red de telecomunicaciones de banda ancha que comunica varias redes LAN en una zona geográficamente cercana. Por lo general, se trata de cada una de las sedes de una empresa que se agrupan en una MAN por medio de **líneas arrendadas**. Para ello, entran en acción routers de alto rendimiento basados en fibra de vidrio, los cuales permiten un rendimiento mayor al de Internet y la velocidad de transmisión entre dos puntos de unión distantes es comparable a la comunicación que tiene lugar en una red LAN.

Los operadores que desempeñan actividades internacionales son los encargados de poner a disposición la infraestructura de las redes MAN. De esta manera, las ciudades conectadas mediante Metropolitan Área Networks pueden contar a nivel suprarregional con **Wide Área Networks (WAN)** y a nivel internacional con **Global Área Networks (GAN)**.

Para una red MAN, la red **Metro Ethernet** supone una técnica especial de transmisión con la que se pueden construir redes **MEN (Metro Ethernet Network)** sobre la base de Carrier Ethernet (CE 1.0) o Carrier Ethernet 2.0 (CE 2.0).

El estándar para redes inalámbricas regionales de mayor envergadura, es decir, las denominadas **Wireless Metropolitan Área Networks (WMAN)**, fue desarrollado con IEEE 802.16. Esta tecnología de **WiMAX (Worldwide Interoperability for Microwave Access)** permite crear las llamadas redes WLAN hotzones, que consisten en varios puntos de acceso WLAN interconectados en diferentes localizaciones. Las redes WMAN se utilizan para ofrecer a los usuarios una potente conexión a Internet en aquellas regiones que carecen de infraestructura para ello, y es que el DSL, el estándar habitual de transmisión, solo está disponible técnicamente donde hay hilos de cobre.

Wide Area Network (WAN)

Mientras que las redes Metropolitan Área Networks comunican puntos que se encuentran cerca unos de los otros en regiones rurales o en zonas de aglomeraciones urbanas, las **Wide Área Networks (WAN)** o redes de área amplia se extienden por zonas geográficas como países o continentes. El número de redes locales o terminales individuales que forman parte de una WAN es, en principio, ilimitado.

Mientras que las redes LAN y las MAN pueden establecerse a causa de la cercanía geográfica del ordenador o red que se tiene que conectar en base a Ethernet, en el caso de las Wide Area Networks entran en juego técnicas como IP/MPLS (Multiprotocol Label Switching), PDH (Plesiochronous Digital Hierarchy), SDH (Synchronous Digital Hierarchy), SONET (Synchronous Optical Network), ATM (Asynchronous Transfer Mode) y, rara vez, el estándar obsoleto X.25.

En la mayoría de los casos, las Wide Área Networks suelen pertenecer a una organización determinada o a una empresa y se **gestionan o alquilan de manera privada**. Los proveedores de servicios de Internet también hacen uso de este tipo de redes para conectar las redes corporativas locales y a los consumidores a Internet.

Global Area Network (GAN)

Una **red global** como Internet recibe el nombre de Global Área Network (GAN), sin embargo, no es la única red de ordenadores de esta índole. Las empresas que también son activas a nivel internacional mantienen redes aisladas que comprenden varias redes WAN y que logran, así, la comunicación entre los ordenadores de las empresas a nivel mundial. Las redes GAN utilizan la infraestructura de fibra de vidrio de las redes de área amplia (Wide Área Networks) y las agrupan mediante **cables submarinos internacionales o transmisión por satélite**.

Virtual Private Network (VPN)

Una red privada virtual (VPN) es una **red de comunicación virtual** que utiliza la infraestructura de una red física para asociar sistemas informáticos de manera lógica. En este sentido, se puede tratar de todos los tipos de redes expuestos anteriormente. Lo más común es utilizar **Internet como medio de transporte**, ya que este permite establecer la conexión entre todos los ordenadores a nivel mundial y, al contrario de lo que ocurre con las redes MAN o WAN privadas, está disponible de forma gratuita. La transferencia de datos tiene lugar dentro de un túnel virtual erigido entre un cliente VPN y un servidor VPN.

Si se utiliza la red pública como medio de transporte, las Virtual Private Networks o redes privadas virtuales suelen **cifrarse** para garantizar la confidencialidad de los datos. Las VPN se emplean para conectar redes LAN en Internet o para hacer posible el acceso remoto a una red o a un único ordenador a través de la conexión pública.

Ya indagaremos más profundamente en algunos de estos aspectos, pero debemos entender que también tenemos la conformación de una red de acuerdo a su composición física, que es esto, significa que una red podemos conectarla de forma física por medio de cables o bien por medio inalámbrico, como se usa una red Wifi; pero no siendo esto único, antes de encontrar la conexión por wifi que fue una alternativa inalámbrica al mundo de internet y redes, encontramos que ya existía la conexión por medio de bluetooth.

La problemática de esta conexión es que tenía rangos limitados muy cortos, así como la cantidad de dispositivos que se podía interconectar entre sí, y que para conectarse el uno con el otro debían estar muy cerca en la conexión inicial para pedir los permisos necesarios.

Esto la hacía una red bastante frágil y muy lenta en lo que transferencia de datos muy grandes o pesados se refería.

Por lo que en la búsqueda de mejorar esta es que tenemos hoy día la conexión Wi-Fi; la cual es recurrente de una conexión inalámbrica apuntada a internet o mejor dicho a poder conectar un dispositivo o más a un modem o distribuidor de servicio de internet de forma inalámbrica, claro está que esto fue creciendo y las redes se usan no solo para internet si no también para conectar dispositivos entre sí, de forma remota y así poder sin la necesidad de un cableado poder transferir datos.

También en esto encontramos deficiencias, problemas y limitantes, como ser el hecho de que la ser de forma inalámbrica es que el alcance es limitado, a mayor distancia es que encontramos más degradación o problemas con la fidelidad en la transferencia de datos; para solucionar el tema distancia es que encontramos herramientas para suplirlas tales como repetidores o acces point.

Repetidor

un repetidor es un dispositivo electrónico que recibe una señal débil o de bajo nivel y la retransmite a una potencia o nivel más alto, de tal modo que se puedan cubrir distancias más largas sin degradación o con una degradación tolerable.

Un repetidor WiFi es un dispositivo de red conectado a un enchufe que permite ampliar el alcance de nuestra conexión a Internet de manera **totalmente inalámbrica**, aunque existen modelos que pueden conectar con nuestro router de forma cableada a través de un **puerto Ethernet**.

Su utilidad está fuera de toda duda ya que un repetidor WiFi nos permite cubrir zonas muertas, aquellas en las que **la señal de nuestro router no llega** y por tanto no hay conexión a Internet, y también nos ayuda a mejorar la calidad y la estabilidad de la señal en otras zonas donde la conexión WiFi es **muy débil**.

Los repetidores WiFi tienen dos grandes ventajas: **son muy sencillos de utilizar**, puesto que no requieren complicadas configuraciones y nos permiten clonar los ajustes de nuestra red (los ajustes del router), y **son muy económicos**.

Por lo general para utilizar un repetidor WiFi basta con enchufarlo y llevar a cabo el proceso de **sincronización con nuestro router**. Podemos hacerlo de forma automática mediante WPS o de forma manual, dos procesos muy sencillos y rápidos de completar.

¿Qué posibilidades ofrecen?

Un repetidor WiFi se encarga de repetir la conexión a Internet de nuestro router ampliando **el alcance de la misma de forma inalámbrica**. Esa es su diferencia más importante frente a un PLC tradicional basado en cable.

Los modelos más básicos trabajan bajo el estándar WiFi N, operan en la banda de 2,4 GHz y alcanzan velocidades máximas de **300 Mbps**. También hay modelos compatibles con el estándar WiFi AC que operan simultáneamente en las bandas de 2,4 GHz y 5 GHz, ya sea de forma real o «simulada» (cuando el router no trabaja en la banda de 5 GHz pero el repetidor sí).

Como hemos indicado en al inicio del artículo un repetidor WiFi nos permite ampliar el alcance de la señal de nuestra conexión WiFi para eliminar zonas muertas y para mejorar la velocidad y la estabilidad de la señal de una manera **sencilla, económica y fiable**.

Sin embargo, debemos tener en cuenta que **no todos los repetidores son iguales**, y que tendremos que elegir un modelo en concreto en función de nuestras necesidades básicas haciendo una valoración a corto y a medio plazo.

Consejos para elegir y para utilizarlos correctamente

Como ya hemos dicho los repetidores WiFi son muy fáciles de utilizar, pero debemos tener en cuenta que su alcance es limitado y que por tanto **no hay que apurar las distancias**, ya que salirnos del nivel óptimo intentando apurar unos metros puede acabar siendo contraproducente.

La mayoría de los repetidores vienen con un indicador de señal que nos ayuda a encontrar el **punto óptimo de colocación**, así que sólo tenemos dejarnos guiar por él y evitar colocarlo a una distancia tan grande que reduzca la intensidad de la señal que refleja dicho indicador. En este sentido lo ideal es no sacrificar ninguna línea del indicador.

A la hora de elegir un repetidor es importante tener en cuenta nuestras necesidades y nuestro presupuesto. Los modelos más básicos con WiFi N a 300 Mbps que sólo trabajan en la banda de 2,4 GHz pueden ser una buena opción para ampliar el alcance de nuestra conexión **con un coste mínimo**, pero si queremos disfrutar de un mayor rendimiento y de las ventajas que ofrece la banda de 5 GHz lo ideal es ir a por un modelo **que trabaje con ambas de forma simultánea** y que sea compatible con **WiFi N y WiFi AC**.

Existen repetidores WiFi con antenas extensibles que además se pueden orientar en determinadas direcciones. **No son imprescindibles** ya que la mayoría de repetidores WiFi con antenas integradas funcionan sin problema, pero puede ser de ayuda en algunos casos concretos.

Por último, es importante tener en cuenta las posibilidades de configuración que ofrece un repetidor WiFi **a nivel de software**, tanto en lo que respecta a la seguridad y a la gestión de la red como a la posibilidad de configurarlo como punto de acceso.

Obviamente tenemos cientos de tipos de repetidores y debemos tener algún tipo de conocimiento previo, para poder elegir de forma correcta, de acuerdo a su alcance, configuración y prestancia, pero aun así es la forma más práctica y sencilla de extender el alcance de nuestra red inalámbrica.

Access Point (AP)

Los AP o WAP (Access point o Wireless Access point) También conocidos como **puntos de acceso**. Son dispositivos para establecer una conexión inalámbrica entre equipos y pueden formar una red inalámbrica externa (local o internet) con la que interconectar dispositivos móviles o tarjetas de red inalámbricas. Esta red inalámbrica se llama WLAN (Wireless local área network) y se usan para reducir las conexiones cableadas.

¿Qué usos tienen los puntos de acceso?

- Crear un acceso inalámbrico LAN de un lugar de trabajo.
- Dar acceso a una red inalámbrica a los clientes.
- Llevar una conexión a internet a donde no había antes, sin perder ancho de banda con repetidores.
- Cubrir grandes áreas con una conexión de calidad, reduciendo el uso de cableado.
- Permite interconexiones entre dispositivos convencionales y inalámbricos si se conecta el AP a un switch.

¿Cuáles son las ventajas de un punto de acceso?

- Permite la conexión de dispositivos inalámbricos a la WLAN como móviles u ordenadores portátiles.
- Se basan en emisiones de ondas de radio, capaces de traspasar muros, por lo que son perfectos para conectar edificios cercanos dentro de la misma red, con antenas potentes es posible crear una red WLAN de hasta a un kilómetro de distancia.
- Tienen un radio de acción de entre 30 metros a 100 metros.
- Proporciona información del estado de red y descongestionan la red dividiendo las redes y enviando la información de manera paralela más rápidamente que de forma convencional.
- Si dispone de conexiones PoE es posible con un único cable Ethernet RJ-45 dar acceso a internet sin la necesidad de conectarlo a un enchufe convencional.
- Permite más usuarios conectados, al mismo tiempo.

Las ventajas de usar puntos de acceso inalámbrico

Si tanto sus empleados como sus invitados se conectan a la red usando sus ordenadores de sobremesa, portátiles, smartphones y tabletas el cupo máximo de 20 dispositivos conectados se llenará con rapidez. Dando la posibilidad de manejar hasta 60 conexiones simultáneas los puntos de acceso le ofrecen la libertad de escalar el número de dispositivos que la red puede admitir. Sin embargo, esta es solo una de las ventajas de utilizar estos potenciadores de redes, tenga en cuenta también las siguientes:

- Los puntos de acceso profesionales pueden ser instalados en cualquier ubicación donde pueda colocar un cable de Ethernet. Los modelos más modernos son compatibles también con la función Power over Ethernet Plus (PoE+), un combo entre un cable Ethernet y uno de alimentación, por lo que no es necesario instalar cableado eléctrico adicional o un enchufe cerca del punto de acceso.
- Algunas funciones estándar complementarias incluyen Portal Cautivo y la Lista de Control de Acceso (ALC), para que pueda limitar el acceso a los usuarios invitados sin comprometer la seguridad de la red y gestionar las cuentas de usuarios dentro de su red Wi-Fi.
- Algunos puntos de acceso incluyen la función de clústering, que ofrece un punto único desde el que el administrador de TI puede visualizar, instalar, configurar y proteger una red

Wi-Fi como una única entidad en vez de como múltiples configuraciones de puntos de acceso.

¿Dónde poner tu punto de acceso?

Para elegir una ubicación para estos puntos de acceso, se debe tener en cuenta estar lo más cerca posible del dispositivo de esta forma se conseguirá la mejor señal posible. Sin embargo, También se tiene que tener en cuenta que las paredes, tuberías de agua, masas de agua, planchas metálicas y emisores de frecuencias similares como microondas interfieren en la conexión de estos dispositivos. Por lo que es importante tenerlas en cuenta a la hora de situarlos.

¿en qué se diferencia un AP y un router?

Los puntos de acceso y routers **requieren de un módem para transformar la señal** (modular y demodular la señal). El router se encarga de llevar conexión a los dispositivos, sin embargo, los puntos de acceso sirven para llevar conexión donde no la hay. Además, se pueden crear WLAN con las que transmitir datos entre dispositivos conectados a la misma red WLAN.

¿Qué es Roaming AP?

El roaming entre puntos de acceso, se trata de múltiples puntos de acceso en una zona, que intercambian de forma automática cuando el dispositivo que está conectado encuentra otro punto de acceso con mayor intensidad de la señal.

De esta forma se puede abarcar una gran zona en la que poder trabajar con dispositivos inalámbricos, en la que este dispositivo se conecta a redes secundarias utilizando su identificador de la red principal. Lo que hace innecesario dar nuevas credenciales a la nueva fuente a la que se conecta. De esta forma la conexión del dispositivo no es interrumpida.

¿Que modos tiene un punto de acceso?

Se pueden configurar para distintas funciones para adaptarlos a nuestras necesidades. Estas son algunas de las funciones:

Modo cliente

Se utiliza como un receptor y actúa como un cable de red uniéndose a una red

Modo AP (punto de Acceso)

El Punto de acceso sirve de núcleo para la instalación del cableado, de forma que los múltiples usuarios acceden a la red por medio del punto de acceso.

Modo Repetidor

Este modo se puede usar para extender la señal de forma que el punto de acceso amplifica la señal que recibe para optimar el rango de acción.

Modo Bridge

Este modo se hace para cubrir grandes distancias, como dos edificios separados. Con dos puntos de acceso conectados entre si podemos conseguir una red WLAN a distancias considerables.

¿Qué es un extensor de red?

Como su propio nombre indica un extensor de red incrementa el alcance de una red Wi-Fi ya existente. Como los extensores de red se conectan inalámbricamente a los routers Wi-Fi es necesario emplazarlos allí donde la señal del router Wi-Fi sea fuerte y no donde esté debilitada. Por

ejemplo, si su router se ubica en el sótano de un edificio de dos plantas instalar un extensor de red en la primera (donde la cobertura todavía es robusta) eliminará las posibles zonas sin cobertura en la segunda planta.

Pero todo esto nos hace avanzar ya en las redes, sus aspectos complejos y el mundo a través de su interconexión, pero no hay que olvidarnos que antes de llegar a esto tenemos miles de términos que intervienen en el mundo de la red y su configuración.

Empecemos tal vez por lo más importante o primordial de ya un dispositivo dentro de la red, el mismo se identifica de una manera única, y esta manera es una dirección IP.

Pero antes de entrar en esto, debemos entender que esta dirección sufre de cambios o deformaciones dependiendo de a donde apunte y que hagamos con ella, es por lo que encontramos que aun dentro de esta identificación que es única tenemos diferentes conceptos.

Pero aun así esta ip no va solo y es en esos detalles que la ayudan a ser única, así imaginemos que cuando estamos navegando por internet en un simple sitio como la página de un diario, hay millones de usuarios al mismo tiempo conectados leyendo diferentes artículos o incluso el mismo que yo, pero aun así este que me brinda la información debe entender que yo lo estoy leyendo siendo único y con migo hay millones más, también cada uno de ellos es único, este entendimiento que esta cifrado es de magnitudes complejas, que jamás podría depender de una y solo una cosa.

Así que en primera instancia veremos que es un IP.

Dentro de las características más destacadas de un punto de acceso se encuentran:

- **Trabajan por medio de ondas de radio**, lo que permite evitar el uso de cables para conectar los equipos.
- **No sólo admite la conexión de dispositivos sino también de otros puntos de acceso**, por lo que es recomendable su uso cuando se necesita ampliar la red para mejorar la señal inalámbrica.
- **Trabaja con cualquier dispositivo que tenga una tarjeta de red**, sin importar el tipo de sistema operativo que tenga el equipo.
- **Soporta también la conexión por cables** para formar redes LAN.
- Al contar con puertos LAN puede trabajar de forma mixta. Es decir, puede enrutar los datos de forma inalámbrica y por cables al mismo tiempo sin que se saturen los equipos.
- **Dispone de antenas para mejorar la transmisión de la señal**, pero son vulnerables a la distancia y a la interferencia de objetos.
- Trabaja con frecuencias 2,4 y 5 GHz, lo cual convierte a un AP en un hardware muy versátil para crear redes WLAN.
- Los estándares que usa en general son de tipo IEEE **11b**, **802.11g** y **802.11n**. Por lo que la velocidad puede superar en promedio los 300 Mbps, aunque también se puede encontrar los que superan los 1,6 Gbps.
- **Admiten la conexión** por medio de Bluetooth.

¿Qué es una dirección IP?

IP son las siglas de “**Internet Protocol**» que, si lo traducimos al español, significa «**Protocolo de Internet**». Este protocolo, al igual que otros muchos como HTTP, TCP, UDP, etc., se encarga de establecer las comunicaciones en la mayoría de nuestras redes. Para ello, asigna una **dirección**

única e irrepetible a cada dispositivo que trata de comunicarse en Internet. ¡Hasta una nevera puede tener una dirección IP! Entendemos dispositivo como, por ejemplo, un router, un servidor, un teléfono, un ordenador, una televisión, etc.

No existe dispositivo en el mundo que pueda comunicarse con otro sin tener una IP. **Las direcciones IP son los nombres numéricos** que se asignan a un dispositivo a modo de «matrícula» para que pueda ser llamado por otros dispositivos. Existen dos tipos de IP: las direcciones **IP públicas** y las direcciones **IP privadas**.

Tanto las **direcciones IP públicas como las privadas** están construidas en **cuatro bloques numéricos**. Cada bloque es un número del 0 al 255 y está separado por un punto («.»). Por ejemplo, una **dirección IP pública** podría ser **63.45.12.34** y una **dirección IP privada**, **192.168.0.11**.

¿Pueden existir direcciones IP públicas o privadas iguales?

La respuesta es no y sí. Vaya, te habrás quedado estupefacto. Te explico. **Una dirección IP pública jamás puede estar duplicada**, ya que cada conexión a Internet es única. Dentro de una red privada, **las direcciones IP privadas tampoco pueden estar duplicadas**. Pero sí es posible que, por ejemplo, un amigo tuyo sí tenga una dirección IP privada para uno de sus dispositivos y que pueda coincidir con una dirección IP privada tuya que tengas para un dispositivo.

Esto se debe a que, por ejemplo, cualquier hogar tiene una red con direcciones IP privadas para sus dispositivos pero no quiere decir que la red de la casa de tu amigo deba tener direcciones IP privadas diferentes. Es decir, en cada hogar existe un router y este router asigna direcciones IP privadas a cada dispositivo que pueden coincidir con las direcciones IP privadas asignadas por el router de la casa de tu amigo a sus dispositivos. ¿Ya vas entendiendo qué es una dirección IP?

¿Qué es una dirección IP pública?

Una **IP pública es la identificación que te asigna tu proveedor de internet para ser reconocido en Internet**. Al igual que tú no puedes salir con el coche a la calle sin una matrícula, tampoco podrás salir a Internet sin una referencia o identificación.

Normalmente estas direcciones IP suelen ser rotadas por tu ISP (proveedor de internet) cada vez que reinicias el router o cada cierto tiempo. A estas direcciones IP se las conoce como direcciones **IP dinámicas**. Si por algún motivo necesitamos tener una dirección **IP estática o fija** para un dispositivo, debemos ponernos en contacto con el ISP y solicitar que nos la pongan manualmente.

¿Qué relación tiene una dirección IP pública y un dominio web?

Cuando nació Internet existían muy pocos servidores y **la única forma de acceder a ellos era saber su dirección IP pública**. Si una persona quería acceder a un recurso determinado no valía con escribir, por ejemplo, **recursos.com** (más que nada porque aún no existían los nombres de dominio), sino que tenía que conocer la dirección IP del servidor donde estaba alojado ese recurso. **Imaginemos que la dirección IP de ese servidor fuera: 156.87.234.176.**

¿Verdad que no es útil, eficiente ni fácil recordar todos esos números? Los centros de datos seguían creciendo y cada vez albergaban más servidores con más información diferente. ¡Sería una locura tener que apuntar o recordar cada dirección IP para cada recurso! **Por eso nacieron los nombres de dominio que conocemos muy bien hoy en día.**

Actualmente, usamos los famosos DNS (**Domain Name Servers**) para **suplantar con un nombre de dominio a una dirección IP**. Ahora, para acceder a un material de **recursos.com** ya no hay que poner la IP 156.87.234.176 sino indicar **recursos.com**. Usar nombres de dominio tiene una lista de ventajas enorme frente a usar direcciones IP:

- Son más fáciles de recordar que una dirección IP
- Son más cortos
- Son más atractivos para usos con fines publicitarios, por ejemplo
- Sirven para crear branding/marca
- Son más fáciles de escribir
- De la misma forma, varios nombres de dominio pueden apuntar a una misma dirección IP

¿Qué es una dirección IP privada?

Una dirección IP privada es exactamente lo mismo que las direcciones IP públicas, solo que estas **se caracterizan por ser fijas para cada dispositivo y no son accesibles desde Internet**. El típico ejemplo es el de una casa donde dispositivos como un ordenador, un móvil, una televisión y hasta una lavadora están conectados a una misma red WiFi o cable. Esta red asigna una dirección IP fija e irrepetible a cada dispositivo para que se puedan reconocer entre ellas.


Existen **diferentes rangos de direcciones IP privadas** que veremos a continuación. De momento, quiero ponerte un ejemplo de cómo sería tener direcciones IP privadas en un ámbito de hogar pequeño:

- **Router:** 192.168.0.1
- **Móvil de papá:** 192.168.0.10
- **Móvil de mamá:** 192.168.0.11
- **Mi móvil:** 192.168.0.13
- **Impresora:** 192.168.0.12
- **Tablet:** 192.168.0.98

Los rangos de direcciones IP privadas

A diferencia de las direcciones IP públicas, las privadas tienen asignado un rango en función del tipo de red que veremos a continuación. Las direcciones IP públicas son libres, te puede tocar cualquiera:

- **Rango clase A:** 10.0.0.0 a 10.255.255.255.
- **Rango clase B:** 172.16.0.0 a 172.31.255.255.
- **Rango clase C:** 192.168.0.0 a 192.168.255.255.

-
- **CLASE A:** Usada para las **redes gigantescas**, como las de las empresas internacionales. El primer bloque de la dirección es usado para identificar la red, mientras los otros tres bloques son usados para identificar a los dispositivos (xxx.yyy.yyy.yyy). Esto nos permite crear hasta 126 redes distintas y tener un máximo de 16.777.214 equipos conectados por red.
 - **CLASE B:** Usadas por redes de tamaño mediano, como puede ser una **universidad o instituciones de similar envergadura**. Utiliza los dos primeros bloques para identificar la red, mientras que los dos restantes son utilizados para identificar a los dispositivos conectados (xxx.xxx.yyy.yyy). Esto nos permite crear un mayor número de redes, pero menos equipos conectados por red (16.384 redes y 65.534 equipos).
 - **CLASE C:** Las que el 99% de la población usamos. **Son reservadas para pequeñas redes domésticas**. Los tres primeros bloques son usados para identificar la red y el último como identificador de equipo (xxx.xxx.xxx.yyy). Esto nos hace tener más redes distintas aún, pero menor número de equipos por red (2.097.152 redes y 254 equipos por red).
- 

Luego existen otro tipo de rangos, pero no los vamos a ver. Si ya es difícil ver las de clase A y B, las D e Y más todavía. Como decía antes, las de clase C son las que vemos a diario y empiezan por 192.168.X.X.

Tienes que tener muy claro que tu dirección IP privada es totalmente diferente a la dirección IP pública. Esta última solo la usarás cuando salgas a navegar por Internet.

¿Y qué es la máscara de red?

La máscara de red permite hacer que una misma dirección IP sirva para dos dispositivos. Por ejemplo, podrías tener la dirección 192.160.0.1 bajo dos máscaras distintas haciendo que sirvan para identificar a ambos. Las máscaras también son las que permiten separar las redes en las distintas categorías que ya hemos explicado. La máscara de red es la que dictamina cuántas redes se pueden crear y cuántos hosts pueden existir según la clase de IP privada que tengamos. Recuerda que ya sabemos cuáles son los tipos de clases de IP, las vimos más arriba. Por norma general y seguro que la has visto miles de veces, **la principal máscara de red que existe es la 255.255.255.0**, que es la que se asigna a **redes de tipo C**.

- Para **direcciones IP clase A**: 255.0.0.0
- Para **direcciones IP clase B**: 255.255.0.0
- Para **direcciones IP clase C**: 255.255.255.0

Sin entrar en muchos datos muy técnicos ni en la razón, **los bloques 255 representan la cantidad de redes que puede haber y los números 0 cuántos host puede haber**. No es que puedan existir 255 redes y 0 hosts. Esa es la traducción humana para que podamos entender que si traducimos 255.255.255.0 a código binario, será un código de este tipo: **11111111111111111111111100000000**. ¿Te acordarías tú de esa cantidad de números de bits del código binario? **Esos 1 y 0 son los que dictaminan el tipo de red, el límite de redes que puede haber y los hosts que pueden existir**.

Por ejemplo, por no complicar mucho la cosa: sabemos que la máscara de red 255.255.255.0, traducido a binario, tiene ocho (8) ceros (0). Ergo si elevamos dos (2) a ocho (8) obtenemos 256. Ese 256 es el número de dispositivos que puede haber conectados a una misma red. Bueno, debemos saber que aunque teóricamente haya 256 oportunidades, en la práctica tenemos 254 ya que, por ejemplo, una la usamos para **broadcast**, que suele ser la **192.168.1.255**.

Ten en cuenta que estas máscaras las hemos simplificado. Pueden existir máscaras con otros números que no sean 0 o 255, como por ejemplo: 255.252.0.0, 255.255.255.128, etc.

¿Qué son las direcciones IP IPv4 e IPv6?

Si ya explicar **que son las direcciones IP** es un poco lioso, imagínate cuando te explique ahora qué son las **direcciones IPv6**. Pues resulta que las direcciones IPv4 son las que hemos estado viendo ahora y las direcciones IPv6 son un nuevo tipo de protocolo que viene a sustituir a las IPv4 debido a que ya casi no quedan direcciones IPv4 y hay que saltar a las direcciones IPv6. No vamos a entrar mucho en materia, solo quiero dejar como apunte un dato curioso:

Curioso, ¿verdad? Las direcciones IPv6 son el futuro. Bueno, más bien el presente ya. Su composición es distinta a la de las direcciones IPv4, ya que las primeras juegan con **caracteres alfanuméricos**. Por eso, las combinaciones son infinitas.

Solo entramos en el mundo de la IP y vimos cuantas diferencias encontramos dependiendo del país, el sitio, el uso y aun así a esta la acompañan cosas como mascarar de red o de subred, cuando hablamos o entablamos temas de redes fuera del mundo internes; pero aun así no se detiene hay.

A veces por distintas razones es que necesitamos esconder esta dirección así aun conectándonos a donde queremos este sitio es que no puede dar con nosotros, al menos no de forma directa, a este procedimiento se lo conoce como enmascarar la IP.

Esto nos abre una referencia que hemos dejado más adelante en el texto, la forma más rápida común para lograr esto es crear lo que se llama una VPN.

Pero ¿Qué es una VPN?

En términos que son tal vez los más simplistas y no del todo correctos, podríamos mencionar que el uso de una dirección IP que no es la nuestra y usamos otra dirección ip para acceder a donde queremos y así de esta manera el servidor que nos recibe cree que somos otro usuario que realmente no somos.

VPN

Empecemos por lo básico. VPN son las siglas de *Virtual Private Network*, o **red privada virtual** que, a diferencia de otras palabras informáticas más crípticas como DNS o HTTP, sí nos dan pistas bastante precisas sobre en qué consisten.

La palabra clave aquí es **virtual**, pues es esta propiedad la que genera la necesidad de la VPN en sí, así como la que permite a las conexiones VPN ofrecerte los múltiples usos que veremos más adelante.

Para conectarse a Internet, tu móvil, PC, televisión y demás dispositivos generalmente **se comunican con el router o módem** que conecta tu casa con tu proveedor de Internet, ya sea mediante cable o inalámbricamente. Los componentes son distintos si estás usando la conexión de datos de tu móvil (que incluye su propio módem y habla con la antena de telefonía) pero la esencia es la misma: tu dispositivo se conecta a otro, que le conecta a Internet.

Lo más normal es que no tengas uno, sino varios dispositivos conectados al mismo router: móviles, ordenadores, consolas... En este caso cada uno tendrá asignada una dirección IP local, que no es visible desde Internet. Esto es una **red local**, un conjunto de dispositivos conectados de tal modo que puedan compartir archivos e impresoras sin necesidad de pasar por Internet.

Una conexión VPN lo que te permite es crear una red local **sin necesidad que sus integrantes estén físicamente conectados entre sí**, sino a través de Internet. Es el componente "virtual" del que hablábamos antes. Obtienes las ventajas de la red local (y alguna extra), con una mayor flexibilidad, pues la conexión es a través de Internet y puede por ejemplo ser de una punta del mundo a la otra.

Cuando te conectas a una conexión VPN, esto cambia. Todo tu tráfico de red sigue yendo desde tu dispositivo a tu proveedor de Internet, pero de ahí **se dirige directo al servidor VPN**, desde donde partirá al destino. Idealmente la conexión está cifrada, de modo que tu proveedor de Internet realmente no sabe a qué estás accediendo. A efectos prácticos, tu dirección IP es la del servidor VPN: en muchos aspectos es como si estuvieras físicamente ahí, conectándote a Internet.

Para qué sirven las conexiones VPN

1. Teletrabajo

El uso más obvio de una conexión VPN es la interconectividad en redes que no están físicamente conectadas, como es el caso de **trabajadores que están en ese momento fuera de la oficina** o empresas con sucursales en varias ciudades que necesitan acceder a una única red privada.

Desde el punto de vista de la **seguridad**, permitir el acceso indiscriminado a la red propia de una empresa desde Internet es poco menos que una locura. Aunque el acceso esté protegido con una contraseña, podría ser capturada en un punto de acceso WiFi público o avistada por un observador malintencionado.

Por el contrario, el riesgo disminuye si el trabajador y la empresa se conectan mediante una conexión VPN. El acceso está protegido, la conexión está previsiblemente cifrada y el trabajador tiene **el mismo acceso que si estuviera presencialmente ahí**.

2. Evitar censura y bloqueos geográficos de contenido

Con el apogeo de Internet y la picaresca tanto de los proveedores de contenidos como de los usuarios, se han ido popularizando otros usos más lúdicos de las conexiones VPN, muchos de ellos relacionados con un concepto muy sencillo: **falsear dónde estás**.

Al conectarte con VPN, **tu dispositivo se comunica con el servidor VPN, y es éste el que habla con Internet**. Si tú estás en China y el servidor VPN está en Estados Unidos, generalmente los servidores web creerán que estás navegando desde este país, dejándote acceder a los contenidos disponibles solo allí, como podría ser Netflix.

De igual modo, esta misma lógica se puede usar para acceder a aquellos contenidos que estuvieran **censurados o bloqueados en tu país**, pero no allí donde se encuentra el servidor VPN. Así es como millones de ciudadanos chinos logran conectarse a Facebook y otras 3.000 webs bloqueadas en el país.

3. Capa extra de seguridad

Aunque no es estrictamente necesario, sí es común que las conexiones VPN vengan acompañadas de un **cifrado** de los paquetes que se transmiten con ellas, por lo que es normal oír la recomendación de que, si necesitas conectarte a un punto de acceso Wi-Fi público, al menos uses te conectes con una VPN.

Iniciar sesión en tus cuentas bancarias mientras estás conectado a una red WiFi pública en la que no confías probablemente no sea la mejor idea del mundo, pues es relativamente sencillo para un ladrón **capturar los paquetes sin cifrar** y hacerse con tus cuentas de usuario. Aquí es donde entra la capa extra de seguridad que puedes conseguir mediante una conexión VPN, pues los paquetes se enviarían cifrados, de modo que aquel que está escuchando probablemente no podría hacer nada con ellos.

No obstante, hay letra pequeña en esto, pues mientras estás desconfiando de la red pública Wi-Fi, estás poniendo toda tu fé en el servidor de VPN, que puede de igual modo capturar todo tu tráfico, guardar registros de lo que haces o incluso vender tu ancho de banda al mejor postor. Una VPN es tan segura y útil como su proveedor. **Si no confías en tu VPN, no la uses**, pues en vez de tener una capa de seguridad adicional, tendrás al enemigo en casa y mirando absolutamente todo lo que haces en Internet.

4. Descargas P2P

Otro uso común de las conexiones VPN se encuentra en las descargas P2P, lo cual en estos tiempos generalmente es sinónimo de descargar desde BitTorrent. Antes de que me pongas un parche en el ojo, una pata de palo y me obligues a pasar por la quilla, las conexiones VPN también tienen usos en la descarga P2P **aunque bajes torrents completamente legales**.

Desgraciadamente es cada vez común que los proveedores de Internet decidan meter las narices en cómo enviamos y recibimos los ceros y unos en la Red, y aunque les encanta que visitemos páginas web normales, que descarguemos no les hace tanta gracia: **demasiado tráfico**, y además probablemente te estás descargando algo ilegal.

Algunos proveedores **bloquean por completo las descargas P2P**, mientras que otros simplemente la boicotean para que funcione mal y te rindas por ti mismo. Igual que puedes usar una conexión VPN para evitar la censura de tu país, también puedes en ocasiones evitar que tu proveedor de Internet boicotee tus descargas P2P.

Ventajas de las conexiones VPN

Ahora que ya sabemos qué es una conexión VPN y para qué sirve, es hora de resumir una lista de las ventajas e inconvenientes que te supone el uso de esta tecnología. Primero, la parte positiva:

- **Funciona en todas las aplicaciones**, pues enruta todo el tráfico de Internet, a diferencia de los servidores proxy, que solo puedes usar en el navegador web y un puñado de aplicaciones más que te dejan configurar las opciones de conexión avanzadas.
- **Se conecta y desconecta fácilmente**. Una vez configurado, puedes activar y desactivar la conexión a tu antojo.
- **Seguridad adicional** en puntos de acceso WiFi, siempre y cuando la conexión esté cifrada, claro
- **Falseo de tu ubicación**, como ya hemos visto en el apartado anterior, una conexión VPN es un modo eficaz de evitar la censura o acceder a contenido limitado a cierta región.
- **Tu proveedor de Internet** no puede saber a qué te dedicas en Internet. ¿No te apetece que tu proveedor de Internet sepa que te pasas horas viendo vídeos de gatitos en YouTube? Con una VPN no sabrán a que te dedicas, pero ojo, que sí lo sabrá la compañía que gestiona el VPN.

Y así vemos que hay múltiples usos de un mismo sistema o servicio, cuando como herramienta que es depende de nosotros que le demos el correcto uso o no.

Desventajas de las conexiones VPN

Una conexión VPN puede afectar el uso de Internet de diversas maneras. Algunas de las más comunes son:

- Una conexión a Internet más lenta
- Bloqueos específicos a los servicios VPN (por ejemplo, por Netflix)
- Uso ilegal de las propias VPN
- No saber cómo de fuerte es el cifrado proporcionado por la VPN
- El registro y la posible reventa a terceros de tus hábitos en Internet
- Pérdidas de conexión
- Una injustificada sensación de impunidad al estar conectado
- VPN gratuitas: a veces peor que no tener ninguna

Una VPN puede disminuir la velocidad

Debido a que la conexión a Internet con una VPN se redirige y se cifra a través del servidor VPN, tu conexión a Internet podría ralentizarse ligeramente. Es por eso que es importante comprobar la velocidad de una VPN cuando la estás probando. Puedes encontrar una gran sección con respecto a la velocidad en todas nuestras reseñas. La mayoría de los servicios VPN premium como NordVPN y ExpressVPN no ralentizarán demasiado tu conexión a Internet, pero la velocidad rara vez se mantiene igual.

La mayoría de usuarios de Internet no notarán la diferencia. Quienes hacen cosas en línea que necesitan una conexión rápida pueden tener algunos problemas con la VPN errónea. Por ejemplo, los gamers que quieran jugar a juegos en línea para múltiples jugadores deben buscar las mejores VPN para juegos, para asegurarse de que no experimentarán ningún retraso.

Puedes correr el riesgo de ser bloqueado por ciertos servicios

Algunos servicios desalientan el uso de una VPN. Esto suele significar que hay algo a lo que se supone que no debes tener acceso, pero lo haces con una VPN. Por ejemplo, algunos gobiernos bloquean ciertos contenidos a sus ciudadanos porque piensan que no es adecuado o que amenaza sus valores. O, a veces, ciertos proveedores de contenidos bloquean a los usuarios de otros países porque simplemente no han pagado parte del precio de la licencia, por ejemplo. Este es el caso del BBC iPlayer. Puedes usar una VPN para evitar estas restricciones y acceder al contenido de todos modos. Por esta razón, las VPN no son muy populares entre estos gobiernos. Esto puede incluso acabar en una prohibición general de todas las VPN.

Las VPN también están bloqueadas por servicios de streaming como Netflix y Hulu. Debido a que estas empresas tienen contratos con distribuidores de películas que solo les permiten mostrar algunos contenidos en países específicos, han empezado a ir contra las VPN. Con una VPN se puede acceder al contenido de otro país en estos servicios de streaming. Dado que Netflix podría no tener los derechos para mostrar ese contenido en tu país, están luchando contra el uso de las VPN. Lo hacen bloqueando las direcciones IP que acceden a su servicio con grandes cantidades de usuarios al mismo tiempo. Por ejemplo, cuando accedes a ellos a través de una dirección IP compartida al mismo tiempo que otros usuarios. Esto puede ser muy molesto si solo quieres ver una película. Afortunadamente, hay algunos proveedores de VPN que se aseguran de que siempre haya un servidor que puedas usar para ver Netflix. Si quieres una VPN premium que te permita usar Netflix, echa un vistazo a ExpressVPN.

Las VPN no son legales en todos los países

Aunque puede considerarse sospechoso, el uso de una VPN es legal en la mayoría de los países. De hecho, la mayoría de las grandes empresas y corporaciones usan una VPN como parte de su seguridad. Sin embargo, hay algunas excepciones. Algunos países quieren tener un control completo sobre lo que sus ciudadanos pueden ver en Internet. Debido a que una VPN se puede usar para evitar la censura del gobierno, es ilegal en algunos países totalitarios.

En algunos países, como Rusia y China, solo puedes usar las VPN aprobadas por el gobierno. El uso de una VPN no es necesariamente ilegal allí, pero quieren mantener el control sobre ella. Sin embargo, algunos proveedores de VPN de calidad, como NordVPN, han desarrollado «servidores ofuscados» especiales que deberían poder usarse en países como China, incluso si el gobierno no lo permite. En otros países, como Corea del Norte, el uso de una VPN está completamente prohibido, lo que significa que no está permitido usar una VPN. Sin embargo, esto solo es un problema si vives en uno de los países que restringe o prohíbe el uso de las VPN.

Es difícil para los consumidores comprobar la calidad del cifrado

Puede ser difícil saber si los proveedores de VPN hacen realmente lo que prometen. A menudo sueles descubrir que no lo hacen cuando algo sale mal. El usuario medio no tiene conocimientos de criptografía. ¿El servicio prestado es realmente tan seguro? Por esta razón, los análisis son bastante importantes en esta rama. Antes de comprometerte con una suscripción con un proveedor de VPN, es inteligente leer algunas reseñas y análisis (de usuarios).

En nuestras reseñas, puedes averiguar qué registros dice un proveedor que guarda y leer más sobre la calidad y seguridad en general de la VPN. Esto incluye una breve explicación de qué protocolos y tipos de cifrado emplea el proveedor de VPN. Puedes encontrar reseñas de todos los grandes proveedores de VPN en nuestra web. También puedes consultar nuestras principales recomendaciones.

El registro y la posible reventa de tus hábitos en Internet a terceros

La idea de contratar una suscripción de un proveedor de VPN es que esta dirija el tráfico de Internet a través de sus servidores. Cifran tus datos y te permiten usar uno de sus muchos servidores para ocultar también la dirección IP. Esto significa que debes tener confianza en tu VPN, de que no abusarán de los datos que viajan a través de sus servidores. Esencialmente has pagado por conseguir

seguridad y anonimato. Muchos proveedores de VPN mantienen su parte del trato e ignoran por completo tus datos personales. No registran lo que haces ni almacenan tus datos.

Sin embargo, algunos proveedores de VPN *sí* registran los datos. Muchas VPN gratuitas lo hacen (más sobre esto más adelante) y algunos proveedores dejan claro en su acuerdo de licencia que pueden hacerlo. Por supuesto, esto deja en nada el propósito de contratar un servicio VPN. Pero estos no son los peores casos. Los casos realmente preocupantes son los de proveedores de VPN de pago que afirmaban que no registraban nada, pero más tarde se descubrió que sí lo hacían. Por ejemplo, el FBI le pidió a un proveedor de VPN (HideMyAss) que proporcionara información sobre uno de sus clientes debido a la sospecha de actividades ilegales en la dark web. Aunque la empresa inicialmente se negó, terminaron entregando registros muy específicos sobre el usuario, incluidos los tiempos de inicio de sesión, descargas, uso de ancho de banda, etc.

Este cuento con moraleja nos recuerda una vez más que debemos mirar múltiples fuentes y análisis antes de contratar una suscripción con un proveedor de VPN.

Pérdidas de conexión

Muchos proveedores de VPN incluyen un botón de emergencia en su software. Esta es una característica muy útil. Cuando se desconecta la conexión al servidor VPN, de repente te quedas sin protección y lo que hagas estará vinculado a tu dirección IP real. Para evitarlo, el botón de emergencia interrumpe inmediatamente toda tu conexión a Internet y solo se restaura una vez que se restablece la conexión a la VPN.

La desventaja de esto es que, bueno, ya no estás conectado a Internet. Sin embargo, con proveedores de VPN de calidad rara vez puedes encontrarte con este problema.

Una injustificada sensación de impunidad al estar conectado

Hay quienes creen que su conexión VPN los convierte en completamente anónimos y que no se ven afectados por el malware. Esto lleva a la falsa creencia de que son intocables en Internet. Está claro que no es así.

Incluso con una conexión VPN estable y fuertemente cifrada, aún puedes:

- Ser seguido por toda la web por anunciantes, rastreadores, hackers, agencias de inteligencia, etc.
- Ser un objetivo y caer presa de los ataques de phishing
- Infectarte con algún tipo de malware
- Que se bloqueen ciertas redes, bases de datos, páginas de la deep web, etc.

Las VPN se aseguran de que tus datos estén cifrados, tu dirección IP esté oculta y de que puedas obtener acceso a contenido que anteriormente no estaba disponible para los extranjeros. Pero si un hacker o una agencia de inteligencia quiere rastrearte, existen otras formas de identificarte, además de tu dirección IP. Tu dirección IP es solo la primera pista en que podrían buscar. Como tal, una conexión VPN es cualquier cosa menos una licencia para participar en un comportamiento despectivo, ilegal o imprudente, en Internet. Usa siempre el sentido común y ten cuidado.

VPN gratuitas: a veces es peor que no tener ninguna

Algunos optan por probar un servicio VPN gratuito. No hay nada malo en ello. Sin embargo, desafortunadamente, muchos proveedores VPN gratuitos no fueron diseñados para proporcionar al usuario medio más privacidad y anonimato en Internet, sino únicamente para ganar dinero. Un buen ejemplo es Hola VPN, un servicio VPN del que debes mantenerte alejado. Este tipo de VPN no se dedica a vender un servicio VPN, si no a vender tus datos personales a terceros. Cuando usas un servicio VPN, dirige tu tráfico a través de sus servidores. Tú les pagas una tarifa de suscripción, cifran los datos y prometen no registrar ni almacenar todos tus datos. Sin embargo, muchos servicios VPN gratuitos ganan dinero vendiendo tus datos a, por ejemplo, anunciantes. En este caso,

es mejor no tener ningún servicio VPN y, en su lugar, instalar un Adblocker o algunas otras características de seguridad.

Muchos proveedores de VPN gratuitos también tienen límites de datos, límites de velocidad, anuncios y restricciones de descargas. Simplemente no es una experiencia agradable debido a estas limitaciones. Además, muchas aplicaciones VPN gratuitas no son seguras, ya que contienen spyware o malware. Ten cuidado antes de probar algunos servicios VPN gratuitos. Si quieres probar uno o dos, consulta nuestro artículo sobre los principales proveedores de VPN gratuitos. Una VPN gratuita que tiene nuestro sello de aprobación es ProtonVPN.

Ya hemos visto que empezaron a intervenir otros términos como DHCP, DNS, Mac, son solo algunos términos sueltos que por separado nada tengan que ver, pero si están conectados por ser todos propios de las redes.

El DHCP y la configuración de redes

Conectar dispositivos a una red TCP/IP ya no es tan difícil como antes, porque en lugar de tener que asignar las direcciones IP manualmente e introducirlas en los diferentes sistemas, hoy la gestión de direcciones tiene lugar automáticamente. Si los **routers, hubs o conmutadores** pueden asignar de forma automática una dirección individual a los dispositivos que solicitan conectarse a una red, es gracias al protocolo de configuración dinámica de host, en inglés, Dynamic Host Configuration Protocol o más comúnmente **DHCP**.

Qué es el DHCP

El DHCP es una extensión del protocolo Bootstrap (BOOTP) desarrollado en 1985 para conectar dispositivos como terminales y estaciones de trabajo sin disco duro con un Bootserver, del cual reciben su sistema operativo. El DHCP se desarrolló como solución para redes de gran envergadura y ordenadores portátiles y por ello complementa a BOOTP, entre otras cosas, por su **capacidad para asignar automáticamente direcciones de red reutilizables y por la existencia de posibilidades de configuración adicionales**.

Tras unas primeras definiciones del protocolo en 1993 en los RFC 1531 y 1541, su especificación definitiva llegó en 1997 con el **RFC 2131**. La IANA (Internet Assigned Numbers Authority) provee al protocolo de los puertos UDP **67 y 68** (para IPv6, los puertos 546 y 547), también reservados para el protocolo Bootstrap.

La asignación de direcciones con DHCP se basa en un modelo cliente-servidor: el terminal que quiere conectarse solicita la configuración IP a un servidor DHCP que, por su parte, recurre a una base de datos que contiene los **parámetros de red asignables**. Este servidor, componente de cualquier router ADSL moderno, puede asignar los siguientes parámetros al cliente con ayuda de la información de su base de datos:

- **Dirección IP** única
- **Máscara de subred**
- **Puerta de enlace** estándar
- Servidores **DNS**
- **Configuración proxy** por WPAD (Web Proxy Auto-Discovery Protocol)

Así se comunican el cliente DHCP y el servidor DHCP

La **asignación automática** de direcciones mediante el protocolo de configuración dinámica de host tiene lugar en cuatro pasos consecutivos:

1. El cliente DHCP envía un paquete **DHCPDISCOVER** a la dirección 255.255.255.255 desde la dirección 0.0.0.0. Con esta denominada difusión amplia o broadcast, el cliente establece contacto con **todos los integrantes de la red** con el propósito de localizar servidores DHCP disponibles e informar sobre su petición. Si solo hay un servidor, entonces la configuración es extremadamente sencilla.
2. Todos los servidores DHCP que escuchan peticiones en el puerto 67 responden a la solicitud del cliente con un paquete **DHCPOFFER**, que contiene una dirección IP libre, la dirección MAC del cliente y la máscara de subred, así como la dirección IP y el ID del servidor.
3. El cliente DHCP escoge un paquete y contacta con el servidor correspondiente con **DHCPREQUEST**. El resto de servidores también reciben este mensaje de forma que quedan informados de la elección. Con esta notificación, el cliente también solicita al servidor una confirmación de los datos que le ha ofrecido. Esta respuesta también sirve para confirmar parámetros asignados con anterioridad.
4. Para finalizar, el servidor confirma los parámetros TCP/IP y los envía de nuevo al cliente, esta vez con el paquete **DHCPACK** (DHCP acknowledged o «reconocido»). Este paquete contiene otros datos (sobre servidores DNS, SMTP o POP3). El cliente DHCP guarda localmente los datos que ha recibido y se conecta con la red. Si el servidor no contara con ninguna dirección más que ofrecer o durante el proceso la IP fuera asignada a otro cliente, entonces respondería con **DHCPNAK** (DHCP not acknowledged o «no reconocido»).

La dirección asignada se guarda en la base de datos del servidor junto con la dirección MAC del cliente, con lo cual **la configuración se hace permanente**, es decir, el dispositivo se conecta a la red siempre con esa dirección que le ha sido asignada automáticamente y que ya no está disponible para ningún otro cliente, lo que significa que los clientes DHCP nuevos no pueden recibir ninguna dirección si ya están todas asignadas, incluso aunque algunas IP ya no se usen activamente. Esto ha llevado a la expansión de las direcciones dinámicas y, en casos especiales, a la asignación manual vía servidor DHCP, que explicamos en los párrafos que siguen.

Asignación dinámica y manual de direcciones con DHCP

El problema del **agotamiento del rango de direcciones** es más bien improbable en el caso de la asignación dinámica. En principio, este procedimiento es ampliamente equiparable con la asignación automática, aunque con una pequeña pero decisiva diferencia: los parámetros de configuración que envía el servidor DHCP no son válidos para un periodo indeterminado de tiempo, sino por un tiempo de “préstamo” definido por el administrador que se conoce como **concesión o alquiler de direcciones** (lease time). Este indica cuánto tiempo puede acceder un dispositivo a la red con esa dirección. Antes de que se agote (transcurrida la mitad del tiempo), los clientes han de solicitar una prolongación de la concesión enviando una nueva DHCPREQUEST. Si no lo hace, no tiene lugar el **DHCP refresh** y, en consecuencia, el servidor la libera.

Si en las variantes automática y dinámica los administradores no tienen mucho que hacer, la situación es algo diferente en el caso de la **asignación manual**, que también se conoce como DHCP estático y en el cual las direcciones IP se asignan “a mano” con ayuda de las direcciones MAC definidas por el servidor DHCP sin limitación temporal.

Debido a sus elevados costes de gestión, que contradice la misma razón de ser del Dynamic Host Configuration Protocol, este tipo de asignación solo se reserva para unos **pocos escenarios**. Las direcciones IP estáticas son necesarias, por ejemplo, cuando en un ordenador se alojan servicios de

servidor que han de estar permanentemente disponibles para los otros integrantes de la red, o en las redirecciones de puerto, en las que la dirección IP no puede variar.

El servidor DHCP informa al Domain Name System

La dirección IP asignada a un cliente tiene que poderse asociar con su nombre de dominio. Es aquí donde entra en juego un servidor DNS, que se ocupa de la **resolución de nombres**.

Cuando una dirección registrada o el nombre de host se modifican, es necesario **actualizar el servidor de nombres de dominio**. Para un administrador, así como para el usuario que se conecta a Internet desde su casa, la actualización manual del DNS en el caso de las direcciones IP variables asignadas dinámicamente por un servidor DHCP conllevaría mucho trabajo. El que no tengan que hacerlo es posible gracias al servidor DHCP, que se encarga de hacer llegar la nueva información al DNS tan pronto como se asigna una nueva dirección IP.

¿Es seguro el DHCP?

El Dynamic Host Configuration Protocol tiene un punto débil y es su capacidad para ser manipulado fácilmente. Como el cliente hace un llamamiento a discreción a todos los servidores DHCP que podrían responder a su petición, a un atacante le sería relativamente sencillo entrar en la red y hacerse pasar por uno de ellos si tuviera acceso a ella. Este denominado servidor DHCP “Rogue” (corrupto) intenta adelantarse con su respuesta al servidor legítimo y si tiene éxito envía **parámetros manipulados o inservibles**. Si no envía puerta de enlace, asigna una subred a cada cliente o responde a todas las peticiones con la misma dirección IP, este atacante podría iniciar en la red un ataque de denegación de servicio o Denial of Service.

Más dramático, pero factible, sería el intento de colarse en un router utilizando datos falsos sobre la puerta de enlace y el DNS, de modo que se estaría en posición de copiar o desviar el tráfico de datos. Este ataque man in the middle no tiene el propósito, como el primero, de ocasionar una caída de la red, sino de **apropriarse de información sensible** como datos bancarios, contraseñas o direcciones postales.

Sea cual sea el tipo de ataque, sus artífices necesitan tener acceso directo a la red para abusar del protocolo DHCP, así que no dejes de implementar las medidas de seguridad necesarias que te permitan disfrutar las ventajas de este protocolo de comunicación sin temor a sufrir las consecuencias de una amenaza de este tipo. Para el responsable de una red local es fundamental la **protección absoluta ante intentos externos e internos de ataque** y la **supervisión constante de todos los procesos de red** con herramientas como Nagios. En nuestra guía sobre la seguridad WLAN también repasamos las opciones de que dispones para proteger redes inalámbricas.

DNS

Las **DNS** son las siglas que forman la denominación **Domain Name System** o **Sistema de Nombres de Dominio** y además de apuntar los dominios al servidor correspondiente, nos servirá para traducir la dirección real, que es una relación numérica denominada IP, en el nombre del dominio.

Para que Sirven las DNS

Pues bien, los **DNS** sirven para indicarle al usuario que teclea un dominio a que servidor debe ir a recoger la página web que desea consultar.

Efectivamente las páginas web realmente están **hospedadas** bajo una dirección IP, por ejemplo nuestra web www.digival.es realmente responde a la IP 85.112.29.231 pero este sistema es capaz de convertir estos números en el nombre de dominio www.digival.es. Recordar las IP de cada página web sería un trabajo demasiado duro, por eso se creó el sistema de nombres de dominio, para permitir crear términos y denominaciones más fáciles de recordar.

Cómo funcionan las DNS

Que mejor que explicarlo con un ejemplo práctico, y con acciones que realizamos todos los días. Siguiendo con el ejemplo de nuestra página web o de cualquier otra que se haya contratado con nuestros planes de **hosting web**, supongamos que un usuario desea acceder a ella, para lo cual, teclea en su navegador nuestro dominio www.digival.es. Al pulsar la tecla enter, **el navegador consultará con el servidor DNS cuál es la dirección IP de nuestro dominio**, y a su vez casará la información entre la IP y el nombre de dominio, por último entregará al navegador la IP 85.112.29.231 que podrá devolver nuestra página web a nuestro usuario.

Para evitar realizar constantes consultas al **servidor DNS**, el navegador guardará esta información de forma temporal, de manera que se pueda servir la web sin realizar esa consulta previa. Por eso en muchas ocasiones nos piden que actualicemos la consulta con la tecla F5, para que el dominio vaya a la dirección IP más actual.

Como se cambian las DNS

Como **registrador de dominios** que somos proporcionamos un panel de control que permite realizar estos cambios de forma online. En nuestro caso, es importante tener claro, que para **cambiar las DNS** de un dominio individual, es necesario acudir a la sección “Dominios” y **configurar las DNS** del dominio individualmente, bien escribiendo las nuevas que queremos asignar o bien eligiendo entre las que tenemos grabadas en nuestra Área de Clientes.

Hay que tener cuidado con la gestión de DNS, pues como ya hemos explicado, de ellas depende que funcione nuestro dominio, o lo que es lo mismo, nuestra web, nuestro correo o nuestras aplicaciones y bases de datos.

Tipos de registros DNS

- **A** = Dirección (*address*). Este registro se usa para traducir nombres de servidores de alojamiento a direcciones IPv4.
- **AAAA** = Dirección (*address*). Este registro se usa en IPv6 para traducir nombres de hosts a direcciones IPv6.
- **CNAME** = Nombre canónico (*canonical Name*). Se usa para crear nombres de servidores de alojamiento adicionales, o alias, para los servidores de alojamiento de un dominio. Es usado cuando se están corriendo múltiples servicios (como FTP y servidor web) en un servidor con una sola dirección IP. Cada servicio tiene su propia entrada de DNS (como `ftp.ejemplo.com.` y `www.ejemplo.com.`). Esto también es usado cuando corres múltiples servidores HTTP, con diferentes nombres, sobre el mismo host. Se escribe primero el alias y luego el nombre real.
- **NS** = Servidor de nombres (*name server*). Define la asociación que existe entre un nombre de dominio y los servidores de nombres que almacenan la información de dicho dominio. Cada dominio se puede asociar a una cantidad cualquiera de servidores de nombres.
- **MX** = Intercambio de correo (*mail exchange*). Asocia un nombre de dominio a una lista de servidores de intercambio de correo para ese dominio. Tiene un balanceo de carga y prioridad para el uso de uno o más servicios de correo.
- **PTR** = Indicador (*pointer*). También conocido como 'registro inverso', funciona a la inversa del registro A, traduciendo IPs en nombres de dominio. Se usa en el archivo de configuración de la zona DNS inversa.
- **SOA** = Autoridad de la zona (*start of authority*). Proporciona información sobre el servidor DNS primario de la zona.
- **SRV** = Service record (*SRV record*).
- **ANY** = Toda la información de todos los tipos que exista. (No es un tipo de registro, sino un tipo de consulta)

Tipos de servidores DNS

Estos son los tipos de servidores de acuerdo a su función:

- **Primarios o maestros:** guardan los datos de un espacio de nombres en sus ficheros.
- **Secundarios o esclavos:** obtienen los datos de los servidores primarios a través de una transferencia de zona.
- **Locales o caché:** funcionan con el mismo software, pero no contienen la base de datos para la resolución de nombres. Cuando se les realiza una consulta, estos a su vez consultan a los servidores DNS correspondientes, almacenando la respuesta en su base de datos para agilizar la repetición de estas peticiones en el futuro continuo o libre.

Dirección MAC

La dirección MAC es un identificador único que cada fabricante le asigna a la tarjeta de red de sus dispositivos conectados, desde un ordenador o móvil hasta routers, impresoras u otros dispositivos como tu Chromecast. Sus siglas vienen del inglés, y significan Media Access Control. Como hay dispositivos con diferentes tarjetas de red, como una para WiFi y otra para Ethernet, algunos pueden tener diferentes direcciones MAC dependiendo de por dónde se conecten.

Las direcciones MAC están formadas por 48 bits representados generalmente por dígitos hexadecimales. Como cada hexadecimal equivale a cuatro binarios ($4 \times 4 = 16$), la dirección acaba siendo formada por **12 dígitos agrupados en seis parejas** separadas generalmente por dos puntos, aunque también puede haber un guión o nada en absoluto. De esta manera, un ejemplo de dirección MAC podría ser 00:1e:c2:9e:28:6b.

Otra cosa que tienes que tener en cuenta es que la mitad de los bits de una dirección MAC, tres de las seis parejas, identifican al fabricante, y la otra mitad al modelo. Por ejemplo, los números 00:1e:c2 del ejemplo de dirección **pertenecen siempre al fabricante Apple Inc**, mientras que los últimos seis determinan el modelo de dispositivo. Hay buscadores especializados para saber el fabricante de un dispositivo dependiendo de los primeros seis dígitos de su MAC.

Como son identificadores únicos, las MAC pueden ser utilizadas por un administrador de red para permitir o denegar el acceso de determinados dispositivos a una red. En teoría son fijas para cada dispositivo, aunque **existen maneras de cambiarlas** en el caso de que quieras hacerlas más reconocibles en tu red o evitar bloqueos.

Esta exclusividad de cada MAC hacia un único dispositivo también exige que tengas especial cuidado. Por ejemplo, cuando te conectas o intentas conectarte a un router, **tu móvil u ordenador le enviará automáticamente su MAC**. Es una de las razones por las que tienes que saber siempre dónde te conectas a Internet y a quién le pertenece esta red.

Finalmente, dentro de estos temas encontramos un tema similar a los vistos anteriormente, que es el de topología de red y es que encontramos algo llamado jerarquía dentro de las redes, esto en realidad no es muy complejo y en parte también se asocia con un tema conocido como las capas del modelo OSI.

Pero sin irnos por las nubes es que debemos entender que la jerarquía no busca otra cosa más que hacernos entender de forma representativa como esta esa red interconectada entre sí, dándonos una vista rápida de quienes depende cada interconexión y las mismas como están establecidas.

Por CISCO

Las siguientes son las tres capas:

La capa núcleo (The Core layer)

La capa de distribución (The Distribution layer)

La capa de acceso (The Access layer)

La capa de núcleo (core layer)

La capa central es, literalmente, el núcleo de la red. En la parte superior de la jerarquía.

La capa central es responsable de transportar grandes cantidades de tráfico de manera confiable y rápido.

El único propósito de la capa central de la red es mover tráfico lo más rápido posible.

El tráfico transportado a través del núcleo es de todos los usuarios. Sin embargo, recuerde que los datos del usuario se procesan en la capa de distribución., que reenvía las solicitudes al núcleo si es necesario.

Si hay una falla en el núcleo, todos los usuarios pueden verse afectados.

Por lo tanto, tolerancia a fallos en esta capa es un problema. El núcleo es probable que vea grandes volúmenes del tráfico, por lo que la velocidad y la latencia son las principales preocupaciones.

Dada la función del núcleo, ahora podemos considerar algunos detalles de diseño. Comencemos con algunos cosas que no queremos hacer:

- No hagas nada para frenar el tráfico. Esto incluye usar el acceso listas, enrutamiento entre redes de área local virtuales (VLAN), y filtrado de paquetes.
- No apoyes el acceso al grupo de trabajo aquí.
- Evite expandir el núcleo cuando la red interna crece (es decir, agregando enrutadores). Si el rendimiento se convierte en un problema en el núcleo, dar preferencia Para actualizaciones sobre expansión.

Ahora, hay algunas cosas que queremos hacer cuando diseñamos el núcleo. Ellos Incluya lo siguiente:

- Diseñar el núcleo para una alta fiabilidad. Considerar tecnologías de enlace de datos que facilitan la velocidad y la redundancia, como FDDI, Fast Ethernet (Con enlaces redundantes), o incluso ATM.
- Diseñar pensando en la velocidad. El núcleo debe tener muy poca latencia. Seleccione protocolos de enrutamiento con menores tiempos de convergencia. Rápido y La conectividad de enlace de datos redundante no es útil si sus tablas de enrutamiento se disparan!

La capa de distribución (The Distribution layer)

La capa de distribución a veces se denomina capa de grupo de trabajo y es el punto de comunicación entre la capa de acceso y el núcleo. El primario.

La función de la capa de distribución es proporcionar enrutamiento, filtrado y Acceso a la WAN y determine cómo los paquetes pueden acceder al núcleo, si es necesario.

La capa de distribución debe determinar la manera más rápida en que el servicio de red, las solicitudes son manejadas; por ejemplo, cómo se reenvía una solicitud de archivo a un servidor. Una vez que la capa de distribución determina la mejor ruta, reenvía la solicitud a la capa núcleo. La

capa central luego transporta rápidamente la solicitud al servicio correcto.
La capa de distribución es el lugar para implementar políticas para la red.
Aquí puede ejercer una flexibilidad considerable para definir el funcionamiento de la red.
Hay varios elementos que generalmente se deben hacer en la distribución.
capa.

Incluyen los siguientes:

- Implementación de herramientas tales como listas de acceso, de filtrado de paquetes y de hacer cola, Implementación de políticas de seguridad y red, incluyendo dirección. traducción y cortafuegos
- Redistribución entre protocolos de enrutamiento, incluido el enrutamiento estático
Enrutamiento entre VLAN y otras funciones de soporte de grupos de trabajo
Definiciones de dominios de difusión y multidifusión.
- Las cosas que se deben evitar en la capa de distribución se limitan a aquellas funciones que
Pertenecen exclusivamente a una de las otras capas.

La capa de acceso (The Access layer)

La capa de acceso controla el acceso de usuarios y grupos de trabajo a los recursos de la red interna.
Los recursos de red que la mayoría de los usuarios necesitan estarán disponibles localmente en esta capa.

La capa maneja cualquier tráfico para servicios remotos.

Los siguientes son algunos de las funciones a incluir en la capa de acceso:

- Control de acceso continuo (desde la capa de distribución) y políticas
- Creación de dominios de colisión separados (segmentación)
- Conectividad de grupos de trabajo en la capa de distribución.
- Tecnologías como la conmutación DDR y Ethernet se ven con frecuencia en la capa de acceso se ve el enrutamiento estático (en lugar de los protocolos de enrutamiento dinámico)
aquí también, como ya se señaló, tres niveles separados no implican tres enrutadores separados.
Podría ser menos, o podría ser más. Recuerde, este es un enfoque en capas.

Lo más importante es entender que la jerarquía nos sirve para entender como es la estructura de nuestra red y de esta manera podemos aislar o identificar problemas de forma más rápidos y específicos, así como saber a qué debemos afrontar. Entendiendo que tenemos dispositivos como ruters, switch, repetidores, Access point, es confuso a veces entender en una red donde tenemos el problema, pero debemos entender que nosotros o más bien nuestra pc o dispositivo es la parte final de esa cadena de la jerarquía y de ahí iremos escalando tratando de encontrar el problema, sabiendo que puede ser por cuestiones físicas como un dispositivo defectuoso, así como una mala configuración o bloqueo de algún tipo, siendo este el problema lógico.

Aquí ya entramos en otro aspecto de nuestras redes que son los distintos dispositivos que nos permiten justamente concretar diversos y múltiples dispositivos entre si y a su vez, algunos de ellos que todos tengan la conectividad a internet.

Empecemos por entender que tenemos como dispositivos de redes, los Hub, switch y routers.

Cada uno en lo suyo y a su manera son más o menos útiles, así como también combinables entre sí, justamente a veces usando las ventajas de uno u el otro según sean más convenientes, pero con todo esto también debemos entender que a la hora de usar estos dispositivos de manera fascia es que todo

se encarece, así es que también existen maneras de poder usarlos de forma virtual o lógica, haciendo múltiples dispositivos abaratando los costos, como todo proceso sea el físico como el virtual ambos tiene sus beneficios y contras que iremos viendo.

Qué es un hub y para qué sirve

Un hub -también conocido por su nombre en español: concentrador- es el dispositivo gracias al cual podrás conectar varios aparatos entre sí: desde tu *smartphone*, TV y USBs, hasta tarjetas SD, *tablets* u ordenadores.

Puede que debido a esta capacidad de conectar dispositivos de tan diverso tipo pienses que se trata de un aparato complejo, sin embargo, no es así. Un hub es mucho más simple que un *switch* o un *router*.

Mientras que un *switch* crea un canal de comunicación para distribuir datos a cada máquina de destino, el hub limita su red únicamente a equipos de envío. El *switch* es además capaz de funcionar en redes con una cantidad mayor de equipos que el hub.

El *router*, sin embargo, es el encargado de comunicar nuestros dispositivos con redes remotas, siendo capaz de interconectar diversas redes, una función que ni el *switch* ni el hub pueden llevar a cabo.

La misión principal de un hub es la de convertirse en punto central de conexión en una red. Todos los puertos de entrada están conectados eléctricamente. Esto significa que se compartirán datos e información de forma simultánea entre todos los dispositivos conectados al hub para que pueda verse desde cualquiera de ellos.

Los hubs suelen utilizarse también para conectar distintos segmentos de una red LAN a través de sus diferentes puertos. De este modo se crea una red común entre todos los dispositivos conectados.

Ahora que ya sabes qué es un hub, seguramente te estés preguntando: “¿Necesito yo un concentrador capaz de conectar todos mis dispositivos entre sí?”. ¡Sigue leyendo antes de responder a esta pregunta!

A quién le puede interesar un hub

La gran virtud de los hubs o concentradores es su versatilidad y capacidad para adaptarse a las necesidades de cada usuario. Eso se debe principalmente al hecho de tener todo tipo de puertos que, eso sí, pueden variar de un dispositivo a otro.

Puede darse el caso de que tengas un ordenador con algunos años ya, lo que puede significar a su vez que no cuente con demasiadas entradas USB o que algunas de ellas hayan dejado ya de funcionar.

Si este es tu caso, un hub puede ser la solución, ya que la mayoría de ellos sirven también como multipuerto USB. Así, podrás consultar los documentos de tu memoria USB a la vez que cargas tu *smartphone* y tienes tu impresora conectada.

Asimismo, si tu viejo portátil no cuenta con una ranura para las tarjetas de memoria, un concentrador también te servirá como lector de tarjetas. Puedes optar también por conectarlo a tu televisor y hacer un pase de diapositivas desde el sofá de tu casa.

Precisamente, otra función de los multiconectores es permitir la duplicación de una pantalla, principalmente gracias a su puerto HDMI. Si uno de los monitores que quieres vincular no tiene esta entrada, un hub también funcionará como adaptador.

Los hubs incluso pueden servirte para conectar tu portátil a un *router* o *modem* -de hecho esta es su función principal-, lo que significa que podrás disfrutar de la velocidad de una red Ethernet directamente desde tu ordenador.

Así pues, un hub puede interesar a todo aquel que necesite como mínimo un puerto extra, pero del que no dispone en el dispositivo que le interesa utilizar en aquel momento. Solo deberás asegurarte de que el concentrador que utilizas es compatible.

Qué tener en cuenta antes de comprar

Antes de adentrarnos en especificar cuáles son las claves a considerar antes de hacerse con un hub o concentrador, hay que dejar claro que todo dependerá de los usos que quieras darle a este nuevo dispositivo.

Uno de los primeros factores a tener presente es, lógicamente, el precio. El coste de un hub varía, por ejemplo, según la marca y los puertos que incluyen, pero en términos generales oscila entre los 10 y los 60 €.

También hablando en general, a más precio, más variedad de puertos y mayor su capacidad. Es importante, por lo tanto, saber qué tipo de entradas necesitas, ya sea HDMI, LAN, USB Type-C, USB 3.0, tarjeta SDHC, tarjeta micro SDHC o cualquier otra.

Asimismo, y como ya adelantábamos en el apartado anterior, es muy importante conocer la compatibilidad del hub con tus otros dispositivos electrónicos. De nada te servirá un concentrador si no puedes conectarlo a tu portátil o tu televisor.

SWITCH

Los dispositivos de interconexión tienen dos ámbitos de actuación en las redes telemáticas. En un primer nivel se encuentran los más conocidos, los routers, que se encargan de la interconexión de las redes. En un segundo nivel estarían los **switches**, que son los encargados de la **interconexión de equipos dentro de una misma red**, o lo que es lo mismo, son los dispositivos que, junto al cableado, constituyen las redes de área local o LAN.

Un **switch** o **conmutador** es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet (o técnicamente IEEE 802.3)

En realidad, los switches no son los únicos elementos encargados de la interconexión de dispositivos en una red local. Los switches realizan esta función para medios cableados. Cuando la interconexión se realiza de forma inalámbrica el dispositivo encargado de ello se denomina Punto de acceso inalámbrico.

En la actualidad las redes locales cableadas siguen el estándar Ethernet (prácticamente el 100 %) donde se utiliza una **topología en estrella** y donde el switch es el elemento central de dicha topología.

En las primeras versiones de Ethernet, la topología en estrella se implementaba con otro dispositivo conocido como **hub**. En la actualidad, los hubs se pueden considerar obsoletos. Y es importante tener en cuenta que, aunque externamente son muy parecidos, **los switches tienen prestaciones muy superiores a los hubs** por lo que si aún encontramos alguna red que utilice un hub es muy recomendable sustituirlo por un switch.

El switch es posiblemente uno de los dispositivos con un nivel de escalabilidad más alto. Existen switches de cuatro puertos con funciones básicas para cubrir pequeñas necesidades de interconexión. Pero también podemos encontrar switches con cientos de puertos y con unas prestaciones y características muy avanzadas.

La mayor parte de las redes residenciales utilizan un router de acceso que incluye tanto capacidades de interconexión cableadas como inalámbricas. O dicho de otro modo, un router residencial es un dispositivo 3-en-1. Incluye un router de acceso (ADSL o cable), un switch (normalmente con cuatro puertos) y un punto de acceso inalámbrico.

¿Para qué sirve un switch?

La función básica de un switch es la de **unir o conectar dispositivos en red**. Es importante tener claro que un switch **NO** proporciona por si solo conectividad con otras redes, y obviamente, **TAMPOCO** proporciona conectividad con Internet. Para ello es necesario un router.

- **Compartir archivos.** Un equipo de la red habilita la compartición de archivos y el resto de equipos pueden acceder a dichos archivos a través de la red.
- **Compartir impresoras.** Todos los equipos de la red pueden utilizar la misma impresora.
- **Compartir la conexión a Internet.** Todos los equipos pueden acceder a Internet a través de router de acceso, que está conectado en la red.

Características básicas de los switches

Puertos

Los puertos son los elementos del switch que permiten la conexión de otros dispositivos al mismo. Como por ejemplo un PC, portátil, un router, otro switch, una impresora y en general cualquier dispositivo que incluya una interfaz de red Ethernet. El número de puertos es una de las características básicas de los switches. Aquí existe un abanico bastante amplio, desde los pequeños switches de 4 puertos hasta switches troncales que admiten varios cientos de puertos.

El estándar Ethernet admite básicamente dos tipos de medios de transmisión cableados: **el cable de par trenzado** y **el cable de fibra óptica**. El conector utilizado para cada tipo lógicamente es diferente así que otro dato a tener en cuenta es de qué tipo son los puertos. Normalmente los switches básicos sólo disponen de puertos de cable de par trenzado (cuyo conector se conoce como **RJ-45**) y los más avanzados incluyen puertos de fibra óptica (el conector más frecuente, aunque no el único es el de tipo **SC**).

Velocidad

Dado que Ethernet permite varias velocidades y medios de transmisión, otra de las características destacables sobre los puertos de los switches es precisamente la velocidad a la que pueden trabajar sobre un determinado medio de transmisión. Podemos encontrar puertos definidos como 10/100, es decir, que pueden funcionar bajo los estándares **10BASE-T** (con una velocidad de 10 Mbps) y **100BASE-TX** (velocidad: 100 Mbps). Otra posibilidad es encontrar puertos 10/100/1000, es decir, añaden el estándar **1000BASE-T** (velocidad 1000 Mbps). También se pueden encontrar puertos que utilicen fibra óptica utilizando conectores hembra de algún formato para fibra óptica. Existen puertos **100BASE-FX** y **1000BASE-X**.

Por último, los switches de altas prestaciones pueden ofrecer puertos que cumplan con el estándar **10GbE**, tanto en fibra como en cable UTP.

Puertos modulares: GBIC y SFP

La mayor parte de los switches de gamas media y alta ofrecen los llamados puertos modulares. Estos puertos realmente no tienen ningún conector específico si no que a ellos se conecta un módulo que contiene el puerto. De esta forma podemos adaptar el puerto al tipo de medio y velocidad que necesitamos. Es habitual que los fabricantes ofrezcan módulos de diferentes tipos con conectores RJ-45 o de fibra óptica. Los puertos modulares proporcionan flexibilidad en la configuración de los switches.

Existen dos tipos de módulos para conectar a los puertos modulares: el primer tipo de módulo que apareció es el módulo **GBIC** (*Gigabit Interface Converter*) diseñado para ofrecer flexibilidad en la

elección del medio de transmisión para Gigabit Ethernet. Posteriormente apareció el módulo **SFP** (*Small Form-factor Pluggable*) que es algo más pequeño que GBIC (de hecho también se denomina **mini-GBIC**) y que ha sido utilizado por los fabricantes para ofrecer módulos tanto Gigabit como 10GbE en fibra o en cable UTP.

Power Over Ethernet

Power Over Ethernet (*Alimentación eléctrica por Ethernet*), también conocido como **PoE**, es una tecnología que permite el envío de alimentación eléctrica junto con los datos en el cableado de una red Ethernet. La primera versión de esta tecnología se publicó en el estándar **IEEE 802.3af** en 2003 y en el año 2009 se publicó una revisión y ampliación en el estándar **IEEE 802.3at**.

La tecnología PoE permite suministrar alimentación eléctrica a dispositivos conectados a una red Ethernet, simplificando por tanto la infraestructura de cableado para su funcionamiento. **Un dispositivo que soporte PoE obtendrá tanto los datos como la alimentación por el cable de red Ethernet.**

Los dispositivos que utilizan esta característica son puntos de acceso inalámbricos Wi-Fi, cámaras de video IP, teléfonos de VoIP, switches remotos y en general cualquier dispositivo que esté conectado a una red Ethernet, que no tenga un consumo energético muy elevado y que su ubicación física dificulte la instalación de cableado.

En el mercado podemos encontrar multitud de modelos de switches que incluyen puertos con PoE. En dichos puertos podemos conectar un dispositivo que admita esta característica y recibirá la alimentación eléctrica por el propio cable Ethernet.

Funcionamiento de un switch: la conmutación

La función básica que realiza un switch se conoce como conmutación y consiste en transferir datos entre los diferentes dispositivos de la red. Para ello, los switches procesan la información contenida en las cabeceras de la trama Ethernet.

En la actualidad ya hay versiones de Ethernet que pueden cubrir distancias de decenas de kilómetros por lo que Ethernet no sólo se usa en redes locales sino que también puede usarse en redes metropolitanas (MAN)

Sin entrar mucho en detalle en el funcionamiento de Ethernet podemos decir que Ethernet es una tecnología de transmisión de datos para redes locales cableadas que divide los datos que se tiene que transmitir en **tramas** y a cada trama se le añade una determinada información de control llamada **cabecera**. Dicha cabecera contiene la dirección MAC tanto del emisor como del receptor.

Los switches guardan en una tabla las direcciones MAC de todos los dispositivos conectados junto con el puerto en el que están conectados, de forma que cuando llega una trama al switch, dicha trama se envía al puerto correspondiente.

Si utilizamos como referencia el modelo OSI, el switch es un dispositivo que opera en el nivel 2 o nivel de enlace

Buffers

El elemento clave en los switches para llevar a cabo el proceso de conmutación son los buffers, que son zonas de memoria donde las tramas son almacenadas antes de ser reenviadas al puerto correspondiente. Esta característica además, permite al switch conectar puertos que trabajen a diferentes velocidades.

Los buffers pueden ser implementados en la salida de los puertos, en la entrada de los puertos o una combinación de ambos. Lo más habitual es implementarlos en la salida ya que es el modo más eficiente, consiguiéndose unos índices de eficacia cercanos al 98%.

Los buffers se implementan en memorias RAM integradas en la circuitería del dispositivo.

Técnicas de conmutación

Existen dos técnicas para llevar a cabo la transferencia de los datos entre puertos de un switch:

- **Reenvío directo** (*cut-through*). En esta técnica, cuando un switch comienza a recibir datos por un puerto, no espera a leer la trama completa para reenviarla al puerto destino. En cuanto lee la dirección de destino de la trama MAC, comienza a transferir los datos al puerto destino.

Esta técnica proporciona unos tiempos de retardo bastante bajos, sin embargo, tiene como inconveniente que sólo puede usarse cuando las velocidades de todos los puertos son iguales.

Otro problema que plantea la técnica cut-through, debido a su forma de funcionamiento, es que los switches propagan tramas erróneas o tramas afectadas por colisiones. Una posible mejora para evitar la propagación de tramas con colisiones es retrasar el reenvío hasta que se lean los primeros 64 bytes de trama, ya que las colisiones sólo se pueden producir en los primeros 64 bytes de la trama. Esta mejora sin embargo aumenta el tiempo de retardo.

- **Almacenamiento y reenvío** (*Store and Forward*). En este caso, cuando un switch recibe datos por un puerto, almacena la trama completa en el buffer para luego reenviarla al puerto destino. La utilización de esta técnica permite realizar algunas comprobaciones de error antes de ser enviada al puerto de destino.

El tiempo de retardo introducido es variable ya que depende del tamaño de la trama, aunque suele ser superior al proporcionado por la técnica cut-through, sin embargo, es imprescindible utilizar esta técnica cuando existen puertos funcionando a diferentes velocidades.

Gestión y configuración

La función básica que llevan a cabo los switches, que es la conmutación de tramas Ethernet, no necesita ninguna configuración manual. Una de las características incluidas en el estándar Ethernet (concretamente en la especificación IEEE 802.3u) es la **autonegociación**. Esta función permite que se establezca un diálogo entre el switch y cualquier equipo que se conecte a uno de sus puertos para que “negocien” los parámetros de la comunicación de forma transparente al usuario.

Sin embargo, las funciones avanzadas que ofrecen algunos modelos (como por ejemplo, la configuración de redes VLAN) sí requieren una configuración manual. A los switches que proporcionan mecanismos de configuración y gestión se les conoce como **switches gestionables** (*managed switches*).

El acceso a la configuración de dichos switches se puede hacer, o bien por un puerto especial de configuración, o por un servicio web interno que proporciona el propio switch. En el primer caso, es necesario conectar un PC a dicho puerto y acceder mediante algún software específico (como por ejemplo un programa de terminal de comandos). En el segundo caso basta con utilizar un navegador web en algún PC conectado en un puerto Ethernet del switch. **El acceso a la interfaz de configuración del switch requiere que se configure en el mismo una dirección IP dentro del rango de la red donde esté conectado.**

Algunas de las características que suelen incluir los switches gestionables y que describiremos en detalle en próximos artículos son:

- Gestión de VLAN

- Monitorización de puertos (Port Mirroring)
- Agregación de enlaces (Link Aggregation / Port Trunking)
- Seguridad IEEE 802.1X
- Control de bucles: Spanning Tree

Switches de Nivel 3 y Nivel 3 / 4

Los switches de gama alta utilizados en el troncal de redes Ethernet de mediana y gran envergadura suelen ofrecer capacidades de enrutamiento de paquetes IP. A este tipo de switches se le conoce como switches de nivel 3. Un switch de nivel 3 realiza todas las funciones de conmutación de un switch pero además proporciona funciones de enrutamiento IP. Esta característica es especialmente útil para switches que utilicen VLAN y necesiten comunicar algunas de sus redes LAN virtuales.

Además, pueden existir switches que ofrezcan características relacionadas con funciones del nivel 4, como control de puertos. A estos switches se le conoce como switches de nivel 3 / 4.

Arquitectura de las redes Ethernet

Como hemos visto anteriormente, las redes actuales basadas en Ethernet siguen una topología en estrella donde el elemento central es el switch. En los casos en los que el número de equipos supera la capacidad del switch, es posible ampliar dicha capacidad conectando otro switch a la red. En este caso, la topología sigue siendo en estrella.

Cuando el número de dispositivos de la red es alto, normalmente se sigue una cierta estructura jerárquica donde lo normal es que haya dos o tres niveles jerárquicos. En este caso la estructura de la red se corresponde a una **topología en árbol**. En las siguientes figuras se pueden ver dos ejemplos de redes Ethernet con dos y tres niveles jerárquicos respectivamente.

ROUTERS

¿Qué es un router?

Básicamente el router es un dispositivo dedicado a la tarea de administrar el tráfico de información que circula por una red de computadoras. Existen **dispositivos específicamente diseñados para la función de router**, sin embargo, una computadora común puede ser transformada en un router, tan sólo con un poco de trabajo, conocimiento y paciencia.

En la actualidad, un router puede ser usado para compartir internet, a través de cable, ADSL o WiFi con otras computadoras, **proveer protección de firewall**, controlar la calidad del servicio y otras varias tareas, principalmente en el ámbito de la seguridad.

Un router Wireless o WiFi nos provee acceso a la red local y a internet de forma inalámbrica a cualquier dispositivo, ya sea notebook, tablet, impresoras, discos de almacenamiento o smartphones que esté dentro del alcance de la señal.

Un router WiFi para el hogar o para pequeñas empresas, generalmente viene equipado de fábrica con 4 puertos para red local por cable (LAN) y un **puerto Ethernet para conectar el modem de internet** (puerto WLAN). Así, de forma simple, internet se puede compartir con cualquier dispositivo WiFi que se encuentre al alcance de la señal y que esté configurado para eso.

Es posible dar permisos a través de la dirección física de la red, del Media Access Control Address (MAC Address), **configurar los puertos de acceso a VNC, Spotify y software de descarga**. Asimismo, si un padre cree que sus hijos no deben navegar por internet a la madrugada, **el router posee controles para impedir la navegación en determinadas horas**. El control de internet y de

la red está a disposición del administrador del router. Y todo es realizado a través de una interfaz web, en el propio dispositivo.

¿Qué es un router WiFi?

Más de una vez habremos observado con el rabillo del ojo esa cajita que se encuentra cercana a nuestra PC, cuyas luces destellan permanentemente creando la magia de poder **disfrutar en toda nuestra casa de Internet por WiFi**. Esa cajita, como todos lo sabemos es un router. Pero **¿qué es en realidad este dispositivo?**

Como vimos más arriba, **un router es un dispositivo que se utiliza para distribuir señal de Internet entre todos los equipos locales conectados en red**, ya sea a través de Ethernet por intermedio de un cable, o bien por medio de la tecnología de ondas de radio, haciendo que la red se caracterice por ser inalámbrica.

En general, ambos tipos de redes poseen beneficios y desventajas, **aunque lo cierto es que la mayoría de los usuarios suelen optar por las redes inalámbricas**, debido fundamentalmente a que éstas suelen ser menos costosa y más sencillas de configurar porque no requieren tediosas conexiones de cable entre las PCs y el router.

Claro está que para poder **utilizar Internet en las computadoras que son parte de la red inalámbrica**, además del router será necesario contar con un módem. A través del módem llega la señal de Internet, por lo que el router inalámbrico debe ser conectado al módem para poder proporcionar a toda la red acceso a Internet.

No obstante, cabe destacar que en el mercado actual también **existen routers inalámbricos que poseen un módem incorporado**, lo que puede ser una excelente opción en el caso que deseemos reducir la cantidad de dispositivos.

Por supuesto, que antes de **elegir un router inalámbrico con módem incorporado**, debemos saber qué tipo de acceso a Internet poseemos, si es por cable o por DSL, ya que en base a ello podremos elegir el modelo correcto.

Otro punto importante a destacar es que como mencionamos **los routers inalámbricos funcionan utilizando ondas de radio**, las cuales se propagan realizando un patrón circular, es decir parten del router y se diseminan por el exterior del mismo. Es por ello que se vuelve importante el hecho de tener en cuenta la **fuerza de señal y velocidad que puede llegar a alcanzar el router**, ya que cuanto más fuerte es la señal, más lejos llegará la conexión.

No debemos olvidarnos que para que todo este proceso funcione, cada una de las PCs de escritorios, portátiles y dispositivos en general **deben contar con su propia tarjeta inalámbrica de WiFi interna**, y de no ser así deberemos añadirle un dispositivo externo portátil WiFi que soporte el mismo protocolo que el router inalámbrico.

Qué es un Router inalámbrico USB?

Cuando se habla de router USB, este término se refiere a los dispositivos que se utilizan para **compartir una conexión a Internet de banda ancha entre varias computadoras**, y que fundamentalmente están diseñados para ser utilizados cuando una computadora no tiene una conexión Ethernet disponible.

Pero el término «**router USB**» también suele ser utilizado para designar a un dispositivo que se conecta a una **PC que se encuentra conectado a Internet y comparte dicha conexión con otras computadoras de manera inalámbrica**. Este tipo de conexionado se conoce como una conexión ad-hoc.

Es importante destacar que **este tipo de configuración que requiere una conexión ad-hoc es mucho menos flexible que la tradicional con router**, ya que la misma necesita que la computadora principal se encuentre siempre encendida y conectada a Internet en todo momento

para que la red funcione, porque cuando el equipo principal se encuentra apagado, las otras máquinas no pueden acceder a la conexión.

Consejos para elegir un buen Router WiFi

Disponer de una conexión a Internet de calidad en un espacio amplio, como puede llegar a ser nuestro hogar o nuestro negocio, requiere necesariamente de la adquisición de un Router WiFi que nos brinda características adecuadas para ello, es decir que al comprar uno de estos dispositivos debemos tener en cuenta que **cuanto más potente es el Router, mayor será la calidad de la señal de Internet.**

Por tal motivo, **la elección del Router no debe tomarse a la ligera**, porque lo cierto es que al adquirir un buen Router podremos asegurarnos de esta forma de disponer de una cobertura amplia, una buena velocidad de transferencia de datos, mayores prestaciones en cuanto a la seguridad de la red, y al mismo tiempo también deberíamos tener en cuenta de **comprar un Router que sea sencillo de instalar.**

Claro está que con la gran variedad de Routers disponibles en el mercado actual, la elección del mismo muchas veces puede volverse un tanto tediosa, y de esta manera, en el apuro, podemos llegar a **comprar un router que no reúna las características necesarias para lograr el alcance y la potencia** que estamos requiriendo para nuestra red doméstica.

Por ello, aquí te presentamos algunas de las pautas que se deben tener en cuenta al adquirir un Router que pueden ayudarte a realizar la mejor elección:

Seguridad del router: En este aspecto, debemos **asegurarnos que el Router es compatible con los parámetros de WPA2 y no solamente con WPA.** De ninguna manera debemos optar por uno que sólo sea compatible con WEP, aunque lo cierto es que actualmente la mayoría de los Routers soportan WPA2, pero siempre debemos estar atentos para que no nos engañen.

Velocidad de transferencia del router: En el caso que nos encontremos construyendo una red en nuestro hogar, debemos **elegir un Router que soporte la velocidad de transferencia para proveer de Internet a los diversos equipos que se conectarán**, sobre todo en el caso en que todos ellos se conecten por cable, ya que los Routers poseen una cantidad limitada de salidas de Ethernet.

Router con norma Wireless compatible: Debemos **asegurarnos que el Router elegido sea compatible con Wireless-N (802.11n)**, ya que de esta forma podremos obtener velocidades de transferencia más rápidas. En este sentido, cabe destacar que Wireless-N es compatible con Wireless-G (802.11g) y con dispositivos Wireless-B (802.11b), por lo que incluso podremos conectar nuestros equipos y gadgets más antiguos.

Router de Doble banda: Si estamos buscando un Router que nos permita disponer de una mayor compatibilidad con más dispositivos inalámbricos, lo ideal es invertir un poco más de dinero y **adquirir un Router de doble banda, ya que este tipo de dispositivos transmiten señales inalámbricas en las bandas de 2,4 GHz y de 5GHz**, de manera independiente o simultánea. No obstante, el costo adicional que debemos invertir para adquirir un Router de doble banda, debemos evaluarlo cuidadosamente, en base a si realmente se ajusta a nuestras necesidades, ya que en muchos casos para una red doméstica alcanza con un Router de simple banda.

Router con WiFi Protected Setup (WPS): Si el Router que vamos a comprar posee esta leyenda en su packaging con esto nos aseguramos que la instalación del mismo será realmente sencilla, sobre todo en lo que respecta a la **conexión de nuestros dispositivos inalámbricos al Router** en cuestión.

Puertos USB: Es sumamente importante **que el Router disponga de puertos USB** en el caso en que deseemos crear una unidad de red compartida, ya que algunos modelos de Routers nos brindan la posibilidad de **conectar un disco rígido externo al Router a través del puerto USB**, y de esta

manera podemos compartir esa unidad de almacenamiento entre los diversos dispositivos que se conectan a la red.

Si bien se trata de una funcionalidad realmente muy útil, **lo cierto es que en ocasiones puede llegar a ir en detrimento de la velocidad del Router**, y volver la conexión lenta y con inconvenientes, aunque esto siempre puede solucionarse utilizando un servidor FTP para acceder a la unidad. En el caso en el que no dispongamos de dispositivo de almacenamiento del tipo NAS, **que el Router posea o no puertos USB** ya será una elección muy personal.

Tengamos en cuenta que **algunos Routers también nos permiten conectar una impresora al puerto USB** para brindar la posibilidad de disponer de impresión en red, y de esta manera utilizar el Router como servidor de impresión, claro que esto puede también tender a ralentizar el Router y por ende la fluidez de la conexión.

Firewall y soporte VPN: Esto es algo frecuente en la mayoría de los modelos de Routers disponibles en el mercado actual, ya que casi todos disponen de firewall y soporte VPN. Aquí es importante tener en cuenta que dentro de la plataforma VPN, el Router posea soporte para las normas IPSec, PPTP y L2TP.

Acceso remoto, 3G / 4G y más: Los Routers más modernos disponen de una gran cantidad de funcionalidades, como por ejemplo ser capaces de acceder a computadoras conectadas a la red en forma remota, a través del Router, como así también permitir **compartir conexiones de banda ancha 3G y 4G**. En algunos casos incluso, estos dispositivos poseen la característica de poder conectarse más fácilmente a televisores y equipos multimedia, pero como no todos los Routers soportan estas nuevas características, y los que sí lo hacen tienen un costo más elevado, deberemos evaluar si realmente requerimos de ello.

La cantidad de antenas: Es importante tener en cuenta que **la cantidad de antenas que posea el Router permite mejorar el rendimiento** del mismo al administrar una red a la cual se conecten gran cantidad de dispositivos. Por ello, siempre debemos optar por Routers con antenas externas, ya que estos poseen una mayor cobertura que aquellos que poseen antenas internas.

Configuración del hardware: Es recomendable **elegir un Router que nos permita una instalación fácil**, para poder llevar a cabo el proceso por nosotros mismos. Por ello es aconsejable optar por un dispositivo que incluya una interfaz y un manual del usuario en nuestro idioma de origen, es decir español, para entender claramente todas las instrucciones y la información de configuración del hardware.

Repetidores WiFi: En algunos casos en los que requerimos una mayor cobertura, nunca está de más la **instalación de repetidores WiFi**, ya que en un espacio cerrado, como puede ser una casa, la señal de WiFi puede llegar a sufrir diversas interferencias. Lo cierto es que las paredes, las puertas, las ventanas, las columnas y otros objetos de nuestro hogar pueden llegar a convertirse en verdaderas barreras que **reducen notablemente el rendimiento de la red**.

Por ello, es sumamente importante **elegir el lugar exacto más adecuado para colocar el Router**, y al mismo tiempo evaluar la posibilidad de instalar repetidores WiFi donde la señal es débil. Es importante también detectar interferencias, ya que tengamos en cuenta que la señal del Router es una señal de radio, debido a lo cual otros dispositivos que utilizan tecnologías similares, como por ejemplo teléfonos inalámbricos o microondas, puede llegar a causar interferencias en la red, y es allí donde **se recomienda la instalación de repetidores WiFi**.

Previsión a futuro: Por último, y no menos importante, al adquirir un Router WiFi debemos tener en cuenta que se trata de un dispositivo que nos servirá durante varios años, por lo que debemos ser previsores y elegir un Router que nos sea útil en el futuro, **teniendo en cuenta que las conexiones a Internet son cada vez más rápidas**, y que cada vez transmitimos a través de la red doméstica archivos más grandes, como por ejemplo una película que tenemos en la PC y queremos ver en la tablet.

¿Qué tiene que tener un router?

Prácticamente todos los routers vendidos en el mercado actualmente poseen el mismo conjunto mínimo de funcionalidades que seguramente van a colmar tus expectativas. En este punto, las siguientes preguntas pueden servirnos como guía a la hora de comprar un router para que se adapte perfectamente a nuestras necesidades.

- ¿Cuáles son los protocolos disponibles?
- ¿IP estático y dinámico? Servidor DHCP?
- ¿Tiene NAT para TCP y UDP?
- ¿Soporta PPPoE y SNTP?
- ¿Posee DMZ, Firewall, Reglas de acceso, interfaz de administración por browser?
- ¿Cuántos puertos externos posee?
- ¿Cuál el límite de usuarios simultáneos WiFi soporta?
- ¿Qué protocolos WiFi soporta? 802.11a b/g/n?
- ¿Cuál el alcance de la señal WiFi?
- ¿Cuál es la capacidad para conexiones simultáneas?
- ¿Tiene puerto WLAN?
- ¿Tiene servidor de impresión incluido?
- Es de marca reconocida, como por ejemplo DLink, Linksys, Netgear, 3COM, Trendnet, Encore o TPLink?

Como ampliar el alcance de nuestro router WiFi

El alcance inalámbrico que ofrece el router puede variar dependiendo de la conexión WiFi estándar que soporta y los obstáculos que puedan interferir entre los diferentes puntos de conexión. La norma inalámbrica 802.11n, ofrecen por lo general un mayor alcance, pero incluso así es posible que la señal no alcance a todos los rincones de nuestro hogar o negocio. A partir de este punto conoceremos **como ampliar la señal WiFi con un router viejo**.

Como sabemos, realizar esta tarea sería muy sencillo, tan sólo **comprando todo el hardware necesario como repetidores WiFi y dispositivos de puntos de acceso inalámbrico** estaríamos en condiciones de implementarla, pero si deseamos ahorrarnos un importante dinero, podremos hacerlo mediante un simple router inalámbrico en desuso y un cable Ethernet.

Como ejemplo podemos tomar una edificación de aproximadamente 30 metros por 60 metros con algunas paredes ofreciendo un importante obstáculo. Aun así, todavía podemos tener **acceso a Internet en la mayor parte de las instalaciones**.

Lograr ampliar el alcance de la señal es muy sencillo. Como sabemos **nuestra señal WiFi proviene de un router inalámbrico conectado al modem** provisto por nuestra operadora de Internet.

Lo único que tendremos que hacer es conectar un segundo router inalámbrico Wireless-G al router principal mediante un cable Ethernet.

Usar un segundo router como punto de acceso

Para comenzar con la tarea, lo primero que tenemos que hacer es diferenciar los routers. Para ello, vamos a denominar «**Router1**» al dispositivo que ya estamos utilizando en la red local inalámbrica, y «**Router2**» al segundo router que usaremos para aumentar el alcance inalámbrico.

Configuración de «Router1»

Paso 1

Primero tenemos que determinar la dirección IP de «**Router1**». Para ello debemos copiar y pegar el siguiente comando «**cmd /k ipconfig**» en el cuadro «**Ejecutar**» de Windows y anotar el valor de «Puerta de enlace predeterminada.», ya que esa es la dirección IP de nuestro router.

Vamos a suponer que la dirección IP del router es 192.168.30.1. Cabe destacar que también debemos anotar el valor de la máscara de subred, que suele ser 255.255.255.0.

Paso 2

Ejecutamos nuestro navegador favorito e introducimos la dirección IP de «**Router1**» en la barra de direcciones.

En este punto es posible que debamos proporcionar una **contraseña para acceder a la configuración del router**. Esto puede variar dependiendo del fabricante del router.

Si no estamos seguros, podemos usar Google para saberlo introduciendo la siguiente búsqueda: «**MARCA-ROUTER contraseña por defecto**»

Paso 3

Una vez en la configuración del router «**Router1**», cambiamos a la pestaña de configuración inalámbrica y tomamos nota de la modalidad inalámbrica, el SSID y el canal.

En el caso de que tengamos protegida nuestra red WiFi con una contraseña, también debemos tomar nota del modo de seguridad utilizado (WPA, WEP y WPA2) y la contraseña.

Configuración de «Router2»

Paso 4

En primer lugar tendremos que reiniciar el router a los valores de fábrica pulsando el botón de reinicio incorporado en el dispositivo durante unos 10 segundos.

Conectamos «**Router2**» a nuestra computadora mediante el cable Ethernet. Enchufamos un extremo del cable en cualquiera de los **puertos LAN disponibles en el router** y el otro extremo al puerto Ethernet de la computadora. Es importante comprobar que el router está encendido.

Paso 5

Abrimos el navegador e introducimos la siguiente dirección: 192.168.1.1, la cual es la dirección IP de Internet por defecto del router «**Router2**».

Una vez que accedemos al router, será necesario cambiar los valores de la SSID por defecto, el modo inalámbrico, el canal, el modo de seguridad y la contraseña de manera que coincidan con el router «**Router1**».

A continuación, nos desplazamos hasta «**Configuración>Opciones avanzadas de enrutamiento**» y cambiamos el modo actual de «**puerta de enlace**» a «**router**». También es necesario deshabilitar el servidor DHCP del router ya que «**Router1**» se encargará de la tarea de asignar direcciones IP a los dispositivos de conexión a la red inalámbrica.

Por último, también es necesario cambiar la dirección IP del router «**Router2**» a cualquier dirección libre en nuestra LAN. Por ejemplo, si la dirección IP del router «**Router1**» es 192.168.30.1, podremos asignarle a «**Router2**» la dirección 192.168.30.2 sin dificultades.

Es necesario asegurarse también de que la máscara de subred es la misma que la establecida en el paso 1.

Luego de ello, es necesario guardar la configuración.

Conexión de los routers

Ahora que hemos configurado ambos dispositivos, es momento de conectarlos físicamente con cables.

Lo más seguro es **«Router1»** cuente con una configuración de 5 puertos.

El puerto WAN deberá conectarse al modem de la proveedora ISP.

Ahora podemos seleccionar cualquiera de los puertos disponibles en el router **«Router1»** y conectarlo a cualquiera de los puertos LAN del router **«Router2»** con un cable Ethernet.

Ahora que todo está configurado, podremos **conectar nuestra computadora y los dispositivos móviles con el segundo router con una conexión cableada o por WiFi**. Cabe destacar que los tres puertos restantes siguen estando disponibles.

Como **tenemos asignado el mismo SSID** y configuraciones de seguridad para el segundo router, no debemos configurar ningún parámetro en la computadora portátil mientras nos encontremos cerca de la fuente de emisión.

Además, **como se acaba de ampliar el alcance de una red inalámbrica existente y no crear una nueva**, todas las carpetas compartidas, bibliotecas de música, imágenes y otros archivos serán accesibles desde todas las computadoras y dispositivos móviles conectados a la red doméstica.

Cómo convertir la PC en un router WiFi

Desde que las conexiones inalámbricas a Internet se han vuelto la plataforma de este tipo más utilizada en todo el mundo, **WiFi ha pasado a ser la conexión por excelencia**, no sólo en los ámbitos laborales y públicos, sino también a nivel hogareño.

Esto se debe obviamente a varios factores, pero sobre todo a la comodidad que brinda poder instalar los equipos sin la utilización de cables, y sobre todo al hecho de poder **disponer de conexión a Internet en cada espacio de la casa**, con lo cual podemos aprovechar la señal no sólo en la tradicional computadora de escritorio, sino también en notebooks, tablets y teléfonos inteligentes.

Lo cierto es que además en líneas generales la instalación de un router WiFi, e incluso de repetidores en espacio determinados, en la actualidad es una labor más que sencilla, que cualquier usuario puede llevar a cabo, ya que sólo hace falta **conectar el router al módem** y a la corriente eléctrica, y ya podemos disfrutar de conexión en todos los ambientes de nuestro hogar.

No obstante, **si no disponemos de router WiFi**, siempre podemos recurrir a algún truco que nos permita establecer este tipo de conexión inalámbrica, como por ejemplo utilizar una computadora de escritorio o una portátil, que posean el sistema operativo Windows 7, para convertirla en un router inalámbrico. Aunque parezca mentira, esto es posible.

Precisamente, aquí te contamos cuál es el **método a seguir para lograr distribuir la conexión a Internet desde una PC al resto de los dispositivos**. Para ello, debemos llevar a cabo los siguientes pasos:

Paso 1

Lo primero que debemos hacer es descargar la aplicación gratuita **Free WiFi Hotspot**, la cual podemos encontrar en este enlace.

Paso 2

Una vez que hayamos instalado el programa, lo ejecutamos y completamos el campo en el cual deberemos **ponerle nombre a la conexión inalámbrica**, como así también la contraseña que nos permitirá proteger el acceso.

Paso 3

Luego, en la siguiente ventana de la **configuración de Free WiFi Hotspot** deberemos seleccionar el tipo de conexión que deseamos compartir desde la PC que será el router y el resto de los dispositivos, para lo cual podemos elegir entre Ethernet, Bluetooth o WiFi, y aquí por supuesto optamos por WiFi.

Paso 4

A continuación, debemos hacer clic en el botón **“Start”**, para iniciar la conexión.

Paso 5

Una vez finalizado todo el proceso, debemos corroborar en la PC que se encuentra cumpliendo el rol de router, si la conexión se encuentra disponible.

Es importante tener en cuenta que **el equipo que distribuye la señal no podrá conectarse al punto de acceso virtual creado con Free WiFi Hotspot**, por lo cual debemos llevar a cabo las pruebas de la existencia de la red desde cualquier otro dispositivo que utilice conexión WiFi, como puede ser una tablet o un smartphone.

Cabe destacar que Free WiFi Hotspot además de ser una herramienta que permite **convertir una computadora de escritorio o una notebook en un punto de acceso a Internet WiFi** para distribuir la señal, también ofrece para los usuarios más avanzados, información acerca del estado de la conexión de red.

Para ello, sólo debemos hacer clic sobre el botón **“Info”**, y de esta forma el programa nos proporciona datos tales como la dirección IP de la red, el canal utilizado y el número de clientes conectados, entre otros. Además se trata de una aplicación que posee una interfaz gráfica realmente intuitiva, por lo que es muy sencilla de instalar y utilizar.

¿Cómo proteger mi router de las amenazas de Internet?

Desde hace años, Internet ha sido no sólo una plataforma fantástica para la comunicación y la difusión de información, sino también un espacio que muchos malintencionados han encontrado para llevar a cabo sus daños. Lo cierto es que según las cifras, **la mayor parte de los virus informáticos, el malware y el código malicioso se propagan a través de Internet**, y muchas veces por la falta de conciencia o de conocimiento podemos llegar a convertirnos en víctimas de algún hacker.

Dentro de lo que contiene la plataforma de Internet, **el router que suministra conexión en nuestro hogar o en nuestro trabajo** es considerado como la puerta de ingreso para estos ataques, por lo que para evitar inconvenientes de este tipo, es sumamente importante proteger los routers de forma eficaz, sobre todo los equipos que brindan conexión inalámbrica WiFi.

Por ello, a continuación te acercamos algunos procedimientos que son de gran utilidad para poder **proteger el router y evitar daños en los equipos**.

Cambio de la contraseña del router: Como muchos saben, **los routers incluyen de fábrica un usuario y una contraseña**, los cuales vienen incorporados por defecto para poder comenzar a utilizarlos de manera sencilla. Esto hace que muchas veces la contraseña se vuelva reconocible por los hackers, y de esta forma **estos piratas informáticos pueden acceder de forma sencilla**, a través de nuestro router, a la red privada, y desde allí causar el daño que deseen.

Por ello se recomienda al adquirir un router, llevar a cabo la **modificación del código de seguridad de la conexión WiFi**, para lo cual en principio debemos abrir el navegador y escribir la dirección IP del router. Esta dirección la podemos hallar impresa en el cuerpo del dispositivo.

Una vez realizado esto, **introducimos el nombre de usuario y la contraseña por defecto que vino de fábrica con el router**. Es importante mencionar que en la mayoría de los casos, ambos son **«admin»**, no obstante puede llegar a variar de acuerdo al modelo y marca del dispositivo, pero

no debemos desesperar, ya que para poder disponer de esta información sólo bastará con realizar una simple búsqueda en la web especificando la marca y el modelo del router.

Cuando ya hayamos ingresado con el nombre de usuario y la contraseña por defecto, **nos dirigimos al apartado de la configuración de la seguridad del dispositivo**, y allí encontraremos las opciones para cambiar el nombre de usuario y contraseña.

Podemos optar por sólo modificar la contraseña, aunque se recomienda también modificar el nombre de usuario, claro que **debemos tener en cuenta que el nuevo nombre de usuario que elijamos no debe tener ni nuestro nombre ni nuestro apellido**, como así tampoco términos que puedan llegar a señalar alguna relación entre el router y nosotros, como por ejemplo un apodo conocido por todos.

Actualización del firmware: Muchos usuarios suelen llegar a resultar incluso obsesionados con la **actualización del software**, pero lo cierto es que mantener el software al día es fundamental para reforzar la seguridad informática. En el caso de los router sucede lo mismo, ya que las actualizaciones del firmware del mismo permiten corregir errores críticos de seguridad que puedan haber incluido el software del dispositivo al salir de la fábrica.

Para realizar este proceso, si bien el mismo puede variar de acuerdo a la marca y el modelo del dispositivo, no obstante en las páginas webs oficiales de los fabricantes de los router siempre podemos hallar para **descargar las actualización del firmware**, por lo que sólo debemos buscar el sitio del fabricante, y luego descargar e instalar el que sea correcto al modelo de router del cual disponemos.

Utilizar WPA o WPA2 en vez de WEP: Si bien en la actualidad la gran mayoría de los modelos de router disponibles en el mercado suelen estar preprogramados para operar con WEP, lo más recomendable es **cambiar la contraseña para conectarse a la red a WPA o WPA2**, ya que estas son más seguras que la primera, debido a que utilizan plataformas desarrolladas a prueba de «aircrack-ng».

Para ello, lo que debemos hacer es en principio iniciar sesión en el router, y dirigirnos a las opciones de “**Wireless**” y “**Conexión Primaria**”. A continuación comprobamos allí si se encuentra habilitada WEP, y si es así lo que haremos es **deshabilitar WEP y habilitar WPA/WPA2**. En algunos casos es posible que el sistema nos solicite el reingreso de la contraseña, es decir la creación de una contraseña nueva.

En este punto, **se recomienda elegir una contraseña segura**, es decir que la misma incluya letras, números y caracteres especiales, con el fin de evitar que esta password sea sencilla de descubrir.

Desactivar la WPS: Si bien no es el caso de todos los modelos, lo cierto es que **muchos routers actuales soportan WPS**, siglas de WiFi Protected Setup, brindando de esta forma un método de configuración de seguridad mucho más sencillo para el usuario.

No obstante, **el recurso WPS hace que el dispositivo se vuelva más vulnerables**, y con la utilización de números de PIN de 8 números, hace que los mismos puedan ser más fácilmente descifrados por los hackers. Por ello, se recomienda desactivar la función también en el menú «**Seguridad**» del router.

Ocultar nuestro nombre en la red: Debido a parámetros propios de la plataforma, de forma predeterminada todas las redes WiFi quedan a la vista de todos, **ya que esto facilita hallarlas cuando queremos conectarnos a la red**, claro que esto también vuelve a las redes mucho más vulnerables a los ataques informáticos.

Por ello, lo más aconsejable es **ocultar el nombre de nuestra red**, y de esta manera cada vez que un usuario desee conectarse deberá escribir manualmente su nombre para poder conectarse. Para activar esta función sólo debemos buscar en el apartado “**Broadcast SSID**” o “**SSID Broadcast**”, y desactivar la casilla de muestreo de la red, para que permanezca oculta.

Establecer sólo conexiones permitidas: Sin lugar a dudas, una de las mejores alternativas para poder prevenir el **acceso de personas no autorizadas a nuestra red** reside en configurar una serie de permisos específicos en el router, de acuerdo con la dirección MAC de cada dispositivo que tengamos en casa o en la oficina.

Para ello, debemos primero acceder a la configuración de seguridad del router, y allí buscar la opción **“Access Control”** o **“Control de Acceso”**. Luego habilitamos la casilla para que funcione el filtro por dirección MAC, e introducimos la lista de los dispositivos que poseen permisos para acceder a la red.

Así atendemos que hay muchas características y posibilidades entre cada uno de los distintos dispositivos.

Solo destacar que, si bien el switch es mucho mejor, estable, configurable y permite más dispositivos a la hora de montar una red, es un router el que necesitamos si es que queremos que la misma tenga acceso a internet. Ya que encontramos que es muy fácil que en la estructura de una red encontremos ambos dispositivos siendo que incluso a veces el modem del proveedor de servicios es que lo encontramos como una suerte de router, solo que este nos provee solo de la conexión y no está pensado para poder montar una red, haciendo que todos los dispositivos conectados a él se vean entre sí, para poder transferir archivos de forma privada.

Así que podemos sumar el modem del proveedor de servicios como otro dispositivo más, siempre toda esta estructura es dependiente de la red que montemos, en una red simple y hogareña, más de una vez con un simple modem y después un router Wi-Fi, es más que suficiente, pero en redes empresariales es normal que encontremos todo lo visto anteriormente, de diversas maneras, siempre siendo que lo más importante de todo es la protección de datos, después la fidelidad de los mismos y finalmente la estabilidad de la conexión para que la misma no se interrumpa bajo ninguna circunstancia.

SERVER - HOST

Así es que encontramos y entramos en el mundo de los server y host. Pero ¿Qué es esto en realidad?

Básicamente un servidor es una terminal o pc, apuntada al almacenamiento y tráfico de la información, claro está que estos servidores son estructuras complejas y caras, en cuanto a que no son simple terminales para que un usuario acceda, sino que son más bien computadoras selladas a las cuales se accede por fuera siendo un usuario especializado y solo bajo ciertas circunstancias es que se accede a la misma por el propio modulo del servidor en cuestión.

Su mayor virtud es la seguridad de los datos y la protección de los mismos.

Los datos pueden accederse de forma remota como directa, a través de internet como ciertos programas de acceso remoto directo.

Acá encontramos ya principales diferencias y en ellas las ventajas y desventajas.

En el mundo de los servidores principalmente encontramos que hay de 2 tipo.

Los dedicados y los NO dedicados, de ellos después podemos desprender diferentes tipos de servidores, como por ejemplo un servidor SMTP que es el que se encarga solamente del manejo de correos electrónicos, por solo citar un ejemplo; pero eso no es más importante como si destacar la diferencia entre dedicado a NO dedicado. Así que entraremos en el mundo de los servidores.

¿Qué es un servidor?

El término servidor tiene **dos significados** en el ámbito informático. El primero hace referencia al ordenador que pone recursos a disposición a través de una red, y el segundo se refiere al programa que funciona en dicho ordenador. En consecuencia, aparecen **dos definiciones de servidor**:

- **Definición Servidor (hardware):** un servidor basado en hardware es una máquina física integrada en una red informática en la que, además del sistema operativo, funcionan uno o varios servidores basados en software. Una denominación alternativa para un servidor basado en hardware es "host" (término inglés para "anfitrión"). En principio, todo ordenador puede usarse como "host" con el correspondiente software para servidores.
- **Definición Servidor (software):** un servidor basado en software es un programa que ofrece un servicio especial que otros programas denominados clientes (clients) pueden usar a nivel local o a través de una red. El tipo de servicio depende del tipo de software del servidor. La base de la comunicación es el modelo cliente-servidor y, en lo que concierne al intercambio de datos, entran en acción los protocolos de transmisión específicos del servicio.

¿Cómo funciona un servidor?

La puesta a disposición de los servicios del servidor a través de una red informática se basa en el **modelo cliente-servidor**, concepto que hace posible distribuir las tareas entre los diferentes ordenadores y hacerlas accesibles para más de un usuario final de manera independiente. Cada servicio disponible a través de una red será ofrecido por un servidor (software) que está permanentemente en espera. Este es el único modo de asegurar que los clientes como el navegador web o los clientes de correo electrónico siempre tengan la posibilidad de acceder al servidor activamente y de usar el servicio en función de sus necesidades.

Tipos de servidores

La comunicación entre cliente y servidor depende de cada servicio y se define por medio de un protocolo de transmisión. Este principio puede aclararse partiendo de los siguientes **tipos de servidores**:

- **Servidor web:** la tarea principal de un servidor web es la de guardar y organizar páginas web y entregarlas a clientes como navegadores web o crawlers. La comunicación entre servidor (software) y cliente se basa en HTTP, es decir, en el protocolo de transferencia de hipertexto o en HTTPS, la variante codificada. Por regla general, se transmiten documentos HTML y los elementos integrados en ellos, tales como imágenes, hojas de estilo o scripts. Los servidores web más populares son el servidor HTTP Apache, los servicios de Internet Information Server de Microsoft (ISS) o el servidor Nginx.
- **Servidor de archivos:** un servidor de archivos se encarga de almacenar los datos a los que acceden los diferentes clientes a través de una red. Las empresas apuestan por dicha gestión de archivos para que sea mayor el número de grupos de trabajo que tengan acceso a los mismos datos. Un servidor de archivos contrarresta los conflictos originados por las diferentes versiones de archivos locales y hace posible tanto la creación automática de las diferentes versiones de datos como la realización de una copia de seguridad central de la totalidad de datos de la empresa. En el acceso al servidor de archivos por medio de Internet entran en juego protocolos de transmisión como FTP (File Transfer Protocol), SFTP (Secure File Transfer Protocol), FTPS (FTP over SSL) o SCP (Secure Copy). Los protocolos SMB (Server Message Block) y NFS (Network File System) se encuentran habitualmente en las redes de área locales (LAN).

- **Servidor de correo electrónico:** un servidor de correo electrónico consta de varios módulos de software cuya interacción hace posible la recepción, el envío y el reenvío de correos electrónicos, así como su puesta a punto para que estén disponibles. Por regla general funciona mediante el protocolo de transferencia simple de correo (SMTP). Los usuarios que quieran acceder a un servidor de correo electrónico necesitan un cliente de correo electrónico que recoja los mensajes del servidor y los entregue en la bandeja de entrada, proceso que tiene lugar a través de los protocolos IMAP (Internet Message Access Protocol) o POP (Post Office Protocol).
- **Servidor de base de datos:** un servidor de base de datos es un programa informático que posibilita que otros programas puedan acceder a uno o varios sistemas de bases de datos a través de una red. Las soluciones de software con una elevada cuota de mercado son Oracle, MySQL, Microsoft SQL Server, PostgreSQL y DB2. Los servidores de bases de datos ayudan a los servidores web, por regla general, a la hora de almacenar y entregar datos.
- **Servidor de juegos:** los servidores de juegos son servidores (software) creados específicamente para juegos multijugador online. Estos servidores gestionan los datos del juego online y permiten la interacción sincrónica con el mundo virtual. La base de hardware de un servidor de juegos se encuentra en el centro de datos de los proveedores especializados o está disponible en una red doméstica local.
- **Servidor proxy:** el servidor proxy sirve como interfaz de comunicación en las redes informáticas. En su papel de intermediario, el servidor proxy recibe las solicitudes de red y las transmite a través de su propia dirección IP. Los servidores proxy se usan para filtrar la comunicación, para controlar el ancho de banda, para aumentar la disponibilidad a través del reparto de cargas, así como para guardar datos temporalmente (caching). Además, los servidores proxy permiten una amplia anonimización, ya que la dirección IP del cliente queda oculta en el proxy.
- **Servidor DNS:** el servidor DNS o servidor de nombres permite la resolución de nombres en una red. Los servidores DNS son de vital importancia para la red informática mundial (WWW), ya que traducen los nombres de host como www.example.com en la correspondiente dirección IP. Si quieres saber más sobre los servidores de nombres y sobre el sistema de nombres de dominio (DNS), visita nuestra guía digital.

¿Qué es un servidor no dedicado o compartido?

Una de las grandes diferencias entre los *Servidores Dedicados y No Dedicados* es que los servidores no dedicados o servidores compartidos son aquellos que te permiten alojar un sitio web utilizando los recursos de un servidor, no obstante deberás compartir los recursos físicos de hardware con otros sitios web, este tipo de servidores resultan apropiados y muy recomendables para aquellos sitios web que apenas están empezando y por el momento no esperan tener altos índices de tráfico.

Dentro de las ofertas de servidores compartidos podrás encontrar un gran número de posibilidades, desde aquellos servicios que hospedan o permiten que hospedes un solo sitio web, es decir, un solo dominio; hasta aquellos que permiten alojar dominios ilimitados, en cualquier caso una vez tu sitio web incremente su tamaño y su número de visitas, tendrás que retirarte de este servicio.

¿Qué es un servidor dedicado?

La principal diferencia entre los *Servidores Dedicados y No Dedicados* es que los servidores dedicados son servidores físicos que contienen una o varias páginas web de un mismo propietario en su interior, es decir que un solo servidor alojará tus páginas web, de este modo te permitirá tener

la gran ventaja de que todos los recursos se encuentran disponibles para ti, fuera de esto tendrás una mayor garantía sobre la seguridad de tu sitio web, esto quiere decir que no se podrá acceder a través de otras páginas webs como en los servidores no dedicados o servidores compartidos.

Los recursos de los cuales dispone un servidor dedicado pueden ir desde los 1 Ghz hasta procesadores de 8X2 Cores a 3 Ghz cada uno, si consideras que esto es demasiada capacidad, entonces puedes dar un vistazo por los Big Boards, en los cuales la RAM va desde los 256 Mb, hasta los 64 Gb por cada uno de los servidores.

Sin lugar a dudas, otra diferencia importante entre los ***Servidores Dedicados y No Dedicados*** es el costo, ya que los servidores dedicados son mucho más caros que los servidores no dedicados o compartidos; su uso es principalmente recomendable en caso tal de que tu web cuente con una gran afluencia de usuarios o una gran actividad web, por lo tanto este puede ser un factor determinante para elegir así el tipo de servidor al cual accederás ya que si tu página web está empezando entonces no necesitarás acceder a los servicios de un servidor dedicado.

En el mundo de los servidores encontramos que también disponemos de diferentes maneras del manejo del almacenamiento de nuestra información, tenemos simplemente diferentes sitios de alojamiento de datos, algunos gratuitos y otros pagos, claro está que en las diferentes modalidades encontraremos diferentes prestaciones.

Para citar algún ejemplo de lo más popular, encontramos el sitio de MEGA (www.mega.nz) es un sitio de almacenamiento de información que nos facilita un enlace con el cual al pegarlo en nuestro navegador web o algún gestor (Ej: JDownloader) es que podemos descargar lo subido a nuestro pc, la particularidad es que lo que subimos no lo manejamos en el lugar asignado cosa que, si podemos hacer a veces con los servidores, solo podemos subir y descargar datos.

Acá entramos en el mundo del hosting o más bien que es un hosting

¿Qué es un hosting? Hosting web explicado para principiantes

El web hosting es un servicio en línea que te permite publicar un sitio o aplicación web en Internet. Cuando te registras en un servicio de alojamiento, básicamente alquilas un espacio en un servidor donde puedes almacenar todos los archivos y datos necesarios para que tu sitio web funcione correctamente.

¿Cómo funciona el hosting web?

Un servidor es una computadora física que funciona ininterrumpidamente para que tu sitio web esté disponible todo el tiempo para cualquier persona que quiera verlo. Tu proveedor de alojamiento es el responsable de mantener el servidor en funcionamiento, protegerlo de ataques maliciosos y transferir tu contenido (texto, imágenes, archivos) desde el servidor a los navegadores de tus visitantes.

Cuando decides crear un nuevo sitio web, tienes que encontrar una empresa de hosting que te proporcione espacio en un servidor. Tu proveedor de hosting almacena todos tus archivos, medios y bases de datos en el servidor. Cada vez que alguien escribe tu **nombre de dominio** en la barra de direcciones de su navegador, tu servidor transfiere todos los archivos necesarios para atender la solicitud.

Así que, debes elegir el plan de alojamiento que mejor se adapte a tus necesidades y comprarlo. De hecho, el hosting web funciona de manera similar al alquiler de viviendas, tienes que pagar el alquiler regularmente para poder mantener el servidor funcionando continuamente.

Diferentes tipos de hosting

La mayoría de los proveedores de alojamiento ofrecen diferentes tipos de hosting web para poder satisfacer las necesidades de diferentes clientes, ya sea que desees crear un **blog personal simple** o

ser dueño de un gran negocio en línea y necesites un sitio web intrincado para tu empresa. Estas son las opciones disponibles más populares:

- **Hosting Compartido**
- **Hosting VPS (Servidor privado virtual)**
- **Alojamiento en la nube (Cloud Hosting)**
- **Hosting WordPress**
- **Hosting con servidor dedicado**



[FTP](#)

Servidor FTP

Y un servidor FTP es otra aplicación -o servicio- que usa el protocolo FTP (File Transfer Protocol) para compartir archivos con otros usuarios. El acceso a este servidor FTP se hace introduciendo ciertos datos necesarios para la conexión, como la dirección del servidor. El FTP es un protocolo de red: un conjunto de reglas que establecen cómo deben comunicarse dos o más entidades para lograr la transmisión de información. En el caso específico del FTP, es un protocolo centrado en la transferencia de archivos a través de una red de tipo TCP/IP que se basa en la arquitectura cliente-servidor.

El equipo cliente, en este marco, se conecta al servidor mediante el FTP con el objetivo de enviar o descargar archivos. Este protocolo busca maximizar la velocidad, sin apelar al cifrado para proteger la información. Por eso muchas veces se recurre a aplicaciones que posibilitan la transferencia del material, pero con el tráfico cifrado.

Gracias al FTP, se pueden comunicar dos computadoras (ordenadores) que no utilizan el mismo sistema operativo. Eso es posible ya que las entidades en comunicación emplean el mismo protocolo que ya está estandarizado.

Lo que hacen las reglas del FTP es establecer los parámetros necesarios para lograr la conexión (indicando el modo de transferencia, los puertos, etc.) y especificar qué tipo de operación se llevará a cabo en el sistema de archivos (agregar, eliminar, copiar). Como la conexión es bidireccional, se pueden descargar y enviar archivos de manera simultánea.

Por lo general, para establecer la comunicación el usuario usa un cliente FTP, que es un software que apela al FTP para conectarse a un servidor FTP (otro programa, cuya función es posibilitar el intercambio de archivos entre distintas computadoras). El cliente FTP, al conectarse al servidor FTP, puede subir o descargar archivos de otro equipo.

Además del hecho de que los equipos conectados no deban tener el mismo sistema operativo para subir o descargar archivos, tampoco es necesario que compartan la misma arquitectura. En este caso, el término arquitectura hace referencia a la estructura y el diseño de un sistema que describe de manera funcional todas las características y los requisitos para la fabricación de un tipo de dispositivo dado, con un enfoque primordial en el modo que tiene el procesador principal de trabajar y acceder a la memoria.

A grandes rasgos, podemos decir que los teléfonos móviles con el sistema operativo Android se basan en una arquitectura de procesador diferente a los ordenadores que usan Windows, por ejemplo. Esto no impide, por lo tanto, que estos dos grupos se conecten entre sí para intercambiar archivos por medio de un servidor FTP. De esta manera,



podemos enviar fotografías y vídeos del teléfono a nuestro ordenador para realizar copias de seguridad, una práctica muy común.

Es importante señalar que si el intercambio de archivos por medio de un servidor FTP se lleva a cabo entre dispositivos que compartan la misma conexión de red no es necesario el acceso a Internet; dicho de otra manera, aquellos usuarios que pagan por una conexión medida a Internet, con un límite de consumo al mes, no deben preocuparse ya que todas las subidas y las descargas que realicen en este contexto no usarán datos de sus planes.

La familia de productos más usada con estos propósitos es FileZilla, que ofrece tanto un cliente como un servidor FTP de código abierto. Gracias estas dos opciones, ambas gratuitas, millones de personas configuran a diario sus sistemas de intercambio de archivos sin problemas. En sus orígenes, FileZilla funcionaba exclusivamente en el sistema operativo Windows, pero en la actualidad también se puede instalar en macOS, FreeBSD y GNU/Linux, entre otros. Cabe aclarar que no tiene relación alguna con la empresa Mozilla, a pesar de su nombre

Como se usa:

En cuanto a **cómo funciona el protocolo FTP**, es muy sencillo. Una persona abre desde su ordenador un programa cliente **FTP** para conectar con otro ordenador que tiene un programa servidor **FTP**. Cuando la conexión se establece, el cliente debe autenticarse con un nombre de usuario y una contraseña

IPCONFIG

1. QUÉ ES IPCONFIG

Muchos usuarios piensan que **ipconfig** es un comando del símbolo del sistema, pero de hecho es una utilidad de Windows que se ejecuta desde el símbolo del sistema. Además de darle la dirección IP de la computadora actual, también le brinda la **dirección IP de tu enrutador (router)**, su **dirección MAC** y le **permite eliminar tu DNS**, entre otras cosas. Funciona con varias otras opciones de línea de comando para brindarte esta información.

Puede ejecutar el comando *ipconfig* en una ventana de símbolo del sistema normal, es decir, no necesita derechos administrativos para ejecutarlo.

2. COMANDO IPCONFIG

Si ejecuta el comando *ipconfig* sin opciones de línea de comando adicionales, mostrará una lista de todas las interfaces de red, incluidos los adaptadores de red virtuales. Para su adaptador LAN y WiFi, le dará la dirección IP local.

Si está conectado a Internet a través de WiFi, verá los valores de IPv6 y máscara de subred debajo de él. Para un adaptador de Ethernet que no está conectado a una red, no verá ninguna de esta información. Simplemente le dirá que el adaptador no está conectado. Los adaptadores virtuales, estén o no conectados, tendrán una dirección IPv6 e IPv4, así como un valor de máscara de subred.

3. OPCIONES DE LÍNEA DE COMANDO IPCONFIG

La herramienta *ipconfig* en Windows tiene las siguientes opciones de línea de comando adicionales con las que puede usarla.

- **ipconfig /all:** este comando enumera información de IP para cada adaptador de red en tu sistema. A diferencia del comando simple *ipconfig*, este comando muestra información adicional, como si DHCP está habilitado, la dirección IP de los servidores DHCP, su dirección IPv6 local y cuándo se obtuvo su concesión DHCP, y cuándo caducará, entre otras cosas. También puede usar este comando para encontrar la dirección física, es decir, **la dirección MAC** para tu sistema.
- **ipconfig /release:** este comando le permite dejar/renunciar tu dirección IP actual. Cuando ejecuta este comando, la dirección IP de tu sistema, sea lo que sea, se libera para que otros dispositivos en la red puedan usarla.
- **ipconfig /renew:** este comando generalmente se ejecuta justo después del comando *ipconfig /release*. Una vez que el comando *ipconfig /release* ha ‘abandonado’ una dirección IP, tu sistema necesitará una nueva. Este comando permite que tu sistema obtenga una nueva dirección IP. Esta opción, junto con la anterior, es lo que necesita ejecutar para resolver el error de “**conflicto de dirección IP**” que puede darse a veces.
- **ipconfig /showclassid:** Esto le permite ver las ID de clase DHCP. Estas ID de clase normalmente están configuradas para aplicaciones particulares en una red. Como usuario promedio, no le preocuparán en absoluto.
- **ipconfig /setclassid:** esta opción de comando se usa con la opción previa *ipconfig /showclassid* para establecer la ID de clase DHCP.
- **ipconfig /displaydns:** esta opción le permite visualizar el caché de DNS. El caché DNS es un registro de sitios web públicos que ha visitado. Es una copia local del sitio web y tu dirección IP pública. Básicamente, cuando escribes www.google.com en tu navegador, tu caché de DNS ya sabe dónde encontrar este sitio web porque tu dirección IP está guardada en el caché.
- **ipconfig /flushdns:** el DNS no es omnipotente. Es propenso a guardar información incorrecta que a su vez le impide acceder a sitios web. Este comando le permite descargar, es decir, borrar el caché de DNS en Windows y crear uno nuevo.
- **ipconfig /registerdns:** esta opción te permite actualizar tus configuraciones de DNS. Si el DNS no ha podido registrar un nombre o no se ha podido conectar a un servidor DHCP, este comando puede resolver el problema volviendo a registrar el DNS.

Esto sirve como comando interno a la hora de poder ver datos, así como dentro de aspectos básicos poder manejar nuestra red interna, cuando esto se traduce a cuestiones del manejo de nuestro proveedor de internet por lo general depende del mismo para aspectos o cambios más avanzados.

PING

QUÉ ES EL COMANDO PING

Ping es el comando TCP/IP principal que se usa para solucionar problemas de conectividad, disponibilidad y resolución de nombres. Si se usa sin parámetros, este comando muestra el contenido de la Ayuda. También puede usar este comando para probar el nombre del equipo y la dirección IP del equipo.

-t

Hace ping al host especificado hasta que se detiene.
Para detener, pulse Control-C

-a	Resolver direcciones de nombres de host
-n	Número de solicitudes de eco para enviar.
-l	Enviar tamaño del búfer
-f	Establecer el indicador <i>Don't Fragment flag</i> (no fragmentar) en el paquete (solo IPv4)
-i	Establecer el indicador <i>Time To Live</i> (tiempo de vida).
-v	Establecer el indicador <i>Type of Service</i> (tipo de servicio, pero ya no se usa)
-r	Registrar ruta para el recuento de saltos (solo IPv4)
-s	Marca de tiempo para el recuento de saltos (solo IPv4)
-j	Ruta de origen imprecisa a lo largo de la lista de hosts (solo IPv4)
-k	Ruta de origen estricta a lo largo de la lista de hosts (solo IPv4)
-w	Tiempo de espera en milisegundos para esperar cada respuesta
-R	Usar un encabezado de enrutamiento para probar también la ruta inversa (solo IPv6, en desuso según RFC 5095)
-S	Dirección de origen a usar
-c	Identificador del compartimento de enrutamiento

-p	Hacer ping a una dirección de proveedor de virtualización de red de Hyper-V
-4	Forzar el uso de IPv4
-6	Forzar el uso de IPv6

NETSTAT

QUÉ ES EL COMANDO NETSTAT

El comando netstat genera visualizaciones que muestran el estado de la red y estadísticas de protocolo. El estado de los protocolos TCP, SCTP y los puntos finales de UDP puede visualizarse en formato de tabla. También puede visualizarse información sobre la tabla de enrutamiento e información de interfaces.

La opción netstat -s muestra estadísticas de los protocolos UDP, TCP, SCTP, ICMP e IP.

- a netstat -a Enumerar también los puertos abiertos
- e netstat -e Estadísticas de interfaz (paquetes de datos recibidos y enviados, etc.)
- i netstat -i Abrir el menú general de netstat
- n netstat -n Visualización numérica de direcciones y números de puerto
- b Muestra el ejecutable implicado en la creación de cada conexión o puerto de escucha. En algunos casos, los ejecutables conocidos hospedan varios componentes independientes y, en estos casos, se muestra la secuencia de componentes implicados en la creación de la conexión o el puerto de escucha. En este caso, el nombre del ejecutable se encuentra en la parte inferior entre []. En la parte superior se encuentra el componente al que llamó, y así sucesivamente hasta que se alcanzó el TCP/IP. Tenga en cuenta que esta opción puede llevar mucho tiempo y producirá un error a menos que cuente con los permisos suficientes.
- o Muestra las conexiones TCP activas e incluye el identificador de proceso (PID) para cada conexión. Puede encontrar la aplicación en función del PID en la pestaña Procesos del Administrador de tareas de Windows. Este parámetro se puede combinar con -a, -n y -p.
- p <Protocol> Muestra las conexiones para el protocolo especificado por Protocol. En este caso, el Protocol puede ser tcp, udp, tcpv6 o udpv6. Si este parámetro se usa con -s para mostrar estadísticas por protocolo, Protocol puede ser tcp, udp, icmp, ip, tcpv6, udpv6, icmpv6 o ipv6.
- S Muestra las estadísticas por protocolo. De forma predeterminada, se muestran estadísticas para los protocolos TCP, UDP, ICMP e IP. Si se instala el protocolo IPv6, se muestran estadísticas para los protocolos TCP a través de IPv6, UDP a través de IPv6, ICMPv6 e IPv6. El parámetro -p se puede usar para especificar un conjunto de protocolos.
- r Muestra el contenido de la tabla de enrutamiento de IP. Esto equivale al comando route print.
- <interval> Vuelve a mostrar la información seleccionada cada x segundos de un intervalo. Pulse CTRL+C para evitar que se vuelva a mostrar la información. Si se omite este parámetro, este comando imprime la información seleccionada una sola vez.
- /? Muestra la ayuda en el símbolo del sistema.

VLAN

En primer lugar, vamos a empezar por saber qué son. Del inglés *Virtual LAN* (Red de área local y virtual), es un método que permite crear redes que lógicamente son independientes, aunque estas se encuentren dentro de una misma red física. De esta forma, un usuario podría disponer de varias VLANs dentro de un mismo router o switch. Podría decirse que cada una de estas redes agrupa los equipos de un determinado segmento de red. Crear estas particiones tiene unas ventajas bastante claras a la hora de administrar una red.

Qué uso tienen y ventajas

A día de hoy se configuran a través de software y poseen grandes beneficios a la hora de garantizar la seguridad y administrar los equipos de forma eficaz, tal y como a hemos puntualizado. En lo que concierne a la seguridad, hay que tener en cuenta que los dispositivos pertenecientes a una VLAN no tienen acceso a los que se encuentren en otras y viceversa. Resulta útil cuando queremos segmentar los equipos y limitar el acceso entre ellos por temas de seguridad.

De lo dicho con anterioridad se deduce que la gestión también será mucho más sencilla, ya que tendríamos a los dispositivos divididos en «clases» aunque pertenezcan a una misma red.

Tipos de VLANs

Dependiendo de la fuente consultada incluso del fabricante se pueden distinguir hasta seis tipos de redes virtuales. Sin embargo, nosotros solo nos vamos a centrar en tres: a nivel de puerto, MAC y aplicación.

- **Puerto.** También conocida como *Port Switching* en los menús de configuración de los routers y switches, se trata de la más extendida y utilizada. Cada puerto se asigna a una VLAN y los usuarios que estén conectados a ese puerto pertenecen a la VLAN asignada. Los usuarios dentro de una misma VLAN poseen de visibilidad los unos sobre los otros, aunque no a las redes virtuales vecinas. El único inconveniente es que no permite dinamismo a la hora de ubicar los usuarios y en el caso de que el usuario cambie de emplazamiento físicamente se debería reconfigurar la red virtual.
- **MAC:** El razonamiento es similar a la anterior, salvo que en vez de ser una asignación a nivel de puerto lo es a nivel de dirección MAC del dispositivo. La ventaja es que permite movilidad sin necesidad de que se tengan que aplicar cambios en la configuración del switch o del router. El problema parece bastante claro: añadir todos los usuarios puede resultar tedioso.
- **Aplicaciones:** Se asignarían redes virtuales en función de la aplicación utilizada, y en este caso intervienen varios factores, como por ejemplo la hora en la que nos encontramos, la dirección MAC o la subred, permitiendo distinguir entre aplicaciones SSH, FTP, Samba o incluso SMTP.

Aplicaciones en equipos domésticos

¿Cuántos lectores poseen conexiones FTTH? En este servicio tenemos un claro ejemplo de utilización de VLANs pero a gran escala. Los operadores ubican los diferentes servicios en redes lógicas separadas. Por ejemplo, en el caso de Movistar, el servicio de televisión, VoIP e Internet se encuentran en redes separadas, algo que los usuarios que hagan uso de routers diferentes a los ofrecidos por la operadora conocerán.

Hablando de qué uso se puede dar, resulta bastante claro. Por ejemplo, separar aquellos equipos que acceden a Internet de los que no lo hacen. Esto evita que los intrusos no lleguen a estos y que por ejemplo *malware* pueda distribuirse gracias a unidades de red que estarían disponibles.

Encantamos que a medida que avanzamos tenemos aspectos más complejos y combinados, encontraremos términos no vistos pero relacionadas como Swichin entre otros, así que se podrán incorporar más datos a medida que avanzamos en la información vista.