

## SSID

El **SSID** (*Service Set Identifier*) es una secuencia de un máximo de 32 octetos incluida en todos los paquetes de una red inalámbrica para identificarlos como parte de esa red. El código consiste en un máximo de 32 caracteres, que la mayoría de las veces son alfanuméricos (aunque el estándar no lo específica, así que puede consistir en cualquier carácter). Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID.

Existen algunas variantes principales del SSID. Las redes *ad-hoc*, que consisten en máquinas cliente sin un punto de acceso, utilizan el **BSSID** (*Basic Service Set Identifier*); mientras que en las redes de infraestructura que incorporan un punto de acceso se utiliza el **ESSID** (*Extended Service Set Identifier*). Es posible referirse a cada uno de estos tipos como SSID en términos generales. A menudo al SSID se le conoce como “nombre de la red”.

Uno de los métodos más básicos de proteger una red inalámbrica es desactivar la difusión (*broadcast*) del SSID, ya que para el usuario medio no aparecerá como una red en uso. Sin embargo, no debería ser el único método de defensa para proteger una red inalámbrica. Se deben utilizar también otros sistemas de cifrado y autentificación.



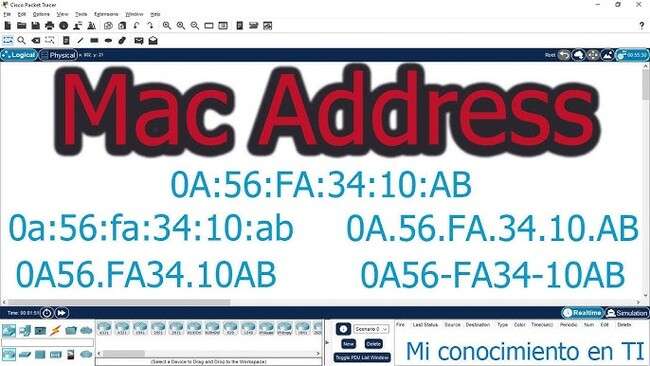
## MAC

La**dirección MAC** (Control de Acceso al Medio) es un identificador único asignado a la tarjeta de red de un dispositivo, como una computadora, teléfono móvil o tableta. La dirección MAC se utiliza para identificar de manera única el dispositivo en una red local.

A diferencia de la dirección IP, que puede ser asignada dinámicamente y cambiada por el dispositivo o por la red, la dirección MAC es una identificación fija y única que no puede ser cambiada por el usuario. La dirección MAC está compuesta por una serie de números y letras que se asignan al dispositivo en el momento de su fabricación.

La dirección MAC se utiliza para el control de acceso a la red y la seguridad, como por ejemplo en el filtrado de direcciones MAC que permite o niega el **acceso a la red.**

Existen dos tipos principales de la Dirección MAC, pero la mayoría de las redes Ethernet tradicionales utilizan direcciones MAC Universal (MAC-48) de 48 bits. Las direcciones MAC Extendidas (EUI-64) son más comunes en el contexto de protocolos como IPv6, donde se requiere una mayor cantidad de direcciones debido al crecimiento de la Internet y la proliferación de dispositivos conectados.



## CLAVE WPA2

WPA, abreviatura de Acceso protegido Wi-Fi®, es una especificación de cifrado de datos para una LAN inalámbrica. Ella mejora con la función de seguridad WEP utilizando un Protocolo de Autenticación Extensible (EAP, por sus siglas en inglés) (Extensible Authentication Protocol) para proteger el acceso a la red y un método de codificación para proteger la transmisión de datos.

WPA está diseñado para funcionar con un servidor de autenticación 802.1X que distribuye diferentes claves para cada usuario. Sin embargo, también se puede utilizar en un modo de clave pre compartido (PSK) menos seguro. PSK está diseñado para redes en hogares y oficinas pequeñas donde cada usuario tiene la misma frase contraseña. WPA-PSK también se conoce como WPA-Personal. WPA-PSK le permite a la máquina inalámbrica de Brother asociarse con puntos de acceso utilizando el método de codificación TKIP o AES. WPA2-PSK le permite a la máquina inalámbrica de Brother asociarse con puntos de acceso utilizando el método de codificación AES.

El Protocolo de Integridad de Clave Temporal (TKIP, por su sigla en inglés) (Temporal Key Integrity Protocol) es un método de codificación. El TKIP proporciona una clave por paquete que mezcla la integridad de un mensaje con un mecanismo de re-escritura. AES (abreviatura de Advanced Encryption Standard) es el estándar de cifrado fuerte autorizado por Wi-Fi. WPA-PSK, WPA2-PSK y TKIP o AES utilizan una Clave Pre-Compartida (PSK) que tiene entre 8 y hasta un máximo de 63 caracteres de largo.

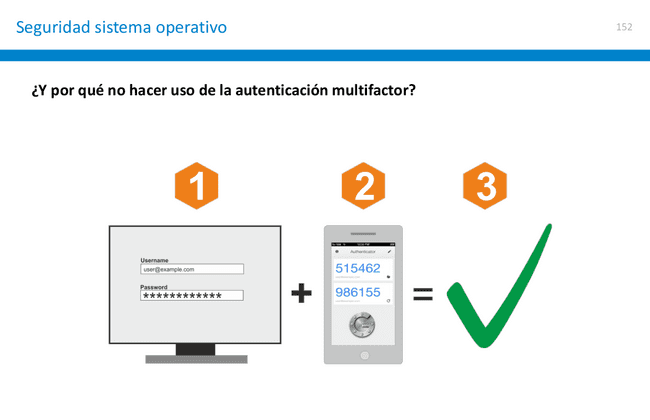


## PASSWORD

Uno de los elementos de la seguridad informática que se utiliza con mayor frecuencia en los sistemas de cómputo, es la llamada contraseña o password. De hecho, cuando accedemos al correo electrónico, al sistema operativo de nuestra computadora o algún sistema del Instituto como la base de datos académica (SDBAII), el sistema de control de estudiantes (SICOE).

Sin embargo, muchas veces el usuario no vislumbra la importancia que tiene la secrecía de una contraseña y por comodidad,  desconocimiento o descuido, la evidencia o expone ante personas no autorizadas para ingresar a los sistemas, vulnerando la seguridad y provocando problemas potencialmente peligrosos no sólo para el usuario mismo, sino para toda la organización. Ya desde 1985, la NIST1 publicó el estándar Password Usage, en donde cuestiona la efectividad de las contraseñas fundamentalmente porque los usuarios la olvidaban fácilmente o porque se la proporcionaban a otras personas sin el menor reparo de ello.

Esto conlleva a pensar que gran parte del trabajo debe centrarse en la concientización de  la importancia que tiene la contraseña para un usuario. Pero no es tan sencillo, por ejemplo, ¿qué posibilidades hay de recordar una contraseña como la siguiente? Mo9YT5FB1aab@54. Aunque por la longitud y la combinación de caracteres, se consideraría como altamente efectiva (se recomienda que la longitud sea de al menos 8 caracteres y se combinen letras, dígitos y signos), lo más seguro es que por su complejidad, el usuario la escribirá en un papel y lo guardará en un lugar de fácil acceso (en el cajón, debajo del teclado o incluso en la misma pantalla de la computadora), luego entonces,  la efectividad y la seguridad se vulneran.



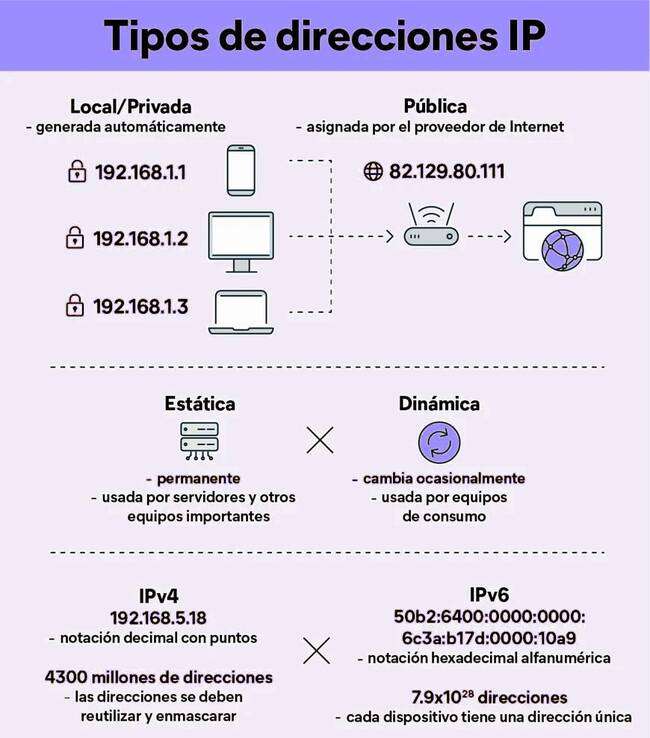
## IP

Lo primero que debes saber es qué es IP. **Ellos son las iniciales de Internet Protocol, que traducido al español lo podemos llamar como Protocolo de Internet**. En otras palabras, es el sistema estándar mediante el cual funciona la internet, por medio de un proceso de envío y recepción de información.

Una dirección IP es un conjunto de números, únicos e irrepetibles, que identifica a un dispositivo con la capacidad de conectarse a internet, ya sea una computadora, tableta, celular, o incluso dispositivos inteligentes preparados para IoT (Internet de las cosas).

**Pensemos en un ejemplo más sencillo para explicar qué es una dirección IP.**Imagina que las carreteras de tu ciudad son la Internet, y que los vehículos que circulan en ellas son los dispositivos desde donde navegan las personas.

Sea cual sea el medio de transporte, todos tienen una matrícula y es esa la que los identifica y diferencia. En este sentido, podríamos decir que la matrícula de un vehículo en este ejemplo es la dirección IP de tu dispositivo conectado a Internet.



## DHCP

El Protocolo de Configuración Dinámica de Host (DHCP) es un sistema para asignar direcciones IP a cada dispositivo de red (conocido como host) en la red de una organización. Un host puede ser una computadora de escritorio, una portátil, una tableta, un dispositivo móvil, un cliente ligero u otros tipos de dispositivos. Cada host debe tener una dirección IP para comunicarse con otros dispositivos a través de internet.

El protocolo de red DHCP asigna direcciones automáticamente, sin necesidad de que los administradores de red las asignen manualmente. DHCP también se encarga de asignar automáticamente nuevas direcciones IP cuando los dispositivos se trasladan a nuevas ubicaciones en la red. Además de las direcciones IP, un servicio DHCP asigna parámetros de configuración como direcciones del Sistema de Nombres de Dominio (DNS), máscaras de subred y puertas de enlace predeterminadas, esenciales para las comunicaciones de red.

Cuando un dispositivo (también llamado cliente DHCP) se une a la red, envía un mensaje de "descubrimiento DHCP" a la subred, solicitando una dirección IP junto con otra información de configuración. Cuando los servidores DHCP de la red reciben el mensaje de descubrimiento, responden con ofertas DHCP que pueden incluir una dirección IP seleccionada de un conjunto de direcciones IP, junto con parámetros de red e información DHCP, como servidores DNS , máscara de subred, puerta de enlace predeterminada y duración de la concesión de la dirección IP.

