Configuración y gestión de dispositivos inalámbricos

Breve descripción:

Este componente formativo aborda aspectos generales y claves sobre el proceso de configuración y gestión de los dispositivos inalámbricos requeridos, de acuerdo con la arquitectura planteada en la fase de planeación.

Noviembre 2023

Tabla de contenido

Introducción

Aquí comienza el estudio del componente formativo denominado **Configuración y gestión de dispositivos inalámbricos**; explore la información del video que se muestra enseguida, la cual le contextualiza sobre los aspectos más importantes de los temas por desarrollar. ¡**Adelante**!

Video 1. Configuración y gestión de dispositivos inalámbricos

Enlace de reproducción del video

Síntesis del video: Configuración y gestión de dispositivos inalámbricos
Las redes inalámbricas han impactado la dinámica general de las sociedades, en términos de la economía, las comunicaciones, el mercado, la cultura y todas las dimensiones del desarrollo colectivo.

Gracias a su implantación y avances permanentes, estas han facilitado, sobre todo, la forma de comunicarse e informarse; hoy por hoy, las redes están al alcance de cualquier persona; con lo cual se han convertido en elemento indispensable para obtener información, capacitación, contacto, interacción, inclusión, etc.

Gracias a las redes inalámbricas, se han modificado sustancialmente las dinámicas de los entornos laborales, organizacionales.

Son muchas las compañías que hacen uso de ellas para acercar a sus usuarios, acompañarlos, brindarles asesoría, seguridad, opciones de compras, velocidad en instrucciones, formación, etc.

En la actualidad, no solo las grandes empresas cuentan con redes inalámbricas sino también las medianas y pequeñas e, incluso, las microempresas tienen acceso a ellas. Esto refleja la importancia que tiene esta tecnología.

En el ámbito educativo, por ejemplo, son usadas en los centros de cómputo, laboratorios y es implementada para facilitar a los alumnos sus estudios y trabajos. En el social, sirven para conocer y comunicarse con otros por medio de las redes sociales.

Una desventaja de las redes inalámbricas es que, si no se cuenta con una buena seguridad informática, suelen ser robadas o desvirtuadas por potenciales “hackers”.

1. Introducción a las redes inalámbricas

Una red inalámbrica es la red que no emplea cables para transmitir la información. El primer ejemplo de comunicación sin cables se dio en 1880; en ese año, Graham Bell y Summer Tainter inventaron el fotófono; implemento que permitía transmitir sonido por medio de una emisión de luz. Luego, en 1888 el físico alemán Rudolf Hertz descubrió la propagación de las ondas electromagnéticas; así, seis años después, las ondas de radio ya eran un medio de comunicación.

Se menciona que en 1899 el italiano Guillermo Marconi logró establecer comunicaciones mediante señales inalámbricas a través del canal de la Mancha, entre las ciudades de Dover y Wilmereux. Para 1907 se comunicaron los primeros mensajes completos a través del Atlántico.

Otro dato a tener en cuenta sobre el año 1971 es que un grupo de investigadores bajo la dirección de Norman Abramson, de la Universidad de Hawái, fueron pioneros con el sistema de conmutación de paquetes mediante una red de comunicación por radio llamada **ALOHA**. Se puede decir que esta fue la primera WLAN, la cual estaba formada por siete computadores situados en distintas islas que se podían comunicar por medio de un servidor. De ahí nació lo que hoy en día se conoce como **wifi**. En 1997 sale al mercado gracias a la creación del comité 802.11, en el que se dio paso a la estandarización IEEE, ("Institute of Electronics and Electrical Engineers"), para redes de área local inalámbricas (WLAN).

1.1. Clasificación de redes inalámbricas

Según Andreu (2011) las redes inalámbricas se clasifican en los siguientes grupos:

a. **Red WBAN**. Redes inalámbricas de área corporal o WBAN (“Wireless Body Area Network”) con cobertura entre 1 a 2 metros.
b. **Red WPAN**. Redes inalámbricas de área personal o WPAN (“Wireless Personal Area Network”). Su alcance es por debajo de los 10 metros, usadas para para comunicar dispositivos de un usuario como, por ejemplo, el PC y la impresora, ya sea por uso de “Bluetooth” o de IEEE 802.15.
c. **Red WLAN**. Redes inalámbricas de área local o WLAN (“Wireless Local Area Network”). Tienen un alcance de cientos de metros, utilizadas para comunicar dispositivos ubicados en un mismo edificio o grupos de edificios como, por ejemplo, “HomeRF” o wifi.
d. **Red WMAN**. Redes inalámbricas de área metropolitana o WMAN (“Wireless Metropolitan Area Network”). Tienen como función cubrir una ciudad, utilizando protocolo LMDS (“Local Multipoint Distribution Service”) o MMDS (“Multichannel Multipoint Distribution Service”).
e. **Red WWAN**. Redes inalámbricas de área extensa o WWAN (“Wireless Wide Area Network”). Conocidas también como de área global o WGAN, tienen cobertura de una gran región, país o grupo de países, basadas en tecnología celular y son consideradas como la evolución de las redes de voz.

1.2. Funcionamiento de las redes inalámbricas

Para el funcionamiento de las redes inalámbricas es relevante diferenciar algunas características, como la frecuencia de trabajo, la velocidad de transmisión y cobertura, por ejemplo. Para ello, se utilizan ondas de radio que llevan la información hacia el destino.

Las ondas de radio se refieren a portadoras que llevan la información y la energía a un receptor remoto; los datos que se envían se superponen a la portadora de radio y, finalmente, se deben extraer en el receptor. A este proceso nombrado anteriormente se le conoce como modulación de la portadora: si las ondas se transmiten con frecuencias diferentes, pueden existir envíos al mismo tiempo y espacio sin que haya interferencia.

En las redes inalámbricas WLAN se presentan dos formas de funcionamiento que son:

a. **Ad hoc (IBSS)**. Aquí cada equipo de la red se conecta con los demás; es considerado cliente y punto de acceso, pero con un máximo de nueve clientes.
b. **Infraestructura (BSS)**. Para este caso la conexión se hace utilizando un AP (punto de acceso), el cual permite que la red inalámbrica acceda la red cableada, dicho AP trabaja como puerta de entrada a la red inalámbrica con una cobertura determinada y en un lugar específico para los dispositivos que necesiten acceder.

1.3. Ventajas y desventajas

Entre las ventajas que tiene el uso de redes inalámbricas, están:

- Permiten una amplia libertad de movimientos.
- Facilitan reubicar las estaciones de trabajo.
- Evitan establecer cableado.
- Rapidez en la instalación de la red.
- De menor costo.
- Tienen mayor cobertura en puntos de difícil acceso con cables.

- Permiten la ampliación de redes locales cableadas.
- Poseen facilidad de expansión o limitación de usuarios en la red con solo añadir o quitar módulos.

Y sus desventajas son:

- Menor ancho de banda que las redes cableadas.
- Las redes que usan señales infrarrojas deben estar perfectamente alineadas, y no pueden atravesar obstáculos como paredes, árboles, etc.
- Son inseguras puesto que cualquiera puede acceder a la red inalámbrica.
- Poseen un menor ancho de banda que las redes que se unen mediante cables.

1.4. Componentes de las redes inalámbricas

Se encuentran integradas por los siguientes dispositivos:

a. Antena. Elemento que permite transmitir y recibir ondas de radio por medio de una comunicación natural como el aire o el espacio libre.

b. Punto de acceso. Dispositivo de capa 2, por medio del cual las estaciones "Wireless" pueden integrarse rápida y fácilmente a cualquier red cableada, actuando como núcleo de la red inalámbrica y puente de conexión entre redes inalámbricas y cableadas. El punto de acceso se conecta a un "router", "switch" o "hub" con un cable "Ethernet" y radia la señal wifi en un área específica; como ejemplo, si desea habilitar el acceso wifi en el área de recepción de una empresa, pero no existe un "router" que pueda cubrirla, se instala un punto de acceso cerca de la recepción y se conecta con un cable hacia el salón de equipos donde está el servidor.

c. **“Bridge” inalámbrico**. Dispositivo que permite conectar dos o más redes ubicadas en diferentes edificios, proporcionando más velocidad de transmisión de datos, además conecta sitios difíciles de cablear, pisos no contiguos, instalaciones de campus de escuelas o empresas, etc.

d. **“Router” inalámbrico**. Es el que permite la conexión de redes inalámbricas, enrutar los paquetes de datos hacia la red correcta de destino y facilita la conexión a la WLAN de dispositivos inalámbricos; es la tecnología de comunicación de ondas de radio que admite la conexión ADSL para el manejo de Internet de banda ancha y que se distribuya hacia otros computadores.

e. **Adaptadores**. Son tarjetas para expandir la capacidad de conexión, envían y reciben datos sin necesidad de cables en las redes WLAN, poseen una antena para la recepción y envío de datos y están diseñados para algunos estándares de redes inalámbricas.

1.5. Modos de operación

Para el estándar 802.11 es importante tener en cuenta dos modos fundamentales de uso para este tipo de redes: el modo “ad hoc” y el modo infraestructura BSS, los cuales se detallarán a continuación.

Modo “ad hoc”

Se conoce también como punto a punto, en este método los clientes inalámbricos establecen comunicación directa entre sí, por tanto, no es necesario un punto de acceso o AP; cada terminal inalámbrica en una red “ad hoc” configura el adaptador inalámbrico en este modo, y debe usar el mismo SSID y canal dentro de la red. Este método limita el número de dispositivos y, si estos aumentan, el rendimiento

de la red disminuye, además la conexión “ad hoc” es temporal entre dispositivos para un mismo fin, por ejemplo, compartir impresoras, archivos o juegos en la red.

La conexión de los equipos se realiza por medio de los adaptadores de red sin necesidad de un punto de acceso. Una infraestructura “ad hoc” tendría mínimo 2 computadores, tarjetas de red inalámbrica y, de hecho, los “drivers” de tarjetas de red.

En la tabla que aparece a continuación, puede consultar tanto las ventajas como desventajas del modo “ad hoc”:

Tabla 1. Ventajas y desventajas modo “ad hoc”

Ventajas	Desventajas
No necesita conexión a Internet.	Compatibilidad de tarjetas de red para conexión en modo ad–hoc.
Hay acceso a los datos de los dispositivos conectados a la red.	Es necesario configurar cada vez que se va a usar.
Realiza el envío directo de información.	No conecta dispositivos ubicados dentro del área de cobertura.
Tiene gestión no centralizada.	En la transmisión entre dos o más nodos simultáneos se presenta interferencia y competencia para acceder al medio.
La configuración es mínima.	

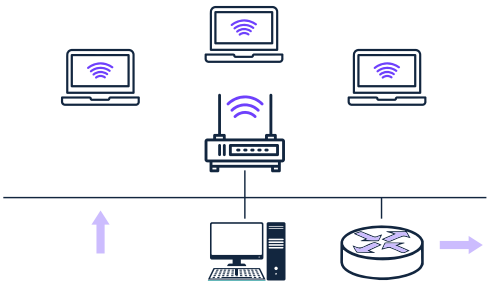
Modo infraestructura BSS

Para las redes que trabajan con el estándar IEEE 802.11, el modo de infraestructura se conoce como Conjunto de Servicios Básicos (BSS – "Basic Service Set") y las denominan también cliente - servidor o maestro - esclavo. Para este modo de infraestructura existe un dispositivo central que corresponde al punto de acceso o estación base que, generalmente, se conecta a una red "Ethernet" cableada, y así los clientes inalámbricos pueden acceder a la red fija por medio del punto de acceso. En el proceso de interconexión de los dispositivos inalámbricos hacia los puntos de acceso se debe configurar con el mismo SSID, lo que garantiza optimizar la capacidad total de la red.

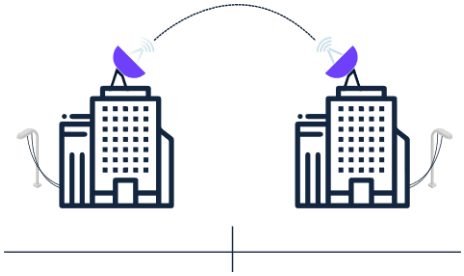
Para este caso se pueden encontrar varias formas de distribuir los elementos conectados a la red, las cuales se presentan a continuación:

Tipos de infraestructuras inalámbricas BSS

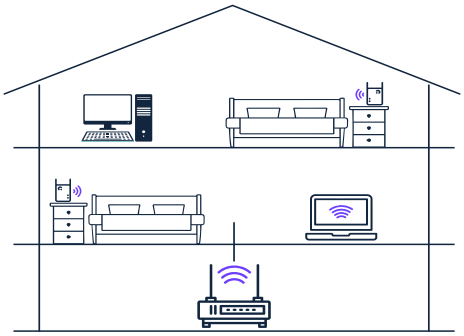
- **Tipo 1, Estrella**.



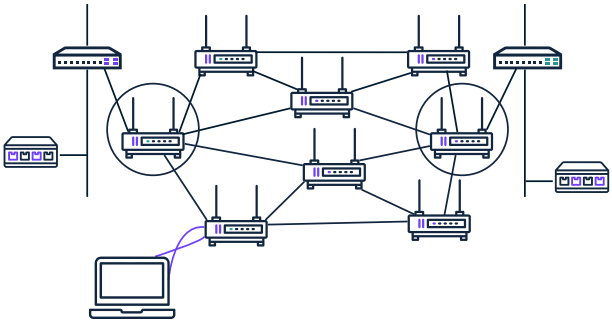
- **Tipo 2, Punto a punto**.



- **Tipo 3, Con repetidores**.



- **Tipo 4, Malla**.



1.6. Tecnologías de redes inalámbricas

En la actualidad, existen dos tipos de redes inalámbricas: para exteriores e interiores; en los sistemas para exteriores el sistema de posicionamiento global conocido como GPS por su sigla en inglés (“Global Positioning System”), es el estándar de referencia por la precisión que consigue el receptor en línea directa con varios satélites de forma simultánea.

Para interiores, este estándar no sirve, pues tantas paredes, techos y demás obstáculos, apantallan la señal y el receptor no puede sincronizarse a algún satélite, impidiendo dar su localización. Entonces, estas tecnologías por utilizar, dependen de los requisitos necesarios para acceder a una u otra aplicación o servicio. También es importante tener presente para la tecnología por escoger, el consumo de energía, precio, ancho de banda y velocidad, entre otros factores.

A continuación, se describen las diferentes tecnologías utilizadas para redes inalámbricas:

a. **"Bluetooth"**. Es la tecnología inalámbrica más utilizada para transmitir datos entre dispositivos cercanos, basada en radiofrecuencia, en la banda libre de 2.4 GHz y 3 Mbps de velocidad máxima; es muy frecuente su uso para pasar fotos y música entre teléfonos móviles. Los autos disponen del sistema "Bluetooth" para atender llamadas telefónicas con manos libres al estar conduciendo; en los dispositivos domésticos es más frecuente como en el "mouse", los auriculares, entre otros.
b. **"European Installation Bus"**. Usado para interconectar redes eléctricas inteligentes.
c. **"HomePlug"**. Protocolo utilizado para tender cableado doméstico de energía eléctrica.
d. **IrDA**. Estándar físico para la transmisión y recepción de datos por rayos; el espectro infrarrojo sirve para la comunicación bidireccional entre dos extremos con velocidades que oscilan entre 9.600 bps y 4 Mbps.
e. **INSTEON**. Red que trabaja en dos bandas de frecuencia, integrando comunicaciones por radiofrecuencia (RF) con tendido doméstico para energía eléctrica "HomePlug".
f. **nanoNET**. Se trata de protocolos inalámbricos tipo propietario, creados para sensores, como competencia de la tecnología "ZigBee".
g. **OBEX**. Abreviatura de "Object Exchange" o intercambio de datos; este protocolo fue creado para facilitar el intercambio de información binaria entre dispositivos.

h. **RadioRa**. Protocolo de tipo propietario desarrollado por Lutron para radiofrecuencia (RF) doble vía, usado en el control de iluminación residencial.

i. **"Topdog"**. Protocolo tipo propietario inalámbrico, utilizado en el control de iluminación comercial y residencial.

j. **UPB**. Protocolo desarrollado para mejorar el desempeño y confiabilidad en cableados de energía eléctrica.

k. **Wifi**. Sigla usada para el término en inglés "Wireless Fidelity" (wifi), tecnología para redes del tipo WLAN "Wireless Local Area Network", basada en el estándar IEEE 802.11. Permite realizar la transmisión de información con señales de radiofrecuencia, conectar en una misma red diferentes dispositivos como celulares, PC, "blu-ray" e impresoras que estén ubicados dentro del radio de cobertura wifi.

l. **Wi-Max**. Tecnología para red inalámbrica de área metropolitana con un alcance de 50 Km, velocidad de transmisión de hasta 70 Mbps, basada en el estándar 802.16, que opera en el rango de frecuencias de 10 GHz a 66 GHz con línea de vista, con el estándar 802.16a, opera entre los 2 y 11 GHz y sin línea de vista, puede usarse para receptores en vehículos móviles siempre que no superen 100 Km/h de velocidad, se creó como competencia para la tecnología xDSL y el acceso por cable módem.

m. **"Wireless USB"**. "Wireless Universal Serial Bus" (WUSB) en inglés, hace referencia a una conexión de alta velocidad, eficaz y sin cables, basada en la tecnología USB usada para PC.

n. **"Z-wave"**. Protocolo tipo propietario usado en redes inalámbricas de control de hogares.

o. **“ZigBee”**. Especificación global creada para sistemas de control inalámbrico llamados “**ZigBee Alliance**”, se basa en el estándar IEEE 802.15.4, usado para radios digitales de baja frecuencia, con velocidad de transmisión 250 Kbps, y limitado a controladores de 8 bits.

1.7. Radio, elementos y frecuencias del espectro

Hoy por hoy, el espectro radioeléctrico es utilizado de forma ineficiente, debido a que las bandas de frecuencia para su uso se realizan de manera fija; para ello surge una tecnología novedosa que es la radio cognitiva, la cual trae consigo varias funcionalidades que garantizan el acceso dinámico al usar el espectro. Aquí se nombran las cuatro más importantes:

- Identificar la oportunidad de acceso al espectro
- Seleccionar las bandas de frecuencia a usar
- Coordinar el acceso al espectro entre usuarios
- Movilidad espectral.

Los dos tipos más usados de radio cognitiva son:

a. **Radio cognitiva completa (radio de mitola)**. Aquí, cualquier aspecto que se observe en un nodo inalámbrico será tenido en cuenta para la toma decisiones en el cambio de parámetros de transmisión y/o recepción.
b. **Radio cognitiva detectora del espectro**. Para este caso, las decisiones se toman basadas solo en el estado del espectro de radiofrecuencia.

Igualmente, de acuerdo con las bandas del espectro disponibles para la radio cognitiva, se tiene también:

a. **Con licencia**. Se utilizan bandas asignadas a usuarios bajo licencia e, incluso, se usan bandas libres como la banda UNII o la ISM.
b. **De acceso libre**. Aquí, la radio cognitiva solo puede hacer uso de bandas libres del espectro de radiofrecuencia.

1.8. Diseño e instalación de red

Para el diseño de una red inalámbrica no solo se debe realizar la distribución de los dispositivos activos y pasivos, sino que es pertinente definir protocolos, estándares, normas y demás regulaciones necesarias para cumplir con los requerimientos establecidos. En la planeación de un diseño de red se debe tener en cuenta varios aspectos, entre los cuales se nombran los siguientes pasos que ayudan a optimizar el diseño de la red solicitada:

a. Recolección de información.
- Analizar requerimientos solicitados.
- Establecer el tipo de servicios a utilizar.
- Definir el tipo de dispositivos inalámbricos a conectar en la red (PC portátiles, de oficina, “smartphone” y “tablets”).
- Estudiar características y ubicación de los dispositivos activos para la red wifi.

b. Revisión de las instalaciones.
- Definir el tipo de instalación del punto de acceso en cada zona.
- Determinar canalizaciones del cableado hasta cada punto de acceso.
- Comprobar los obstáculos existentes que degraden el rendimiento de la red.

- Ubicación de los terminales usuario, equipos de red, como “switches”, “routers” y servidores.
- Realizar el plano de la planta, basado en el espacio disponible, la alimentación, la seguridad y el sistema de aire acondicionado del lugar.

c. Elección de dispositivos.

- Determinar las características de las antenas y que cumplan con los requerimientos solicitados.
- Definir el tipo de radio a utilizar de acuerdo con la tecnología y estándar de acceso seleccionado.

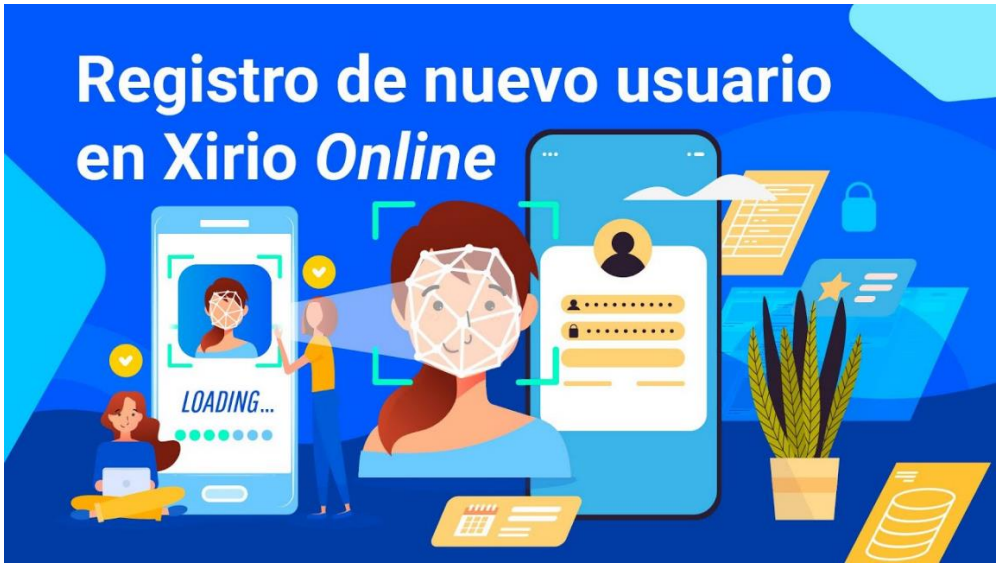
d. Diseño preliminar.

- Escoger una herramienta digital para realizar el diseño, por ejemplo, Xirio-“online”.
- Realizar el diseño basado en cobertura, con un equipo principal o central cubrir la mayor área posible.
- Realizar el diseño basado en capacidad, lo cual permite mejor capacidad, más puntos de acceso y contar con ajustes de la potencia transmitida, que permita calcular posibles interferencias conjuntas con la misma red u otras redes.
- Definir la ubicación de los equipos y analizar la precisión de los niveles de cobertura.

En relación con el diseño de una red inalámbrica, chequee los dos videos que se proponen enseguida y aprópiese del procedimiento de simulación profesional de cobertura radioeléctrica online, con la herramienta de planificación radioeléctrica Xirio-“Online”, para un caso específico de red:

Interfaz principal Xirio “Online”

Video 2. Registro de nuevo usuario en Xirio “Online”



Enlace de reproducción del video

Síntesis del video: Registro de nuevo usuario en Xirio “Online”
En este video la experta SENA ofrece las pautas y acciones, requeridas en el registro como nuevo usuario para el uso de la herramienta de planificación radioeléctrica Xirio “online”.

Video 3. Creación estudio de enlace

Enlace de reproducción del video

Síntesis del video: Creación de estudio de enlace
En este video la experta SENA ofrece el paso a paso y los requerimientos suficientes para crear un estudio de enlace con la herramienta Xirio "Online".

Topología de la red

Escoger la topología inicial de la red depende esencialmente de varios aspectos como:

- Persona manejando servidores.
- Requerimientos del cliente.
- Cantidad y ubicación de usuarios.
- Crecimiento esperado de la red.

- Estándares inalámbricos y de cableado.
- Capacidad de expansión de la red.
- Entorno de la red.
- Dispositivos y servicios requeridos por la red.
- Desempeño deseado.
- Elegir recorrido simple desde el nodo y demás componentes para minimizar costos.
- Facilitar detección de fallas.
- Optimizar instalación y reconfiguración de la red.

Servicios

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 computadores portátiles, 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.

Para asignar direcciones con DHCP se toma el modelo cliente-servidor, donde el terminal o usuario solicita la configuración IP al servidor DHCP, que es quien asigna la respectiva dirección IP acompañada de la máscara de subred, puerta de enlace predeterminada, servidor DNS y configuración proxy por WPAD ("Web Proxy Auto-Discovery Protocol") necesarios para poder acceder a los servicios. La asignación de esta dirección dinámica es de carácter temporal mientras dura la conexión con el

servicio solicitado, una vez se termina la conexión, esta dirección es liberada para ser asignada a otro usuario.

El servidor DHCP informa al Domain Name System

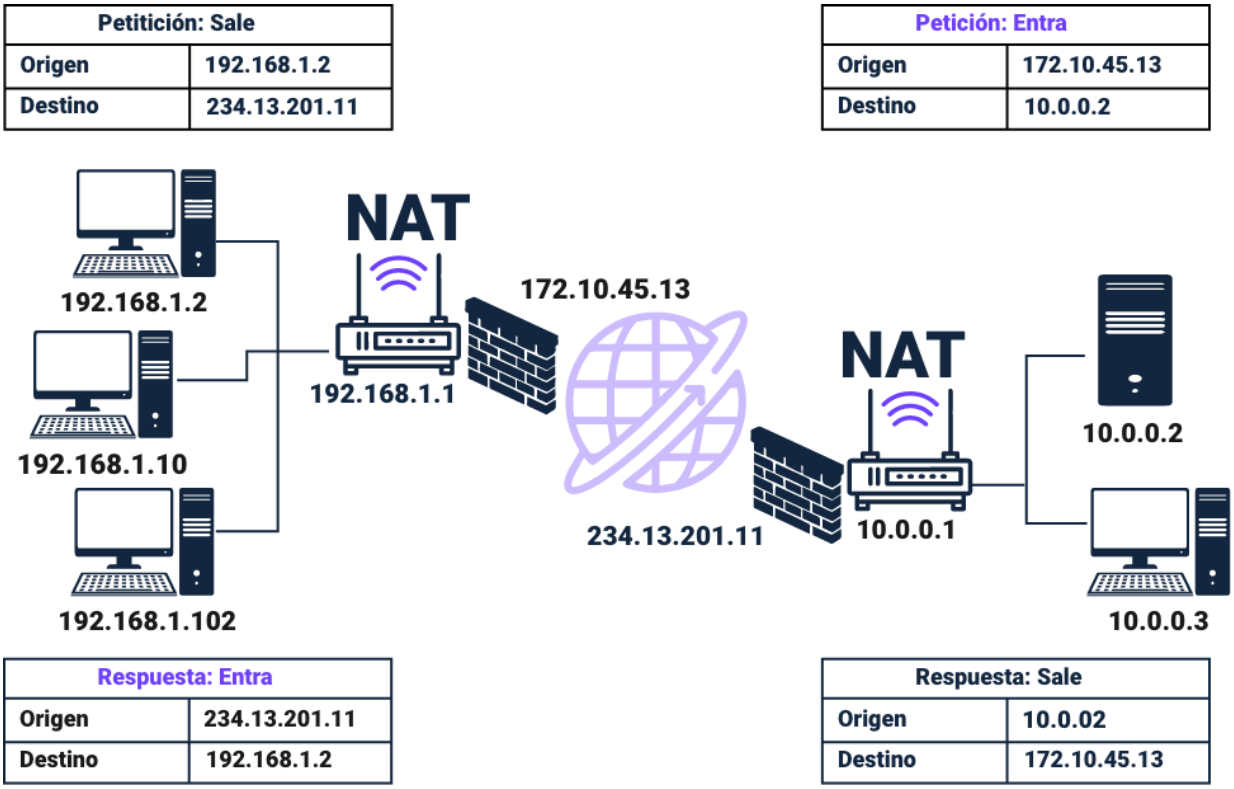
El servidor DHCP es el encargado de enviar la información al DNS al asignar una nueva dirección IP, la cual se asocia con su nombre de dominio correspondiente. El DHCP no es muy seguro, pues es de fácil manipulación por parte de atacantes a la red que desean apropiarse de la información sensible de sus usuarios.

Servidor NAT

Este servidor surge a raíz del crecimiento exponencial de terminales que día a día acceden a Internet; se usa para traducción de direcciones de red con su sigla en inglés NAT o "Network Address Translation" y, con ello, permitir que los dispositivos de una red utilicen un rango de direcciones especiales (IP privadas) y para conectarse a Internet utilice una dirección IP única (IP pública). Se trata de una mejora o actualización en la que las redes grandes solo usarían una dirección IP y no gran cantidad de ellas.

En la siguiente figura se muestra el funcionamiento de este servidor:

Figura 1. Funcionamiento del servidor NAT



Nota. Página web Profesional review (s.f.).

Modos de funcionamiento para NAT

El servidor DHCP es el encargado de enviar la información al DNS al asignar una nueva dirección IP, la cual se asocia con su nombre de dominio correspondiente. El DHCP no es muy seguro, pues es de fácil manipulación por parte de atacantes a la red que desean apropiarse de la información sensible de sus usuarios.

- **Estática**. La dirección IP privada siempre se traduce en la misma dirección IP pública. Cualquier "host" dentro de la red será así visible desde Internet.

- **Dinámica**. A cada dirección IP privada le corresponde, al menos, una dirección IP pública de las que posee el "router"; así, cuando un "host" requiera una conexión a Internet el "router" asignará la dirección IP pública que no esté siendo usada. De este modo hay más seguridad.
- **Sobrecarga**. Aquí se mapean varias direcciones IP privadas por medio de una dirección IP pública, evitando así contratar más de una dirección IP pública y se ahorran direcciones IPv4. Se le denomina también PAT ("Port Address Translation") y es la más usada en los hogares.
- **Solapamiento**. Para evitar el conflicto de direcciones, si hay una dirección IP privada de una red es igual a una dirección IP pública que está en uso, el "router" reemplaza dicha dirección IP por otra.

Tabla 2. Ventajas y desventajas del servidor NAT

Ventajas	Desventajas
Ahorro de direcciones IPv4 al conectarse múltiples máquinas de una red a Internet, con una única dirección IP pública.	Mayor potencia de computación en el "router" para recalcular el "Checksum" TCP y UDP de cada paquete modificado.
Seguridad, pues las máquinas conectadas a la red mediante NAT no son visibles desde el exterior.	Incompatibilidad de NAT con varias aplicaciones y protocolos que no permiten al "router" modificar los paquetes.
Mientras se llevan a cabo tareas de mantenimiento de la red solo es necesario modificar la tabla de reenvío de un "router" para desviar todo el tráfico.	

Instalación

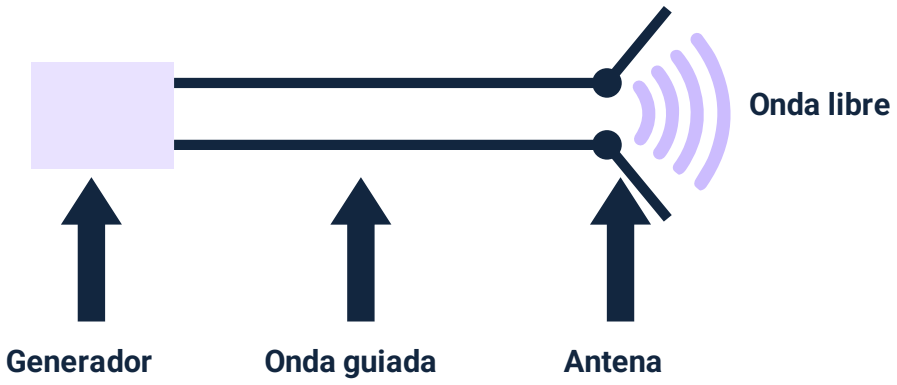
Para realizar la correcta instalación de la red inalámbrica es vital realizar un aprestamiento o verificación del entorno, los componentes y herramientas necesarios, aplicando una lista de chequeo que verifique la disponibilidad, estado y características de estos, con la debida antelación (4 a 8 días) para poder tomar los correctivos a los que haya lugar. Igualmente, al menos un día antes o el mismo día muy temprano, se debe realizar el alistamiento de los elementos, materiales, herramientas necesarias para la instalación de todos y cada uno de los dispositivos como antenas, repetidores adaptadores, "routers" y puntos de acceso.

Una vez cumplidos los anteriores aspectos se procede a realizar la instalación de los componentes de la red inalámbrica por parte del personal idóneo, que cumpla con todos los requisitos y normas vigentes para dicha labor.

Antenas

Una antena es un sistema conductor, metálico, con capacidad de radiar y recibir ondas electromagnéticas del espacio. Estos dispositivos adaptan ondas guiadas desde conductores o guías, al espacio libre.

Figura 2. Representación de una antena



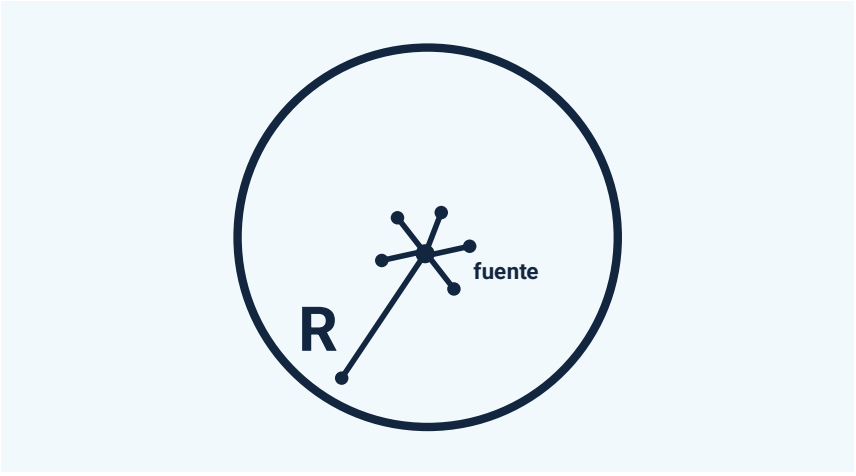
La estructura y funcionamiento de una antena, como lo sugiere la imagen inmediatamente anterior, implica: la antena misma, la cual sirve de flujo para las ondas libres, un generador y la conducción de onda guiada.

Existen varios tipos de antenas, entre ellos:

a. **Direccionales**. Aquellas que orientan la señal en una determinada dirección, con un haz estrecho de largo alcance.
b. **Omnidireccionales**. Este tipo de antenas irradian la señal con un haz amplio, de corto alcance y dirigido hacia todas direcciones.
c. **Sectoriales**. Irradian la señal con un haz más amplio que las direccionales; se consideran la unión de una antena "omni" y de una direccional.

La ganancia de una antena es la relación entre la densidad de potencia radiada en una dirección y la densidad de potencia que radia una antena isotrópica, en la misma distancia y potencia entregadas a la antena. La antena isotrópica es una antena puntual que no se puede realizar en la práctica y que radia de igual manera en todas las direcciones; la ganancia se mide en **dBi** (decibeles isotrópicos).

Figura 3. Representación de antena isotrópica



La pérdida de la señal puede ser ocasionada por varios motivos, entre los cuales se puede enumerar los siguientes:

- Cable o guía de onda roto o desconectado.
- El equipo de transmisión o amplificador de la señal no envía la potencia por daño o se encuentra apagado.
- Antena descompuesta, rota o deteriorada.

Los siguientes son los pasos de instalación de los adaptadores y el "router"

- **Paso 1**. Conectar el adaptador de red USB a un puerto USB que esté disponible, sin necesidad de apagar el computador.
- **Paso 2**. Encender el computador e instalar los controladores ("drivers") de la tarjeta de red. Si el sistema operativo es Windows, este reconocerá el "hardware" recién agregado y abrirá una ventana de diálogo «nuevo "hardware" encontrado», el cual se debe completar. Luego, insertar el CD de configuración y seguir el asistente para terminar la instalación. El "software/drivers" de la tarjeta de red USB se puede descargar desde el sitio web del fabricante.
- **Paso 3**. Una vez que la tarjeta de red se ha instalado con éxito se deben establecer los valores de configuración de la tarjeta como dirección IP, máscara de subred, puerta de enlace o "Gateway", y servidores DNS (se recomienda ponerse en contacto con el administrador de red para comprobar los valores de configuración).
- **Paso 4**. Reiniciar el equipo si es necesario o en su defecto verificar si el adaptador de red está listo para su uso.

Instalación del “router”

Este dispositivo posee puertos RJ45 para red LAN, en los cuales se deben conectar los cables “patch cord” hacia los dispositivos cableados y red WAN, donde se debe colocar el cable “patch cord” de alimentación a Internet del ISP; igualmente, se debe colocar la antena para acceso inalámbrico de los dispositivos a la red WLAN. Por tratarse de un dispositivo activo se debe conectar el respectivo cable o adaptador de alimentación para su funcionamiento y proceder a configurar las características básicas y necesarias como elemento de la red.

En el siguiente video podrá observar el procedimiento para la configuración de dispositivos.

Video 4. Configuración IP del equipo

Enlace de reproducción del video

Síntesis del video: Configuración IP del equipo
En este video la experta SENA hace un recorrido específico por las acciones y requerimientos establecidos para el proceso de configuración de la dirección IP de un equipo o dispositivo.

2. Configuración de la red

Una interfaz es una herramienta que permite dar acceso directo a la configuración, sistema operativo y demás funcionalidades de cada dispositivo. Generalmente, se trata de una interfaz gráfica que, por medio de un monitor, pantalla o terminal, da acceso a una serie de menús e íconos para que sean utilizados por el usuario en la interacción con los dispositivos de la red que necesitan ser configurados o actualizados para su correcto funcionamiento dentro del sistema.

Algunas de las características que posee una interfaz son:

- Facilidad de uso, aprendizaje y comprensión.
- Representación fija y permanente del área de trabajo o fondo.
- Fácil identificación del objeto o dispositivo de interés.
- Diseño ergonómico con menús, barras de acción e íconos de fácil acceso.
- Operaciones rápidas, incrementales y reversibles, con efectos inmediatos.
- Variedad de herramientas de ayuda y consulta.

Los tipos de interfaz de usuario más conocidos son:

a. **Interfaz GUI**. Usadas para aplicaciones web, móviles, escritorio y juegos que permiten interacción al usuario.
b. **Interfaz de usuario de pantalla táctil**. Diseñadas para pantallas táctiles, sin botones físicos, se encuentran en “smartphone”, “tablets”, cajeros automáticos, etc.
c. **Interfaz natural de usuario (NUI)**. En estos casos se interactúa con un sistema, aplicación y demás, sin utilizar dispositivos de entrada como ratón, teclado y lápiz óptico; a cambio de estos se utilizan las manos o las yemas de los dedos.

El video que se propone enseguida, detalla el proceso de configuración de "router" TPLINK con frecuencia TL-MR3220:

Video 5. Configuración de "router" TP LINK TL MR3220

Enlace de reproducción del video

Síntesis del video: Configuración de "router" TP LINK TL MR3220
En este video la experta SENA muestra, detalladamente, el proceso de configuración, por medio de la interfaz gráfica de un "router" TP LINK con referencia TL MR3220.

Protección de la red inalámbrica

Una red inalámbrica es más vulnerable, pues la señal se difunde en el espacio libre, permitiendo que los usuarios con equipos cercanos puedan acceder a la información almacenada en los equipos de la red y usar la conexión a Internet.

Se debe cambiar el nombre de usuario, contraseña y SSID predeterminados para proteger el enrutador. Es importante configurar una contraseña para la red inalámbrica, dependiendo del tipo de protección deseada por parte del usuario; para ello existen, entre otros, tres tipos de seguridad o protección en el menú "wireless security" que son:

- WPA/WPA2 "personal"
- WPA/WPA2 "enterprise"
- WEP

Autenticación

La autenticación de sistema abierto consta de dos comunicaciones:

a. En primer lugar, se envía una solicitud de autenticación desde el dispositivo móvil que contiene el ID de la estación (normalmente la dirección MAC).

b. A continuación, una respuesta de autenticación del PA/enrutador con un mensaje de éxito o de fallo.

Con la autenticación de clave compartida o frase de contraseña se configura manualmente tanto en el dispositivo móvil como en el PA/enrutador.

2.1. Seguridad, "firewall", filtros, aplicaciones

Se debe tener en cuenta que son muchos los ataques que pueden existir para una red inalámbrica. Así mismo, que una gran cantidad de puertos se deben bloquear para minimizar estos riesgos, con la aplicación de normativas, protocolos, estándares y demás medidas que sean necesarias.

Un “firewall” funciona como una barrera entre Internet y otras redes públicas y los dispositivos. Todo el tipo de tráfico que no esté en la lista permitida por el “firewall” no entra ni sale de los dispositivos de la red; para ello contiene un conjunto de reglas predefinidas que permiten:

- Autorizar una conexión (“allow”).
- Bloquear una conexión (“deny”).
- Redireccionar un pedido de conexión sin avisar al emisor (“drop”).

También existe el “firewall” de “software” que se puede instalar y utilizar libremente o con licencia, en los dispositivos de la red o con acceso a redes que se encargan de monitorear y bloquear, siempre que sea necesario, el tráfico sospechoso o de Internet.

- Los gratuitos se incluyen con el sistema operativo y normalmente son para uso personal.
- Facilita la integración con otros productos de seguridad.
- No es necesario “hardware” para su instalación.
- Un “firewall” comercial incluye protecciones extra, más control sobre su configuración y funcionamiento.

Por el contrario, un “firewall” por “hardware” viene normalmente instalado en los “router” que se utilizan para acceder a Internet. Por tanto, todos los dispositivos que se conecten a un “router” estarán protegidos por un “firewall” que está incluido en el “router”.

2.2. Características adicionales de las redes

Las redes inalámbricas tienen diversas características dependiendo del rango de frecuencias, el medio y la velocidad de transmisión, entre las cuales están:

a. **Ondas de radio**. Son ondas electromagnéticas (combinación de campos eléctricos y magnéticos oscilantes, que se propagan a través del espacio, transportando energía de un lugar a otro). Son omnidireccionales, así que no son necesarias antenas parabólicas. La transmisión no es sensible a las atenuaciones producidas por la lluvia, ya que se opera a frecuencias que no son demasiado elevadas.
b. **Microondas por satélite**. Se hacen enlaces de dos o más estaciones terrestres, a las cuales se denomina estaciones base. El satélite recibe la señal (denominada señal ascendente) en una banda de frecuencia, la amplifica y la retransmite en otra banda (señal descendente). Cada satélite opera en unas bandas concretas. Las fronteras frecuenciales de las microondas, tanto terrestres como por satélite, con los infrarrojos y las ondas de radio de alta frecuencia, se mezclan suficientemente, de modo que puede haber interferencias con las comunicaciones en determinadas frecuencias.
c. **Infrarojos**. Hay enlaces de transmisores y receptores que modulan la luz infrarroja no coherente. Deben estar alineados directamente o con una reflexión en una superficie. Las señales infrarrojas trabajan en la banda de 300 GHz hasta 384 THz.
d. **Microondas terrestres**. Estas se utilizan en antenas parabólicas con un diámetro aproximado de unos tres metros. Tienen una cobertura de kilómetros, pero con la necesidad de tener perfectamente alineados al emisor

con el receptor; por ello, se les denomina enlaces punto a punto en distancias cortas.

En concreto, dentro de las características adicionales, se encuentran:

a. **Control parental**. Se realiza para impedir o limitar el acceso al manejo de dispositivos destinados a la reproducción o recepción de imágenes e información, de determinados contenidos para los menores de edad; determinando con exactitud los dispositivos que se deben bloquear o proteger.
b. **Acceso restringido**. Dado que el acceso a Internet de estudiantes, niños, adolescentes, adultos mayores o población sensible es, hoy en día, muy fácil. Cada vez, crece el acceso a edades más tempranas mediante dispositivos multimedia como “smartphones” o “tablets”.
c. **Educación digital**. Es imprescindible una buena educación digital. Con ella, se mitigan las posibilidades de riesgos del consumo de información, peligros propios de la conectividad, distorsión de la intencionalidad de las redes y servicios tecnológicos, entre otras.
d. **Filtros de control**. Otro apoyo es el uso de filtros y herramientas de control parental que protejan de sitios y contenidos inseguros e inapropiados para ciertas edades o cierto tipo de personas. Por lo tanto, servirá para limitar el acceso a determinados contenidos en Internet, limitar el tiempo que se usa para navegar o la naturaleza de la información que se intercambia en Internet.

Está claro, entonces, que se puede modificar los DNS de un equipo para que se filtre la información a través de ellos y llegue de manera segura, pero como alternativa

a ello, hay otros métodos para instaurar un sistema de control parental cuando se tienen computadores que usan Windows como sistema operativo.

Si se utiliza Windows 10, hay que saber que tiene su propio sistema de control parental, al cual se puede acceder desde la configuración y también desde una cuenta Microsoft, a través de cualquier navegador. La idea es asignar a cada menor de la casa una cuenta de Windows y arrancar el computador desde esa cuenta. Las cuentas de adultos o sin restricciones se protegen mediante una contraseña alfanumérica y las cuentas de los menores estarán protegidas a través de un PIN de 4 dígitos.

El siguiente video, detalla generalidades y aspectos clave sobre la configuración del control parental. Chequéelo con atención:

Video 6. Configuración de control parental

Enlace de reproducción del video

Síntesis del video: Configuración de control parental
En este video la experta SENA muestra el paso a paso para lograr la configuración de control parental.

Como es de esperar, este tipo de sistema de control parental de Windows 10 solo funciona en navegadores Microsoft Edge y Explorer; para evitar el uso de otro navegador se puede bloquear como se mencionó antes o, también, instalar el control parental del que también disponen Google Chrome o Mozilla Firefox.

Estas son algunas generalidades que, sobre el control parental de Windows 10, usted debe tener presentes:

a. **Configuración de acceso**. La opción que ofrece el control parental de Windows 10 es la de configuración de acceso a contenidos multimedia, aplicaciones y juegos. Todos los contenidos multimedia como canales de televisión, películas, etc., tienen una clasificación de edad para su visionado, así como los juegos tienen su propio sistema de clasificación por edad en cada país.
b. **Límites de edad**. Se introduce el límite de edad y el explorador solo mostrará contenidos hasta esa edad. Para edades mayores se mostrará el mensaje de bloqueo por control parental y el niño o menor de edad, no podrá acceder a ellos. Otro dato importante es que se puede usar también este tipo de control en consolas XBOX, ya que hacen parte de este gigante tecnológico: se puede bloquear el uso de la consola a ciertas horas, establecer una cuota de tiempo de uso o, incluso, una franja horaria de funcionamiento.

c. **Control de servicios de pago**. De la mano de este filtro se puede también controlar el dinero que se gasta desde una cuenta en la tienda Microsoft. Este tipo de cuentas son débito: se ingresa una cantidad en la cuenta, de la que se dispondrá para gastarla, tanto en la consola como en el computador y en los contenidos que se hayan permitido. Este sistema de control parental también da la opción de restringir el tipo de transacciones por efectuar.

d. **Gratuidad del control parental**. Sin duda, si se dispone de un equipo con Windows 10, el control parental que ha desarrollado Microsoft es de lo mejor y más completo que se puede encontrar en el mercado, y de manera gratuita. Este viene de serie con la licencia de Windows 10. Si no utiliza Windows 10 o quiere alternativas al control parental de Microsoft, la opción más clara es usar programas o aplicaciones específicamente diseñados para este fin.

e. **Otras opciones**. Existe una herramienta para instalar en el computador que se llama **Qustodio**. Está disponible tanto para Windows, MacOS, Android y iOS, dispone de dos versiones: una gratuita y otra de pago; viene diseñada tanto para ámbitos familiares como escolares. Permite controlar tiempos de conexión, filtros de contenido prohibido e inapropiado. Incluso, cuenta con restricción de palabras no apropiadas.

f. **Personalización del control**. Se pueden personalizar filtros de contenido y ver la actividad del computador que se quiera. Para ampliar la versión de pago, se ofrecen informes mucho más detallados, bloqueo total de pornografía, bloqueo de aplicaciones, juegos y contenidos, monitorización de YouTube, seguimiento en redes sociales, control de llamadas y SMS, geolocalización por GPS y un botón de pánico instalable en el "smartphone" del usuario que podrá usar en cualquier momento para pedir ayuda.

2.3. Red wifi para invitados

Con seguridad, son varias las ocasiones en que las personas como usted se han encontrado en la situación de que amigos o familiares piden la clave del wifi. Una visita, por ejemplo, quiere conectarse a la red.

Ahora bien, en ocasiones puede ser un problema, puede ocurrir que simplemente no se recuerde la clave o que se quiera, sencillamente, mantener la seguridad de la red o, incluso, poner cierto límite y que no se consuma todo el ancho de banda. Esto último especialmente es interesante en conexiones más lentas, como puede ser ADSL, en la que los recursos son más limitados.

Lo primero que hay que tener en cuenta es que:

- No en todos los "routers" funciona de la misma manera.
- No obstante, sí se tiene una función similar.
- En la mayoría de los dispositivos modernos está disponible esta opción de conexión.
- Ya se sabe que evitar la pérdida de señal wifi es vital.

El video que se muestra enseguida, expone las generalidades de configuración de wifi para invitados:

Video 7. Configuración de una red de invitados

Enlace de reproducción del video

Síntesis del video: Configuración de una red de invitados
En este video, la instructora SENA ofrece el paso a paso para la configuración de una red de invitados, usando un "router" TP LINK modelo AC1750.

Si se realiza una prueba de velocidad con una conexión ADSL en la que se tiene a toda la familia conectada y viendo videos de YouTube, por ejemplo:

- Los datos no son los que se desearían.
- En algunos modelos incluso se puede limitar el ancho de banda.
- Se puede asignar que únicamente el 20% del total de la red (o lo que se quiera) esté disponible en la red wifi para invitados.

De esta manera se puede crear una red wifi para invitados. Una forma práctica para que las visitas se puedan conectar a la red sin revelar la clave principal, ni poner en peligro el resto de los equipos conectados a la red.

2.4. Prioridad de medios

Cambie la prioridad de los adaptadores de red en Windows 10 desde el centro de redes de este sistema operativo. Lo primero que se debe hacer es abrir el centro de redes y recursos compartidos; para ello, en el siguiente video se explicará la configuración de la prioridad de medios:

Video 8. Configuración de la prioridad de medios

Enlace de reproducción del video

Síntesis del video: Configuración de la prioridad de medios
En este video, la experta SENA muestra las acciones y requerimientos para ejecutar la configuración de prioridad de medios.

2.5. Reenvío de puertos

Es posible que una aplicación determinada o, por ejemplo, un juego en un momento concreto pida algo denominado reenvío de puertos; sin ese reenvío de puertos no podría haber conexión entre la aplicación o juego y el tráfico entrante o datos ingresados en Internet. No se puede hacer uso de determinadas funciones con las que cuenta un "software" determinado.

Este problema se puede solucionar si se configura el reenvío de puertos en Windows 10; es un proceso sencillo y simplemente hay que llevar a cabo una serie de pasos que se explican en el siguiente video:

Video 9. Reenvío de puertos

Enlace de reproducción del video

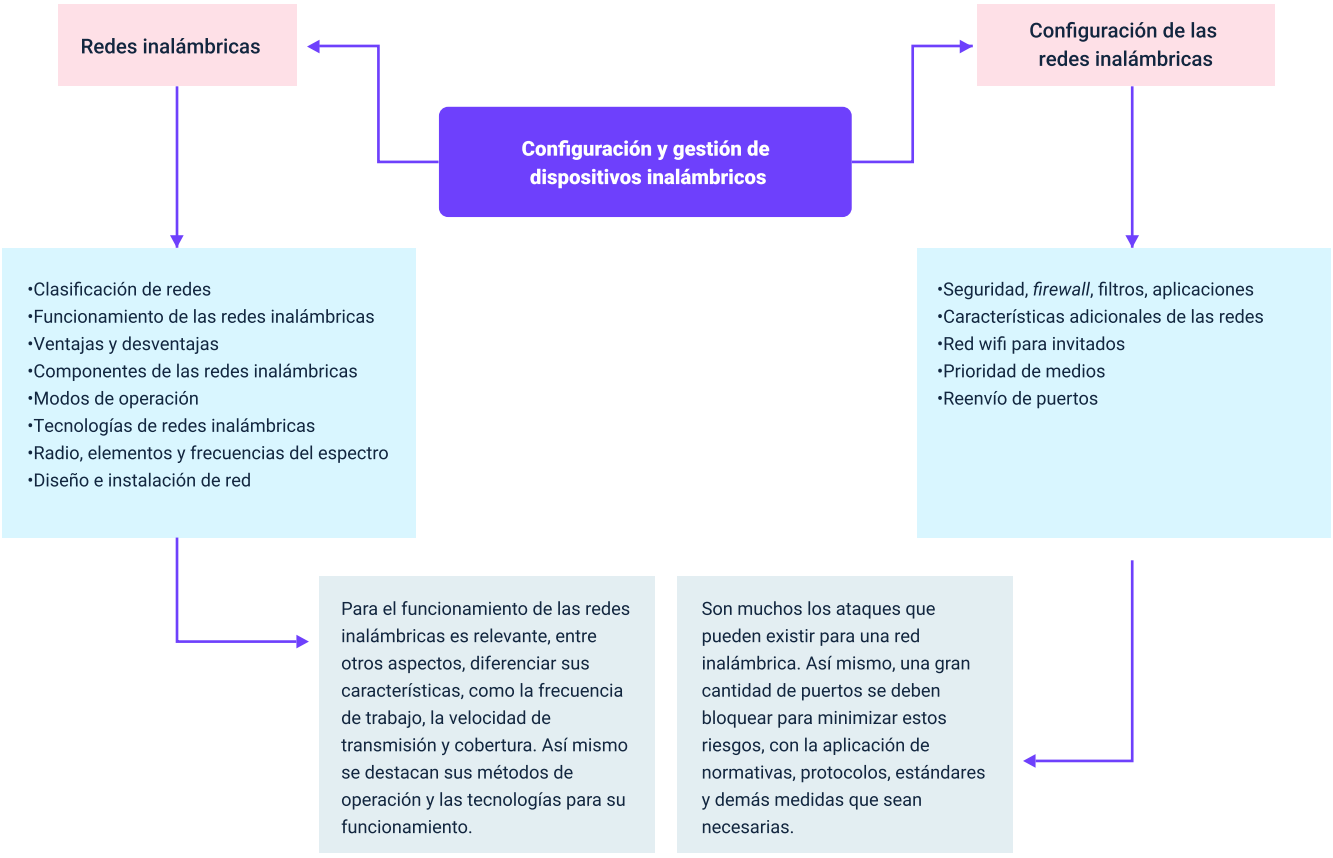
Síntesis del video: Reenvío de puertos
En este video, la instructora SENA y experta en el tema, da cuenta de una serie de pasos para completar la configuración para el reenvío de puertos.

Cuando se haya creado la regla se unirá a todas las que ya estaban presentes. Se puede modificar, hacer que se aplique solo a unos determinados programas o servicios, etc. En definitiva, siguiendo estos pasos que se han mencionado se pueden reenviar puertos en Windows 10, en caso de que una aplicación o servicio pida hacerlo.

Finalmente, todo lo indicado anteriormente es un proceso sencillo, rápido y que se puede lograr a través de la propia configuración del sistema operativo, sin tener que instalar nada adicional. Por otra parte, es necesario recordar la importancia de contar con herramientas de seguridad; un buen antivirus y "firewall" pueden evitar la entrada de amenazas. En este sentido, se tiene la posibilidad de hacer uso de **Windows Defender**, que está disponible en el sistema operativo de Microsoft de forma gratuita.

Síntesis

Aquí finaliza el estudio de los temas de este componente formativo. En este punto, analice el esquema que se muestra enseguida y realice su propia síntesis de lo estudiado. ¡**Adelante**!



El esquema general de contenidos de este componente formativo muestra el enfoque de los temas hacia el abordaje de las generalidades y aspectos clave del proceso de configuración y gestión de los dispositivos inalámbricos requeridos, de acuerdo con la arquitectura planteada en la fase de planeación:

- Clasificación de redes
- Funcionamiento de las redes inalámbricas

- Ventajas y desventajas
- Componentes de las redes inalámbricas
- Modos de operación
- Tecnologías de redes inalámbricas
- Radio, elementos y frecuencias del espectro
- Diseño e instalación de red
- Seguridad, “firewall”, filtros, aplicaciones
- Características adicionales de las redes
- Red wifi para invitados
- Prioridad de medios
- Reenvío de puertos

Material complementario

Tema	Referencia	Tipo de material	Enlace del recurso
1. Introducción a las redes inalámbricas	XIRIO online. (s.f.) Planificación de redes de acceso. XIRIO.	Página web	https://www.xirio-online.com/web/help/es/index.htm
2. Configuración de la red	Cisco Networking Academy. (s.f.). Networking CCNA: Switching, Routing, and Wireless Essentials. Cisco.	Página web	https://www.netacad.com/courses/networking/ccna-switching-routing-wireless-essentials

Glosario

Adaptador de red: dispositivo de hardware que se inserta en la estación de trabajo de una red y le permite comunicarse con otros elementos unidos a esta red.

Capa de aplicación: capa 7 del modelo OSI que proporciona autenticación, privacidad y restricción de información a los usuarios.

Capa de enlace de datos: capa 2 del modelo OSI que soporta la capa física (capa 1), proporcionando direccionamiento, control de errores y sincronización a un dispositivo físico.

Capa de presentación: capa 6 del modelo OSI que administra la conversación de la información entrante y saliente de un formato de datos a otro.

Capa de red: capa 3 del modelo OSI que define la manera como se enruta la información a una dirección destino.

Capa de sesión: capa 5 del modelo OSI que inicia y termina conversaciones, intercambios y diálogos entre aplicaciones a través de la red.

Capa de transporte: capa 4 del modelo OSI que proporciona control de un extremo a otro para transferencia de la información a través de la red.

Capa física: capa 1 del modelo OSI que define la manera como la corriente eléctrica de bits se transporta a través del "hardware" y los dispositivos mecánicos de la red.

Datagrama: agrupamiento lógico de información enviada como unidad de capa de red a través de un medio de transmisión sin establecer previamente un circuito virtual. Los datagramas IP son las unidades principales de información de Internet. Los

términos trama, mensaje, paquete y segmento también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.

Dirección IP (protocolo de Internet): es la dirección de red o lógica de un nodo. Está compuesta por cuatro números de ocho "bits" (cada uno de ellos llamado octeto) que se combinan para identificar no solo la estación de trabajo o nodo, sino también su red. La dirección IP identifica una estación de trabajo con la LAN, WAN e Internet.

DNS: sistema de nombre de dominios. Un sistema de Internet que resuelve los nombres de dominios en direcciones IP.

Enrutador: dispositivo de red que dirige o enruta paquetes a través de las redes. Un enrutador funciona con una dirección de mensajes IP, a fin de determinar la mejor ruta hacia su destino.

Enrutamiento: proceso utilizado para determinar la mejor ruta y hacer avanzar la información a lo largo de esa ruta, a partir de una red fuente o segmento de red hacia una dirección de red de destino.

"Host": sistema informático en una red. Similar al término nodo, salvo que "host" normalmente implica un computador, mientras que nodo generalmente se aplica a cualquier sistema de red, incluyendo servidores de acceso y el "router".

Modelo OSI: modelo de referencia de interconexión de sistemas abiertos, un estándar que define las diversas funciones denominadas capas, que un paquete de red transmite al trasladarse desde una fuente hasta su destino. El modelo OSI de siete capas se aplica tanto a las redes locales como a las extensas, entre ellas Internet.

Referencias bibliográficas

Andreu, J. (2011). Redes inalámbricas (servicios en red). Editex.

Cisco Networking Academy. (s.f.). Networking CCNA: Switching, Routing, and Wireless Essentials. Cisco. https://www.netacad.com/courses/networking/ccna-switching-routing-wireless-essentials

Jiménez, J. (2020). Cómo configurar el reenvío de puertos en Windows 10. https://www.redeszone.net/tutoriales/configuracion-puertos/configurar-reenvio-puertos-windows/

Jiménez, J. (2018). Cómo crear una red wifi para invitados fácilmente en nuestra casa. https://www.redeszone.net/2018/12/24/crear-red-wifi-invitados/

Linksys. (s.f.). Configuración de su extensor de red Linksys en modo Punto de Acceso. https://www.linksys.com/es/support-article/?articleNum=187985

Linksys. (s.f.). ¿Qué es un punto de acceso y en qué se diferencia de un extensor de red? https://www.linksys.com/es/r/qu%C3%A9-es-un-extensor-de-red/qu%C3%A9-es-un-punto-de-acceso/

López, A. (2021). Control parental: todo lo que tienes que saber y cómo llevarlo a cabo. https://www.redeszone.net/tutoriales/seguridad/control-parental-que-es-herramientas/

Stallings, W., Tanenbaum, A., Fall, K. R., & Stevens, W. R. (2000). Comunicaciones y redes de computadores. 6ª edición. Prentice-Hall.

XIRIO online. (s.f.). Planificación de redes de acceso. XIRIO. https://www.xirio-online.com/web/help/es/index.htm

Créditos

Nombre	Cargo	Regional y Centro de Formación
Claudia Patricia Aristizábal	Responsable del Ecosistema	Dirección General
Rafael Neftalí Lizcano Reyes	Responsable de Línea de Producción	Centro Industrial del Diseño y la Manufactura - Regional Santander
Jorge Eliécer Loaiza Muñoz	Experto temático	Centro de Servicios y Gestión Empresarial - Regional Antioquia
Carlos Mauricio Tovar Artunduaga	Experto temático	Centro de Servicios y Gestión Empresarial - Regional Antioquia
Claudia López Arboleda	Experta temática	Centro de Teleinformática y Producción Industrial - Regional Cauca
Fabián Leonardo Correa Díaz	Diseñador instruccional	Centro Industrial del Diseño y la Manufactura - Regional Santander
Blanca Flor Tinoco Torres	Diseñador de Contenidos Digitales	Centro Industrial del Diseño y la Manufactura - Regional Santander
Francisco José Lizcano Reyes	Desarrollador “Fullstack”	Centro Industrial del Diseño y la Manufactura - Regional Santander
Daniela Muñoz Bedoya	Animador y Producción Audiovisual	Centro Industrial del Diseño y la Manufactura - Regional Santander
Emilsen Alfonso Bautista	Actividad Didáctica	Centro Industrial del Diseño y la Manufactura - Regional Santander
Zuleidy María Ruiz Torres	Validador de Recursos Educativos Digitales	Centro Industrial del Diseño y la Manufactura - Regional Santander

Nombre	Cargo	Regional y Centro de Formación
Luis Gabriel Urueta Álvarez	Validador de Recursos Educativos Digitales	Centro Industrial del Diseño y la Manufactura - Regional Santander
Daniel Ricardo Mutis Gómez	Evaluador para Contenidos Inclusivos y Accesibles	Centro Industrial del Diseño y la Manufactura - Regional Santander