Integración de redes inalámbricas.

Caso práctico

"Antonio, el dueño de la academia donde estamos instalando redes aula locales en sus aulas, tiene dudas. Para ello le pregunta a Julia, que es la técnica superior de Administración de Redes que está supervisando la instalación en su academia.

- Julia, además de la red cableada en las aulas, ¿sería posible ofrecer una red inalámbrica en la sala de visitas?
- Por supuesto que sí, Antonio. Podríamos plantearnos la posibilidad de tener una red inalámbrica en toda la academia de manera que si quieres te podrías conectar con cualquier dispositivo que lo permita.
- Julia, eso que dices me parece de lo más interesante, que cualquiera se pueda conectar sin necesidad de cables. Eso sería muy útil.
- Sí, Antonio, y además de la comodidad que ofrecen este tipo de tecnologías…

Es, por este motivo, por el que vamos a estudiar el tema de la interconexión de equipos en redes locales a través de **redes inalámbricas**."

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 hasta 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 de forma que sepamos proteger correctamente nuestra 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

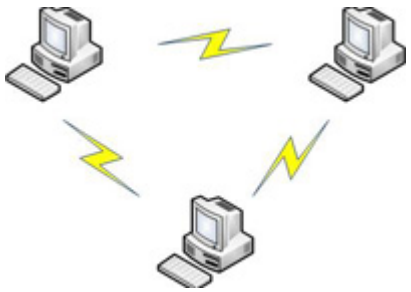
Pero si hablamos de redes inalámbricas, sin duda alguna la tecnología más puntera y que más se está desarrollando en estos momentos es la conocida como 5G, es decir, la nueva red de comunicaciones móviles que permitirá una gran mejora en capacidad y velocidad de transmisión, hasta el punto de interconectar 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:

5G

1. Conceptos sobre redes inalámbricas.

WIFI es una tecnología de transmisión de datos inalámbrica utilizada para Internet –*principalmente*- y que se basa en el estándar 802.11. Es una tecnología que permite la **conexión inalámbrica entre dispositivos electrónicos**, ordenadores, smartphones, tablets, televisores, videoconsolas, etc. Wi-Fi es una marca de Wi-Fi Alliance o Alianza Wi-Fi, la organización que promueve dicha tecnología y que se encarga de certificar todos los productos que se ajustan a las normas establecidas de interoperabilidad.

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 comunicación física, utilizando para su conexión ondas electromagnéticas.



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

- **Movilidad**: Al no estar conectado a un cable el usuario se puede mover libremente dentro del radio de influencia de la red inalámbrica.
- **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.**

Para saber más

En el siguiente enlace puedes ver las principales ventajas de las redes inalámbricas:

Ventajas de las 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. IEEE 802.11

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.

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, que se puede ver desde dos perspectivas:

- 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:

- El estándar **IEEE 802.11b**, alcanza una velocidad de hasta 11 Mbps.
- El estándar **IEEE 802.11g**, alcanza una velocidad de hasta 54 Mbps.
- El estándar **IEEE 802.11a**, conocido como Wifi 5, trabaja desde hace relativamente poco tiempo a frecuencias distintas a los estándares ya enumerados. Trabaja a una velocidad de hasta 54 Mbps, pero tiene menos interferencias que los anteriores.
- Existe también un borrador del estándar **IEEE 802.11n**, para velocidades de hasta 300 Mbps, pero todavía se encuentra en desarrollo.

El otro estándar utilizado, que ya comentamos antes, es **Bluetooth**. Se trata de una especificación industrial para redes inalámbricas de ámbito personal, 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.

Recomendación

Te recomendamos que visites el siguiente enlace sobre los estándares WiFI:

Estándares WiFI, tipos de seguridad y su diseño.

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

Autoevaluación

El estándar [redacted] es una familia de normas inalámbricas creada por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE).

Enviar

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.

- **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.

- **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.

- **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.

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

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

Autoevaluación

Señala cuál de estas afirmaciones no es una ventaja de las redes Wifi:

- Son más cómodas de utilizar porque no dependes del cableado de la red.
- Son compatibles con Bluetooth.
- Permite acceder a varios ordenadores sin ampliar su infraestructura.
- La marca WiFi asegura que los dispositivos son compatibles entre sí.

Incorrecto

Opción correcta

Incorrecto

Incorrecto

Solución

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

1.3. Modos de conexión: tipos de WiFi.

Te interesará saber que las redes inalámbricas se pueden clasificar según el área que abarquen, o, dicho de otro modo, según la cobertura de la red:

- **WPAN** (Wireless Personal Area Network): Este tipo de red es de cobertura personal. Un ejemplo de este tipo de redes son aquellas que utilizan la tecnología Bluetooth para conectarse. Utilizan el estándar IEEE 802.15. Esta red permite establecer comunicaciones inalámbricas para dispositivos como teléfonos móviles y equipos portátiles que se utilizan dentro de un espacio operativo personal (POS). Un POS es el espacio que rodea a una persona, hasta una distancia de 10 metros aproximadamente. La finalidad de estas redes es comunicar cualquier dispositivo personal (ordenador, terminal móvil, PDA, etc.) con sus periféricos, así como permitir una comunicación directa a corta distancia entre estos dispositivos.

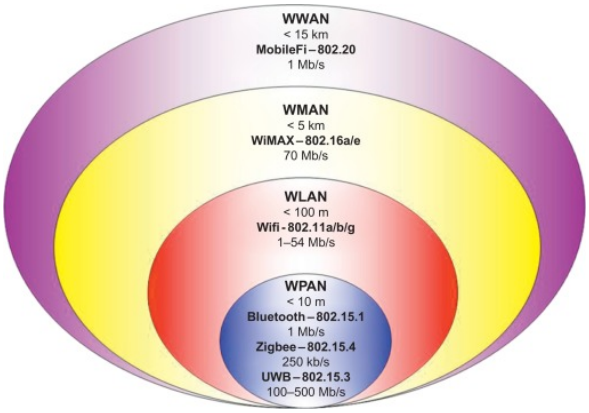
- **WLAN** (Wireless Local Area Network): Se trata de una red de área local de tecnología inalámbrica basada en **WiFi**. El estándar utilizado es el 802.11. Esta red les permite a los usuarios establecer conexiones inalámbricas dentro del área de cobertura. Es una red que cubre un área equivalente a la red local de una empresa, con un alcance aproximado de cien metros, podría cubrir por ejemplo, un edificio corporativo, un campus empresarial, o en un espacio público como un aeropuerto. (Ampliaremos más en el punto 7 de esta unidad).

- **WMAN** (Wireless Metropolitan Area Network): Son redes de **área metropolitana** de tecnología inalámbrica basadas en WiMAX basado en el estándar 802.16. WiMAX es una tecnología basada en WiFi pero con más cobertura y con más ancho de banda. Las redes WMAN permiten a los usuarios establecer conexiones inalámbricas entre varias ubicaciones dentro de un área metropolitana, por ejemplo, entre varios edificios de oficinas de una ciudad o en un campus universitario, sin el alto coste que supone la instalación de cables de fibra o cobre y el alquiler de las líneas.

- **WWAN** (Wireless Wide Area Network) también conocida como red inalámbrica de área extensa: En este tipo de redes encontramos las tecnologías **UMTS**, utilizadas para teléfonos móviles de tercera generación o la tecnología GPRS. Es una manera de conectarse a Internet sin cables usando tecnologías móviles. 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:

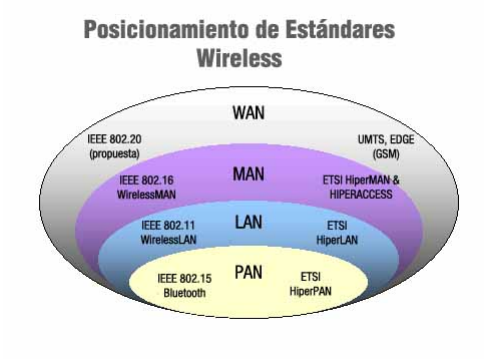
  - **GSM** (Acrónimo en inglés de Global System for Mobile Communication).
  - **GPRS** (Acrónimo en inglés de General Packet Radio Service).
  - **UMTS** (Acrónimo en inglés de Universal Mobile Telecommunication System).

Veamos ahora un esquema de los diferentes tipos de redes inalámbricas que se han visto.



Los diferentes tipos de redes inalámbricas se rigen bajo **normas y estándares**, las cuales fueron establecidas por el instituto de ingenieros eléctricos y electrónicos, mas conocido como la IEEE. La norma mas utilizada es la IEEE 802.X

- Red inalámbrica de área personal: esta red se rige bajo la norma IEEE 802.15.
- Red de área local: esta red utiliza la IEEE 802.11.
- Red de área metropolitana: utiliza la IEEE 802.16.



Para saber más

Puedes ver el siguiente enlace pueds ver 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.

Redes inalámbricas.

Autoevaluación

Una red inalámbrica se nos presenta como:

- Una red en la que obligatoriamente los equipos se conectan a través del cableado.
- Solo existen redes inalámbricas de larga distancia.
- Su principal ventaja es lo que la seguridad no tiene porque ser muy exigente.
- Las redes WLAN son redes inalámbricas con las que se puede prescindir del cableado y las conexiones físicas y permiten la movilidad de los usuarios.

Incorrecto

Incorrecto

Incorrecto

Opción correcta

Solución

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

1.4. La tecnologia satelital VSAT.

Las redes VSAT ofrecen servicios vía satélite capaces de soportar **Internet, LAN, comunicaciones Voz IP, video, datos** y permite crear potentes redes públicas y privadas de comunicación fiable. Este sistema opera en frecuencias **banda C, banda Ku y otras frecuencias.**

La volatilidad y rapidez de la comunicación es uno de los retos a los cuales se enfrentan actualmente miles de empresas que operan en lugares remotos o de difícil acceso. Debido a esto, es común hoy en día que muchas compañías opten por implementar en su flujo de procesos, sistemas satelitales que les permitan tener una red de comunicación **ágil e independiente**; por esta razón existen en el mercado un sinfín de soluciones para esta necesidad, como, por ejemplo: las antenas, las cuales ofrecen todo un ecosistema de aplicaciones y ventajas para recibir y enviar información sin importar la ubicación geográfica.

La tecnologia satelital **VSAT** opera en diferentes frecuencias, formas y tamaños. La tecnología VSAT representa una **solución rentable** para usuarios que quieren tener una red de comunicación independiente y la vez conectar muchos sitios dispersos geográficamente.

VSAT utiliza diferentes plataformas para transmitir y recibir datos por satélite, por ejemplo **iDirect, Newtec, Comtech, Datum.**

Ventajas:

- Fácil gestión de la red.
- Ancho de banda garantizado.
- Servicio a distancia independiente.
- Cobertura global inmediata.
- Establecimiento fácil, incluso en sitios de difícil acceso.
- Reconfiguración fácil y posibilidad de ampliación de la red.
- Con el satélite se puede entrar en contacto con cualquier punto de la zona de cobertura.
- Estabilidad en los gastos de explotación de la red durante un largo periodo.
- Costes independientes del sitio de uso.
- Flexibilidad.
- Etc

Para saber más

En el siguiente enlace puedes ver un proveedor que ofrece servicios

VSAT:

VSAT

Reflexiona

¿Podrías decir qué tipo de empresas o entidades utilizan la tecnología VSAT?

Mostrar retroalimentación

Ejemplos frecuentes de utilización de VSAT configurados para recibir información:

- Bolsa de valores y difusión de información.
- Formación o educación a distancia.
- Distribución de noticias y análisis financieros.
- Introducción de nuevos productos en sitios dispersos.
- Actualización de información de mercados como datos, noticias, precios de catálogo.
- Distribución de vídeo o programas de TV DTH (directo a casa).
- Distribución de música en tiendas y áreas públicas.
- Publicidad para paneles electrónicos.
- Etc

1.5. Identificadores de servicio. Modo con puntos de acceso y Ad Hoc.

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:

- **Nombre de la red**: Cada red inalámbrica utiliza un nombre de red único para identificarse. Este nombre se denomina **Identificador de conjunto de servicio** 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.

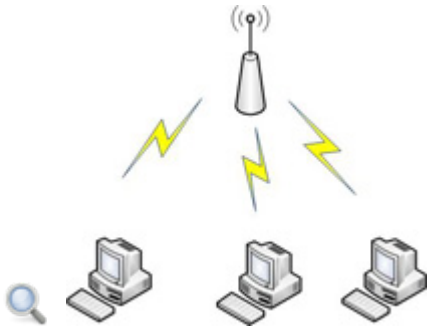
Acabas de aprender que uno de los parámetros necesarios para identificar una red es el **nombre de red**. Pero existen distintas maneras de identificar una red inalámbrica, dependiendo de su tamaño y componentes:

- **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.

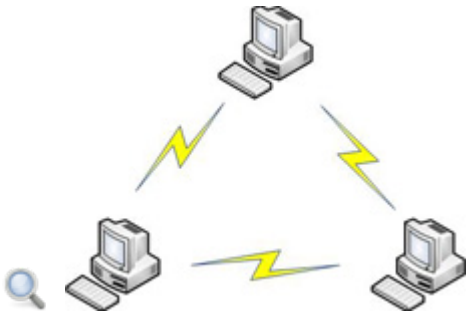
Otra cosa que has de saber es que existen distintos modos de montar una red

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.



- **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.



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. Medios de transmisión.

Caso práctico

Antonio sigue teniendo algunas dudas sobre la idea de la red inalámbrica en la academia, y las comenta con Julia.

- "Veo, Julia, que la red inalámbrica nos proporcionará la posibilidad de poder conectarnos en toda la academia con cualquier dispositivo que reciba ondas electromagnéticas.
- Sí, así es, Antonio. Es muy cómodo el poder tener una red inalámbrica para el alumnado y los visitantes.
- De todos modos, me surgen una serie de dudas respecto a la red inalámbrica, ¿tendremos problemas con la seguridad? ¿Qué elementos extras necesito para realizar la conexión? ¿Cómo llega la señal a los dispositivos que se quieran conectar?...
- Oh, no te preocupes, que eso es algo que tenemos ya muy controlado, yo te cuento…"

Esas preguntas que le surgen a Antonio también serás capaz de responderlas tu cuando te mires el contenido de este capítulo.

Ya has visto en temas anteriores que el medio de transmisión es el canal que permite la transmisión de la información entre dos dispositivos. La **transmisión** se realiza a través de ondas electromagnéticas que se propagan a través de un canal. El canal puede ser un medio físico, como se estudió en el tema anterior, o no, ya que las ondas pueden viajar a través del aire.

Se puede decir que los medios de transmisión se clasifican en medios guiados y en medios no guiados. Los **medios guiados** son aquellos que utilizan un medio sólido (un cable) para la transmisión. Se estudiaron en el tema anterior y eran los cables de pares trenzados, el cable coaxial y el cable de fibra óptica.

Los **medios no guiados** utilizan el aire para transportar los datos: los medios inalámbricos y se basan en la propagación de ondas electromagnéticas por el espacio. Una radiación electromagnética tendrá un comportamiento u otro en función de las características de la onda de la radiación, en especial de su longitud de onda.

Autoevaluación

De las siguientes afirmaciones solo una es cierta. Señala cual:

- Las redes WLAN utilizan la tecnología Bluetooth.
- Las redes WLAN utilizan el estándar IEEE 802.11.
- En las redes inalámbricas hay dos tipos de medios a utilizar, guiados y no guiados.
- Los medios guiados utilizan el aire para transportar los datos.

Incorrecto

Opción correcta

Incorrecto

Incorrecto

Solución

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

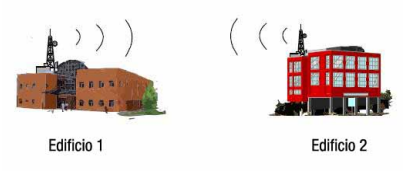
Para saber más

Aquí tenéis un enlace a un artículo de la Wikipedia donde se habla de los medios de transmisión tanto guiados como no guiados. Se trata de un artículo donde se repasan los medios de transmisión guiados que se vieron en el tema anterior y habla un poco de los distintos medios no guiados.

Medios de transmisión.

2.1. Medios no guiados.

Veras ahora una clasificación de los distintos medios no guiados que se pueden utilizar para conectar elementos a una red inalámbrica.



- **Ondas de radio**: Ondas electromagnéticas cuya longitud de onda es superior a los 30 cm. Son capaces de recorrer grandes distancias, y pueden atravesar materiales sólidos, como paredes o edificios. Son ondas **multi-direccionables**: se propagan en todas las direcciones. Su mayor problema son las interferencias entre usuarios. Son las empleadas en las redes WiFi y Bluetooth.

- **Microondas**: Se basa en la **transmisión de ondas electromagnéticas** cuya longitud de onda varía entre 30 cm y un milímetro. Estas ondas viajan en línea recta, por lo que emisor y receptor deben estar alineados cuidadosamente. Tiene dificultades para atravesar edificios. Debido a la propia curvatura de la tierra, la distancia entre dos repetidores no debe exceder nunca de unos 80 km. de distancia. Es una forma económica para comunicar dos zonas geográficas mediante dos torres suficientemente altas para que sus extremos sean visibles.

- **Infrarrojos**: Son ondas electromagnéticas (longitud de onda entre 1 milímetro y 750 *nanómetros*) direccionales incapaces de atravesar objetos sólidos (paredes, por ejemplo) que están indicadas para transmisiones de corta distancia. Las tarjetas de red inalámbrica utilizadas en algunas redes locales emplean esta tecnología: resultan cómodas para ordenadores portátiles. Sin embargo, no consiguen altas velocidades de transmisión.

- **Ondas de luz**: Las ondas láser son **unidireccionales**. Se pueden utilizar para comunicar dos edificios próximos instalando en cada uno de ellos un emisor láser y un fotodetector.

Autoevaluación

Cuáles son las ondas utilizadas en las redes WI-FI:

- Ondas de luz.
- Infrarrojos.
- Ondas de radio.
- Microondas.

Incorrecto

Incorrecto

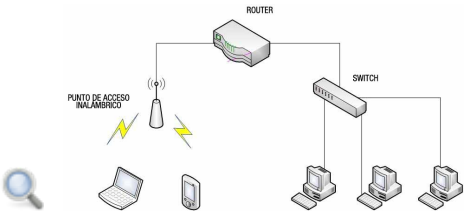
Opción correcta

Incorrecto

Solución

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

2.2. Comparación entre una LAN y una WLAN.



Recuerda que las WLAN comparten un origen común con las LAN Ethernet. El **IEEE** adoptó el **estándar 802** para trabajar distintas arquitecturas de red y los dos grupos dominantes son el **802.3** Ethernet y **802.11** LAN inalámbrica. Pero existen diferencias entre ellos.

La primera de ellas es que **WLAN** utiliza **ondas electromagnéticas** en lugar de cables que veíamos en LAN Ethernet. Las ondas no tienen los límites impuestos por los cables, con lo que las ondas están disponibles para cualquier dispositivo que pueda recibir dichas ondas.

Las ondas no están protegidas de señales exteriores, con lo que pueden existir interferencias con ondas que funcionen en su misma área con frecuencias iguales o similares a la utilizada por nosotros y nosotras.

La transmisión a través de ondas se degradará e incluso dejará de funcionar a medida que te alejas del origen de la señal. Las LAN conectadas tienen cables que son del largo apropiado para mantener la fuerza de la señal.

En las WLAN, cada cliente utiliza un **adaptador inalámbrico** para obtener acceso a la red a través de un dispositivo inalámbrico, como un punto de **acceso inalámbrico** (AP) o un **router inalámbrico**. En el estándar 802.11 se recomienda la prevención de colisiones en WLAN, en lugar de la detección de colisiones para el acceso al medio que se vio en las LAN Ethernet.

Las WLAN tienen mayores inconvenientes de privacidad que las LAN Ethernet.

Autoevaluación

Cuál de las siguientes afirmaciones es correcta respecto a las WLAN:

- Las WLAN trabajan bajo el estándar IEEE 802.11.
- Las LAN Ethernet trabajan con medios no guiados.
- El rendimiento de las WLAN no se degrada a medida que te alejas del origen de las ondas.

El estándar 802.11, recomienda la detección de colisiones como en las LAN Ethernet.

Opción correcta

Incorrecto

Incorrecto

Incorrecto

Solución

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

3. Despliegue de redes inalámbricas.

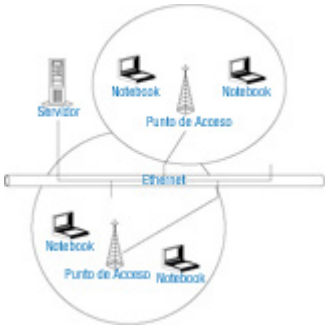
Caso práctico

Antonio sigue teniendo algunas dudas sobre la idea de la red inalámbrica en la academia, y las comenta con Julia.

- "Veo, Julia, que la red inalámbrica nos proporcionará la posibilidad de poder conectarnos en toda la academia con cualquier dispositivo que reciba ondas electromagnéticas.
- Sí, así es, Antonio. Es muy cómodo el poder tener una red inalámbrica para el alumnado y los visitantes.
- De todos modos, me surgen una serie de dudas respecto a la red inalámbrica, ¿tendremos problemas con la seguridad? ¿Qué elementos extras necesito para realizar la conexión? ¿Cómo llega la señal a los dispositivos que se quieran conectar?...
- Oh, no te preocupes, que eso es algo que tenemos ya muy controlado, yo te cuento…"

Esas preguntas que le surgen a Antonio también serás capaz de responderlas tu cuando te mires el contenido de este capítulo.

Como has podido comprobar, en este caso 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.



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.

3.1. 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.

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 hicieron muy populares a estos dispositivos. Evitan muchos metros de cables, especialmente en escuelas y oficinas. Entre las ventajas más destacadas son:

- 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.

3.2. Encaminadores y componentes 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.

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.

Debes conocer

En el siguiente enlace tienes un artículo sobre como configurar un router ADSL con Wifi. El proceso puede variar de un router concreto a otro, pero el grueso de la explicación es genérico.

Configuración de una red wireless.

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.

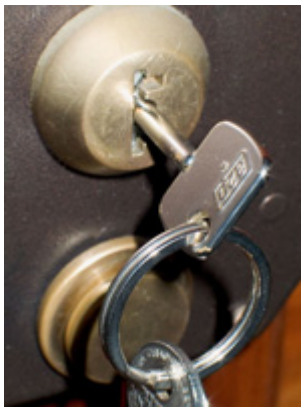
Muy bien. Es su función principal permitir comunicación vía wireless.

Solución

1. Incorrecto
2. Incorrecto

3. Incorrecto
4. Opción correcta

3.3. 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 tengan la misma clave de encriptación. Es como si se compartiera una contraseña. Sin ella, no se puede acceder a la red.

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 por la fuerza bruta. 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:

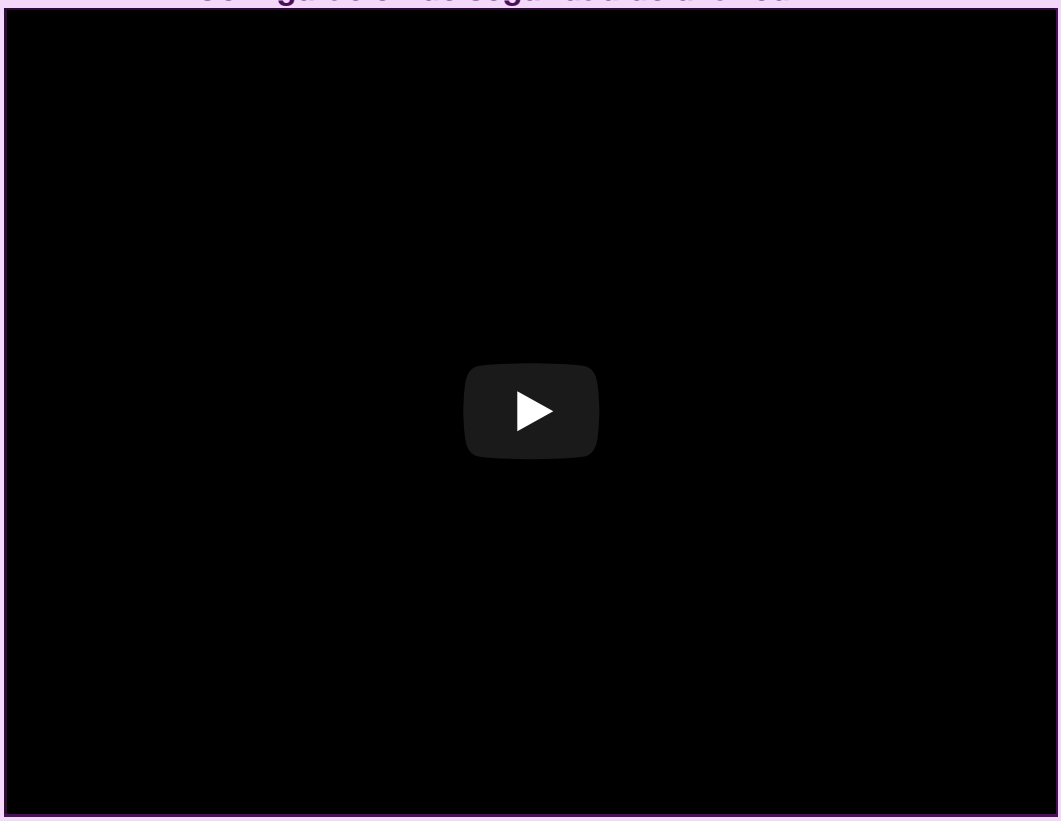
- Cambiarás las claves que tienen por defecto los puntos de acceso.
- Realizarás el control y filtrado de direcciones MAC e identificadores de red para restringir los adaptadores y puntos de acceso que se puedan conectar a la red.
- Utilizarás una configuración de encriptación adecuada a la red. A ser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

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

👀 Debes conocer

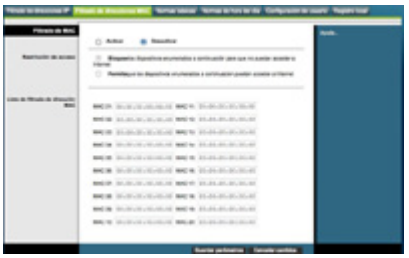
Puedes ver el siguiente vídeo sobre como poner una contraseña en una red inalámbrica.

Configuración de seguridad de una red wifi.



Resumen de texto alternativo

3.4. 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 parejas de dígitos hexadecimales que viene dada por el fabricante.

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

3.5. Software de dispositivos y clientes, firmware.

El **firmware**, también conocido como soporte lógico inalterable, es un programa informático que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo de cualquier tipo. Es el programa básico que controla los circuitos electrónicos de cualquier dispositivo.

Este programa o software es una porción de código encargada de controlar qué es lo que tiene que hacer el hardware de un dispositivo, y el que se asegura de que el funcionamiento básico es correcto.

El código que compone el firmware de cualquier dispositivo suele **venir en chips de memoria a parte** de las principales. Esto quiere decir que en todos los dispositivos hay una mínima memoria ROM en la que está almacenado este firmware, por el que se establece una interfaz para la configuración del sistema y permite controlar el arranque y las conexiones y funciones principales del dispositivo.

El firmware puede ser calificado tanto como parte del hardware como del software de un dispositivo. Es parte del hardware porque siempre está integrado en la electrónica, pero no deja de ser un programa informático, por lo que también es software. Así pues, es prácticamente **uno de los principales puntos de unión** entre ambos.

Un ejemplo clásico de firmware es la BIOS de un ordenador, que se encarga de iniciar, configurar y comprobar que se encuentre en buen estado el hardware del ordenador, incluyendo la memoria RAM, los discos duros, la placa base o la tarjeta gráfica.

Para saber más

En el siguiente enlace puedes ver el desarrollo de Firmware integrado y soluciones de software:

Desarrollo de Firmware integrado y soluciones de software.

Autoevaluación

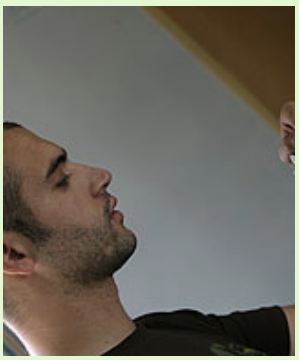
Todos los componentes electrónicos de nuestro PC tienen un **firmware.**

- Verdadero
- Falso

Verdadero

4. Adaptadores de red inalámbricos.

Caso práctico



Antonio le pregunta a Samuel otras dudas que le surgen después de saber cómo se ha hecho la instalación de la infraestructura en la academia.

- "Samuel, tengo un portátil que no tiene conexión Wifi, ¿Cómo puedo hacer para poder conectarme con el portátil a la red inalámbrica?,
- Es sencillo, Antonio, simplemente tendrás que adquirir un adaptador de red inalámbrico, bien, una tarjeta de red para los equipos de sobremesa, o un dispositivo USB que realiza la misma función.
- Ah!, eso sería muy práctico para mi…"

Debes conocer

Debes conocer que un **adaptador de red**, o tarjeta de red o NIC (Network Interface Card) es un elemento hardware que permite la comunicación con aparatos conectados entre sí y también permite compartir recursos entre dos o más ordenadores.

Existen diferentes tipos de **tarjetas de red**, entre ellas están las tarjetas de red tipo **Ethernet** y las tarjetas de red **inalámbricas**.

Para que puedas conectarte a una red inalámbrica necesitas algún dispositivo de recepción de las ondas que viajan por el aire. Existen básicamente tres tipos de dispositivos de recepción: las **tarjetas PCI**, las **tarjetas PCMCIA** y las **tarjetas USB**.

Las tarjetas PCI para WiFi se agregan a los ordenadores de sobremesa. Las tarjetas PCMCIA son un modelo que se utilizó mucho en los primeros ordenadores portátiles, aunque están cayendo en desuso.

Las tarjetas USB para Wi-Fi se puede conectar a un ordenador, ya sea portátil o de sobremesa, haciendo uso de la tecnología USB.

Autoevaluación

Cuál de las siguientes afirmaciones es correcta:

- Para conectarme con un ordenador a una red inalámbrica necesito un adaptador de red Ethernet.
- Para conectarme con un ordenador a una red inalámbrica necesito una tarjeta de red Ethernet
- Para conectarme con un ordenador a una red inalámbrica sólo puedo hacerlo a través de un ordenador portátil.
- Para conectarme a una red cableada podemos utilizar una tarjeta USB como adaptador de red.

Opción correcta

Incorrecto

Incorrecto

Incorrecto

Solución

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

5. Dispositivos de interconexión para redes inalámbricas.

Caso práctico

"Antonio ve que Samuel ahora está subido en una escalera instalando un aparato nuevo por los pasillos de la academia, y no se resiste a preguntar que qué es eso:

- Samuel, ¿Qué es eso que estás poniendo en la pared?
- Ah, esto son los puntos de conexión a la red inalámbrica, serán los emisores de las ondas de la red inalámbrica que cualquiera de nuestros dispositivos podrán recoger.
- Claro, ahora ya me va quedando más clara la idea de donde surgen esas ondas, se necesitarán unos cuantos puntos de esos, ¿verdad?
- Sí, tenemos un radio de acción de cada punto de red inalámbrica y los colocaremos para abarcar toda la extensión de la academia.
- Muy bien, gracias otra vez por aclararme mis dudas".

Considera que para la emisión de ondas WiFi existen básicamente **dos tipos de dispositivos**, que son los routers WiFi y los puntos de acceso inalámbricos (WAP).

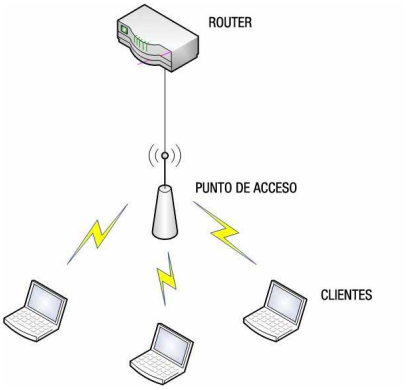
Un **punto de acceso inalámbrico** (WAP o AP por sus siglas en inglés: Wireless Access Point) en redes de ordenadores es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica. Normalmente un WAP también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cable y los dispositivos inalámbricos.

Sabrás que a pesar de que tradicionalmente los enrutadores solían tratar con redes fijas (Ethernet, ADSL, RDSI...), pero en los últimos tiempos han comenzado a aparecer

enrutadores que permiten realizar una interfaz entre redes fijas y móviles (WiFi). Un enrutador inalámbrico comparte el mismo principio que un enrutador tradicional. La diferencia es que éste permite la conexión de dispositivos inalámbricos a las redes a las que el enrutador está conectado mediante conexiones por cable. El **enrutador** o **encaminador** es un dispositivo de hardware para interconexión de red de ordenadores que opera en la capa tres (nivel de red) del modelo OSI. Un enrutador es un dispositivo para la interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes por ejemplo una red local y una red WAN.

Por último considera que los routers son los que reciben la señal de la línea ofrecida por el operador de telefonía. Se encargan de todos los problemas inherentes a la recepción de la señal, incluidos el control de errores y extracción de la información.

5.1. Puntos de acceso inalámbrico.



Ya sabrás que un **punto de acceso** conecta a los clientes o estaciones inalámbricas a la LAN cableada. Los dispositivos de los clientes no se comunican directamente entre ellos, sino que se comunican con el punto de acceso. Básicamente un punto de acceso hace la transformación de los datos de una red inalámbrica a una red cableada.

En una **red inalámbrica** los clientes deben asociarse con un punto de acceso para obtener servicios de red. La asociación es el proceso por el cual un cliente se une a una red 802.11. Este proceso es similar a conectarse a una red LAN conectada por cable.

Un **punto de acceso** es un dispositivo de capa 2 que funciona como un hub Ethernet 802.3. Las ondas que viajan por el aire lo hacen en un medio compartido y los puntos de acceso escuchan todo el tráfico. Al igual que con el Ethernet, los dispositivos que intentan utilizar el medio compiten por él. A diferencia de las tarjetas de red cableadas, con las tarjetas de red inalámbricas es muy costoso que puedan recibir y transmitir información al mismo tiempo, de modo que los dispositivos de radio no detectan colisiones.

La gestión de las **colisiones en las redes inalámbricas** las realizan los puntos de acceso inalámbricos. Se trata de un proceso de prevención de colisiones. Básicamente, cuando una estación quiere retransmitir, pide permiso al punto de acceso. Si no hay ninguna otra estación enviando información, entonces le permite realizar la operación. Si no deja en espera la petición hasta que esté libre el medio para transmitir. Esta técnica de gestión del medio se denomina CSMA/CA (Acceso múltiple con detección de portadora con prevención de colisiones).

Autoevaluación

Señala cual de las siguientes afirmaciones es correcta:

- Un punto de acceso inalámbrico es el equivalente a un hub en una red cableada.
- Un punto de acceso inalámbrico utiliza la técnica CSMA/CD, la misma que en las redes Ethernet.
- La gestión de las colisiones en un entorno inalámbrico la realizan

las propias estaciones.

- Un punto de acceso inalámbrico trabaja en la capa 3 del modelo OSI.

Opción correcta

Incorrecto

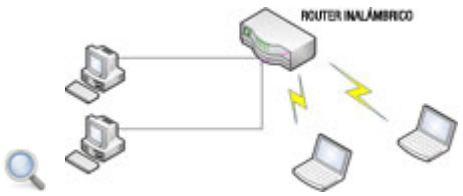
Incorrecto

Incorrecto

Solución

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

5.2. Router inalámbrico.



A estas alturas no te será difícil entender que los **routers inalámbricos** cumplen el rol de punto de acceso, switch Ethernet y router. Muchas veces nos encontramos en que son en realidad tres dispositivos en una sola caja. Primero está el punto de acceso inalámbrico, que cumple las funciones típicas de un punto de acceso. Después también cumple las funciones de switch ya que suele tener integrados una serie de puertos que proporcionan conectividad a los dispositivos conectados por cable para redes Ethernet. Finalmente provee la función de router para hacer de puerta de enlace a otras estructuras de red (conexión a Internet, por ejemplo).

El **enrutador**, **encaminador o router** es un dispositivo de hardware para interconexión de dispositivos en red que opera en la **capa 3 del modelo OSI**. Permite asegurar el encaminamiento de paquetes entre redes o determinar la mejor ruta que debe tomar un paquete de datos.

En la siguiente unidad veremos más detenidamente las características y funcionamiento de los routers.

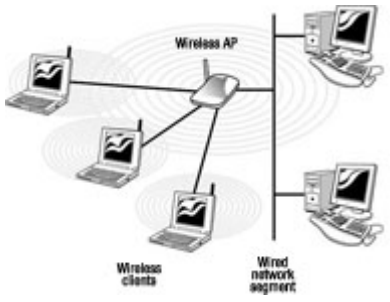
6. Configuración básica de los dispositivos de interconexión.

Caso práctico

Antonio ha estado hablando con Julia, la técnica superior en Administración de Sistemas Informáticos sobre que equitación será necesaria en la academia de Antonio:

- "Ya tiene claro cuáles son los elementos necesarios para que su red inalámbrica en la academia funcione perfectamente. Con un router inalámbrico en el armario principal de comunicaciones será suficiente.
- Vaya Antonio, siento contradecirte, pero además del router inalámbrico vamos a necesitar poner puntos de acceso inalámbricos por el resto de la academia.
- ¿Y cuál es el motivo, Julia? Pensé que con un solo aparato era suficiente.
- No, el problema es que el router inalámbrico tiene un radio de acción limitado y no es suficiente para toda la academia, es por eso que se hace necesario utilizar puntos de acceso para llegar a todos los rincones.
- La verdad, es que nunca dejas de aprender cosas nuevas…"

Al igual que Antonio en el caso práctico, tú tampoco dejarás de aprender cosas nuevas. En este capítulo verás una serie de prácticas que están relacionadas con la teoría que se ha ido comentando en este tema. La primera de las prácticas se trata de la instalación de una tarjeta de red. En esta práctica se ve la **instalación de una tarjeta de red cableada**, aunque el proceso es el mismo para una tarjeta de red inalámbrica.



La segunda práctica aborda la **configuración de un punto de acceso inalámbrico**. Es un proceso genérico que luego será diferente según la marca del punto de acceso en cuestión.

Y la última práctica se verá como se **configura una red inalámbrica**. Es probable que encuentres algún concepto no visto todavía en este curso, pero la lógica global de la práctica la entenderás bien.

6.1. Instalación de un adaptador de red.

Práctica 1: Instalación de un adaptador de red.

Fíjate que este proceso tiene dos partes diferenciadas, la instalación física de un adaptador de red (pasos 1 al 4) y la instalación lógica de la tarjeta (pasos 5 al 12).

La instalación física es un simple proceso de manipulación de equipo de hardware, mientras que la lógica supone la instalación de los **drivers**, elementos que crean un interfaz entre el sistema operativo del equipo y la tarjeta de red.

Cada dispositivo de un equipo dispone de drivers para el sistema operativo que permiten que los distintos dispositivos del ordenador se entiendan. El adaptador de red es el dispositivo de hardware que permite el acceso del PC a la red y la comunicación en ambos sentidos.

Debes conocer

Es necesario que veas esta práctica donde se ve como se realiza la instalación de un adaptador de red.

Instalación de un adaptador de red

Autoevaluación

En la instalación de un adaptador de red:

- La instalación física incluye instalar los drivers de la tarjeta de red.
- La instalación lógica incluye la conexión del dispositivo a la placa base.
- Los drivers de la tarjeta de red hay que instalarlos antes de pinchar la tarjeta en la placa base.
- La instalación de una tarjeta de red incluye una conexión lógica y

otra conexión física.

Incorrecto

Incorrecto

Incorrecto

Opción correcta

Solución

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

6.2. Configuración de un punto de acceso.

Caso práctico

Práctica 2: Configuración de un punto de acceso.

En esta práctica verás que se realizan las siguientes operaciones:

a. Conexión física del punto de acceso a la red local existente.
b. Establecimiento de la comunicación entre el punto de acceso y al menos uno de los equipos de su red.
c. Configuración de los parámetros de red local del punto de acceso.
d. Configuración de los ajustes de red inalámbrica.

Debes conocer

Además de la práctica anterior, es necesario que veas estos vídeos sobre la configuración de un punto de acceso Access Point

Resumen de texto alternativo

6.3. Creación de una red inalámbrica.

Práctica 3: Creación de una red inalámbrica.

Este último proceso que vas a ver ahora consta de tres partes bien diferenciadas:

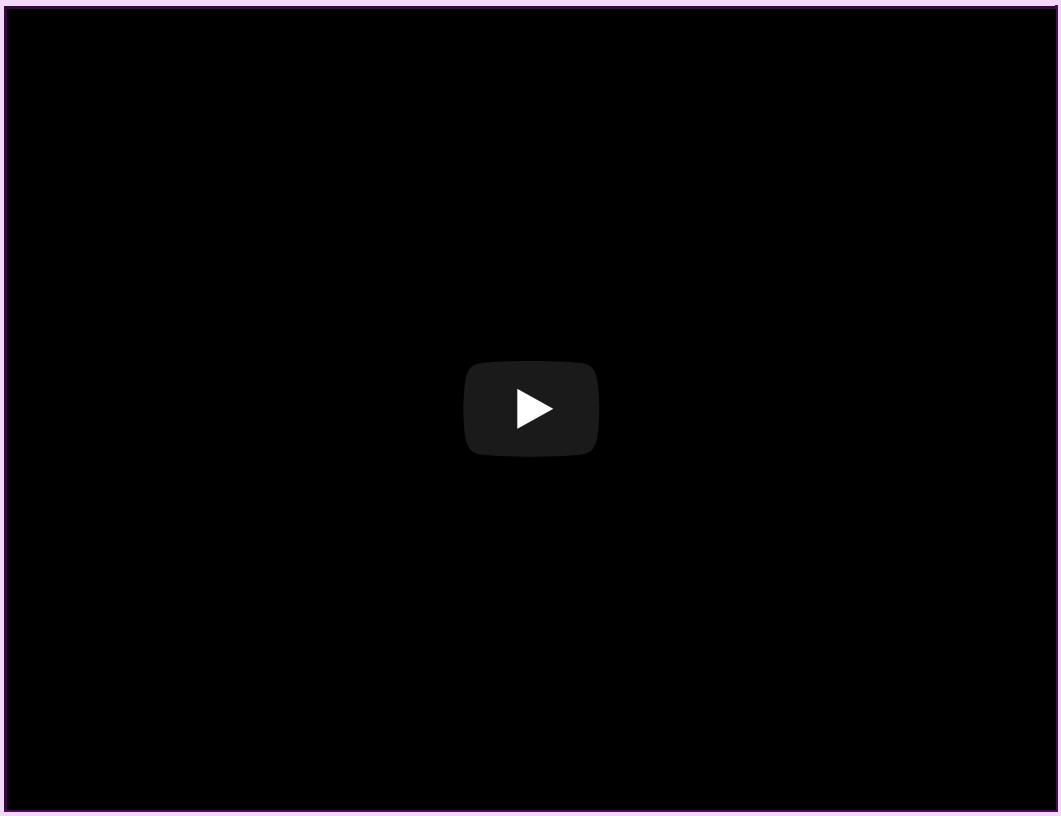
a. Configuración del punto de acceso.
b. Instalación de clientes inalámbricos.
c. Conexión a la red inalámbrica desde el cliente.

Debes conocer

Es necesario que veas esta práctica donde se ve como se realiza la instalación de una red inalámbrica.

Instalación de una red inalámbrica

Además de la práctica anterior, es necesario que veas estos artículos y vídeos sobre configuración de redes inalámbricas



Resumen de texto alternativo

Autoevaluación

En la configuración de una red inalámbrica:

- No es necesario configurar el punto de acceso.
- Los clientes tienen que tener instalados dispositivos de recepción para red inalámbrica.

- No supone una instalación física de ningún elemento extra respecto a una red cableada.
- Al instalar el punto de acceso, los clientes se conectan solos a la red sin necesidad de configurar la red desde el cliente.

Incorrecto

Opción correcta

Incorrecto

Incorrecto

Solución

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

7. Segmentación de redes. VLAN.

Caso práctico

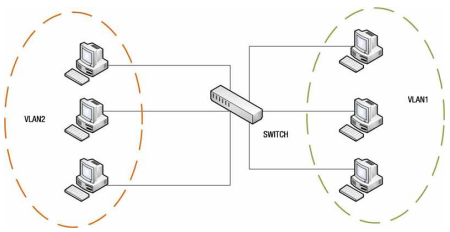
"Antonio sigue siendo un mar de dudas, y no tiene reparos en seguir comentándolas con Julia:

- Julia, ahora que ya tenemos planeada toda la instalación de la academia, ¿existe alguna posibilidad de tener en dos subredes separadas todo el tráfico que se gestiona en cada una de las aulas de manera independiente del tráfico que se genera en la oficina, con los expedientes de los alumnos, etc…?

- Claro que sí, Antonio. Un modo de poder hacer este tipo de segmentaciones en la red es a través de las VLAN, que son subredes virtuales que se realizan con un switch."

En este nuevo apartado del tema verás como se puede conseguir una segmentación de una red de área local gracias al uso de una red **VLAN**, o una red de área local virtual. Permitirá hacer dentro de la misma red distintos segmentos que sean independientes entre sí, de modo que se aumentará la seguridad dentro de la misma.

7.1. Definición de VLAN.



Seguro que identificas que el rendimiento de la red puede ser un factor en la productividad de la red que realice sus transmisiones en la forma prevista. Una de las tecnologías que contribuyen al excelente rendimiento de la red es la división de los grandes dominios de **broadcast** (segmento lógico de una red de ordenadores) en dominios más pequeños con las **VLAN**. Si estos dominios son más pequeños, limitamos el número de dispositivos que participan en el **broadcast** y permiten que los dispositivos se separen según la función que vayan a desempeñar.

Una **VLAN** te permitirá que un administrador de red cree grupos de dispositivos conectados a la red de manera lógica que actúan como si estuvieran en su propia red independiente, incluso, y aquí viene la novedad, aunque los nodos compartan una infraestructura común con otras VLAN. Cuando se configura una VLAN, puede ponerse un nombre para describir la función principal de los usuarios de esa VLAN. En el caso de la academia de Antonio podría ser “Alumnos”. Mediante las VLAN se puede segmentar de manera lógica las redes conmutadas basadas en distintas funciones. Si creamos otra VLAN en la academia llamada “Oficina”, el tráfico generado en una de las subredes no podrá ser interceptado por ningún equipo de la otra subred.

Como resumen de todo esto se puede decir:

- Una VLAN es una red LAN independiente.
- Una VLAN permite que los ordenadores de las distintas subredes estén **separadas**, aunque comparten el mismo cableado, switches, etc… es decir, que comparten la misma infraestructura.
- Se le puede **otorgar un nombre** a la VLAN para facilitar su identificación.

Autoevaluación

En una red de área local de ordenadores:

- Podemos segmentar la red con el uso de VLAN.
- Si la dividimos en dos VLAN, podrán enviarse datos a través de switch.
- No hay manera posible de segmentar la red sin ampliar la infraestructura de la red.

- Si tenemos dos VLAN, tendremos un solo dominio de difusión.

Opción correcta

Incorrecto

Incorrecto

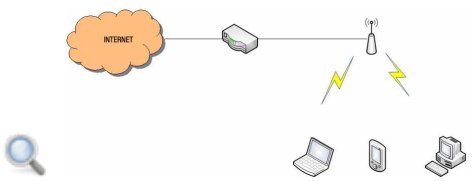
Incorrecto

Solución

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

7.2. Ventajas de las VLAN.

Es evidente que este esfuerzo extra que te puede suponer la implantación de una VLAN dentro de una red de área local es porque a su vez consigues una serie de beneficios. Los más importantes son los que ahora se detallan:



- **Seguridad**: los grupos que tienen datos sensibles se separan del resto de la red, disminuyendo las posibilidades de que ocurran violaciones de información confidencial.
- **Reducción de coste**: el ahorro en el costo resulta de la poca necesidad de actualizaciones de red caras y más usos eficientes de enlaces y ancho de banda existente.
- **Mejor rendimiento**: la división de las redes planas de capa 2 en grupos lógicos de trabajo (dominios de broadcast o dominios de difusión) reduce el tráfico innecesario en la red y potencia el rendimiento.

7.3. Tipos de VLAN.

Debes conocer

Debes conocer que existen fundamentalmente una manera de implementar las VLAN: VLAN basada en puerto. Se asocia cada VLAN con un puerto denominado acceso VLAN.

Sin embargo, en las redes existe una cantidad de términos para las VLAN. Algunos términos definen el tipo de tráfico de red que envían y otros definen una función específica que desempeña una VLAN. Veremos la terminología común de VLAN:

- **VLAN de datos**: es una VLAN **configurada para enviar sólo tráfico de datos** generado por el usuario. Una VLAN podría enviar tráfico basado en voz o tráfico utilizado para administrar un switch, pero este tráfico no sería parte de una VLAN de datos. Es una práctica común separar el tráfico de voz y de administración del tráfico de datos. A este tipo de VLAN también se la puede denominar VLAN de usuario.
- **VLAN de administración**: es cualquier VLAN que se configura para acceder a las **capacidades de administración** de un switch.
- **VLAN predeterminada**: todos los puertos del switch se convierten en un miembro de la VLAN predeterminada después del arranque inicial del switch. Hacer participar a todos los puertos de switch en la VLAN predeterminada hace que todos formen parte del mismo dominio de difusión.

Autoevaluación

En las VLAN:

- En una VLAN de datos se puede enviar tráfico de administración del switch.

  Aumenta la seguridad en la red al tener tráfico segmentado.

- En una VLAN de administración está configurada para enviar datos de usuarios de unos a otros.
- El uso de una VLAN no implica una mayor seguridad en el uso de la red.

Incorrecto

Opción correcta

Incorrecto

Incorrecto

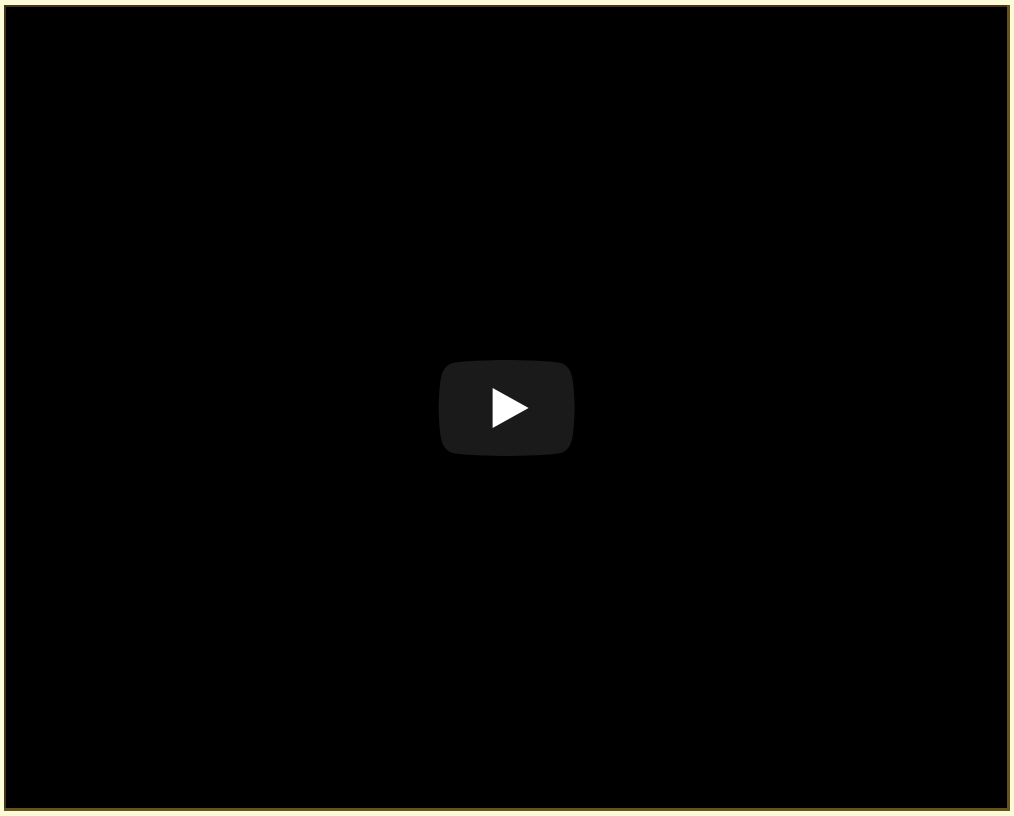
Solución

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

Para saber más

Video explicativo sobre las LANs virtuales I:

Video explicativo sobre las LANs virtuales II:



Video explicativo sobre las LANs virtuales:

Resumen de texto alternativo

8. Recursos de ampliación del tema.

Una vez que ya has terminado el tema actual, vamos a aprovechar una serie de recursos existentes en la red para afianzar o recordar algunos de los conceptos vistos en este tema y en anteriores. Todos los contenidos de este apartado son de ampliación de este tema aunque han aparecido en apartados anteriores o en temas anteriores como contenidos obligatorios.

El primer grupo de recursos trata sobre los dominios de colisión y dominios de difusión. Es importante que tengas claros estos conceptos, por lo que te proponemos que te tomes un tiempo para leer estos dos artículos y que veas un vídeo explicativo.

Para saber más

Artículo sobre los dominios de colisión

Dominio de colisión.

Artículo sobre los dominios de difusión

Dominio de difusión.

Video explicativo sobre dominios de colisión y difusión:

Resumen de texto alternativo.

Para terminar el tema te resultará interesante hacer un repaso general a todos los contenidos tratados en la unidad. Una buena manera de recordar mejor lo que has estudiado será a través del visionado de los siguientes vídeos sobre redes WIFI y un par de artículos sobre estas redes.

Para saber más

Artículo explicativo sobre las redes inalámbricas:

Artículo de las redes inalámbricas.

Artículo explicativo sobre WIFI:

Artículo de WIFI.

9. La seguridad de la red.

¿Conoces el término **hacker**? Aunque no esté todavía en el diccionario de la Real Academia, podemos buscar en cualquier diccionario inglés-español para encontrar la traducción: pirata informático.

El perfil del **pirata informático** ha cambiado en estos años. En un principio eran grandes programadores (como el propio Morris), que trabajaban en solitario o conectados a BBS. Los BBS están hoy anticuados y sustituidos por los foros, pero tuvieron un gran uso entre desarrolladores de software como lugar de intercambio de ficheros.

De esa clandestinidad, hemos pasado hoy a auténticos grupos de hackers, como Chaos Computer Club. La característica que define a estos modernos piratas es la de disponer de ordenadores muy potentes, con programas especializados en realizar ataques, aunque no disponen de unos conocimientos informáticos (en general) tan sumamente avanzados como los pioneros. Además, disponen de cantidades ingentes de información colgada en la red.

¿Qué tipos de Hackers existen?

La clasificación general está compuesta por tres tipos: **Black Hat,** **Grey Hat** **y** **White Hat** pero con el paso de los años ha ido diversificando los tipos hasta formar una larga lista, los principales serían:

- **Black Hat,** llamados también **Ciberdelincuentes**. Estos hackers acceden a sistemas o redes no autorizadas con el fin de infringir daños, obtener acceso a información financiera, datos personales, contraseñas e introducir virus. Dentro de esta clasificación existen dos tipos: **Crackers y** **Phreakers**, los primeros modifican softwares, crean malwares, colapsan servidores e infectan las redes, mientras que los segundos actúan en el ámbito de las telecomunicaciones.
- Para los **Grey Hat** su ética depende del momento y del lugar, prestan sus servicios a agencias de inteligencia, grandes empresas o gobiernos, divulgan información de utilidad por un módico precio.
- **White Hat** o Hackers éticos, se dedican a la investigación y notifican vulnerabilidades o fallos en los sistemas de seguridad.
- Los **Newbies** no tienen mucha experiencia ni conocimientos ya que acaban de aterrizar en el mundo de la ciberseguridad, son los novatos del hacking.
- Los **Hacktivista** ha crecido en los últimos años en número, utilizan sus habilidades para atacar a una red con fines políticos, uno de los ejemplos más representativos sería Anonymous.

Para saber más

¿Quieres conocer más detalles acerca de los hackers? En el enlace te facilitan información acerca de uno de los grupos más activos en la actualidad. El Club de Computación Caos es la mayor asociación de hackers de Europa.

El Chaos Computer Club.

Autoevaluación

Los modernos piratas informáticos se caracterizan por:

- Pertenecer a BBS.
- Tener grandes conocimientos de programación.
- Tener ordenadores muy potentes.

No es correcta. La subscripción a boletines de noticias no se suele utilizar hoy en día, habiéndose sustituido por los foros.

No es la respuesta correcta. En general, los piratas no son grandes programadores.

Correcta. Aunque no es habitual el tener grandes conocimientos informáticos, los piratas se caracterizan por poseer equipos con altas prestaciones.

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta

9.1. Delitos informáticos.

¿Sabrías decir qué es un delito informático? ¿Crees que en alguna ocasión has podido cometer alguno?

Podemos definir como delito informático aquél que ha sido cometido por vía telemática y cuya investigación se sustenta en la prueba informática. Han sido diversos los intentos de tipificar los delitos informáticos, siendo uno de los más ampliamente ratificados el realizado por el Consejo de Europa en el **Convenio de Ciberdelincuencia** (Budapest, 23 noviembre 2001). En él, se establece la siguiente clasificación:

Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:

- Acceso ilícito.
- Interceptación ilícita.
- Ataques a la integridad de los datos.
- Ataques a la integridad del sistema.
- Abuso de los dispositivos.

Falsificación y fraude informático:

- Alteración, borrado o supresión de datos informáticos para generar datos no auténticos (falsificación).
- Alteración, borrado o supresión de datos informáticos para la comisión de fraude.
- Interferencia en el funcionamiento de un sistema informático.

En nuestro país, la legislación más reciente en relación a los delitos informáticos es la que aparece en la reforma del código penal, que entró en vigor el 23 de diciembre de 2010. En ella se especifican los siguientes tipos de delitos informáticos:

- Borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos o programas informáticos ajenos.
- Obstaculizar o interrumpir el funcionamiento de un sistema de información ajeno.
- Acceder sin autorización, vulnerando las medidas de seguridad, a datos o programas informáticos contenidos en un sistema informático o en parte del mismo.

Como se desprende del primer y el segundo tipo, queda tipificado como delito (y por consiguiente aparejada pena para el o los causantes) el ataque de denegación de servicio. El tercer tipo, considera delito a aquellas intromisiones en un sistema informático de manera no consentida, independientemente de si causan o no perjuicios al propietario del equipo. Podríamos citar como ejemplo el acceso a la red social o al correo electrónico de una persona sin su permiso, no siendo eximente el que tengan establecidas las contraseñas por defecto o se aprovechen de las

vulnerabilidades conocidas.

Para saber más

En nuestro país, la unidad de delitos informáticos de la Guardia Civil se encarga de investigar aquellos delitos cometidos a través de Internet.

Delitos informáticos.

¿Qué dice la legislación vigente en nuestro país acerca de los delitos informáticos? En esta web te detallan los artículos que rigen cada delito y las penas asociadas.

Delitos informáticos y Código Penal español.

9.2. Vulnerabilidades (I).

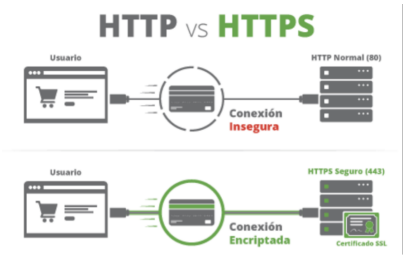
Entendemos por vulnerabilidad la debilidad inherente a la red y a los dispositivos que la forman. Vamos por el momento a posponer las vulnerabilidades propias de una mala configuración de los dispositivos (elección de contraseñas no seguras o no encriptadas, o incluso utilización de nombre de usuario y contraseña por defecto, etc.) que trataremos posteriormente y nos vamos a ceñir a aquellas vulnerabilidades propias del hardware y del software utilizado. A ese tipo de vulnerabilidad se le suele llamar tecnológica.

Las causas de la vulnerabilidad tecnológica se pueden agrupar en tres categorías:

- **Vulnerabilidad de los protocolos TCP/IP:**

  El protocolo HTTP (Hypertext Transfer Protocol, **Protocolo de transferencia de hipertexto)** es un protocolo utilizado en internet para la visita de las páginas web, **es inseguro**. Una de sus debilidades más notables es la posibilidad de que el que solicita la página (cliente) entregue información mediante un programa (código) al servidor de la página web. Normalmente, este código es necesario para formatear de manera adecuada tanto los datos subidos como los bajados, pero presenta un agujero de seguridad importante que **puede poner en peligro al servidor**. Los programas que explotan esta vulnerabilidad suelen estar escritos en lenguaje C. Existen un gran número de ellos y se pueden clasificar atendiendo al tipo específico de servidor que atacan (pop3, smtp, ftp, etc.). Desde estas líneas te desaconsejo la búsqueda de estos programas (conocidos como exploits) en Internet. Ya te hemos indicado que los ataques son delitos informáticos que nunca debes usar contra nadie. Además corres el riesgo de que posiblemente el primer daño te lo hagas inconscientemente a ti mismo.

- **El protocolo HTTPS** (HyperText Transfer Protocol Secure, **Protocolo de transferencia de hipertexto**) es un protocolo de comunicación de Internet **seguro**, el cual protege la integridad y la confidencialidad de los datos de los usuarios entre sus ordenadores y el sitio web. Dado que los usuarios esperan que su experiencia online sea segura y privada. Los certificados SSL/TLS son necesarios para cualquier sitio web que maneje información confidencial, ya que garantizará la seguridad en la transmisión de datos al ser cifradas. Estos **certificados SSL/TLS** funcionan al vincular digitalmente una **clave criptográfica** a la información de identificación de una empresa. Esto les permite cifrar las transferencias de datos de tal manera que no puedan ser descifrados por terceros.

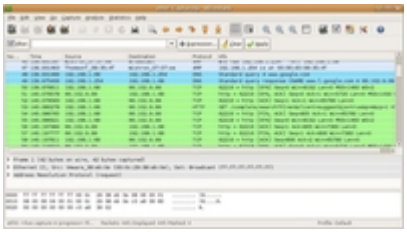


  Los datos que se envían mediante HTTPS están protegidos con el protocolo *Seguridad en la capa de transporte* (**TLS**), ofreciendo estas tres capas clave de seguridad:

- **Cifrado:** se cifran los datos intercambiados para mantenerlos a salvo de miradas indiscretas. Eso significa que cuando un usuario está navegando por un sitio web, nadie puede "escuchar" sus conversaciones, hacer un seguimiento de sus actividades por las diferentes páginas ni robarle información.
- **Integridad de los datos:** los datos no pueden modificarse ni dañarse durante las transferencias, ni de forma intencionada ni de otros modos, sin que esto se detecte.
- **Autenticación:** demuestra que tus usuarios se comunican con el sitio web previsto. Proporciona protección frente a los ataques "man-in-the-middle" y contribuye a la confianza de los usuarios, lo que se traduce en otros beneficios empresariales.

- **El protocolo FTP** es también inseguro. Al utilizarse, transmite en texto plano (sin encriptar) tanto el nombre de usuario como la contraseña, por lo que un atacante puede conseguirlos a través analizadores de paquetes (como Wireshark). Telnet se ve afectado por el mismo problema. Para solucionar el problema de la confidencialidad (cifrado de los datos) en la autenticación y en la transferencia de datos, se decidió añadir una **capa de seguridad SSL/TLS** al propio protocolo FTP. **FTPS** (se le conoce como FTPS implícito), con este protocolo el cliente FTP se conecta a un puerto distinto al puerto TCP 2**, y FTPES** (se le conoce como FTPS explícito), con este protocolo el cliente FTPES se conecta al puerto TCP 21 del servidor. FTPS y FTPES también se conocen como FTP over TLS/SSL, y están basados en el propio protocolo FTP.

  En cuanto al **protocolo TCP**, un tipo específico de ataque se basa en la negociación asociada al establecimiento de una sesión. Son los ataques de denegación de servicio que estudiaremos posteriormente.



- El protocolo **SFTP (SSH File Transfer Protocol)** o también conocido como transferencia de ficheros SSH, es un protocolo que no tiene nada que ver con el protocolo FTP. SFTP **no es la versión segura del protocolo FTP**, ya que está basado en el protocolo SSH por completo. Este protocolo SFTP nos permite autenticarnos y realizar transferencia de ficheros entre equipos como si fuera un servidor FTPES, pero utilizando criptografía del protocolo SSH que tengamos instalado en el servidor de archivos. SFTP tampoco es un protocolo donde FTP utilice SSH para asegurar la conexión, es un protocolo completamente nuevo basado en SSH y no en FTP. El protocolo SFTP hace uso del **puerto TCP 22 por defecto**, el mismo que el protocolo SSH.

Recomendación

En el siguiente enlace puedes ver las diferencias entre los protocolos FTP, FTPS Y SFTP:

Diferencias entre los protocolos FTP, FTPS Y SFTP.

Para saber más

En el siguiente enlace puedes ampliar la información sobre los tipos de Exploits:

Tipos de exploits.

Autoevaluación

La vulnerabilidad del protocolo FTP proviene de que:

- Transmite en texto plano (sin encriptar) tanto el nombre de usuario como la contraseña.
- Transmite el nombre del usuario y la contraseña encriptados.
- Necesita para ejecutarse del analizador de paquetes Wireshark.
-

Correcta. Al transmitir sin encriptar, dichas informaciones pueden ser visualizadas con un analizador de paquetes.

No es correcta. En realidad, esta sería una virtud.

Incorrecto

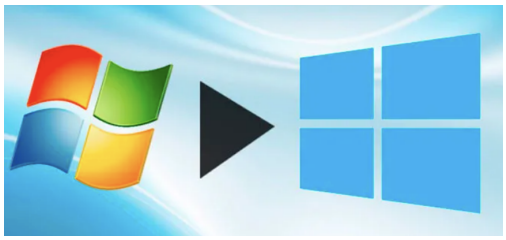
No es la respuesta correcta. De hecho, Wireshark es una herramienta que explota la vulnerabilidad de FTP.

Solución

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

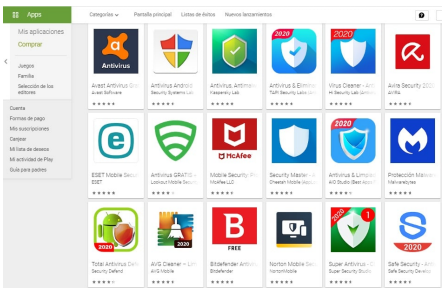
9.2.1. Vulnerabilidades (II).

Ya hemos visto que los protocolos usados en las redes son una fisura en lo que a la seguridad de las redes se refiere, pero **¿hay otras causas que pueden hacer insegura una red?** La respuesta es sí. Vamos a analizarlas a continuación.



- **Vulnerabilidad de los sistemas operativos:** Los modernos sistemas operativos, al tener como una de sus prioridades la fecha del lanzamiento comercial, suelen ser productos no del todo acabados. Todos tenemos la experiencia de la compra de un ordenador, la primera puesta en marcha (con la consiguiente configuración personal) y el primer acceso a Internet. Si hemos activado las actualizaciones del sistema operativo se nos descargará una cantidad enorme de archivos que en su mayor parte tienen como misión la corrección de amenazas de seguridad. Esos archivos son conocidos como parches y su descarga e instalación es la forma más recomendable de combatir esos defectos.

  Además, con el fin de proteger el sistema operativo y el resto de programas y datos instalados, es necesaria la instalación de un **antivirus**. El antivirus puede ser gratuito (de hecho, algunos de los antivirus que aparecen como más efectivos en los análisis de las revistas especializadas lo son) o de pago. En cualquier caso, tan importante como su instalación es la sucesiva actualización, para estar protegido de los virus más recientes.



- **Vulnerabilidad de los equipos:** los equipos utilizados en las redes (routers, switches, firewalls, etc.) sufren de vulnerabilidades entre las que podemos destacar el uso de contraseñas por defecto o no seguras, bien sea por ser fáciles de adivinar o ser transmitidas a través de la red sin encriptar. En este mismo grupo estarían aquellas configuraciones mal realizadas, como listas de control de acceso inadecuadas a la protección que se desea o acceso a Internet permitiendo el uso de JavaScript. Este último caso está casi siempre activado por defecto (compruébalo en tu ordenador).

- **Un script de Java** es utilizado principalmente en el cliente (ordenador que pide visitar una página web). **Es un programa similar a C** que se utiliza para mejorar la interface de usuario. Sin embargo, puede ser utilizado por atacantes, cosa que suele ocurrir al visitar sitios de Internet no confiables.

10. Tipos de ataques.

Sabemos que tanto los equipos como los programas que se ejecutan en ellos no son seguros al cien por cien. Una vez identificadas las principales vulnerabilidades en el apartado anterior, vamos a ponernos en la piel de un pirata. **¿Por dónde empezaríamos?** En la seguridad es muy importante pensar como lo haría un atacante. De hecho, muchos de los grandes especialistas mundiales en seguridad estuvieron en el pasado en el lado de los agresores.

Podemos clasificar los ataques a las redes en cuatro grandes apartados:

- **Reconocimiento:** en general, no causan ningún daño. Tratan de **conseguir información** acerca de organizaciones y de los equipos y el software que utilizan (normalmente para utilizar otro tipo de ataque).
- **Acceso:** ataque mediante el cual, un usuario **accede a un equipo informático** del que no posee ni cuenta (login) ni contraseña (password). Para ello, son utilizados programas que se **aprovechan de las vulnerabilidades** y de las **malas configuraciones de los equipos.**
- **Denegación de servicio:** su objetivo no es acceder al sistema sino **afectar a su funcionamient**o hasta el punto de hacerlo totalmente inoperante.
- **Malware:** con este nombre se suele designar al software malicioso o programas que se instalan y dañan el ordenador sin que el usuario perciba su existencia.

Pasamos a continuación al **estudio detallado de estos ataques.**

10.1. Reconocimiento.

Como hemos adelantado, el primer tipo de ataque de un intruso hacia una red es el reconocimiento o estudio. El objetivo es recopilar información del destino del ataque como el tipo de organismo o empresa de que se trata, dominios asociados, servidores que utiliza, tipo de servicios ofrecidos por los servidores o plataforma sobre la que dichos servidores trabajan.

En el primero de los casos, se utiliza normalmente Internet. Cualquier organismo o empresa que se precie, tiene hoy en día su página web. A partir de la dirección textual o URL y con una herramienta como **ping** o **nslookup** es posible identificar la dirección IP del servidor objeto del ataque.

Una vez obtenida esa información y mediante el uso del comando **fping** se podrá saber la dirección IP de los equipos disponibles en la red. fping no está incluido entre los comandos suministrados por Windows o Linux, pero es una utilidad que puede ser descargada de la red.

Para saber más

El uso de **fping** con fines educativos es más que recomendable. Imagina que estás tratando de poner de manera estática la dirección IP de un equipo en una red en la que desconoces cuántas direcciones han sido ya utilizadas.

Puedes descargar una versión para Windows de la dirección que aparece en el enlace. Una vez descomprimido el archivo, te sugiero lo muevas a la **carpeta C:\WINDOWS\SYSTEM32**, con el fin de que lo puedas ejecutar desde el modo comando (**Ejecutar-> cmd**). La sintaxis es **fping –g host1/host2**, donde host1 y host2 representan la dirección inicial y final que quieres explorar.

Fping.

Para conocer los servicios de red ofertados por los servidores objetivos, los atacantes utilizan programas que escanean los **puertos (port-scanners).**

Para las direcciones IP encontradas en el paso previo, un escáner de puerto identifica aquellos puertos que están abiertos y recopila información acerca del tipo y versión del sistema

operativo y del tipo y versión del servicio. Al atacante solo le queda contrastar con las vulnerabilidades conocidas del software que ha descubierto para proceder al ataque. Programas de este tipo son UPSEROS, Sygate o Grc.

Los escáners de puertos utilizan el proceso que se sigue en toda conexión TCP. Así envían un gran número de paquetes SYN, utilizados como primer paso para establecer conexión, a diversos puertos del equipo destino.

Te recuerdo que una conexión TCP queda definida por una IP y un número de puerto y que el conjunto de esos dos datos se denomina socket. El equipo distante puede responder con un paquete SYN/ACK (con lo que el puerto en cuestión está abierto) o bien responder con un RST (indicando que el puerto está cerrado).

En este caso, el escáner de puertos responde con un RST/ACK terminando la conexión y evitando de esta manera que quede algún registro del ataque. En el caso de que el puerto esté filtrado, por ejemplo por un firewall, se generará un paquete ICMP indicando la incidencia.

Para saber más

Nmap no sólo es una herramienta utilizada por hackers. Un buen administrador de red puede aprovechar la potencia del programa para detectar vulnerabilidades (de la misma forma que haría un hacker) y proceder en consecuencia. El enlace te permitirá conocer con mayor detalle el programa e instalarlo en tu ordenador.

Nmap, un programa de escaneo de puertos.

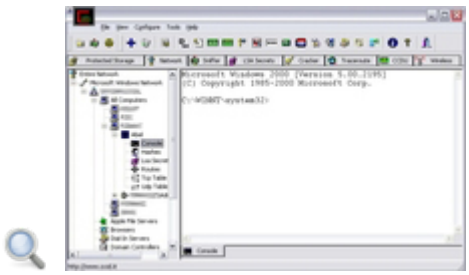
10.2. Acceso.

Suele ser precedido por un ataque de reconocimiento. Con los datos obtenidos en él, el atacante trata de acceder al objetivo, intentando diversas técnicas. Mediante el ataque por acceso, el atacante obtiene los privilegios para entrar de manera ilícita en un equipo.

Algunas de las formas más comunes son:

- **Uso de las vulnerabilidades conocidas.** Hemos adelantado ya los tipos de vulnerabilidades y cómo su conocimiento puede ser utilizado para conseguir acceder a un equipo.

- **Debilidad de las contraseñas.** Al hablar de las vulnerabilidades de los equipos, hemos tratado las contraseñas no seguras. Existen ataques que tratan de adivinar la contraseña de acceso a los equipos. Algunos son los llamados **ataques de diccionario**, que prueban las palabras contenidas en el diccionario como posibles contraseñas. Muchos usuarios eligen contraseñas sencillas, palabras cortas con significado, por lo que este ataque ser efectivo. Otros ataques, más sofisticados, recurren a combinaciones de caracteres para encontrar la contraseña. Evidentemente, si se conociera la longitud de la contraseña, sería un gran avance. Por eso se recomienda el uso de contraseñas largas, de al menos ocho caracteres, que incluyan letras mayúsculas, minúsculas, números y caracteres especiales (como "@" o "#"). Es muy recomendable el cambio de las contraseñas, al menos cada tres meses. Un ejemplo de software especializado en encontrar contraseñas para Windows es Cain & Abel, también existen otras como Ohpcrack, Offline NT Password & Registry Editor (ONTP & RE), Kon-Boot, LCP, John the Ripper, etc.



- **Servicios mal configurados.** Podemos poner como ejemplo el uso de FTP anónimo que puede facilitar un uso abusivo del servicio.

- **Ataque Hombre en el medio (Man in the middle, MITM)**. Un ataque MITM es aquél en el que el atacante logra leer, modificar y crear mensajes entre dos equipos, sin que ninguno de ellos se percate de que la conversación está siendo alterada y/o escuchada.

Para saber más

En la siguiente página puedes ver más información sobre la herramienta de recuperación de contraseñas para Windows Caín y Abel:

Caín y Abel

Los ataques Hombre en el medio son uno de los más utilizados como medio de acceder a equipos de los que no se dispone de permisos. En la dirección de la página web que te proporcionamos, te explican con más detalle los tipos de ataque MITM más comunes.

Ataques MITM.

Autoevaluación

¿Qué programa nos informa de los puertos que tiene abiertos nuestro equipo?

- nslookup.
- fping.
- Cain&Abel.
- NMAP.

No es correcta. nslookup proporciona la IP de uno o varios equipos de los que sabemos su dirección textual.

No es la respuesta correcta. fping muestra las direcciones IP de los equipos que están conectados a una red.

Incorrecta. Es un programa de búsqueda de contraseña.

Correcta. Nmap o su … versión on line.

Solución

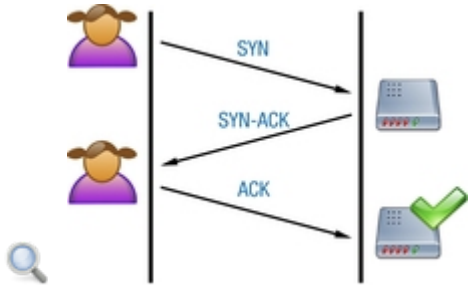
1. Incorrecto
2. Incorrecto
3. Incorrecto
4. Opción correcta

10.3. Denegación de servicio.

A diferencia de los ataques de acceso, en los que el objetivo perseguido es entrar en un equipo sin disponer de permiso para ello, los de denegación de servicio tienen por misión impedir que un determinado equipo pueda funcionar de manera correcta.

Son muchas las posibilidades de conseguir que un equipo deje de prestar servicios a su usuario. Entre otras, podemos citar:

- Solicitar de forma remota tareas que consuman gran cantidad de recursos de equipo atacado (memoria, disco duro, procesador, etc.). Un ejemplo es el ataque **SYN Flood**. Cuando dos equipos acuerdan una sesión TCP, lo hacen mediante un procedimiento de tres vías. En la primera, el equipo que solicita la conexión envía un paquete SYN. En la segunda, el equipo responde con un paquete SYN/S. Por último, el equipo solicitante responde con un paquete ACK y a partir de ese momento se puede empezar la transferencia de datos. El ataque consiste en no enviar la última fase (el paquete ACK) con lo que el equipo atacado queda a la escucha, consumiendo recursos. El protocolo da por cerradas aquellas conexiones que no reciben el ACK de confirmación transcurrido un cierto tiempo, por lo que el ataque se basa en el envío o inundación (flood) de la secuencia descrita.



- Generar gran cantidad de tráfico hacia un equipo de la red, normalmente desde varios equipos atacantes. Un tipo especial de este ataque es el conocido como **mail bombing** consistente en envíos de gran cantidad de correos electrónicos que pueden colapsar el servidor de correo atacado. Otro tipo importante es el ataque **Connection Flood** que trata de anular un servidor, mediante la solicitud de cientos o miles de conexiones simultáneas desde distintos equipos. El problema viene de que un servicio tiene un límite máximo de conexiones simultáneas. Una vez alcanzado ese límite no se admiten nuevas conexiones. A diferencia del anterior ataque, existe un registro de quién lo ha efectuado, ya que se ha completado el procedimiento de las tres vías. Otro caso es el ataque pitufo (**smurf**). Está basado en la generación de gran cantidad de paquetes ICMP (**ping**), cuya dirección origen es modificada para incluir la del equipo víctima y la destino es la dirección de difusión de la red objeto de ataque. La consecuencia es que el equipo atacado se ve sobrecargado con la atención de dichos paquetes y la generación de los consiguientes ecos, que suelen conducir al colapso.

- Generar paquetes de datos que hayan sido manipulados con el fin de que el equipo destino se cuelgue o disminuya de forma apreciable su rendimiento. Un ejemplo es el ataque **Supernuke** o **Winnuke**. Sus objetivos son equipos cuyo

sistema operativo es Windows y que tengan abierto los puertos 137 al 139. Al recibir paquetes UDP manipulados, la máquina atacada disminuye su rendimiento e incluso se puede colgar. Otro ejemplo es **Land Attack**, que explota un fallo de implementación de Windows, en concreto de la pila TCP/IP. El ataque consiste en el envío de un paquete en el que la dirección y el puerto origen coinciden con la dirección y el puerto destino. El resultado suele ser el cuelgue del equipo.

Debes conocer

En la dirección de la web que sigue encontrarás más información sobre los ataques de denegación de servicio. Recuerda que esta información es evaluable.

Ataques de denegación de servicio.

10.4. Denegación de servicio distribuido.

El ataque de denegación de servicio distribuido (DDoS) es producido por un gran número de equipos previamente comprometidos que atacan un equipo destino, produciendo la denegación de servicio por insuficiencia de los recursos disponibles. Lo que caracteriza a este tipo de ataques es que son generados por zombis. Un zombi es un equipo que ha sido infectado por malware, normalmente por un virus o un troyano. El usuario del equipo no tiene constancia de la infección que tiene por resultado la apertura de backdoors o puertas traseras. A través de ellas, los intrusos consiguen el control del equipo infectado y el que éste sea utilizado para generar ataques de denegación de servicio.

Cuando el malware se ha instalado en cientos o miles de equipos, es el momento para que el intruso desate el ataque. Los usuarios legítimos de los equipos ni siquiera sospechan que otros usuarios los estén utilizando para fines perversos. La confirmación de que el equipo en cuestión es un zombi suele provenir del proveedor de servicios de Internet que suministra el acceso al equipo infectado. En efecto, cuando un equipo es utilizado para participar en un ataque (con o sin el consentimiento de su dueño) los ISP notifican el hecho. En caso de que éste se repita, pueden determinar la suspensión del servicio.

Podemos clasificar los ataques DDoS en dos grandes grupos:

- **Ataques preprogramados:** mediante un virus informático se infecta un grupo de ordenadores, cuanto más numeroso mejor. Cuando llega el instante de tiempo para el que se ha programado el ataque, éste se produce. Un ejemplo es el virus Mydoom, que utilizaba el correo electrónico para instalarse en los ordenadores y tuvo por objetivo SCO (la empresa que demandó a Linux por el uso de Unix) y que se produjo el 1 de febrero de 2004.

- **Ataques por control remoto:** un **troyano** es instalado en múltiples ordenadores para, llegado el momento, ejecutar un ataque DoS contra el objetivo elegido. Habitualmente se utiliza una estructura de capas, en la que el atacante infecta a equipos maestros. Una vez infectado el maestro y mediante el uso de rutinas automatizadas cada maestro infecta a ordenadores de su misma red. Estos ordenadores son denominados esclavos y son los ejecutores reales del ataque.

  Ejemplos de programas utilizados para DDoS son TRIN00, Tribe Flood Network, Shaft y Stacheldraht.


Internet

10.5. Malware.

¿Sabes que lo que la gente denomina virus informáticos es en realidad malware? La palabra **malware** es una contracción de malicious software que podríamos traducir al español como programa malicioso. Se trata de programas en general de pequeño tamaño que se infiltran en el ordenador sin que el usuario se dé cuenta de ello y cuyo fin puede ir desde molestar (por ejemplo, haciendo que la pantalla muestre el contenido al revés) a inutilizar totalmente un equipo o borrar todo su contenido.

Podemos **clasificar al malware** en virtud de los mecanismos que utiliza para infiltrarse y por los daños que causa. Así, tenemos los siguientes:

- **Virus informático.** Es aquel tipo de malware que, una vez introducido en el ordenador, infecta otros archivos ejecutables. La misión del virus es variada, pudiendo ir de las bromas a la destrucción de archivos. El virus necesita la intervención del usuario para ser instalado, por lo que normalmente se enmascara la instalación de una manera u otra.

- **Adware.** Son programas relativos a la **publicidad** que a menudo se nos instala en nuestros **navegadores** o incluso como ventanas emergentes, usualmente se instalan junto con la instalación de programas gratuitos. Este tipo de software es menos nocivo para nuestro ordenador, pero puede afectar al rendimiento de nuestro equipo.

- **Spyware o software espía.** Este tipo de programas recopilan información de las páginas web que frecuenta el usuario del programa donde se instalan, para después enviarla a agencias de publicidad. También pueden acceder a la lista de direcciones del correo electrónico para enviarles spam. Este software, se inicia con nuestro equipo y recopila toda la información posible en nuestro ordenador para transmitirla a otro equipo anónimo, afectando a nuestra privacidad, rendimiento de nuestro dispositivo y recursos de red.

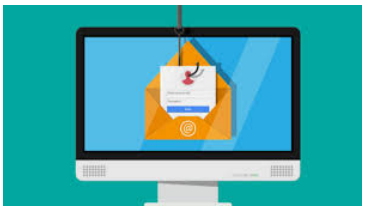
- **Gusano.** Es el malware que persigue multiplicarse e infectar el mayor número posible de ordenadores de una red para ralentizar su funcionamiento. El gusano puede llegar a colapsar la red, haciéndola inoperante. A diferencia del virus, el gusano se propaga sin intervención del usuario. Una vez introducido en un ordenador (muy comúnmente, a través del correo electrónico) el gusano se retransmite, tomando direcciones de correo electrónico de la lista de contactos del ordenador invadido.

- **Troyano.** Es aquel programa malicioso escondido habitualmente en otros programas (como utilidades para el ordenador, presentaciones de diapositivas,

etc.). La finalidad de un troyano es el establecimiento de una puerta de entrada en el ordenador infectado para que otro usuario (a través de la red) acceda. Las consecuencias van desde el robo de la información almacenada al control total del equipo de manera remota.

- **Spam o correo basura.** Consiste en el envío masivo de correos, casi siempre con fines publicitarios. Otra finalidad del correo basura es la saturación de los servidores de correo, con el consiguiente colapso.

- **Phishing.** Es un método para infectarnos con cualquier tipo de software, se basa en mandar información por correo a multitud de usuarios, haciéndose pasar por entidades conocidas y aprovecharse de la curiosidad para que la víctima abra el correo electrónico y así enviarnos a una dirección web maliciosa donde podamos ser infectados por software malicioso.



Para saber más

Mediante el siguiente URL accedes a una interesante página donde tienes más información de otros tipos de malwares:

Tipos de Malwares.

11. Herramientas para asegurar la red.

¿Qué medios podemos utilizar para asegurar nuestra red? La respuesta es software específico y equipos específicos. En varios casos, se utiliza una combinación de ambos.

En el primer apartado está el **protocolo IPsec** y las **redes VPN**. En cuanto a los equipos podemos citar los cortafuegos y las estructuras de zona desmilitarizada.

Para dejar claras las ideas desde este momento, queremos hacer hincapié en el hecho de que IPsec es un protocolo de red, que subsana los fallos de seguridad detectados en TCP/IP.
Por otro lado, las redes VPN tratan de conseguir la protección adecuada, utilizando una red pública para interconectar las redes locales. Habitualmente, VPN utiliza IPsec.

Los cortafuegos son la manera de permitir o no el acceso a nuestro equipo por parte de un usuario externo. Son utilizados en la creación de zonas desmilitarizadas.

Pasamos al estudio detallado de cada uno de estos elementos.

11.1. Protocolo IPSEC.

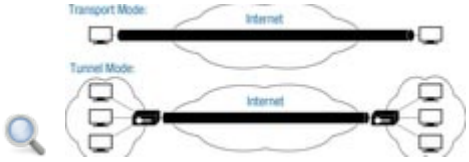
IPsec es una arquitectura, definida en las RFC 1825 a la RFC 1829, destinada a ofrecer servicios de seguridad al protocolo IP (ya sea la versión 4 o la versión 6). Dichos servicios pueden también ser utilizados por protocolos del mismo nivel o de niveles superiores, como por ejemplo ICMP, TCP, UDP, etc. IPsec hace uso principalmente de dos protocolos: AH y ESP.

El protocolo AH es el utilizado para ofrecer servicio de autenticación de origen de los paquetes IP intercambiados entre dos sistemas. El protocolo de autenticación de cabecera verifica que los paquetes intercambiados entre un determinado origen y destino no han sido modificados ni en su cabecera ni en los datos transportados. Date cuenta de que no se produce ninguna encriptación de los datos, por lo que éstos han podido ser objeto de un analizador de paquetes.

El protocolo ESP puede ofertar el servicio de autenticación de origen de los paquetes IP (similar a AH, pero sin incluir en este caso la cabecera), servicio de confidencialidad (mediante la encriptación de los paquetes) o los dos servicios de manera simultánea. En cualquier caso, se deberá elegir al menos una de las opciones (autenticación o encriptación).

Para la implementación de IPsec debemos decidir:

- Elegir AH, ESP o bien AH + ESP. Te recuerdo que el protocolo que permite la encriptación de los datos (y que por tanto éstos no se vean al pasar por la red) es ESP. Esto es especialmente recomendable cuando debamos transferir contraseñas o nombres de usuario.
- Si se ha elegido ESP se debe seleccionar un algoritmo de encriptación. Las opciones son los algoritmos DES, 3DES o AES. DES fue el primer algoritmo de encriptación y tuvo algunos fallos de seguridad que fueron solucionados por 3DES. Además, 3DES utiliza tres claves diferentes para realizar encriptación, desencriptación y nueva encriptación. AES es más moderno, rápido y consume menos recursos.
- Si se ha elegido AH se debe seleccionar un algoritmo de autenticación. Las opciones son MD5 o SHA.



Dos son los **modos de operación de IPsec:**

- **Modo transporte:** en este caso, solamente se cifra o autentica la parte del paquete IP que contiene los datos. No se modifica pues la cabecera IP. Es el modo que se suele utilizar para comunicaciones ordenador-ordenador.
- **Modo túnel:** todo el paquete IP (cabecera más datos) es encriptado o autenticado. Se suele utilizar en comunicaciones a través de VPNs.

Para saber más

En este enlace puedes ver los tipos de conexión VPN:

Tipos de conexión VPN con Windows 10.

Una de las maneras de estar protegido frente a ataques es no contestar al ping. Recuerda que era utilizado para efectuar reconocimiento de equipos, el paso previo para el ataque. En el enlace, te suministran información sobre la instalación de IPsec sobre ICMP. El resultado es que el equipo en cuestión no responderá a la orden ping, a no ser que el equipo solicitante también tenga instalado IPsec con la misma clave. El sistema operativo utilizado es Windows 10:

IPsec en Windows 10

11.2. Redes VPN.

Históricamente, las empresas empezaron utilizando redes de área local para sus equipos. Pronto se vio la necesidad de interconectar redes distantes que hasta entonces funcionaban como entes aislados (por ejemplo, dos sedes de una empresa distantes cientos de kilómetros). Resultaba prioritario que las comunicaciones fueran seguras, por lo que se establecieron conexiones WAN entre ellas. Sin embargo, el uso de enlaces WAN resultaba caro.

El desarrollo de Internet supuso una alternativa viable. Para solucionar los problemas derivados del uso de una red pública en lo que a seguridad y confidencialidad se refiere, surgieron las redes privadas virtuales VPN. Una VPN es una estructura de red corporativa que ha sido implantada sobre una red pública (de manera habitual Internet) y que permite conectar equipos como si estuvieran dentro de la misma red local.

Se pueden considerar tres tipos de VPN:

- **VPN entre redes locales:** también se le denomina VPN entre intranets. Es el caso de una empresa, con varias sedes distantes geográficamente, cada una de las cuales posee una red privada o intranet. A través de la creación de una VPN se puede conseguir la interconexión de todas las redes privadas y de esta manera formar una única intranet.
- **VPN de acceso remoto:** es la utilizada típicamente para conseguir que un trabajador pueda desde un ordenador remoto acceder a la red de su empresa. El ordenador remoto puede ser el ordenador que el trabajador tiene en su casa o un equipo portátil que utiliza en sus desplazamientos.
- **VPN extranet:** en ocasiones, una empresa puede estar interesada en que ciertos usuarios ajenos a la misma (como puedan ser clientes) tengan acceso a su intranet. A la red que permite el acceso a una intranet desde fuera (acceso externo) se le denomina extranet. Evidentemente es un acceso a proteger, de manera que no pueda ser utilizado por cualquiera. La manera de lograrlo es a través de una VPN extranet.

Recomendación

En el siguiente enlace puedes ver cómo configurar un servidor y cliente VPN en Windows 10:

Configuración de un servidor y cliente VPN en Windows 10.

En los siguientes enlaces puedes ver cómo configurar un servidor y cliente VPN en Windows más antiguos:

Configuración VPN con el servidor

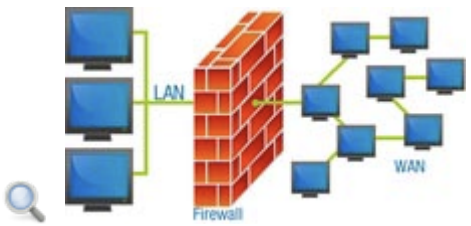
Configuración VPN con el cliente.

Para saber más

En el siguiente vídeo puedes ver un tutorial de cómo configurar una red VPN en Windows 10.

Resumen de texto alternativo

11.3. Cortafuegos.



¿Cómo se puede proteger a nuestro equipo de los accesos desde el exterior no autorizados? La respuesta es a través de un cortafuegos o firewall.

Un cortafuegos es un sistema (hardware, software o más comúnmente una mezcla de ambos) que controla el tráfico entre dos redes. El control consiste en permitir o denegar la comunicación entre las redes dadas mediante el conjunto de protocolos TCP/IP.

El cortafuegos es el mecanismo que protege nuestra red contra el acceso externo no autenticado y el tráfico externo no autorizado. Es el punto de la red donde se debe implantar la política de seguridad. Sin embargo, el cortafuegos no protege frente a malware (virus, gusanos, troyanos…etc.) ni frente ataques desde el interior de la red.

Los primeros cortafuegos aparecieron a finales de 1980. Eran del tipo conocido como filtros de paquetes. Los **filtros de paquetes** inspeccionan la cabecera de los paquetes y toman la decisión de enviarlo o no dependiendo de la norma que se ha fijado. En concreto, el filtrado de paquetes evalúa las direcciones IP origen y destino y los puertos (bien sea TCP o UDP) del origen y destino. Dichos valores son comparados con una serie de reglas que el administrador de la red ha configurado. Si el paquete y la regla impuesta coinciden, el paquete se envía. En caso contrario el paquete se descarta.

Los filtros de paquetes se suelen implementar en los routers. Su principal ventaja es la rapidez. Su mayor inconveniente es que al no examinar el tipo de tráfico que envían proporcionan una seguridad menor que otros firewalls. Las ACL de los routers Cisco pertenecen a este tipo de cortafuego básico.

La segunda generación de firewalls la constituye los llamados **filtros de inspección de estado**. Se examina la cabecera del paquete y se mantiene una tabla que indica si dicho paquete es el correspondiente al inicio de una conexión, si es un paquete erróneo o bien si es parte de una conexión existente. Al igual que los anteriormente citados, los filtros de inspección de estado permiten filtrar paquetes en función de su cabecera. Estos firewalls pueden prevenir ataques de denegación de servicio.

La tercera generación es la llamada **cortafuegos de aplicación**. Actúan sobre la capa de aplicación del modelo OSI (capa 7) y son capaces de tomar decisiones según los datos que viajan en la aplicación. Por ejemplo, se podría denegar el acceso a determinados servicios (DNS, HTTP, etc.) cuando apareciera una determinada palabra. Supón que en un determinado instituto se bloquea todo el acceso a Internet que contenga la palabra "juego". Date cuenta de que este firewall es el más potente de los estudiados. No solamente se puede filtrar en función de la cabecera del paquete sino que también se puede filtrar de acuerdo con el contenido del paquete. La desventaja es que el rendimiento de la red se ve afectado por la supervisión efectuada.

Hoy en día se habla de la cuarta generación de cortafuegos o cortafuegos híbridos. En realidad, son una mezcla de las tecnologías anteriormente expuestas.

Para saber más

El siguiente enlace está dedicado al estudio de los cortafuegos. Podrás ver la seguridad en los protocolos TCP/IP, las características de los cortafuegos así como los servicios adicionales proporcionados por estos.

Comparativa y funcionalidades de los cortafuegos. (0.15 MB)

11.4. Zonas desmilitarizadas.

El concepto de **zona desmilitarizada o DMZ** ha sido tomado de la terminología militar. Podemos pensar en una DMZ como la región entre dos países hostiles uno con el otro, donde habitualmente se producen escarceos militares. En telemática, una DMZ es la **zona que separa una red interna de la conexión con Internet**.

Todos sabemos que Internet es una superred insegura. Deseamos que nuestra red local sea lo más segura posible. Podemos pensar en la DMZ como una red, distinta de las dos anteriores, con una seguridad intermedia. La razón por la que la seguridad en la DMZ sea menor viene del hecho de que debe estar conectada a Internet, para ofrecer servicios como correo electrónico, ftp, http, etc.

Al estar conectada a Internet, la zona desmilitarizada no es segura al cien por cien. El cortafuegos que la protege debe dejar pasar tráfico potencialmente peligroso. Sin embargo, en el caso de que alguno de los ordenadores de la DMZ sea hackeado, la red interna sigue estando protegida. Date cuenta de que las dos redes son diferentes. Tienen pues direcciones de red distintas y precisan del router para pasar de una a otra. Es ahí donde los firewalls intervienen para permitir o no el tráfico. Una variación de esta implementación es crear dos VLAN distintas (una para la red interna y otra para la DMZ).

La figura muestra una manera habitual de implementar una DMZ. El primer cortafuegos separa la DMZ de la conexión a Internet. El segundo cortafuegos proporciona el nexo entre la DMZ y la zona desmilitarizada y deberá configurarse para prohibir todo intento de acceso desde el exterior.

Por último, quisiera que no confundieras este concepto con la DMZ de los routers de bajas prestaciones. Si activas la DMZ en estos últimos, permites la conexión de todos los puertos (como si deshabilitaras el cortafuegos).

Para saber más

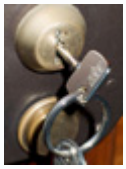
En el siguiente enlace puedes ver cómo activar y desactivar el Firewall de Micros Defender en Windows 10.

Activar o desactivar el Firewall de Microsoft Defender.

Anexo.- Licencias de recursos.

Licencias de recursos utilizados en la Unidad de Trabajo.

Recurso (1)	Datos del recurso (1)	Recurso (2)	Datos del recurso (2)
	Autoría: jmerelo. Licencia: CC BY-NC 2.0. Procedencia: http://www.flickr.com/photos/atalaya/4098201279/in/photostream/		Autoría: HernandoJoseAJ. Licencia: CCO 3.0. Procedencia: http://es.wikipedia.org/wiki/Archivo:Logo_WiFi.svg
	Autoría: DBGthekafu. Licencia: Licencia pública general GNU. Procedencia: http://es.wikipedia.org/wiki/Archivo:Bluetooth_bw.png.		Autoría: Lzur. Licencia: Dominio público. Procedencia: http://commons.wikimedia.org/wiki/File:Planet_WL-8310.JPG?uselang=es.
	Autoría: Rodrigo César. Licencia: Dominio Público. Procedencia: http://commons.wikimedia.org/wiki/File:Access-point-wireless.jpg		Autoría: Dlink. Licencia: Copyright (cita). Procedencia: http://www.solostocks.com/venta-productos/informatica/perifericos/redes-comunicaciones/bridge-inalambrico-108mbps-2685201.
	Autoría: Nuscreen. Licencia: CC 2.0. Procedencia: http://commons.wikimedia.org/wiki/File:D-Link_DI-774_Front.jpg?uselang=es		Autoría: U.S. Robotics. Licencia: Copyright (cita). Procedencia: http://www.solostocks.com/venta-productos/informatica/perifericos/redes-comunicaciones/redes-inalambricas-us-robotics-antena-interior-wifi-54-mb-usr5482-9-dbi-1716125.

	Autoría: Xenia g. Licencia: Dominio público. Procedencia: Montaje sobre: http://es.wikipedia.org /wiki/Archivo: Tipus_xarxa.gif.		Autoría: Nuria Celis Nieto. Licencia: Copyright (cita). Procedencia: Captura de pantalla del programa de configuración del router Linksys WRT54GL.
	Autoría: Raphael Bezerra. Licencia: Dominio público. Procedencia: Montaje sobre: http://es.wikipedia.org /wiki/Archivo: Wireless_rede.jpg		Autoría: Lzur. Licencia: Dominio público. Procedencia: http://es.wikipedia.org /wiki/Archivo:Plane t_WAP-4000.JPG.
	Autoría: Weihao Chiu. Licencia: CCO 3.0. Procedencia: http://commons.wikimedia.org /wiki/File: D-Link_DI-524.jpg.		Autoría: Wax115. Licencia: MorgueFile free photo. Procedencia: http://www.morguefile.com /archive/ display/19605
	Autoría: Nuria Celis Nieto. Licencia: Copyright (cita). Procedencia: Captura de pantalla del programa de configuración del router ONO Cisco 3825.		