

Índice

Objetivo:	2
Introducción	2
Redes Wi-Fi (802.11)	2
Alcance de una red Wi-Fi y sus frecuencias de operación	2
Tasa de transferencia y variantes de Wi-Fi	3
Factores externos a un router inalámbrico	4
Dispositivos para redes inalámbricas	5
Repetidor	5
Punto de acceso (Access-Point)	6
Router inalámbrico	6
Partes de un router inalámbrico	7
Primera configuración de tu router inalámbrico	8
Primer acceso mediante navegador web	8
Cambiar el usuario y contraseña de administrador	8
Configurando aspectos de red LAN/WAN	10
Router inalámbrico	10
Configuración WAN (WAN Settings)	10
Configuración LAN	11
Configuración de DHCP	12
Parámetros de enrutamiento	12
Configuración de la red inalámbrica (WLAN)	13
Frecuencias 2.4 Ghz y 5 Ghz	13
Modo Access Point (AP)	19
Configuración rápida paso a paso	19
Modo extensor de rango	20
Entendiendo un extensor de rango	20
Configuración rápida paso a paso	21
Ajustes de seguridad	23
Configurando el control parental	23
Configurando el control de acceso	25
Parte 1: Host	25
Parte 2: Destino	25
Parte 3: Horario	25
Parte 4: Regla	26
Fuentes	27

Objetivo:

El (La) lector (a) conocerá las características básicas de un router inalámbrico, así como el acceso y configuración básica, aprenderá las semejanzas y diferencias entre el router inalámbrico y un modem-router, diferenciando las áreas de configuración que pueden ser modificadas.

Introducción

Gracias a los nuevos dispositivos fabricados, es posible que una casa cuente con un dispositivo capaz de proveer Internet traído mediante un proveedor de servicios hacia los diferentes dispositivos de una instalación (vivienda, restaurantes, pequeñas y medianas empresas). Sin embargo, debido a la necesidad de poder extender o mejorar los servicios de Internet para poder suplir la demanda de acceso a diferentes partes de una instalación, ha llevado a la necesidad de adquirir diferentes dispositivos cómo lo son los Access-Point (AP), Repetidores y Routers inalámbricos.

Varios de estos dispositivos cuentan con guías simples y predeterminadas para una configuración rápida, lo cual es muy conveniente para lograr hacer tu objetivo de lograr extender tu red, pero ¿Piensas que es la forma más eficiente para mejorar tu red?, ¿Las configuraciones que haces logran que tu red sea segura?, ¿Sabes de las diferentes alternativas que tienes a tu alcance?, no importa si algunas de las respuestas a estas preguntas es “no”, en esta guía te mostraremos qué es un router inalámbrico, sus diferentes modos y cómo configurarlo mediante un navegador web.

Nota: Este manual usa como ejemplo el router inalámbrico Tp-Link Archer para hacer las configuraciones.

Redes Wi-Fi (802.11)

Las redes Wi-Fi están definidas en el estándar IEEE 802.11 y describen las recomendaciones y operación de dichas redes, en este estándar y sus derivados podemos ver datos muy importantes que vamos a necesitar a la hora de querer extender tu red inalámbrica.

Alcance de una red Wi-Fi y sus frecuencias de operación.

Las redes Wi-Fi pueden operar en las frecuencias de 2.4Ghz. y 5Ghz. mediante radiofrecuencia, por lo que provocan ondas de relativamente fácil absorción, esto implica que obstrucciones como paredes, pilares, electrodomésticos entre otros reduzcan considerablemente el alcance de una red Wi-Fi.

El alcance de una red Wi-Fi va a depender de 2 factores importantes:

- **Potencia de transmisión:** Esta característica que la puedes buscar como “Wi-Fi Transmission power” indica qué tanto se puede amplificar una señal para poder enviarla mediante la antena de transmisión, este valor está puesto en decibeles por miliwatt (dBm), el máximo permitido por la FCC en Estados Unidos es de 30dBm, lo que equivale a 1 watt de potencia, al adquirir un Router inalámbrico, un repetidor o un AP, entre mayor sea la potencia de transmisión, mayor será su alcance, este puede oscilar entre 20 y 150 metros.

dBm	Potencia (mW)
40	10000
30	1000
20	100
17	50
10	10
6	4
3	2
1	1.25
0	1
-1	0.8
-3	0.5
-6	0.25
-10	0.1
-17	0.02
-20	0.01
-30	0.001
-40	0.0001

- Obstrucciones de la señal: Diferentes objetos ubicados en el lugar donde instales el dispositivo inalámbrico pueden lograr hacer que la señal se vea atenuada o suprimida por completo, entre los obstructores más comunes están:
 - Paredes: las paredes suelen jugar un papel muy importante ya que dependiendo del grosor y el material logran atenuar mucho o poco la señal Wi-Fi, por ejemplo las paredes de madera o de concreto con un grosor menor a 14 centímetros atenúan la señal, pero logra alcanzar varios metros más, sin embargo una pared de concreto muy gruesa o varias paredes logran reducir significativamente el alcance, el peor caso es una pared con malla metálica o una capa del mismo material, ya que este tipo de paredes pueden lograr el efecto llamado “Jaula de Faraday”, anulando la señal que quiera entrar y salir a través de dichas paredes, cuando tengas en mente extender tu red Wi-Fi te recomendamos analizar el tipo de paredes y la cantidad hasta la zona donde quieres proveer de acceso a la red, para determinar cuál es la mejor solución de entre los tipos de dispositivos que te mostraremos en este artículo.
 - Electrodomésticos: cualquier electrodoméstico desde televisores hasta refrigeradores emiten radiofrecuencias que pueden atenuar la señal Wi-Fi especialmente los hornos de microondas, ya que, para hacer la cocción de un alimento, este emite una gran cantidad de ondas electromagnéticas, por lo que te recomendamos tener el dispositivo transmisor en un lugar relativamente libre de electrodomésticos.

Tasa de transferencia y variantes de Wi-Fi.

Además del estándar 802.11 para Wi-Fi existen diferentes variantes que han sido añadidas conforme se han modernizado la tecnología, cada variante tiene su propio estándar usando el 802.11 como base, dichas variantes

describen la frecuencia de operación y la tasa de transferencia (Data rate) que puede soportar, lo cual puedes consultarlo en la siguiente tabla.

Estándar IEEE	Radiofrecuencia	Tasa de Transferencia (Mbps)	Rango de transmisión aproximado	Compatibilidad
802.11	2.4Ghz	2	Interior: 20m Exterior: 100m	
802.11a	5Ghz	54	Interior: 35m Exterior: 120 – 5000m	
802.11b	2.4Ghz	11	Interior: 35m Exterior: 120m	802.11
802.11g	2.4Ghz	54	Interior: 38m Exterior: 140m	802.11b
802.11n	2.4Ghz, 5Ghz	150 – 600	Interior: 70m Exterior: 250m	802.11b, 802.11g
802.11ac	5Ghz	450 – 1.3 Gbps	Interior: 35m	
802.11ax	2.4Ghz, 5Ghz	450- 10.53 Gbps	-----	802.11n, 802.11ac

A la hora de adquirir un router inalámbrico, te recomendamos revisar los estándares que soporta para que tengas una idea de su posible alcance y la tasa de transferencia para tu conexión a Internet.

Factores externos a un router inalámbrico.

Ya tienes la información suficiente para saber escoger un router inalámbrico, pero no es la única pieza de tu red que se va a encargar de llevarte una conexión a Internet de alta velocidad, existen otros factores que no tienen que ver directamente con escoger y posicionar tu router inalámbrico, estos factores son claves para que puedas disfrutar las bondades de extender tu red.

Tarjeta de red

Las tarjetas de red o NIC (Network Interface Card) de las computadoras y dispositivos móviles son las encargadas de lograr diversas tareas, desde la codificación y decodificación de la información a enviar y recibir, hasta los protocolos de comunicación asociados a los estándares que tienen integrados por el fabricante, este es un componente que, en algunos casos no puede ser sustituido por uno más moderno que pueda soportar los últimos estándares.

En las NIC para Wi-Fi tienen integrada una antena que se encarga de transmitir y recibir las señales de radiofrecuencia, el rango de estas es variable, sin embargo, las que están integradas en un dispositivo suele tener un alcance relativamente corto, por lo que te recomendamos adquirir una tarjeta adicional con una mayor potencia para extender su rango.

Te recomendamos que uses un router inalámbrico capaz de usar el estándar que utilicen los dispositivos en tu área de uso o un estándar que tenga retrocompatibilidad para abarcar la mayoría de los dispositivos posibles, también

puedes considerar el uso del cable Ethernet para los dispositivos compatibles para lograr una mejor conexión frente a un estándar con tasa de transferencia baja.

Servicio contratado

Si tu objetivo es tener una conexión de alta velocidad a Internet mediante la red inalámbrica, además de las recomendaciones anteriores es necesario tener un servicio que pueda satisfacer esta demanda, por ejemplo: Tienes un router inalámbrico con el estándar 802.11ax con una tasa de transferencia de 10.53Gbps y las NIC de los dispositivos lo soportan, pero tienes contratado un plan de Internet de 10Mbps, pues la máxima tasa a la que puedes navegar en Internet es de 10 Mbps, por lo que te recomendamos consultar a tu proveedor de servicio sobre los diferentes planes para poder aumentar la tasa de transferencia.

Conexiones físicas

Este es un punto infravalorado pero clave para lograr la comunicación entre dispositivos, especialmente si el router inalámbrico está conectado a otro, por ejemplo el router-modem otorgado por el proveedor de servicios, lo común es que las conexiones entre estos dispositivos sea mediante cables Ethernet, estos tienen sus propios estándares y categorías, las cuales definen la tasa de transferencia máxima, el tipo de conector entre otros, adicionalmente te agregamos el uso recomendado para cada uno en la siguiente tabla:

Categoría	Shielding	Tasa de transferencia máxima	Uso común	Conector usado
Cat 3	Unshielded	10 Mbps	En desuso	
Cat 5	Unshielded	10/100 Mbps	En desuso	
Cat 5e	Unshielded	1000 Mbps / 1 Gbps	Teléfono IP, Red de casa, Red de oficina	Rj45 8P8C
Cat 6	Shielded or Unshielded	1000 Mbps / 1 Gbps	Teléfono IP, Red de casa, Red de oficina	RJ45 (para Cat6)
Cat 6a	Shielded	10000 Mbps / 10 Gbps	Red de oficina, centro de datos	RJ45 (para cat6)
Cat 7	Shielded	10000 Mbps / 10 Gbps	Centro de datos	GG45
Cat 8	Shielded	25 Gbps o 40Gbps *	En revisión	

Te recomendamos verificar las NIC que tiene el modem-router para elegir apropiadamente el router inalámbrico para extender la red y los cables necesarios para que su comunicación sea óptima.

Dispositivos para redes inalámbricas

En el mercado existe una gran cantidad de dispositivos para poder extender la red Wi-Fi, cada uno con diferente forma de operación ventajas y desventajas, los tres más importantes son los siguientes:

Repetidor

Es un dispositivo que consta de dos partes importantes, un receptor y un transmisor, en el cual el receptor se encargará de recibir las señales de Wi-Fi para posteriormente ser amplificado y emitido mediante el transmisor, su

uso más común es para extender una red Wi-Fi recibiendo la señal de un dispositivo (un router-modem por ejemplo) y propagarlo a otra área a la que el dispositivo no alcanzaría.

Ventajas:

- Es fácil de instalar.
- Fácil configuración

Desventajas:

- Dependen de la capacidad del emisor de Wi-Fi.
- El alcance puede verse afectado a las obstrucciones anteriormente mencionadas, por lo que su posicionamiento es clave para un buen funcionamiento.

Punto de acceso (Access-Point)

Es un dispositivo que se encarga de conectar dispositivos que usen Wi-Fi a una red cableada, por lo que cuentan con antenas para poder comunicarse con los diferentes dispositivos inalámbricos y hace la codificación para poder convertir las señales Wi-Fi a señales eléctricas para posteriormente ser enviadas mediante un cable Ethernet hacia el modem-router, el AP se encarga de hacer la conexión a nivel de enlace, sin embargo lo que es correspondiente a la asignación de direcciones IP y el enrutamiento es llevado a cabo por un router o en el caso de una instalación pequeña, el modem-router.

Ventajas:

- Pueden tener una mayor cantidad de dispositivos conectados simultáneamente.
- El AP genera su propia señal Wi-Fi, algunos soportan la banda dual (2.4 Ghz y 5 Ghz).

Desventajas:

- Se necesita de un cable Ethernet con la distancia suficiente para llegar a el área donde se quiere extender la red.
- El proceso de enrutamiento y asignación IP está administrado por el módem-router.

Router inalámbrico

Es un dispositivo con un funcionamiento parecido a un AP, con la particularidad de que este tiene la capacidad de enrutar, esto hace que los dispositivos conectados mediante Wi-Fi pertenezcan a una red diferente a la red cableada en la que está conectado el router inalámbrico, por lo que el router inalámbrico se encarga de la conexión de los dispositivos, la asignación de direcciones y el enrutamiento del tráfico.

Ventajas

- La conexión de los dispositivos es independiente del módem-router.

- Al tener características de un router, se pueden configurar políticas de seguridad mediante filtros, entre los cuales están las Listas de control de Acceso (ACL's)

Desventajas

- Mayor complejidad de configuración.
- Al ser un dispositivo que separa dominios de red, se necesita del enrutamiento o una traducción de direcciones (NAT), Sin embargo, es necesario tener presente que este tipo de servicio puede ocasionar que no se logre una conexión completa entre un servicio específico de internet y un dispositivo.

En el mercado existen routers inalámbricos con la capacidad de adoptar los modos de repetidor, punto de acceso adicionalmente, por lo que son convenientes para que los puedas ajustar a tus necesidades y posteriormente reconfigurarlo para adaptarlo a un nuevo escenario.

Partes de un router inalámbrico

Un router inalámbrico consta de los siguientes componentes:



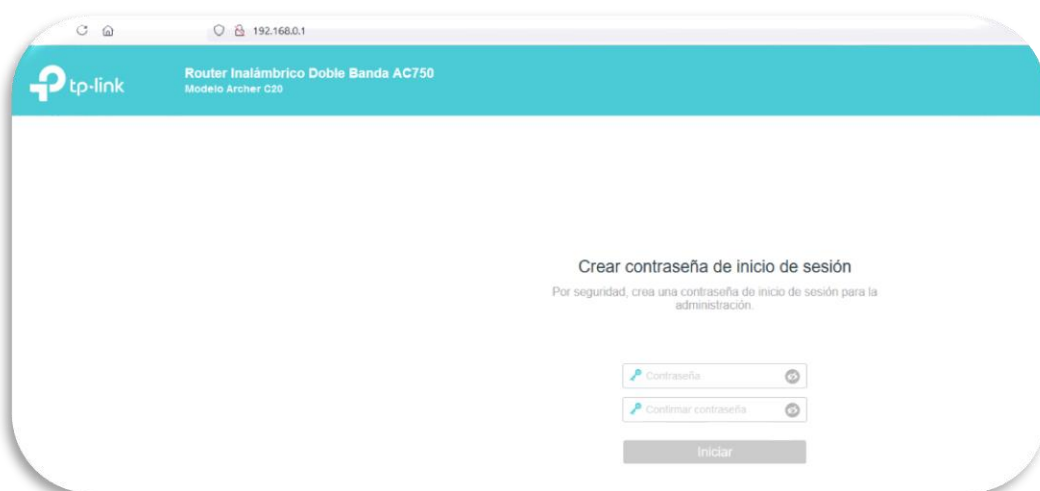
- **Antenas:** Estas son las que reciben y transmiten las señales Wi-Fi, algunos soportan las bandas de 2.4 y 5 Ghz.
- **Puertos Ethernet LAN:** Estos son puertos para conectar a las computadoras o dispositivos vía cable Ethernet, generalmente son identificados con el color azul, los dispositivos conectados por estos puertos forman parte de la red local del router inalámbrico.
- **Puerto Internet (WAN):** Este puerto es el que irá conectado a Internet, cuando es un router comercial como el que se usa en este artículo, este puerto está de color amarillo con la leyenda "Internet", este puerto es el que va a ir conectado al router-modem o a aquel que vaya a enrutar el tráfico a Internet, en el caso de los módem-router, este puerto es sustituido por un conector del tipo de conexión dada por el proveedor de servicios, entre los cuales están el coaxial, fibra óptica o línea telefónica.
- **Interruptor:** Un interruptor simple para encender o apagar el router inalámbrico, el cual se recomienda mantener encendido.
- **Botón de Reset:** Generalmente es un botón pequeño, el cual sólo lo puedes presionar con la ayuda de un objeto delgado (la punta de un lápiz, un desarmador delgado, una aguja gruesa, la punta de un portaminas, etc.), con este botón puedes restaurar un router inalámbrico a sus valores y configuraciones de fábrica, especialmente útil si no recuerdas las contraseñas de administrador o si quieres hacer una nueva configuración desde cero.
- **Botón WPS:** Un botón para usar la función "Wi-Fi Protected Setup"

Primera configuración de tu router inalámbrico

Antes de ponerte manos a la obra, te recomendamos tener a la mano los manuales de fábrica o en línea del router inalámbrico que vayas a configurar, en este artículo configuraremos un Tp-Link Archer c20, por lo que, si tienes el manual del router que tú quieras configurar, te será más fácil identificar las áreas de configuración que sean similares a este artículo.

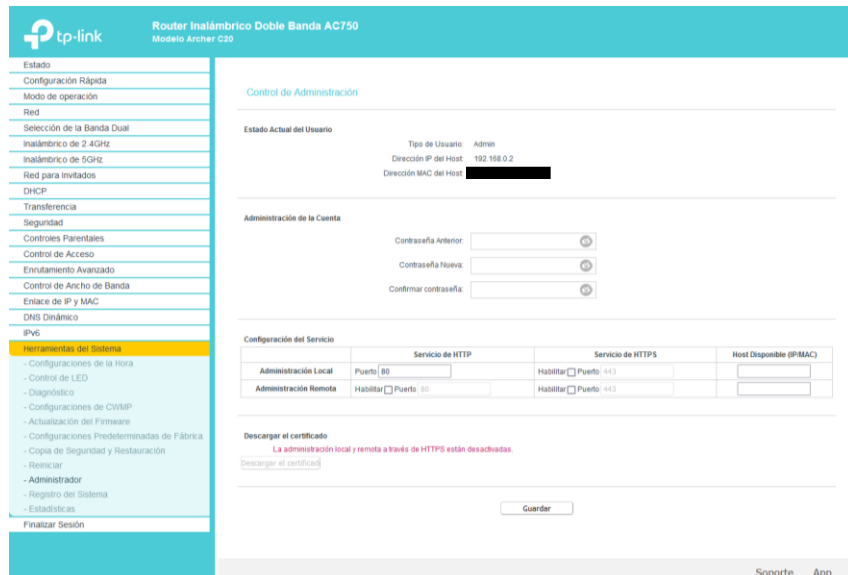
Primer acceso mediante navegador web

Para acceder por primera vez a tu router inalámbrico, debes conectar una computadora o laptop a la red local del router, esto puede ser mediante la red Wi-Fi o un cable Ethernet e ingresar con un navegador web a la página de configuración dada por el fabricante, en este caso es mediante la página <http://tplinkwifi.net> o las direcciones IP predeterminadas <http://192.168.0.1> o <http://192.168.1.1>, dependiendo de la versión del router inalámbrico ingresarás a una primera configuración, en el cual se te solicitará crear una contraseña de acceso.



Otra opción es que ingreses al panel de configuración usando el usuario y contraseña predeterminado, en este caso es admin/admin.

Cambiar el usuario y contraseña de administrador



Lo primero que te recomendamos agregar es un nuevo administrador y/o contraseña segura dependiendo de la versión del router inalámbrico que utilices, para lograr esto, una vez que has ingresado al panel de administración, es ir a “Herramientas del sistema” y luego entrar a “Administrador”.

Administración de la Cuenta

Contraseña Anterior:

Contraseña Nueva:

Confirmar contraseña:

Ahí ingresa la contraseña anterior del administrador (admin), ingresa la nueva contraseña y la confirmación de esta, en otras versiones puedes agregar el campo de usuario, para crear un usuario y contraseña de administración.

Además del cambio de usuario, te recomendamos habilitar el servicio de HTTPS marcando la casilla y posteriormente descargar el certificado para la conexión HTTPS, con esto habilitado y en funcionamiento puedes ingresar a la

Configuración del Servicio

	Servicio de HTTP	Servicio de HTTPS	Host Disponible (IP/MAC)
Administración Local	Puerto <input type="text" value="80"/>	Habilitar <input checked="" type="checkbox"/> Puerto <input type="text" value="443"/>	<input type="text"/>
Administración Remota	Habilitar <input type="checkbox"/> Puerto <input type="text" value="80"/>	Habilitar <input type="checkbox"/> Puerto <input type="text" value="443"/>	<input type="text"/>

Descargar el certificado

[Descargar el certificado](#)

[Guardar](#)

configuración de tu router inalámbrico mediante una conexión cifrada entre el router y tu navegador.

Al hacer este cambio el router utilizará un cifrado usando TLS 1.0 o 1.1, esto indica que utilizará un cifrado débil, ya que es una versión que será sustituida posteriormente.

Una vez aplicados los cambios, aparecerá el siguiente mensaje cuando recargues la página:

Advertencia: Riesgo potencial de seguridad a continuación

Firefox ha detectado una potencial amenaza y no ha continuado a 192.168.0.1. Si visitas este sitio, los atacantes podrían intentar robar tu información como tus contraseñas, correo o datos de tu tarjeta de crédito.

¿Qué puedes hacer al respecto?

Es probable que haya un problema con el sitio web y no hay nada que puedas hacer al respecto.

Si estás usando una red corporativa o un software antivirus, puedes contactarte con el equipo de asistencia técnica. También puedes notificarle al administrador del sitio sobre el problema.

[Saber más...](#)

Puedes ignorar el riesgo, pero te recomendamos instalar los certificados usando el botón de **descargar certificado** en el apartado de administración e instalarlo en tu ordenador.

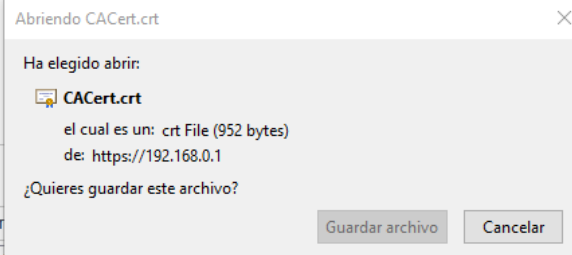
[Volver \(recomendado\)](#)

[Avanzado...](#)

Contraseña Anterior:

Contraseña Nueva:

Confirmar contraseña:



Configuración del Servicio

	Servicio de HTTP		Ser
Administración Local	Puerto <input type="text" value="80"/>	Habilitar <input checked="" type="checkbox"/>	Puerto <input type="text" value="443"/>
Administración Remota	Habilitar <input type="checkbox"/> Puerto <input type="text" value="80"/>	Habilitar <input type="checkbox"/>	Puerto <input type="text" value="443"/>

Descargar el certificado

[Descargar el certificado](#)

Una vez descargado, le haces doble click y aparecerá una ventana indicando la información del certificado, también hay un botón para que instales dicho certificado, al seleccionarlo aparecerá un asistente de importación de certificados, seleccionas la ubicación del almacenamiento (Usuario o Equipo Local), en la siguiente ventana seleccionas la casilla “Colocar todos los certificados en el siguiente almacén”, seleccionas “Examinar...” y luego seleccionas “Entidades de certificación raíz de confianza”, en la ultima ventana verás la configuración que seleccionaste, y solamente seleccionas “Finalizar” para concluir la instalación del certificado.

Con esto ya tienes configurado el servicio de HTTPS para tener una comunicación cifrada entre tu navegador y el router inalámbrico, cabe mencionar que es una versión de TLS que será descontinuada en este caso, si adquieres un dispositivo más reciente, revisa que tenga una versión de TLS reciente para que tengas una comunicación más robusta.

Configurando aspectos de red LAN/WAN

Una vez hayas configurado lo esencial para el acceso seguro a tu dispositivo recién adquirido, lo siguiente es configurarlo para que puedas adaptarlo a tus necesidades, ya sea Router inalámbrico, AP o extensor de rango.

Router inalámbrico

Este es el modo que está por defecto en este router inalámbrico, por lo que te recomendamos empezar la configuración sin usar la configuración rápida, los puntos iniciales claves a configurar son los siguientes:

Configuración WAN (WAN Settings)

Este segmento es para configurar el comportamiento del puerto WAN del router inalámbrico, desde el modo de operación, entre los cuales están:

- Configuraciones para redes Ethernet: Estas opciones son las más comunes cuando quieres crear redes sin hacer cambios en el módem-router dado por el proveedor de servicios.
 - IP Dinámico
 - IP Estático

- Configuraciones para redes WAN: Estas opciones las vas a usar cuando quieres que el módem-router proporcionado por el proveedor de servicios sólo se encargue del reenvío de la información y quieres que los demás aspectos como el enrutamiento y demás servicios sea administrado por el router inalámbrico, para lograr una configuración correcta, debes de leer a fondo el manual del router inalámbrico y del módem router proporcionado por el proveedor de servicios, nosotros te recomendamos tener especial cuidado con este último, y tener a la mano los métodos de restauración de fábrica para poder restaurarlo si lo configuras erróneamente.
 - PPPoE
 - L2TP
 - PPTP
 - Cable BigPond

En este manual cubriremos la configuración para redes LAN

Direcciones IP

Para el direccionamiento del puerto WAN existen dos opciones principales:

Tipo de Conexión:

Dirección IP:

Máscara de Subred:

Puerta de Enlace:

IP Dinámica: En esta opción dejas que el puerto obtenga una dirección IP mediante el protocolo DHCP (Dynamic Host Control Protocol), por lo que depende de la configuración del servidor DHCP, este protocolo asigna de manera automática la dirección IP, la máscara de subred, la puerta de enlace, y los servidores DNS, lo que lo hace una opción muy atractiva debido a su facilidad, sin embargo, debido a que es un protocolo de asignación dinámica, hace más difícil su configuración remota via WAN si su asignación IP cambia constantemente.

IP Estática: En esta opción debes configurar de manera manual la dirección IP, la máscara de subred, puerta de enlace y servidores DNS, a diferencia de una asignación dinámica, esta configuración es constante aun cuando el router inalámbrico se desconecte, ya que la dirección no se renueva de manera automática.

Dirección IP:

Máscara de Subred:

Puerta de Enlace Predeterminada:

Servidor DNS Primario:

Servidor DNS Secundario: (opcional)

Para más información sobre direcciones IP, consulta el anexo sobre direccionamiento IP al final de este artículo.

Configuración LAN

En este apartado vas a configurar el direccionamiento estático del router inalámbrico, el cual consta de una dirección IP y una máscara de subred, este direccionamiento será la base para la red LAN/WLAN que compartirá el router inalámbrico mediante la comunicación inalámbrica o los puertos Ethernet LAN.

Dirección MAC:

Dirección IP:

Máscara de Subred:

Configuración de DHCP

Al tener una red independiente usando como base la configuración de la red LAN, esta nueva red como tal no tiene un protocolo para asignar automáticamente la información necesaria para que un dispositivo que se conecte mediante el router inalámbrico pueda acceder a Internet, por lo que es necesario configurarlo con la información necesaria para que se puedan conectar.

Servidor DHCP: ☐ Deshabilitar ☒ Habilitar

Dirección IP de Inicio:

Dirección IP Final:

Tiempo de Arrendamiento: minutos (1~2880 minutos, el valor predeterminado es 120)

Puerta de Enlace Predeterminada: (opcional)

Dominio Predeterminado: (opcional)

Servidor DNS: (opcional)

Servidor DNS Secundario: (opcional)

Entre los campos a llenar está la dirección IP de inicio y final, estos determinan el rango de direcciones que el protocolo asignará a los dispositivos que se vayan conectando, sin importar si son por los puertos LAN o mediante la WLAN.

El tiempo de arrendamiento indica el tiempo que la dirección IP pueda estar asignada a un dispositivo,

cuando termina el tiempo, el dispositivo conectado puede volver a renovar ese tiempo, si no lo renueva, esta dirección regresa al conjunto de direcciones disponibles.

Puerta de Enlace predeterminada es la dirección que está asignada al router inalámbrico en el campo de LAN, ya que este funciona como una puerta a las demás redes.

El otro campo importante es el Servidor DNS, ya que es el servicio que nos permitirá resolver los nombres de dominio (por ejemplo Facebook.com) a las direcciones IP que utilizan las computadoras para conectarse a los diferentes servicios a los que desees acceder.

Parámetros de enrutamiento

Dependiendo del modelo y tipo de router inalámbrico que adquieras, puedes configurar los métodos de enrutamiento entre las redes que hayas configurado anteriormente, entre las posibilidades de enrutamiento, las más comunes son:

- Enrutamiento estático: En este caso tú configuras las rutas de manera manual para poder acceder a las diferentes redes a las que quieras acceder, desde redes locales hasta Internet, para lograrlo debes configurar cada entrada de enrutamiento estático con los siguientes datos:
 - Dirección IP destino: También es mencionado como red destino o en inglés como “Destination Network” aquí debes de ingresar el Identificador de red en su formato de IPv4 o IPv6 en caso de que sea soportado para que el router reconozca esta dirección como el destino de la información que va a enrutar.
 - Máscara de subred: Este campo lo tienes que llenar con la máscara asociada a la red destino a la que quieres llegar, algunas veces es sustituida por el prefijo (con la representación “/X” donde “X” es un número que oscila entre el 0 y 32 en direcciones IPv4 y entre el 0 y 128 en direcciones IPv6).
 - Puerta de enlace: también conocido como siguiente salto o “Next Hop”, es la dirección IP inmediata o la más próxima desde el router a la red destino que sea externa al router, por ejemplo, la dirección IP del siguiente router conectado mediante el mismo cable Ethernet.

- Enrutamiento dinámico: En esta opción puedes configurar tu router inalámbrico utilizando diferentes protocolos de enrutamiento, entre los que están RIP, OSPF y en caso de ser un router Cisco puedes hacer el uso de EIGRP, en el cual configurarás tu router inalámbrico con los datos necesarios para que este pueda ser parte del protocolo de enrutamiento que ya estas usando en tu red.
- NAT: Este a pesar de que no es una forma de enrutamiento en sí, es una opción muy común en los routers inalámbricos, esto es debido a que, por lo general estos routers son utilizados en redes pequeñas y permite que estos puedan ser conectados fácilmente a la red otorgada por el modem-router usando su puerto WAN en modo DHCP, entonces el trabajo del NAT es hacer la traducción de las direcciones IP de la red LAN a las direcciones en la red WAN, y en la forma más común que es el PAT o NAT de sobre flujo, las direcciones de la red LAN son traducidas a una única dirección de la red WAN.

Nota: En el router inalámbrico usado en esta guía, solo soporta enrutamiento estático y PAT.

Configuración de la red inalámbrica (WLAN)

Este capítulo es utilizado en los diferentes modos utilizados en esta guía ya que son los parámetros que necesitas configurar para el correcto funcionamiento de la red inalámbrica una vez considerados los factores externos mencionados en capítulos anteriores.

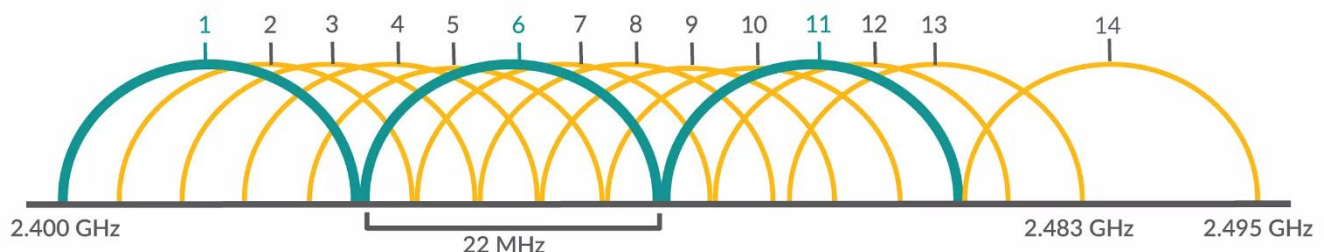
Frecuencias 2.4 Ghz y 5 Ghz

Dependiendo de los estándares que pueda soportar el router inalámbrico, este lo configurarás para una o ambas frecuencias de operación, sin embargo, cada frecuencia tiene protocolos y características de operación diferentes.

WLAN en 2.4 Ghz

En los estándares que usan la frecuencia de 2.4 Ghz. operan las frecuencias entre 2412 Mhz. y 2472 Mhz., estos a su vez son divididos en 13 canales de 20 Mhz., lo cual lo puedes observar en la siguiente imagen.

2.4 GHz Band Channels



-www.redeszone.net

Aquí se observa que, entre los canales de transmisión, si tenemos diferentes transmisores que operen entre ellos, existe la posibilidad de que las señales o la información se empalmen, lo que provoca que la comunicación con los dispositivos no sea óptima, para evitar esto te recomendamos usar los canales 1, 6 y 11.

Configurando WLAN en 2.4 Ghz

Para configurar los parámetros de esta frecuencia, existen tres partes: configuración básica, seguridad inalámbrica e Inalámbrico avanzado.

Configuración básica

Lo básico a configurar en este apartado son los siguientes parámetros:

- **Habilitar red:** Este parámetro indica si está habilitada o no la red mediante 2.4 Ghz.
- **Nombre de la red (SSID):** Es el nombre con el cual los demás dispositivos van a reconocer el router inalámbrico al escanear la red inalámbrica.
- **Región:** Indica la región de operación del router inalámbrico, lo recomendado es usar la región asignada a tu país o escoger tu país si está en esta lista desplegable.
- **Modo:** Aquí indica en que estándar va a operar en esta frecuencia, algunos routers inalámbricos te permiten usar el modo mixto, en el cual permite operar a diferentes estándares simultáneamente.
- **Canal:** En este parámetro tú seleccionas el canal de operación de tu router inalámbrico.
- **Ancho de Canal:** Selecciona si el ancho de canal es de 20 Mhz o 40 Mhz.
- **Habilitar transmisión SSID:** con este parámetro indicas si el SSID va a ser transmitido, al momento de que un dispositivo cliente quiera conectarse a tu WLAN, este escanea las redes WLAN disponibles y los diferentes AP o routers inalámbricos que estén cerca mandan su SSID para que el cliente se pueda conectar, al estar activada la transmisión SSID el router inalámbrico envía esa información para que el cliente pueda iniciar la conexión, de lo contrario la WLAN debe ser registrada manualmente mediante una opción en el cliente que se llama “red oculta” es especialmente útil si quieres mantener oculta tu WLAN de los atacantes.

Configuración Inalámbrica (2.4GHz)

Inalámbrico: ☒ Habilitar ☐ Deshabilitar

Nombre de la Red Inalámbrica: (también se le conoce como SSID)

Región:

Modo:

Canal:

Ancho de Canal:

☒ Habilitar la Transmisión de SSID

Configuración inalámbrica avanzada

En esta sección están parámetros más avanzados, entre los que están:

- **Potencia de transmisión:** Dependiendo el tipo de dispositivo que estás configurando puedes escoger entre un valor numérico en decibeles (Db) o en bajo, medio y alto para determinar la potencia de la señal que genera el router inalámbrico, te recomendamos ajustar la potencia a tus necesidades ya que, entre mayor sea la potencia, mayor es la cantidad de energía que consume.
- **Intervalo de Baliza:** Estas balizas son mensajes enviados por el router inalámbrico para empezar la sincronización de la red inalámbrica, este parámetro puede ser modificado en un valor de 40-1000 milisegundos.

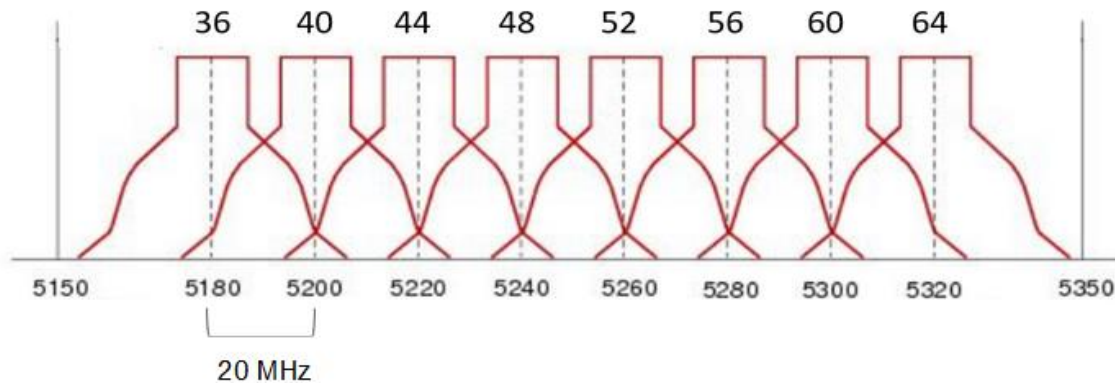
- Umbral de RTS: “Request to Send” o “Petición para enviar” es un mecanismo para reducir la colisión de tramas, en este caso si una trama rebasa el umbral (1-2346 bytes), el cliente hace una negociación con el router inalámbrico para ese envío de trama.
- Umbral de fragmentación: Este parámetro indica el tamaño máximo de un paquete de datos, en caso de ser rebasado, este será fragmentado, por lo que, si el umbral de fragmentación es muy bajo, la red inalámbrica puede congestionarse rápidamente por la gran cantidad de fragmentos enviados, su rango es de 40-2346 bytes.
- Intervalo de DTIM: “Delivery Traffic Indication Message” es un tipo de mensaje especial para informar a los clientes sobre la presencia de datos en el buffer del router inalámbrico, y el intervalo indica cuantas balizas deben pasar antes de enviar un DTIM, este tipo de mensajes son utilizados por dispositivos que estén en modo de bajo consumo, en el cual ignoran las balizas y sólo reciben y procesan DTIM, por lo que, si el intervalo DTIM es mayor, los dispositivos recibirán menos mensajes DTIM.
- Habilitar GI corto: el GI “Guard Interval” es hecho para evitar la pérdida de señal debido al efecto de multiple trayecto, el cual es provocado por los siguientes escenarios:
 - Difracción: cuando la señal se dobla por objetos afilados, creando una nueva señal.
 - Dispersión: cuando una señal de radiofrecuencia se refleja en una superficie no uniforme en múltiples direcciones.
 - Reflexión: la señal entra en contacto con una superficie uniformemente plana y se refleja en un ángulo predecible.
- Habilitar Aislamiento de cliente: Este parámetro hace un aislamiento de los clientes conectados por la red inalámbrica.
- Habilitar WMM (agregar el significado de las siglas): Esta es una opción que aplica la calidad de servicio (Quality of service o “QoS”) priorizando los mensajes que tengan mayor prioridad, por ejemplo, los datos de voz y video.

WLAN en 5 GHz

Las opciones de configuración para la frecuencia de 5 GHz son muy similares a las de 2.4 GHz, con la excepción de los siguientes aspectos.

Configuración básica

- Canal: En esta frecuencia tiene los canales 36, 40, 44, 48, 60, 149, 153, 157, 161, estos canales a diferencia de la frecuencia de 2.4 GHz, son canales que no se empalman entre sí.



- Ancho de canal: En el caso de la frecuencia de 5 GHz. los anchos de canal soportados son 20, 40 y 80 MHz.
- Modo: Esta casilla es para seleccionar la variante del estándar 802.11 a utilizar, ya sea utilizar uno o el modo “mixto” en el cual se hace el soporte de diferentes variantes.

Seguridad inalámbrica

Además de los protocolos y estándares para conectar un dispositivo al router inalámbrico, debes añadir una capa de seguridad para regular el acceso a la red WLAN que estás configurando, para ello están los diferentes métodos de autenticación que se pueden configurar en el router inalámbrico.

WEP

Este algoritmo de autenticación fue creado junto con el estándar 802.11 en 1997, en 2001 se publicó un artículo de criptoanálisis sobre este algoritmo, en el cual revelan sus vulnerabilidades y cómo explotarlas, por lo que este algoritmo está en desuso actualmente.

WPA

Este algoritmo definido en el estándar 802.11i e implementado en 1999, a diferencia de WEP, añade TKIP (Temporal Key Integrity Protocol), en el cual agregan una llave por cada paquete de datos a enviar, además de un MAC (Message authentication code) para verificar la integridad del mensaje, sin embargo, en 2008 Martin Beck y Erik Tews crean un documento en el que explican cómo obtener la llave MIC (Message Integrity check) y posteriormente hacer la transmisión de paquetes, actualmente está en desuso.

WPA2

Este algoritmo es ratificado en 2004 reemplazando el algoritmo WPA, es el estándar actual mientras se hace la migración a WPA3, los cambios más significantes respecto a su versión anterior es el uso de AES (Advanced Encryption Standard) como algoritmo de cifrado, el cual es el más seguro hasta la fecha, esto es utilizado en el protocolo CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol) para dar los siguientes servicios:

- Confidencialidad de los datos.

- Autenticación.
- Control de acceso.

En 2016 se descubrió un ataque llamado KRACK (Key Reinstallation Attack), el cual es un ataque de repetición, en el cual al repetir o restaurar el Nonce usado en un paso de WPA, el atacante puede conseguir la clave usada en la transmisión de datos para lograr un ataque llamado “Man-in-the-middle”, para mitigarlo, se crearon actualizaciones o “parches” en los dispositivos clientes para evitar esta vulnerabilidad, te recomendamos usar éste método de autenticación o su siguiente actualización llamada WPA3 si es que tu router inalámbrico lo soporta, en el caso del Archer c20 no tiene soporte para WPA3, así que te mostraremos cómo configurarlo para el uso de WPA2.

WPA2 PSK (Pre-shared Key) y Enterprise

WPA2 tiene dos opciones de configuración:

- PSK: Esta es la opción más utilizada, ya que simplemente debes configurar una contraseña única de acceso, además de seleccionar el método de cifrado, puedes elegir entre TKIP y AES, te recomendamos encarecidamente usar AES, y la contraseña inalámbrica la puedes escribir usando los caracteres ASCII con una longitud de contraseña entre 8 y 63 caracteres.
- Enterprise: Esta opción es la más común para empresas, ya que a diferencia de PSK, en esta opción haces el uso del protocolo RADIUS (Remote Authentication Dial-In User Service), mediante un servidor RADIUS, en el cual debes tener el registro de credenciales usuario-contraseña con las que tus usuarios(as) se identificarán para poder tener acceso a la red WLAN.

Configurando WPA2 PSK

Para configurar WPA2, basta con marcar su casilla y poner los siguientes parámetros:

- Versión: Debes seleccionar WPA2 como la versión a usar.
- Encriptación: Están las opciones TKIP y AES, selecciona usar AES a menos que tengas dispositivos que no lo soporten.
- Contraseña inalámbrica: aquí escribes la contraseña o passphrase de acceso a la WLAN.
- Periodo de actualización de clave del grupo: Este parámetro es para determinar el periodo de actualización de una llave de grupo conocida como GTK (Group Temporal Key) usada en uno de los pasos de un proceso llamado “4 way handshake”, esto es para evitar el uso constante de la misma GTK, los valores que puedes usar un valor de 0 a 30, en el cual “0” indica que no se actualizará la GTK, fuera de eso entre menor sea el número más rápido será el cambio de la GTK.

☒ WPA/WPA2 - Personal(Recomendado)

Versión:	<input type="text" value="WPA2-PSK"/>
Encriptación:	<input type="text" value="AES"/>
Contraseña Inalámbrica:	<input type="text" value="ElenoTrejo2018"/>
Periodo de Actualización Clave del Grupo:	<input type="text" value="0"/>

Configurando WPA2 Enterprise

Antes de intentar usar este modo es necesario que tengas en funcionamiento un servidor RADIUS, además de una ruta configurada a la red del servidor RADIUS en caso de estar en una red externa al router inalámbrico que vas a configurar. Una vez que tengas este servidor en funcionamiento ya puedes configurar WPA 2 Enterprise con los siguientes parámetros:

- Versión: Selecciona WPA2 como versión a usar.
- Encriptación: Selecciona AES.
- IP del servidor RADIUS: Aquí debes escribir la dirección IP que está asignada al servidor RADIUS previamente configurado.
- Puerto del servidor RADIUS: Aquí escribe el puerto con el que esta operando tu servidor RADIUS para que el router inalámbrico pueda establecer una conexión, el puerto predeterminado es el 1812 UDP.
- Contraseña del servidor RADIUS: Aquí ingresas la contraseña para empezar una sesión en el servidor RADIUS.
- Periodo de actualización de clave del grupo: Igual que en WPA2 PSK, es el periodo para el cambio de la GTK.

☐ WPA/WPA2 - Empresarial

Versión:	<input type="text" value="Automático"/>
Encriptación:	<input type="text" value="Automático"/>
IP del Servidor RADIUS:	<input type="text"/>
Puerto del Servidor RADIUS:	<input type="text" value="1812"/> (1-65535, 0 representa el puerto predeterminado 1812)
Contraseña del Servidor RADIUS:	<input type="password"/>
Periodo de Actualización Clave del Grupo:	<input type="text" value="0"/>

WPS (Wi-Fi Protected Setup)

Es un estándar introducido en 2007 diseñado para facilitar la configuración de seguridad en una red WLAN usando WPA2, pensado para minimizar la intervención del usuario final en la configuración de dispositivos que se conecten a la WLAN.

WPS está diseñado para redes de casa con los siguientes modos:

- Método PIN: En este modo se puede acceder a la red WLAN a través de un PIN hecho de 8 caracteres, con las siguientes formas:
 - PIN del cliente: En este caso se puede conectar un nuevo dispositivo cliente ingresando el PIN generado por el cliente mediante Wi-Fi Direct al router inalámbrico para que se inicie el proceso del envío de credenciales para conectarse a la red WLAN.
 - PIN del Autenticador: En este caso el autenticador (Router inalámbrico) generará el PIN que debe ser ingresado en el dispositivo cliente para hacer el proceso de envío de credenciales.
- Mediante botón: En este método se utiliza un botón físico o virtual para que ambos, el router y el dispositivo cliente para que estos estén en modo “emparejamiento” y puedan sincronizarse entre ellos para la obtención

de las credenciales de acceso, en este modo el router aceptará la primera conexión mediante WPS que acepte para evitar más de una conexión.

- Comunicación cercana: En este método se valen de tecnologías que permitan la comunicación muy cercana entre dispositivos, por ejemplo, la tecnología NFC (Near-Field communication), con el cual al acercar un dispositivo con soporte NFC al router inalámbrico que también lo soporte, se sincronizan las credenciales de acceso a la WLAN.

A pesar de que WPS es una opción muy atractiva de utilizar gracias a su facilidad de uso, te recomendamos evitar este tipo de métodos para hacer una red segura, ya que existen diferentes formas de atacar a cada uno de los métodos de WPS descritos, esto es porque al ser diseñados para su facilidad de uso, dejan vulnerabilidades que un atacante puede aprovechar.

Modo Access Point (AP)

Este modo es para que tu router inalámbrico se comporte como un AP, esto quiere decir que ya no tendrá sus funcionalidades de enrutamiento haciendo que en lugar de separar la red WLAN de la red cableada, este pertenezca a la misma red, haciendo al AP una extensión de la red LAN.

Para pasar a este modo es muy recomendado usar la configuración rápida y después configurar los parámetros específicos del AP, esto es para configurar de manera rápida la dirección IP del AP con una dirección estática y poder configurarlo después del cambio de modo, esto es para evitar los siguientes escenarios:

- En el modo router inalámbrico tiene configurada una dirección IP que no pertenezca a la LAN, esto puede provocar que el acceso a la página de configuración mediante navegador sea muy difícil.
- La dirección IP configurada en el router inalámbrico sea dinámica (mediante DHCP), esto hará que tengas que escanear cada dirección IP hasta hallar la dirección para configurar el router inalámbrico cuando pase a modo AP.

Configuración rápida paso a paso

El primer paso es ingresar a “Configuración rápida”, seleccionar el modo de operación “Punto de acceso” y seleccionar “siguiente”.

Configuración Rápida
Modo de operación
Red
Selección de la Banda Dual
Inalámbrico de 2.4GHz
Inalámbrico de 5GHz
Red para Invitados
DHCP
Transferencia
Seguridad
Controles Parentales

Configuración Rápida - Modo de Operación

Elija el Modo de operación:

☒ Router inalámbrico
Compartir conexión a Internet desde un cable Ethernet. Por ejemplo, habitación de hotel, ...

☐ Punto de acceso

☐ Extensor de Rango

Con esto empezará las primeras dos ventanas de configuración del modo AP, en estas configurarás los parámetros básicos y opcionalmente avanzados de las frecuencias 2.4 y 5 Ghz, esto incluye el SSID, región y seguridad en dichas frecuencias, para ello te recomendamos repasar el capítulo “Configuración básica” de esta guía.

Configuración rápida - 2.4G inalámbrico

Inalámbrico: ☒ Habilitar ☐ Deshabilitar

Nombre de la Red Inalámbrica: (también se le conoce como SSID)

Región:

Seguridad:

☒ WPA2-PSK (Recomendado)

Contraseña Inalámbrica

(Ingresar los caracteres ASCII entre 8 y 63 o caracteres Hexadecimales entre 8 y 64.)

☐ Deshabilitar la Seguridad Inalámbrica

☐ Más Configuraciones Inalámbricas Avanzadas

Regresar

Siguiente

Una vez que hayas configurado las WLAN en 2.4 y 5 GHz lo siguiente es configurar la dirección IP del modo AP, existe la asignación dinámica por DHCP y la asignación manual por IP estática, te recomendamos mucho usar IP estática para que posteriormente a la configuración rápida tengas la facilidad de entrar a la configuración del AP mediante el navegador.

Al asignar la dirección IP, esta debe pertenecer a la misma red que el módem-router para que puedas acceder fácilmente mediante un navegador y poder hacer cambios cuando lo necesites, además de asignar la misma máscara de subred del módem-router al que está conectado, por lo general es 255.255.255.0.

Tipo de LAN:

Nota: Los parámetros IP no se pueden configurar si ha elegido Smart IP (DHCP)

(En esta situación, el dispositivo le ayudará a configurar automáticamente los parámetros de IP según sea necesario).

Dirección IP:

Máscara de Subred:

Le recomendamos que configure este AP con la misma subred IP y máscara de subred, pero una dirección IP diferente de su AP / Router raíz.

Servidor DHCP: ☐ Habilitar ☒ Deshabilitar

Regresar

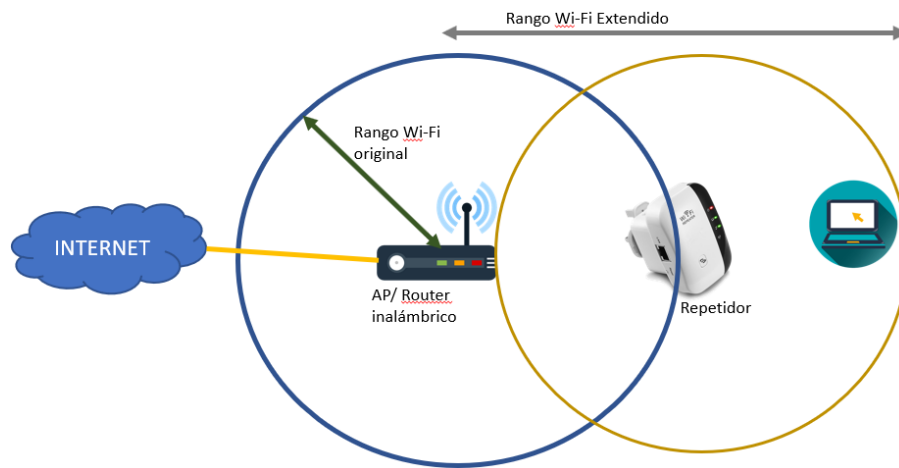
Siguiente

Por ultimo está la opción de activar o no el servidor DHCP, al activarlo hace que el AP funcione como servidor DHCP para configurar los dispositivos que se vayan conectando a la red WLAN del AP, te recomendamos usarlo si sabes la configuración del servidor DHCP del módem-router para evitar la doble asignación de direcciones IP, de lo contrario te recomendamos deshabilitarlo, de esta manera el router-módem se encargará de la asignación IP para los dispositivos que se vayan conectando mediante el AP.

Modo extensor de rango

Entendiendo un extensor de rango

Un extensor de rango o “Repeater” (repetidor) es un dispositivo que se encarga de recibir una señal y la retransmite a una nueva área de cobertura, normalmente usando el mismo canal de comunicación, esto provoca que, cuando el



extensor retransmita la señal en el mismo canal, el AP o router inalámbrico que está siendo extendido tenga un funcionamiento sub-óptimo debido a la saturación del canal de comunicación, para evitar esto hay extensores que tienen más de una antena para usar un canal diferente en el proceso de retransmisión, por lo que te recomendamos que, al configurar un extensor de rango uses canales que no se empalmen entre sí.

Configuración rápida paso a paso

Empieza ingresando a “Configuración rápida” y selecciona el modo extensor de rango

Estado	Configuración Rápida - Modo de Operación
Configuración Rápida	Elija el Modo de operación:
Modo de operación	<input type="radio"/> Router inalámbrico
Red	<input type="radio"/> Punto de acceso
Selección de la Banda Dual	<input checked="" type="radio"/> Extensor de Rango
Inalámbrico de 2.4GHz	Amplíe el alcance de una red Wi-Fi existente
Inalámbrico de 5GHz	
Red para Invitados	
DHCP	
Herramientas del Sistema	
Finalizar Sesión	Regresar Siguiente

En las siguientes ventanas tienes que seleccionar las redes WLAN que vas a extender para las frecuencias de 2.4 GHz y 5 GHz respectivamente para facilitar la configuración.

Los AP escaneados son los siguientes

Números AP: 16

Actualizar

ID	Banda	BSSID	SSID	Potencia de la Señal	Canal	Encriptación	Conectar
1	2.4GHz	[REDACTED]	[REDACTED]ES	76	9	WPA2-PSK/AES	<input type="checkbox"/>
2	2.4GHz	[REDACTED]	[REDACTED]	68	4	WPA2-PSK/AES	<input type="checkbox"/>
3	2.4GHz	[REDACTED]	[REDACTED]	64	9	WPA2-PSK/AES	<input type="checkbox"/>
4	2.4GHz	[REDACTED]	[REDACTED]vi	61	6	WPA2-PSK/AES	<input type="checkbox"/>
5	2.4GHz	[REDACTED]	[REDACTED]34	59	11	WPA2-PSK/AES	<input type="checkbox"/>
6	2.4GHz	[REDACTED]	[REDACTED]	51	6	Ninguno	<input type="checkbox"/>
7	2.4GHz	[REDACTED]	[REDACTED]do	50	6	WPA2-PSK/AES	<input type="checkbox"/>
8	2.4GHz	[REDACTED]	[REDACTED]	45	11	WPA2-PSK/AES	<input type="checkbox"/>
9	2.4GHz	[REDACTED]	[REDACTED]5C91	44	3	WPA2-PSK/AES	<input type="checkbox"/>
10	2.4GHz	[REDACTED]	[REDACTED]B_2.4	44	10	WPA2-PSK/AES	<input type="checkbox"/>
11	2.4GHz	[REDACTED]	[REDACTED]EXT	41	6	WPA-PSK/AES	<input type="checkbox"/>
12	2.4GHz	[REDACTED]	[REDACTED]8	40	6	WPA2-PSK/AES	<input type="checkbox"/>
13	2.4GHz	[REDACTED]	[REDACTED]01	36	11	WPA2-PSK/AES	<input type="checkbox"/>
14	2.4GHz	[REDACTED]	[REDACTED]8600	35	1	WPA2-PSK/AES	<input type="checkbox"/>
15	2.4GHz	[REDACTED]	[REDACTED]0A9A	35	9	WPA2-PSK/AES	<input type="checkbox"/>
16	2.4GHz	[REDACTED]	[REDACTED]36	34	11	WPA2-PSK/AES	<input type="checkbox"/>

Regresar

Siguiente

Una vez hecho esto, entrarás a una ventana de configuración extendida para las redes que vas a extender, en el cual tienes que definir los parámetros para que el extensor pueda conectarse a las redes WLAN que vas a extender, entre estos están:

- **Habilitar:** para habilitar la retransmisión de la señal en la frecuencia indicada.
- **SSID de la estación fuente.**
- **La dirección MAC de la estación fuente.**
- **Tipo de clave:** Es el método de autenticación que utiliza la red que vas a extender, debe ser la misma.
- **Encriptación:** Es el método de cifrado usado por la red que vas a extender.
- **Contraseña:** la contraseña definida en la red que vas a extender.

Adicionalmente puedes definir si mantener o cambiar el SSID de la red que vas a extender, esto lo puedes modificar a tu gusto, puedes seleccionar “Copiar desde la raíz AP” para que use la misma SSID del AP fuente o “personalizar” si quieres cambiar el nombre de los SSID respectivos.

Configuración Rápida - Inalámbrico

Región: México

Inalámbrico de 2.4GHz: ☒ Habilitar

SSID (a ser conectado en puente): [REDACTED]

Dirección MAC (a ser conectada en puente): [REDACTED] e.g. 00:1D:0F:11:22:33

Tipo de Clave: WPA2-PSK

Encriptación: AES

Contraseña:

Inalámbrico de 5GHz: ☒ Habilitar

SSID(to be bridged): [REDACTED]

MAC Address(to be bridged): [REDACTED] e.g. 00:1D:0F:11:22:33

Tipo de Clave: WPA2-PSK

Encriptación: AES

Contraseña:

Escanear

Nombre del extensor de rango inalámbrico: ☐ Copiar desde la raíz AP

Extended 2.4GHz SSID: [REDACTED]

Extended 5GHz SSID: [REDACTED]

☒ Personalizar

Extended 2.4GHz SSID: [REDACTED]_Ext

Extended 5GHz SSID: [REDACTED]_Ext_5G

Regresar

Siguiente

Ajustes de seguridad.

Los routers inalámbricos tienen diversas funciones adicionales para proteger tu red de ataques o accesos sin autorización, estas funciones sólo están disponibles en el modo router inalámbrico para que se puedan configurar.

Entre las funciones disponibles están:

- Seguridad: Está dividida en dos partes, seguridad básica y avanzada, en el cual puedes configurar parámetros como lo son:
 - Firewall SPI (Statefull packet inspection).
 - VPN (Virtual Private Network).
 - ALG (Application Layer Gateway).
 - Protección DoS (Denial of Service).
- Control Parental: Es una función diseñada para controlar la actividad de menores en la LAN y WLAN del router inalámbrico, en el cual puedes restringir el acceso a sitios de Internet o limitar el horario de acceso a la red, todo esto con una interfaz amigable y con una cantidad de usuarios a controlar limitada.
- Control de acceso: En esta función puedes controlar el acceso a la red, limitar el horario de acceso mediante direcciones MAC o rangos de direcciones IP, a diferencia del control parental, aquí puedes configurar una gran cantidad de reglas a un conjunto más extenso de usuarios, ya sea identificados mediante direcciones IP o mediante direcciones MAC, sin embargo, la complejidad de configuración aumenta.

Configurando el control parental

En el modelo Archer C20 activas el control parental marcando la casilla de habilitación y escribiendo la dirección MAC

Controles Parentales

Los Controles Parentales pueden ser usados para administrar toda la actividad de Internet incluyendo limitar el uso y/o acceso a sitios web específicos a todos los clientes en El Horario se basa en la hora del Router. La hora puede ser configurada en "Herramientas del Sistema -> [Configuraciones de la Hora](#)".

☒ Habilitar los Controles Parentales

La Dirección MAC de la PC Parental:

La Dirección MAC de la PC Actual:

[Copiar lo Citado Más Arriba](#)

de la computadora o dispositivo inteligente que va a funcionar como el administrador de las configuraciones.

En la siguiente sección tienes cuatro espacios en los que puedes ingresar hasta 4 dispositivos a los cuales se les aplicarán las reglas de horario y filtros de páginas.

Dirección MAC - 1:

Dirección MAC - 2:

Dirección MAC - 3:

Dirección MAC - 4:

Dirección MAC en la LAN actual: Copiar a

Luego está la sección de horario, el cual es un panel de cuadros gris y otro color de contraste para que definas los días y rangos de horas en las cuales los dispositivos tendrán acceso a la red de Internet, en el ejemplo de la imagen el horario permitido es de las 00:00 horas a las 11:00 horas.

Aplicar A: Hora de Inicio: Hora Final:

Hora	0:00	1:00	2:00	3:00	4:00	5:00	6:00	7:00	8:00	9:00	10:00	11:00	12:00	13:00	14:00
Dom.															
Lun.															
Jue.															
Mier.															
Jue.															
Vie.															
Sab.															

Por último, hay una sección en la que debes indicar los sitios a los que se podrán conectar los dispositivos definiéndolos por su nombre de dominio mientras estén en el horario permitido, si no hay ningún sitio registrado, se permitirá el acceso a cualquier página respetando el horario descrito en la sección anterior.

Agregar URL:

<input type="checkbox"/>	Detalles
<input type="checkbox"/>	www.youtube.com
<input type="checkbox"/>	www.google.com
<input type="checkbox"/>	www.facebook.com

(No tomarán efecto hasta que guarde estos cambios)

Nota: Dependiendo de la versión del router inalámbrico puede tener una forma diferente de configurar el control parental, en el caso del Archer c20 se podía acceder a la página en el horario permitido, sin embargo, cuando la página depende de otros dominios para diferentes servicios (cargar imágenes, audio o vídeo), al tener un dominio diferente, este los bloquea impidiendo la carga del contenido de la página, por lo que no es muy recomendado usar la sección de los sitios permitidos.

Configurando el control de acceso

Esta sección “Control de acceso” está dividida en cuatro partes principales para determinar las reglas, los dispositivos afectados, el destino u horario de aplicación de las reglas del control de acceso, estas secciones son las siguientes:

Parte 1: Host

Este hace referencia a los dispositivos finales a los cuales les quieres aplicar las reglas, en esta sección defines los dispositivos que van a ser afectados por una regla o filtro, los puedes definir de dos maneras:

- Mediante direcciones IP: Aquí defines la dirección o rango de direcciones IP a las cuales vas a afectar con una determinada regla.
- Mediante direcciones MAC: Aquí defines la dirección MAC de un único dispositivo para que se le apliquen una o más reglas definidas.

En cualquiera de las dos maneras hay un espacio para añadir una descripción del “Host”, el cual es obligatorio para identificar a los dispositivos a los que posteriormente aplicarás reglas.

Parte 2: Destino

En esta parte se define a los sitios, direcciones IP o dispositivos únicos a los que se busca permitir o restringir, hay 3 formas de definir a los “Destino”:

- Dirección IP: Aquí defines la dirección o rango de direcciones IP a los que vas a permitir o restringir el acceso.
- Dirección MAC: Aquí defines la dirección MAC del dispositivo al cual vas a permitir o restringir el acceso, solo funciona a nivel LAN o WLAN del router inalámbrico.
- Dirección URL: Aquí defines la URL del sitio al cual vas a permitir o restringir el acceso.

En cualquiera de las tres formas debes agregar una “descripción” para identificar el “Destino”.

Parte 3: Horario

Esta parte es para definir los horarios que se pueden aplicar en las reglas, se definen con una tabla utilizada en el control parental, además de una descripción para identificar el horario.

Aplicar A:

Hora de Inicio:

Hora Final:

Hora	0:00	1:00	2:00	3:00	4:00	5:00	6:00	7:00	8:00	9:00	10:00	11:00	12:00	13:00	14:00
Dom.															
Lun.															
Jue.															
Mier.															
Jue.															
Vie.															
Sab.															

Esta descripción está en el apartado “Control Parental”.

Parte 4: Regla

Esta es la parte donde se crean las reglas de acceso para permitir o restringir el acceso desde un “Host” a un “Destino”, opcionalmente agregar el horario de permisión o restricción, dependiendo como está definida la regla, es importante que hayas creado los registros de las partes 1 a 3 para poder crear las reglas apropiadamente.

Hay dos formas de políticas de seguridad que pueden ser implementadas en esta sección:

- Política restrictiva: Se deniega todo el tráfico a excepción de lo que está descrito en las reglas añadidas.
- Política permisiva: Se permite todo el tráfico a excepción de lo que está descrito en las reglas añadidas.

Una vez seleccionada la política de seguridad que quieres seguir, lo siguiente es crear las reglas que van a permitir o negar el acceso del “Host” al “Destino”.

Los parámetros que se llenan para crear a cada regla son los siguientes:

- Descripción: Es el identificador de la regla que vas a crear.
- Host de LAN: Aquí seleccionas el “Host” definido previamente o usar la opción cualquier Host para que la regla aplique a todos los dispositivos.
- Destino: Aquí seleccionas el “Destino” definido previamente o “cualquier Host” para aplicar la regla a todas las direcciones IP o sitios.
- Horario: Aquí seleccionas el horario en el cual se va a aplicar la regla que estas creando.
- Regla: Aquí defines si la regla va a permitir o restringir lo descrito por los tres parámetros anteriores.
- Estado: Seleccionas si la regla está habilitada o no.
- Dirección: Aquí seleccionas si aplicar la regla cuando entra un paquete o cuando va a salir un paquete de datos.

Descripción:

Host de LAN: [Agregar Host de LAN](#)

Destino: [Agregar Destino](#)

Horario: [Agregar Horario](#)

Regla:

Estado:

Dirección:

Protocolo:

- Protocolo: aquí indicas si se aplica para puertos TCP, UDP, ICMP o todos.

Fuentes

FCC límite de potencia para redes Wi-Fi

<https://afar.net/tutorials/fcc-rules/>

Tabla estándares 802.11

Laboratorio de Redes y Seguridad
2021

Elaboración: Ing. Fernando Eleno Trejo
Revisión: M.C. Jaquelina López Barrientos

<https://www.pearsonitcertification.com/articles/article.aspx?p=1329709&seqNum=4>

<https://www.bboxservices.com/resources/blog/bbns/2018/04/30/802.11-wireless-standards-explained>

<https://www.intel.com/content/www/us/en/support/articles/000005725/wireless/legacy-intel-wireless-products.html#legacy>

Categorías cables Ethernet

<https://www.electronics-notes.com/articles/connectivity/ethernet-ieee-802-3/cables-types-pinout-cat-5-5e-6.php>

<https://www.fastercables.com/blog/category-cable-comparison-chart>

Dispositivos:

https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/what-is-access-point.html#~what-is-an-access-point

Configuración Tp-Link Archer c20:

https://www.tp-link.com/us/user-guides/Archer-C20_V5/conventions#ug-sub-title-10

Imagen canales 2.4 Ghz.

<https://www.redeszone.net/tutoriales/redes-wifi/por-que-routers-tienen-2-redes-wifi/>

Gi corto

<https://www.sonicwall.com/support/knowledge-base/wireless-basic-configuration-short-guard-interval-and-multipath-effect-faq/170504672960493/>

WPS

[https://documentation.help/Microchip-TCP.IP-Stack/Wi-Fi_Protected_Setup_\(WPS\).html](https://documentation.help/Microchip-TCP.IP-Stack/Wi-Fi_Protected_Setup_(WPS).html)

Tablas de potencias

<https://support.huawei.com/enterprise/en/doc/EDOC1000113315/c3242b10/power-and-signal-strength>