Redes inalámbricas.

Caso práctico

Julián, el director del centro IES Montes Claros, está hablando con Elena, la jefa del departamento de Latín. Su despacho se encuentra bastante alejado del resto de los departamentos. Cuando se hizo el cableado para la red del centro, no lo hicieron en esa habitación, puesto que en principio su función no era para departamento. Con lo cual, ahora Elena no tiene acceso a la red ni a Internet.

Flickr / jmerelo (CC BY-NC)

Hablan de las posibles soluciones que pueden encontrar al hecho de no tener acceso a la red desde ese punto del instituto.

- Julián, debes entender que no es nada operativo que, para realizar cualquier tarea que requiera conexión a Internet, tengamos que buscar un ordenador libre en el centro y no podamos trabajar desde el Departamento.

- Sí, Elena, tienes toda la razón. Cuando se cableó toda la red del centro, en principio, lo que ahora es vuestro departamento era un pequeño aula de apoyo. Pero al ampliar otros departamentos, se habilitó ese lugar.

- Ya, eso es la consecuencia de improvisar y no planificar la organización de los recursos –remarcó Elena.

- Tienes razón, pero el problema que tenemos ahora, es que es muy costoso realizar el cableado hasta ese lugar. Tendríamos que buscar alternativas más cómodas y baratas para este caso –señaló Julián.

- Yo no tengo mucha idea de redes, pero, ¿tú crees que se podría realizar una conexión sin la necesidad de tener que cablear hasta nuestro departamento? Yo, en mi casa, tengo conexión a Internet con un módem inalámbrico, y me conecto con el portátil desde cualquier habitación. ¿Algo parecido no sería posible?

- Seguro que sí, Elena. Yo sé de otros centros que han buscado una solución parecida instalando redes inalámbricas.

- Déjame que consulte el tema con Alberto, el encargado de mantenimiento informático del centro, y te comento las soluciones posibles –continuó diciendo Julián.

- Muchas gracias, Julián. Cuando tengas novedades, pues me cuentas –se despidió Elena.

Debes comprender, que la mejor manera de interconectar diversos equipos entre sí, en un área reducida, no siempre ha de pasar por tener una red cableada. Existen ocasiones, bien sea por la dificultad de pasar el cable, o atendiendo a una futura demanda de ampliaciones, que la mejor solución es tener una red inalámbrica para un área concreta. Puedes ofrecer conexión a distintos espacios y a través de dispositivos de diferentes características, desde un ordenador portátil o un teléfono móvil. Una de sus principales ventajas es la movilidad dentro del espacio de trabajo de la que disfrutarán todos los usuarios y usuarias de la red.

Pero, como te puedes imaginar, este tipo de tecnología también puede acarrear una serie de inconvenientes. El principal será la **seguridad** ofrecida que puede hacer que la red sea más vulnerable a ataques indeseados desde el exterior. Es por eso que, en esta unidad, haremos hincapié en los aspectos relativos a la seguridad en redes inalámbricas para proteger la red.

Debes conocer

Antes de comenzar con el grueso del tema, puedes ver este vídeo en el que se presentan algunas de las tecnologías que vamos a estudiar en esta unidad.

Algunas tecnologías inalámbricas

https://www.youtube.com/embed/tkmJM2yEU1o

Pero si hablamos de redes inalámbricas, sin duda alguna la tecnología más puntera y que más se está desarrollando en estos momentos es la conocida como 5G, es decir, la nueva red de comunicaciones móviles que permitirá una gran mejora en capacidad y velocidad de transmisión, hasta el punto de interconectar millones de dispositivos de todo tipo y funcionalidad.
Es la tecnología que permitirá implantar el paradigma conocido como **IoT (Internet of Things).** Este artículo permite conocer un poco más sobre 5G:
https://www.thalesgroup.com/es/countries/americas/latin-america/dis/movil/inspiracion/5g

1.- Conceptos sobre redes inalámbricas.

Caso práctico

En estos momentos, Julián, el director del centro IES Montes Claros, se encuentra hablando con Alberto, el encargado del mantenimiento del centro.

Stockbyte. (Uso educativo nc)

- Bueno, Alberto, Elena me ha planteado un problema que tienen en su departamento, y es que no tienen conexión a Internet, ni a la red local del centro. ¿Qué soluciones ves tú?

- El problema no es sencillo, Julián. Las alternativas que tenemos, creo que son dos. Una de ellas, sería hacer un cableado desde el armario principal de telecomunicaciones hasta el departamento.

- ¿No está muy lejos? –preguntó Julián.

- Sí, el problema es que la distancia es grande y tendremos que salvar numerosos obstáculos. Otra solución que se me ocurre –valoró Alberto- es instalar un punto de acceso inalámbrico desde un lugar cercano desde donde haya llegado el cableado de red, y se ofrece la posibilidad de acceso a la red, no solo a los equipos del departamento, sino a todos aquellos que se encuentren dentro de su radio de acción.

- Ya veo que controlas del tema, Alberto, pero hace falta saber los costes económicos de cada una de las soluciones y ver quién nos podría realizar ese trabajo –planteó Julián.

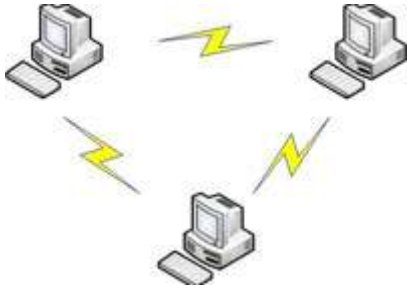
- Yo si quieres, puedo hablar con la empresa que nos ayuda con las tareas de mantenimiento, y le pido consejo y ayuda. Ellos también se dedican a dar este tipo de servicios a las empresas. ¿Te parece que me ponga en contacto con ellos, a ver que dicen? –sugirió animosamente Alberto.

- Me sería de gran ayuda si te encargas y resuelvas tú el problema. Muchas gracias, Alberto, eres un gran profesional –agradeció Julián.

- De nada Julián, ya te comentaré en qué queda todo –se despidió Alberto.

Te conviene recordar que una red inalámbrica, en inglés Wireless Network, es un conjunto de equipos que se conectan entre sí, sin necesidad de utilizar una conexión física, utilizando para su conexión ondas electromagnéticas.

Las **principales ventajas** que encontrarás al trabajar con este tipo de redes son las siguientes:



Nuria Celis Nieto. (Uso educativo nc)

- **Movilidad:** No estás sujeto a estar conectado a un cable.
- **Flexibilidad**: Permite conectar dispositivos inalámbricos sin haberlo previsto anteriormente.
- **Acceso a zonas de difícil cableado.**
- **Coste reducido**, puesto que las tarjetas de red son solo ligeramente más caras que las tarjetas de red convencionales.
- **Velocidad moderada**: unos 50 Mbps (megabits por segundo).
- **Distancia de conexión**: desde 50 a 500 metros, si se utilizan antenas especiales.

Pero, como supondrás, este tipo de tecnologías también tiene una serie de **desventajas**, que son las siguientes:

- **Seguridad**: es más fácil interceptar la señal para usuarios no autorizados.
- **Incompatibilidades de redes inalámbricas.**

Autoevaluación

¿Cuál de las siguientes opciones sería un inconveniente en las redes inalámbricas?

- ○ El coste de las infraestructuras necesarias.
- ○ La seguridad es un punto débil en este tipo de redes.
- ○ No permite la movilidad de los usuarios o usuarias.
- ○ La distancia de conexión, que suele ser demasiado pequeña.

No es correcto, en realidad esto no es un inconveniente de las redes inalámbricas.

Muy bien. Probablemente, sea su principal inconveniente.

Incorrecta, puesto que la movilidad es una de sus ventajas.

No es así, puesto que las distancias de conexión pueden ser bastante largas.

Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

1.1.- Estándares de conexión.

Tendrás que hacer un pequeño repaso de algunos conceptos que ya aprendiste en módulos anteriores. En este caso, vamos a recordar los diferentes estándares de conexión existentes en las redes inalámbricas.

HernandoJoseAJ. (CC0)

Los dos estándares de conexión de redes inalámbricas más utilizados, y que seguramente ya conoces, son **Wifi** y **Bluetooth**. Las principales diferencias entre los estándares inalámbricos es su definición:

- Definición de las **especificaciones** técnicas.
- Definición de las **aplicaciones** de ese estándar.

Empezarás repasando las características más importantes del **estándar Wifi**. Has de saber, que existen diferentes tipos de Wifi. Todos ellos están basados en el estándar IEEE 802.11. Verás a continuación un repaso de las características más importantes de algunas variantes de este estándar:

Para conocer todos los estándares y sus características: https://es.wikipedia.org/wiki/IEEE_802.11 El estándar **IEEE 802.11b**, funciona en la banda de 2,4 GHz y alcanza una velocidad de hasta 11 Mbps.

- El estándar **IEEE 802.11g**, en la banda de 2,4 GHz, alcanza una velocidad de hasta 54 Mbps.
- El estándar **IEEE 802.11a**, conocido como Wifi 5, opera en la banda de 5 GHz, admitiendo una velocidad de hasta 54 Mbps, pero tiene menos interferencias que los anteriores.
- El estándar **IEEE 802.11n**, para velocidades de hasta 600 Mbps.

DBGthekafu (GNU/GPL)

El otro estándar utilizado, que ya comentamos antes, es **Bluetooth**. Se trata de una especificación industrial para redes inalámbricas de ámbito personal (WPAN), que nos posibilita la transmisión de voz y datos. Los dispositivos que suelen utilizar esta tecnología suelen ser ordenadores portátiles, impresoras, cámaras digitales, teléfonos móviles, tabletas electrónicas y agendas personales electrónicas (PDA).

La especificación de Bluetooth nos permite comunicaciones de un máximo de 720 Kb/s (kilobites por segundo) con un rango óptimo de 10 metros. Por este motivo se utiliza normalmente en ámbitos personales.

Para saber más

Para ampliar este tema, visita el siguiente enlace donde se explica con detalle las características de Bluetooth.

Artículo sobre Bluetooth.

Si quieres ampliar sobre las características wifi, te invito a que visites el siguiente enlace:

Artículo sobre Wifi.

Autoevaluación

Busca entre estas cuatro características, aquella que pertenezca a Bluetooth.

- ○ Alcanza velocidades de transmisión de 54 Mbps.
- ○ Es un estándar que se encuentra aún en desarrollo.
- ○ Su rango óptimo de transmisión es de 10 metros de distancia.
- ○ Ninguna opción pertenece a las características de Bluetooth.

No es correcto, esta característica pertenece al estándar 802.11g.

Incorrecta, este estándar está completamente desarrollado.

Muy bien. Esta es una característica de Bluetooth.

No es cierto. Sigue buscando una de sus características.

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

1.2.- Equipamiento para redes inalámbricas.

Como recordarás del módulo de Redes Locales, existen una serie de elementos necesarios para formar una red inalámbrica. En este apartado haremos una pequeña descripción de cada uno de ellos, teniendo en cuenta que no son necesarios todos a la vez, sino que dependerá del caso sobre el que estés trabajando.

Los principales elementos o equipamiento necesario para las redes inalámbricas son los siguientes:

- **Adaptador Wifi**: es el equivalente en una red cableada, la tarjeta de red. El adaptador Wifi es el dispositivo que se pone en los ordenadores para que puedan acceder inalámbricamente a la red.

Lzur. (Dominio público)

- **Punto de acceso o, en inglés, Access Point**: El punto de acceso Wifi es el equivalente en una red cableada al hub (concentrador) o al switch (conmutador). El punto de acceso es el dispositivo que centraliza, recibe y envía la señal a los adaptadores wifi que están en los ordenadores.

Rodrigo César. (Dominio público)

- **Bridge o, en español, puente**: la función del bridge es unir de forma inalámbrica dos redes de cable. Imagínate que tienes que unir dos redes cableadas en dos pisos y queremos unirlas sin cables. En este caso, utilizarás un bridge.

Dlink. (Copyright (Cita))

- **Gateway o, en español, pasarela**: La función del gateway es dar acceso inalámbrico a determinados servicios, como Internet o una impresora. Hace a la vez la función de punto de acceso y de servidor de periféricos.

Nuscreen. (CC BY-SA)

- **Antena**: Puedes utilizar antenas para extender el alcance de una red inalámbrica hasta varios kilómetros.

U.S. Robotics. (Copyright (Cita))

Autoevaluación

¿Qué dispositivo utilizarías para conectar inalámbricamente dos redes LAN cableadas?

- ○ Una antena.
- ○ Un adaptador inalámbrico.

- ○ Punto de acceso.
- ○ Bridge o puente.

No es correcto, es otro dispositivo.

Incorrecta, encuentra la opción válida.

No se trata de este elemento, sigue buscando.

Muy bien. Esta es la opción correcta.

Solución

1. Incorrecto
2. Incorrecto
3. Incorrecto
4. Opción correcta

1.3.- Modos de conexión.

Además de los estándares de conexión que has recordado en este tema, como son Wifi y Bluetooth, existen otros modos de conexión. De esta manera, se puede hacer una clasificación más amplia sobre las distintas redes inalámbricas existentes.

Debes saber que, la clasificación de los distintos modos de conexión inalámbrica está condicionada por el **área que abarca** dicha red. Así, en función del alcance, tenemos los siguientes tipos de redes:

- **Wireless Personal Area Network** (**WPAN**, o redes de área personal inalámbrica): esta red te dará una cobertura personal y está basado en diversas tecnologías, entre ellas, Bluetooth, de la que ya hemos hecho referencia al principio del tema.
- **Wireless Local Area Network** (**WLAN**, o redes de área local inalámbrica): Este modo de conexión es para redes de área local, está basado en la tecnología Wifi, que sigue el estándar IEEE 802.11, como ya has visto al principio de la unidad.
- **Wireless Metropolitan Area Network** (**WMAN**, o redes de área metropolitana inalámbrica): Las WMAN son redes cuya área es metropolitana y está basado en la tecnología WiMax. Es un estándar de comunicación que se basa en la normal IEEE 802.16. Se parece bastante a Wifi, pero tiene más cobertura y ancho de banda. Una de sus ventajas es que da servicios de banda ancha en zonas donde el cableado sería muy costoso porque la densidad de población es baja (zonas rurales). Entre sus ventajas se encuentran las siguientes:
  - Abarca distancias de hasta 80 kilómetros con el uso de antenas.
  - Alcanza velocidades de hasta 75 Mbps.
- **Wireless Wide Area Network** (**WWAN**, o redes de área extensa inalámbrica): Por último, estas redes tienen el alcance más amplio de todas las redes inalámbricas. Es por esta razón, por la que los teléfonos móviles que se conectan a Internet lo hacen a través de redes inalámbricas de área extensa. Las principales tecnologías utilizadas son las siguientes:
  - **GSM** (Acrónimo en inglés de Global System for Mobile Communication).
  - **GPRS** (Acrónimo en inglés de General Packet Radio Service).
  - **UMTS** (Acrónimo en inglés de Universal Mobile Telecommunication System).

En el siguiente gráfico se ve una clasificación de los distintos modos de conexión que acabas de repasar. En el esquema verás el acrónimo de cada uno de los modos de conexión y la norma que regula cada una de ellas:

Xenia g. (Dominio público)

Para saber más

1.4.- Identificadores de servicio.

En este punto aprenderás los elementos básicos que se han de configurar para que funcione una red inalámbrica. En apartados anteriores, ya has observado los elementos físicos necesarios en función del **escenario** donde tengas que montar una red inalámbrica. Una vez que el hardware necesario ya está instalado, hay que pasar a configurar una serie de parámetros, que serán los siguientes:

Nuria Celis Nieto. (Copyright (Cita))

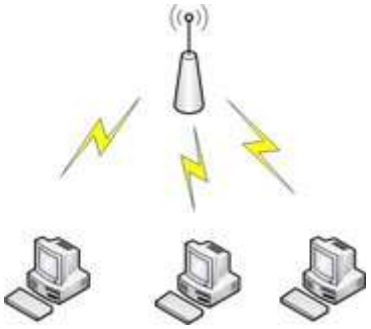
- **Nombre de la red**: Cada red inalámbrica utiliza un nombre de red único para identificarse. Este nombre se denomina **Identificador** de conjunto de servicio (cuyas siglas son **SSID**). Al configurar el adaptador inalámbrico en cada equipo, debe especificarse el SSID de la red a la que te quieres conectar. Si deseas conectarte a una red que ya existe, debes utilizar el nombre de dicha red. Si, por otro lado, estás configurando tu propia red, puedes crear tu propio nombre y utilizarlo en cada equipo. El nombre de la red puede tener hasta 32 caracteres y contener letras y números.
- **Perfiles**: Al configurar el equipo para que acceda a la red inalámbrica, éste creará un perfil que coincide con las opciones inalámbricas de la red. Una vez creados esos perfiles, el equipo se conectará automáticamente cuando se encuentre cerca de la red inalámbrica en cuestión.
- **Seguridad**: Las redes inalámbricas pueden utilizar la codificación para ayudar a proteger los datos. Para utilizar esa codificación, tendrá una clave o contraseña.

Acabas de aprender que uno de los parámetros necesarios para identificar una red es el **nombre de red**. Pero existen distintas maneras de identificar una red inalámbrica, dependiendo de su tamaño y componentes:

- **El Nombre de la red o Identificador del conjunto de servicios (SSID):** Identifica una red inalámbrica. Todos los dispositivos inalámbricos de la red deben utilizar el mismo SSID.
- **SSID de difusión:** Un punto de acceso que difunde su nombre de red. Si se activa esta función en un punto de acceso, cualquier usuario inalámbrico podrá conectarse a él utilizando un SSID en blanco (nulo).
- **Conjunto de servicios básicos (BSS):** Se compone de un mínimo de dos o más nodos o estaciones inalámbricos e incluye al menos un punto de acceso o router inalámbrico, que se han reconocido entre sí y han establecido comunicaciones.
- **Conjunto de servicios básicos independientes (IBSS):** Es un modo de funcionamiento en un sistema 802.11 que permite la comunicación directa entre dispositivos 802.11 sin necesidad de establecer una sesión de comunicación con un punto de acceso.

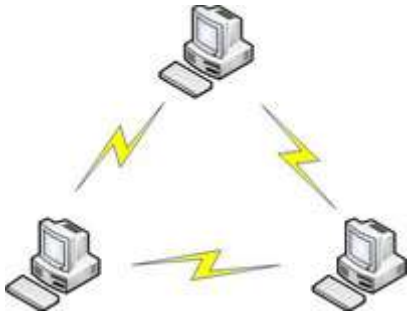
Otra cosa que has de saber es que existen distintos modos de montar una red inalámbrica. Las redes inalámbricas pueden funcionar con o sin puntos de acceso, dependiendo de los usuarios de la red. Verás ahora las diferencias entre utilizar el modo con puntos de acceso o el modo entre dispositivos, o sin puntos de acceso.

- **Modo con puntos de acceso**: Los equipos inalámbricos transmiten al punto de acceso, éste recibe la información y la vuelve a difundir a los demás equipos. El punto de acceso también puede conectarse a una red con cables o a Internet. Varios puntos de acceso pueden trabajar en conjunto para ofrecer cobertura en áreas amplias.



Nuria Celis Nieto. (Uso educativo nc)

- **Modo entre dispositivos**: llamado también Ad Hoc, trabaja sin puntos de acceso y permite a los equipos inalámbricos enviar información directamente a los demás equipos inalámbricos. Este modo puede utilizarse en equipos ubicados en una red en el hogar o una oficina pequeña, o bien, para una red inalámbrica temporal en un área reducida.



Nuria Celis Nieto. (Uso educativo nc)

Autoevaluación

¿Qué siglas corresponden al nombre de la red o identificador el conjunto de servicios?

- ○ SSID.
- ○ BSS.
- ○ IBSS.
- ○ WLAN.

Muy bien. Esta es la opción correcta.

No es correcto, esto son las siglas del conjunto de servicios básicos.

Incorrecta, son las siglas del conjunto de servicios básicos independientes.

No se trata de estas siglas, sigue buscando.

Solución

1. Opción correcta
2. Incorrecto
3. Incorrecto
4. Incorrecto

2.- Despliegue de redes inalámbricas.

Caso práctico

Alberto, el encargado de mantenimiento de los equipos informáticos del IES Montes Claros, ha telefoneado a María, la Técnico Superior en Administración de Sistemas Informáticos en red, que trabaja en la empresa que les ayuda con el mantenimiento del centro. Alberto quiere preguntarle cómo pueden solucionar el problema de la conexión a la red desde el departamento de Latín.

Stockbyte. (Uso educativo nc)

-Hola María, soy Alberto, del IES Montes Claros.

-Hola Alberto, cuanto tiempo sin hablar. ¿Cómo os va todo por ahí? ¿Tenéis algún problema en el centro? –preguntó interesada María.

-Bueno -contestó Alberto-, la verdad es que sí. ¿Recuerdas donde está ubicado el departamento de latín del centro? Al final del pasillo de la primera planta.

-Sí, lo recuerdo. Se que está un poco alejado del resto de los departamentos.

-Así es, María. El problema que tenemos ahora es cómo proporcionarle acceso a la red.

-Yo creo -respondió María-, que la mejor solución sería colocar un punto de acceso inalámbrico en el pasillo del departamento de latín. Este punto de acceso tendrá que estar unido mediante cable a un armario de comunicaciones que hay al otro lado del pasillo. Eso proporcionará un área de alcance para una red inalámbrica suficiente para que incluya también al departamento de latín.

-¿Y con esto sería suficiente, Maria?

-Bueno, además de instalar el punto de acceso, habría que dotar al equipo del departamento de una tarjeta de red inalámbrica para que pueda detectar y conectarse a la señal que transmite el punto de acceso. –Explicó María pacientemente a Alberto- La ventaja es que lo podréis configurar para que se utilice con todos los dispositivos que se encuentren en el área de acción de esta antena.

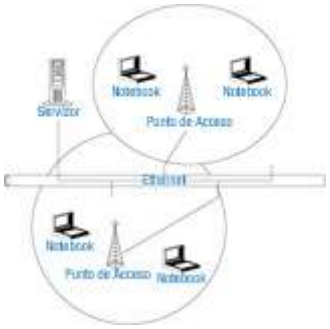
-Eso esta bien, pero ¿No existe la posibilidad de que nuestros alumnos y alumnas se intenten conectar también, por ejemplo, con sus teléfonos móviles? –la duda de Alberto era clara. No quería Internet en los teléfonos del alumnado.

-No te preocupes, Alberto, para eso existen una serie de configuraciones sobre seguridad en redes inalámbricas para que eso no suceda.

-Una vez que ya tengo todas las dudas aclaradas, ¿Podríais pasaros por el centro para darnos presupuesto de lo que nos puede costar esto? –preguntó Alberto.

-Sin problema, ¿te viene bien mañana?

Como has podido comprobar, Alberto y María han tenido una conversación de lo más interesante acerca de una posible solución para dotar a un lugar apartado dentro de un edificio, de conexión a una red local y a Internet. Este es uno de los casos que se podrá presentar a lo largo de tu vida profesional, aunque no es el único. Para poder tomar decisiones en el futuro, necesitas conocer a fondo los elementos con los que te puedes encontrar en una red inalámbrica y tener bien claro para qué sirven cada uno de ellos.



Raphael Bezerra. (Dominio público)

Otro tema del que han estado hablando, y que no debe dejarte indiferente, es el tema de la seguridad en las redes inalámbricas. Es un tema para nada trivial puesto que es, sin lugar a dudas, el punto débil de este tipo de tecnologías. ¿Cómo evitarás que un intruso se "cuele" en tu red inalámbrica? ¿De que medios dispones para evitar las intrusiones? Sabrás responder a estas cuestiones cuando finalices la unidad.

2.1.- Puntos de acceso.

Como has podido recordar en los apartados anteriores, que un **punto de acceso inalámbrico** o **WAP** (acrónimo en inglés de Wireless Access Point), es un dispositivo utilizado para conectar dispositivos en comunicación inalámbrica para formar una red inalámbrica. A veces, también puede conectarse el punto de acceso a una red cableada y podremos transmitir datos entre los dispositivos conectados a la red de cable y los dispositivos inalámbricos. Es importante que sepas, que los puntos de acceso tienen su propia dirección IP asignada, para así poder ser configurados.

Lzur. (Dominio público)

Recuerda que, una de sus características es que un único punto de acceso puede soportar un pequeño grupo de usuarios. Además, debes saber que, puede funcionar en un rango de treinta hasta varios cientos de metros. Esto depende de los obstáculos intermedios que nos podamos encontrar, como las paredes del edificio. El punto de acceso se coloca normalmente en un lugar alto, pero podría colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada.

Existen una serie de **ventajas** que es importante que conozcas porque, desde principio del año 2000, hicieron muy populares a estos dispositivos. Evitan muchos metros de cables, especialmente en escuelas y oficinas. Las ventajas más destacadas son las siguientes:

- **Bajo coste y fácil instalación de los puntos de acceso inalámbricos.**
- **Permite a los usuarios y usuarias gran movilidad, especialmente si se utilizan dispositivos portátiles que puedan conectarse a la red.**

Pero, como te podrás imaginar, no todo es tan sencillo en las redes inalámbricas. También se cuenta con algún que otro **inconveniente**:

- **Las redes inalámbricas pueden verse interferidas** por otros dispositivos que utilizan frecuencias de radio similares, e incluso dispositivos que utilicen microondas.
- Otro problema es la facilidad con que **un usuario no autorizado podría entrar a utilizar la red inalámbrica** si no hay un sistema de seguridad importante establecido. Como seguramente sabrás, a veces, no es necesario ni siquiera entrar en un edificio donde se encuentra el punto de acceso a la red inalámbrica para recibir la señal desde el exterior.

Para este último problema, el de la **seguridad**, la solución que deberás adoptar es incrementar la seguridad en las redes. Para ello, utilizamos la encriptación de datos. En un principio, los dispositivos utilizaban el sistema de encriptación WEP, que era fácil de traspasar. Pero más adelante se empezó a utilizar los sistemas WPA Y WPA2, mucho más seguros. Los veremos a continuación.

Cuando tengas la necesidad de configurar un punto de acceso en tu vida profesional, parte del proceso de instalación y configuración dependerán del modelo del punto de acceso elegido. Además, este tipo de dispositivos suelen venir acompañados de las instrucciones necesarias para realizar dicha tarea.

Debes conocer

En el siguiente enlace se explica el proceso de instalación de dos modelos de puntos de acceso.

Montar una red wifi en casa.

En el siguiente enlace puedes ver el proceso de configuración de un punto de acceso.

Configurar un punto de acceso inalámbrico.

2.2.- Encaminadores inalámbricos.

Como ya estudiaste en el módulo de primero, Redes Locales, un **encaminador** o **router** en inglés, es un dispositivo hardware para la interconexión de redes que trabaja en la capa tres, nivel de red, del **modelo OSI** (acrónimo en inglés de Open System Interconnection). En realidad, este dispositivo permite asegurar el enrutamiento entre redes o elige la mejor ruta que deben tomar los paquetes de datos.

Weihao Chiu. (CC BY-SA)

Anteriormente, los encaminadores solían trabajar con redes fijas, pero en los últimos tiempos ya han aparecido routers que permiten realizar una interfaz entre redes fijas y móviles. Pues bien, un encaminador inalámbrico funciona igual que un encaminador tradicional. La diferencia entre ambos es que, el encaminador inalámbrico, al igual que el tradicional, permite la conexión con dispositivos cableados, pero además, permite la conexión de dispositivos inalámbricos a las redes a las que el encaminador está conectado por cable.
A su vez, las diferencias entre distintos encaminadores inalámbricos vienen dadas por:

- La **potencia** que alcanzan.
- Las **frecuencias** que utilizan.
- Los **protocolos** en los que trabajan.

Otro dispositivo que también reconocerás es el router ADSL. Se trata de un dispositivo que permite que se conecten a él varios equipos o, incluso varias redes de área local. Realmente, funciona como varios componentes en uno y realiza las siguientes funciones:

- **Puerta de enlace**: ya que proporciona salida hacia el exterior a una red local.
- **Router**: cuando le llega un paquete procedente de Internet, lo dirige hacia la interfaz destino por el camino correspondiente. Es decir, es capaz de encaminar paquetes IP, evitando que el paquete se pierda o sea manipulado por terceros.
- **Módem ADSL**: modula las señales enviadas desde la red local para que puedan transmitirse por la línea ADSL y remodula las señales recibidas por ésta para que los equipos de la red local puedan interpretarlos. De hecho, existen configuraciones formadas por un módem ADSL y un router que hacen la misma función que un router ADSL.
- **Punto de acceso inalámbrico**: algunos routers ADSL permiten la comunicación vía wireless (sin cables) con los equipos de la red local.

Como puedes observar, los avances tecnológicos han conseguido introducir la funcionalidad de cuatro equipos en uno sólo.

Autoevaluación

¿Cuáles de estos dispositivos se utiliza para permitir comunicación vía wireless?

- ○ Router.
- ○ Módem ADSL.

- ○ Puerta de enlace.
- ○ Punto de acceso.

No es correcto, si no tiene la condición de inalámbrico.

Incorrecta, si no es a la vez un router inalámbrico.

No es cierto, repasa la teoría.

Muy bien. Es su función principal permitir comunicación vía wireless.

Solución

1. Incorrecto
2. Incorrecto
3. Incorrecto
4. Opción correcta

2.3.- Seguridad en redes inalámbricas.

Se ha destacado a lo largo de la unidad, que las redes inalámbricas son inseguras, aunque sólo sea porque el medio de transporte que utilizan es el aire. Por lo tanto, un elemento esencial, que debes tener en cuenta, en este tipo de redes es la **encriptación**. La encriptación es un modo de codificar los datos que solo podrán ser entendidos por aquellos dispositivos que tengas la misma clave de encriptación. Es como si se compartiera una contraseña. Sin ella, no se puede acceder a la red.

Wax115. (MorgueFile free photo.)

En general, se utiliza como **método de encriptación WEP** (acrónimo en inglés de Wired Equivalent Privacy), que es un mecanismo de encriptación y autenticación especificado en el estándar IEEE 802.11 para garantizar la seguridad de las comunicaciones entre los usuarios y los puntos de acceso. Como **características** destacan:

- **La clave de acceso estándar es de 40 bits.**
- **Existe otra clave opcional de 128 bits.**
- **Se puede asignar de forma estática o manual,** para los clientes y los puntos de acceso.
- Utiliza un **esquema de cifrado simétrico** en el que la misma clave y algoritmo se utilizan para el cifrado y el descifrado.

Otro mecanismo de seguridad que debes conocer es **WPA**, acrónimo en inglés de Wifi Protected Access. Se creó para proteger las redes inalámbricas y para corregir las deficiencias del sistema previo WEP. En este último sistema se comprobó que se podía recuperar la clave de encriptación realizando ataques masivos. Por ello, se decidieron a crear WPA. Implementa la mayoría del estándar IEEE 802.11i, y fue creado como medida intermedia en lo que se acababa de desarrollar dicho estándar. WPA fue creado por la alianza Wi-Fi.

Las **características** más importantes de WPA que debes aprender son:

- Adopta la **autenticación de usuarios mediante el uso de un servidor**, donde se almacenan las credenciales y contraseñas de los usuarios de la red.
- Para no obligar al uso de un servidor, **permite autenticación mediante clave compartida** de modo similar al WEP, que requiere introducir la misma clave en todos los equipos de la red.
- La información en WAP es cifrada, pero con una **clave de 128 bits**.

Por último, debes saber que una vez finalizado el estándar 802.11i, se crea WPA2 que está basado en WPA. Utiliza un algoritmo de encriptación más seguro que los dos métodos anteriores.

Podemos concluir este apartado haciendo referencia a una serie de **consejos en torno a la seguridad** que tendrás en cuenta cuando configures una red inalámbrica:

- Cambiarás las claves que tienen por defecto los puntos de acceso.
- Realizarás el control y filtrado de direcciones MAC e identificadores de red para restringir los adaptadores y puntos de acceso que se puedan conectar a la red.
- Utilizarás una configuración de encriptación adecuada a la red. A ser posible elegirás primero el método WPA2 o WPA en lugar de WEP.

2.4.- Direcciones MAC.

Seguro que recuerdas que, en el ámbito de las redes de ordenadores, **una dirección MAC** corresponden de forma única a una tarjeta o dispositivo de red y es también conocida como dirección física. La MAC (acrónimo en inglés de Media Access Control) es un identificador de 48 bits ó 6 bloques en hexadecimal que viene dada por el fabricante.

Nuria Celis Nieto. (Copyright (Cita))

Haciendo un breve repaso, recordarás cómo se puede obtener la dirección MAC de una tarjeta de red. Dependiendo en qué sistema estés trabajando, los métodos pueden ser de la siguiente manera:

- **En la familia Windows**: En la terminal de línea de comandos, ejecutamos la instrucción **ipconfig /all**. Aparece identificado como dirección física.
- **En la familia Linux**: En un terminal de línea de comandos, ejecutamos la instrucción **ifconfig –a**. Según la distribución que estemos utilizando, es posible que el usuario tenga privilegios de root, o administrador. En ese caso la instrucción será sudo **ifconfig –a**.

Una vez recordado esto, es interesante que conozcas otra medida de seguridad que está bastante difundida dentro de las redes inalámbricas, que es filtrar las direcciones MAC para aportar seguridad a una red wireless.

Los puntos de acceso o los routers inalámbricos pueden programarse con un listado de los dispositivos que están autorizados a conectarse a la red. De esta manera, el punto de acceso o el router, controlan quiénes son los que se están conectando y permite, o no, su acceso al sistema.

Aunque el filtrado parezca un buen método de seguridad presenta **varias desventajas**. Por este motivo, en general, está desaconsejado por los expertos. Pero verás cuales son estas desventajas:

- Como hay que programar cada punto de acceso manualmente, provoca, además de una gran **carga de trabajo**, **errores al introducir los números MAC**.
- Cada nuevo usuario ha de ser dado de alta, con lo que habría que añadir su dirección MAC en todos los puntos de acceso. Si un atractivo de las redes inalámbricas es la movilidad del usuario o usuaria, todos **los puntos de acceso deben estar actualizados.**
- Si el dispositivo con el que nos conectamos se extravía o es robado, hay que **dar de baja** su dirección MAC en todos los puntos de acceso.
- Las **direcciones MAC pueden ser capturadas** por algún intruso y luego, con ese dato, tener acceso libre a nuestro sistema.
- **No cumple el estándar 802.11**, pues no se autentica al usuario, sino a los dispositivos. Además, no aporta solución a las debilidades de la encriptación WEP, como el uso de claves estáticas.

Podríamos acabar diciendo que es una práctica que no soluciona los problemas de seguridad en una red wifi y que solo añade un pequeño elemento de control bastante primitivo.

Para saber más

En el siguiente enlace tienes un artículo sobre como se puede configurar un router para denegar la entrada en una red wireless a través de la dirección MAC.

Denegar el acceso a una red wifi.

Autoevaluación

Busca entre las siguientes afirmaciones, aquella que sea correcta.

- ○ El método más seguro de proteger una red Wifi es con encriptación WPA2.
- ○ El filtrado de direcciones MAC es tan seguro que no necesita ningún método de encriptación.
- ○ El filtrado de direcciones MAC soluciona las debilidades de la encriptación WEP.
- ○ El método de encriptación más seguro es WEP utilizado junto con el filtrado de direcciones MAC.

Muy bien. Es el método más completo.

No es correcto. No es un método demasiado seguro ni recomendado.

Incorrecta, esa afirmación es falsa.

No es correcto, aunque se utilicen conjuntamente, sigue siendo insuficiente.

Solución

1. Opción correcta
2. Incorrecto
3. Incorrecto
4. Incorrecto

Puedes ver el siguiente vídeo explicativo sobre los elementos y componentes necesarios para instalar una red WiMAX.

Redes WiMAX.

En el siguiente enlace encontrarás un documento bastante completo sobre redes inalámbricas. Además, también tiene un apartado de comparativa sobre redes cableadas que es muy interesante.

Documento sobre redes inalámbricas. (1.37 MB)

Respecto al control y filtrado de direcciones MAC, ampliaremos este tema en el siguiente apartado de esta misma unidad.

Debes conocer

Puedes ver el siguiente vídeo sobre como poner una contraseña en una red inalámbrica.

Configuración de seguridad de una red wifi.