Interconexión de equipos en redes locales (2ª Parte).

Caso práctico

"Antonio, el dueño de la academia donde estamos instalando redes 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."

En el tema anterior viste que la mejor solución para interconectar a los equipos situados en un aula será utilizar una red de área local. Se plantea la posibilidad de poder ofrecer conexión a cualquier equipo dentro de la academia sin necesidad de utilizar cableado físico para conectar cualquier dispositivo. Es por esto que vas a estudiar el hecho de poder tener una red inalámbrica por toda la academia para ofrecer conexión en todos los espacios comunes y a través de dispositivos de diferentes características, desde un ordenador portátil o un smartphone. Una de las principales ventajas que nos ofrecen este tipo de redes inalámbricas, también denominadas WLAN, es la movilidad dentro del espacio de trabajo del que disfrutaran todos los alumnos y alumnas de la academia.

Para saber más

Podemos ver en la siguiente presentación un resumen de lo que vamos a ver en este tema:

Resumen de la unidad

INTERCONEXIÓN DE EQUIPOS EN REDES LOCALES (2ª PARTE)

TECNOLOGÍAS INALÁMBRICAS

- Definición de WLAN: conjunto de nodos que se conectan entre sí sin necesidad de utilizar una conexión física, utilizando para su conexión ondas electromagnéticas
- Tipos de WLAN
  - Larga distancia
  - Corta distancia.

Resumen de la unidad

TIPOS DE REDES INALÁMBRICAS

Resumen de la unidad

WIFI

- Definición de WIFI: Se corresponde con el estándar IEEE 802.11
- Ventajas: comodidad y movilidad
- Desventajas: menor velocidad que las cableadas y la seguridad.
- Medio de transmisión: medios inalámbricos

Resumen de la unidad

MEDIOS NO GUIADOS

Distintos medios no guiados:

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

Resumen de la unidad

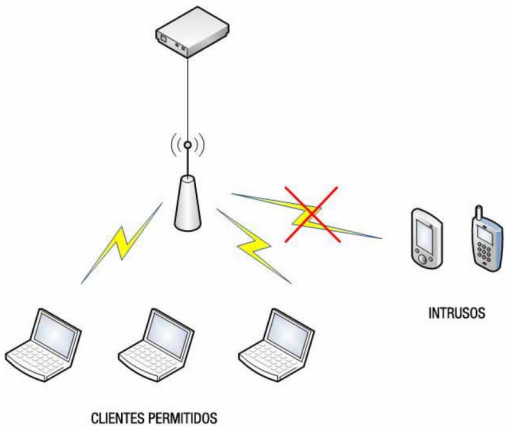
ELEMENTOS NECESARIOS

- Receptor:
  - Adaptador inalámbrico USB
  - Tarjeta de red inalámbrica
- Emisor:
  - Router inalámbrico
  - Punto de acceso inalámbrico

Resumen de la unidad

SEGURIDAD EN LAS REDES INALÁMBRICAS

- Amenazas:
  - Buscadores de redes inalámbricas abiertas.
  - Piratas informáticos.
  - Los propios usuarios



Resumen de la unidad

PROTOCOLOS DE SEGURIDAD

- Clave de autenticación WEP abierta y compartida
- WPA es un sistema para proteger las redes inalámbricas, creado para corregir las deficiencias del sistema previo WEP
- WPA2 es us sitema para proteger las redes inalámbricas, creado para corregir las deficiencias de WPA.

Tecnologías inalámbricas.

Caso práctico

Julia está conversando con Samuel, que es el técnico en Sistemas Microinformáticos y Redes que también participa en la instalación de las redes en la academia de Antonio:

"…
-Las redes inalámbricas están también clasificadas según el área que abarquen, ¿verdad Julia?

- Así es, Samuel, existen redes inalámbricas de ámbito personal, local, metropolitana y extensa. Nosotros en esta academia vamos a instalar una red inalámbrica de ámbito local, cuyo estándar más utilizado es WIFI.

- Recuerdo que también existen otras tecnologías como Bluetooth y WiMax. Aunque sé que estas no son las que vamos a utilizar nosotros para la academia.

- Que buena memoria tienes, Samuel. Da gusto trabajar con gente tan bien preparada…"

Debes aprender que una **red inalámbrica**, o **WLAN**, es un conjunto de nodos que se conectan entre sí sin necesidad de utilizar una conexión física, utilizando para su conexión ondas electromagnéticas.

Su principal ventaja es que elimina todo el cableado que se utilizaba en las redes cableadas Ethernet así como las conexiones físicas. Aunque su principal desventajas es que para este tipo de redes la seguridad ha de ser mucho más exigente para evitar conexiones indeseadas.

Existen dos tipos de redes inalámbricas:

- **Redes de larga distancia**: son utilizadas para redes grandes como puede ser otra ciudad u otro país.
- **Redes de corta distancia**: son utilizadas para redes pequeñas, dentro de una ciudad o dentro de un edificio.

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 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.

Es incorrecta porque precisamente su definición dice que no se utiliza cableado.

Incorrecta, porque también existen redes inalámbricas de corta distancia.

No es correcto puesto que estas redes son más vulnerables que las cableadas.

Muy bien. Has captado la idea.

Solución

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

Tipos de redes inalámbricas.

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.

- **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.

- **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.

- **WWAN** (Wireless Wide Area Network): En este tipo de redes encontramos las tecnologías UMTS, utilizadas para teléfonos móviles de tercera generación o la tecnología GPRS.

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

WIFI.

Cuando oigas hablar de **WiFi** se refieren a una de las tecnologías de comunicación inalámbrica mediante ondas más utilizada hoy en día. Como viste en el apartado anterior, es el equivalente al termino WLAN o al estándar 802.11.

Para tener una red inalámbrica se necesitará un punto de acceso, que se conectaría al módem y un adaptador WiFi que se conectaría en nuestro aparato. Existen adaptadores WiFi que se conectan al ordenador por USB, pero son las tarjetas PCI, que se insertan directamente en la placa, las más recomendadas. En los portátiles actuales todos tiene esta tarjeta integrada.

El funcionamiento de la red es bastante sencillo, normalmente solo tendrás que conectar los adaptadores e instalar su software. Muchos de los routers WiFi incorporan herramientas de configuración para controlar el acceso a la información que se transmite por el aire.

Como trabajamos con conexiones inalámbricas, no es difícil que alguien pueda interferir nuestra señal y tuviera acceso a la conexión. Es por ello recomendable la **encriptación** de la transmisión para emitir en un entorno seguro. Esto es posible hacerlo gracias al WAP, más seguro que su predecesor WEP.

También es posible configurar los puntos de acceso para que emita solo a ciertos dispositivos. Se puede hacer usando la dirección MAC, un identificador único de la tarjeta de red, permitiendo el acceso solo a esas direcciones concretas.

El término WiFi es también una marca de la WiFi Alliance, la organización que adopta, prueba y certifica que los equipos cumplen los estándares 802.11 relacionados con las redes inalámbricas de área local.

Debes conocer

Es necesario que ahora mires una ampliación sobre las redes Wifi en estos enlaces que te proponemos.

Redes Wifi.

Otro artículo de redes Wifi.

Para saber más

Además de los enlaces anteriores, sería interesante que visitaras estas páginas para ampliar conocimientos sobre la comunicación inalámbrica y redes inalámbricas.

Comunicación inalámbrica.

Redes inalámbricas.

Red inalámbrica.

Ventajas e inconvenientes de las redes Wifi.

Si alguna vez has utilizado una red inalámbrica te habrás dado cuenta que tiene una serie de ventajas respecto a las redes cableadas. Entre ellas se pueden destacar las siguientes:

- Al ser redes inalámbricas, son más **cómodas** puesto que puedes conectarte desde distintos puntos dentro de un rango amplio de espacio.
- Una vez configuradas, las redes WiFi permiten el **acceso de múltiples ordenadores** sin gastos extras en infraestructura. La WiFi Alliance asegura la compatibilidad entre dispositivos con la marca WiFi es total, con lo que en cualquier parte del mundo podremos utilizar la tecnología WiFi con compatibilidad total.

Como cualquier tipo de tecnología, las redes WIFI presentan una serie de ventajas, pero has de saber que también tienen alguna desventaja, sobre todo en el campo de la seguridad. Veras ahora cuales son:

- Una de las desventajas es que el sistema WiFi ofrece una **menor velocidad** en comparación a una conexión con cables, debido a las interferencias y pérdidas de señal que el ambiente puede acarrear.
- Otra desventaja fundamental de estas redes existe en el campo de la **seguridad**.
- No Y además de estas, **no es compatible** con otros tipos de conexiones sin cables como Bluetooth, GPRS, UMTS…

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.

Esto si es una ventaja.

Correcto, esto no es cierto.

Esto si es una ventaja.

Esto si es una ventaja.

Solución

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

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.

Es incorrecta, repasa el capítulo de los tipos de redes inalámbricas.

Muy bien.

Incorrecta, repasa el capítulo de medios de transmisión.

No es correcto.

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.

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 Wi-Fi 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.

Es incorrecta, repasa el capítulo de medios no guiados.

Incorrecta, repasa el capítulo de medios no guiados.

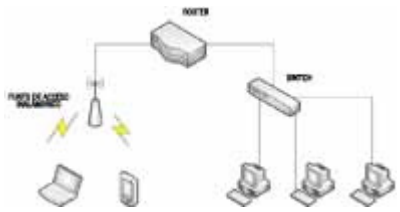
Muy bien, esto está correcto.

No es correcto.

Solución

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

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.

Muy bien, esto está correcto.

Es incorrecta, trabajan con cables.

Incorrecta, sucede justo lo contrario.

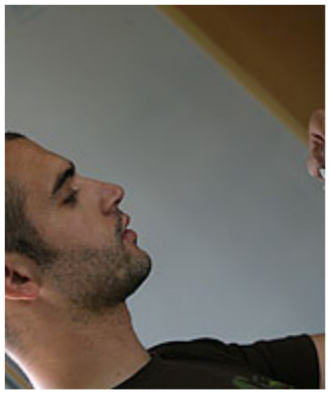
No es correcto.

Solución

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

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

Muy bien, esto está correcto.

Es incorrecta, lee el capítulo otra vez.

Incorrecta, también desde un equipo de sobremesa.

No es correcto.

Solución

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

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.

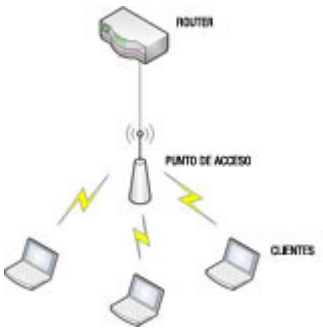
El **enrutador** o **encaminador** es un dispositivo de hardware para interconexión de red de ordenadores que opera en la capa tres (nivel de red) del modelo OSI. Un enrutador es un dispositivo para la interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes por ejemplo una red local y una red WAN.

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 (Wi-Fi). 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.

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.

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.

Esto es correcto.

Repasa este capítulo.

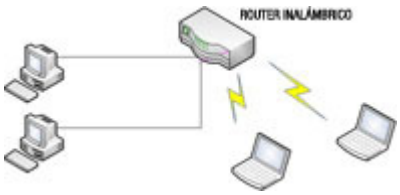
Eso no es correcto.

Vuelve a repasar la teoría.

Solución

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

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.

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:

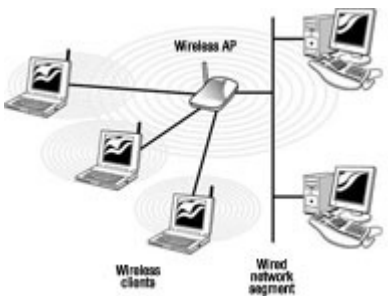
"- Ya tiene claro cuáles son los elementos necesarios para que su red inalámbrica en la academia funcione perfectamente. Con un router inalámbrico en el armario principal de comunicaciones será suficiente.

-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.

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 (1.23 MB)

Además de la práctica anterior, es necesario que veas estos vídeos sobre instalaciones de adaptadores en distintos sistemas operativos.

Instalación de adaptadores de red Wifi en Windows 7 (1ª parte).	Instalación de adaptadores de red Wifi en Windows 7 (2ª parte).
http://www.youtube.com/embed/adumPA7X6E4	http://www.youtube.com/embed/isXvMzCCYMs
Instalación de adaptadores de red Wifi XP (1ª parte).	Instalación de adaptadores de red Wifi XP (2ª parte).
http://www.youtube.com/embed/jGZyE2EVLJs	http://www.youtube.com/embed/ZAHN8vh2ckk

Para saber más

Una vez que has visto los vídeos anteriores, también te proponemos que veas los siguientes, aunque esto es solo como recomendación.

Instalación de Drivers de Tarjetas de Red en Windows.	Activar Wireless (red inalámbrica) en ubuntu 9.10 / 10.4 Solución 100%.	Como activar la red inalámbrica en Ubuntu 9.10.
http://www.youtube.com/embed/28UuTc6aMGw	http://www.youtube.com/embed/PTJZN4ZIJOc	http://www.youtube.com/embed/T0ovUDP-1NU

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.

Vuelve a mirar la práctica…

Repasa la práctica otra vez.

Esto no es correcto.

Muy bien.

Solución

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

Configuración de un punto de acceso.

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

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

Instalación de un punto de acceso. (0.73 MB)

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

Configuración de Access Point D-link (1ª parte).

Configuración de Access Point D-link (2ª parte).

http://www.youtube.com/embed/LKFZ4ydbB-k

http://www.youtube.com/embed/2TQ0pvU5qOE

Para saber más

Una vez que has visto los vídeos anteriores, también te proponemos que veas los siguientes, aunque esto es solo como recomendación.

Configuración de routers inalámbricos y puntos de acceso inalámbricos.

Configurar Router D-Link DI-524.

Cómo configurar router adsl inalámbrico (P2P, Wifi, Contraseña,

http://www.youtube.com/embed/7aks7Heqo4U

http://www.youtube.com/embed/d-q5wd00uXs

Seguridad).

http://www.youtube.com/embed/9DCY8XwButQ

Medir ancho de banda de un enlace.

http://www.youtube.com/embed/w0D9f6in_AM

Configuración de access point en modo repetidor.

http://www.youtube.com/embed/RFpt1jgA-f4

Configuración de un punto de acceso en modo WDS.

http://www.youtube.com/embed/7-dxphK1SmU

Cómo configurar un repetidor inalámbrico.

http://www.youtube.com/embed/rfXi2qLiMhI

Enlaces de Microondas.

http://www.youtube.com/embed/JAIvieqBqqg

Cómo configurar un puente inalámbrico.

http://www.youtube.com/embed/qIYN_dMLavg

WDS - Sistema de distribución inalámbrica.

http://www.youtube.com/embed/tR3zk93MnI8

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. (0.77 MB)

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

Configuración de redes inalámbricas.

Configuración de redes inalámbricas IEEE 802.11 de Windows XP.

Conectarse a una red Inalámbrica.

https://www.youtube.com/embed/iq189i3x6V4

Para saber más

Una vez que has visto lo anterior, también te proponemos que veas los siguientes artículos y vídeos, aunque esto es solo como recomendación.

Configuración de redes inalámbricas.	Configuración de una red Alambrada Básica.	Configurar red inalámbrica en Windows 7.
http://www.youtube.com/embed/6O45e2So1Gg	http://www.youtube.com/embed/Hh3nPzajy7M	http://www.youtube.com/embed/mNDs7ijK7Fs

Configurar red inalámbrica en windows 7.	Configuración de Red Inalámbrica Tipo AD-HOC.	Configuración de red e Internet Inalámbrica AD-HOC.
Configurar red inalámbrica en Windows 7 en Yahoo! Video	http://www.youtube.com/embed/DEqCFOEo6U0	http://www.youtube.com/embed/091Zhp-lLtI

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.

Vuelve a mirar la práctica…

Muy bien.

Repasa la práctica otra vez.

Esto no es correcto.

Solución

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

Segmentación de redes. VLAN.

Caso práctico

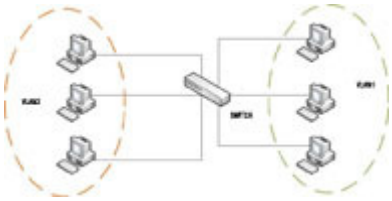
"Antonio sigue siendo un mar de dudas, y no tiene reparos en seguir comentándolas con Julia:

-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.

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 del 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.

Muy bien.

Incorrecto. A través del switch son como dos redes diferentes.

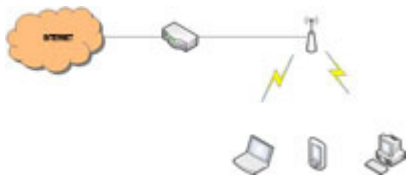
Eso no es correcto.

Eso es incorrecto.

Solución

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

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.

Tipos de VLAN.

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 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.

- **VLAN de administración**: es cualquier VLAN que se configura para acceder a las capacidades de administración de un switch.

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 el 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.

No es correcto.

Muy bien.

No es correcta.

Precisamente, es una de las ventajas de uso que tiene.

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:
VLAN I.	VLAN II.	Configurar una VLAN.
http://www.youtube.com/embed/CVt-1U63f_g	http://www.youtube.com/embed/JOnL02ils5s	http://www.youtube.com/embed/Umd3NCYUtpM

Seguridad básica en redes inalámbricas.

Caso práctico

"Antonio sigue preocupado por la nueva red inalámbrica que se ha instalado en la academia, y comenta sus dudas con Julia, la técnico superior de Administración de Sistemas en Red.

-Julia, ¿estás segura de que esto es fiable? No me gustaría que la red inalámbrica que instalemos en la academia lo pueda utilizar cualquiera que pase por la calle o incluso los vecinos del inmueble.

-Antonio, como ya comentamos, existen técnicas para establecer seguridad en las redes inalámbricas de modo que solo podrá utilizarlas aquellas personas que conozcan las contraseñas de seguridad. De este modo, no tendremos intrusos en la red y solo lo utilizarán los usuarios autorizados para ello."

En este capítulo resolveremos dudas sobre la seguridad básica en las redes inalámbricas.

Es interesante que te pares a pensar un momento en las redes inalámbricas. Desde luego que son muy cómodas de utilizar y presentan una serie de ventajas. Una de las más destacadas es la movilidad que permite en un área acotada según la cobertura del router inalámbrico o del punto de acceso. Además, una vez que están configuradas, permiten el acceso a múltiples ordenadores sin más gastos en la instalación inicial.

Todo esto que a priori parece tan interesante también tiene un punto débil. El principal problema que nos podemos encontrar es la seguridad en este tipo de redes. Debes saber que existen una serie de protocolos que se utilizan para configurar la seguridad en redes inalámbricas, y eso es precisamente lo que vamos a tratar en este apartado y sucesivos. Aunque antes de que comiences con este apartado, tienes aquí unos enlaces que pueden ser de utilidad.

Para saber más

Te recomiendo que antes de abordar este capítulo de seguridad, y para

que te hagas una idea general, te veas estos dos videos sobre seguridad en redes inalámbricas:

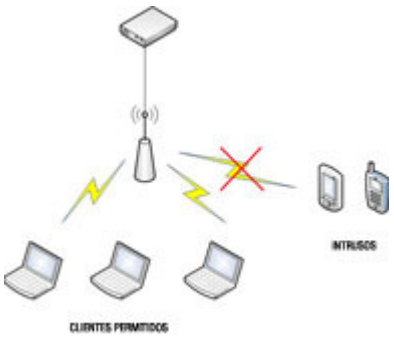
Seguridad en redes inalámbricas.

http://www.youtube.com/embed/SMFJ13v_bsM

Configuración de computadoras con autenticación radius.

http://www.youtube.com/embed/EMwP5qPQf3Y

Amenazas a la seguridad inalámbrica.



Como futuro Técnico de Sistemas Microinformático y Redes, para ti la seguridad debe ser prioritaria en cualquier escenario de trabajo con el que te encuentres. Las dificultades para mantener segura una red conectada por cable se ven multiplicadas con una red inalámbrica. Una WLAN está abierta a cualquiera dentro del alcance de un punto de acceso y de las credenciales apropiadas para asociarse a él. Con un NIC inalámbrico y conocimiento de técnicas de decodificación, sería suficiente para acceder a la WLAN.

Por todo ello, es conveniente que conozcas a que tipo de amenazas reales te vas a enfrentar cuando trabajes con WLAN:

- **Buscadores de redes inalámbricas abiertas**: se trata de intentar localizar redes inalámbricas sin ningún tipo de contraseña a la que podamos conectarnos directamente.

- **Piratas informáticos**: intrusos maliciosos que entran en el sistema y son capaces de explotar las medidas de seguridad débiles.

- **Los propios usuarios y usuarias**: los dispositivos actuales no necesitan de mucha configuración para que funcionen. Los usuarios que no cambian la configuración predeterminada y dejan la autenticación de cliente abierta, dejan a sus redes en una situación más fácil de atacar.

Protocolos de seguridad inalámbrica.

Una vez que ya conoces los puntos débiles de las redes inalámbricas, es el momento en el que debes conocer como se pueden proteger este tipo de redes. Existen una serie de protocolos que nos proporcionan seguridad en redes inalámbricas. Verás ahora cuales son y que características tienen.

En el estándar 802.11 original se introdujeron dos tipos de autenticación: **clave de autenticación WEP abierta y compartida**. Mientras la autenticación abierta en realidad es “no autenticación”, (un cliente requiere autenticación y el punto de acceso la permite), la autenticación WEP debía proveer privacidad a un enlace, como si fuera un cable conectado a un ordenador a una conexión de cable Ethernet. Como se mencionó anteriormente, las claves WEP compartidas demostraron ser defectuosas y se requería algo mejor. Para contrarrestar las debilidades de la clave WEP compartida, el primer enfoque de las compañías fue tratar técnicas como SSID camuflados y filtrado de direcciones MAC. Aunque también son técnicas débiles.

Otro protocolo es **WPA**, un sistema que te permitirá proteger las redes inalámbricas, y que fue creado para corregir las deficiencias del sistema previo WEP. WPA 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 tal servidor para el despliegue de redes, WPA permite la autenticación mediante clave compartida, de modo similar al WEP, que requiere introducir la misma clave en todos los equipos de la red.

Y por último y más reciente de todos es **WPA2**, un sistema para proteger las redes inalámbricas, creado para corregir las deficiencias de WPA. WPA2 está basado en el nuevo estándar 802.11i. WPA, por ser una versión previa, no incluye todas las características de IEEE 802.11i, mientras que WPA2 es la versión certificada de este estándar.

Autoevaluación

Señala la afirmación correcta:

- WEP es más seguro que WPA.
- WPA2 es el sistema más antiguo que se tiene para dar seguridad en redes inalámbricas.
- El usuario de la red no supone una amenaza para la red inalámbrica.
- Es muy recomendable tener algún tipo de contraseña en nuestra red inalámbrica para protegernos de accesos no autorizados.

Repasa la teoría.

Esto no es correcto.

En algunos casos si puede ser una amenaza.

Muy bien.

Solución

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

Redes mixtas.

Caso práctico

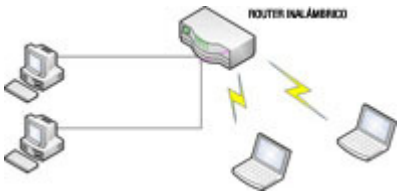
Antonio, el dueño de la academia, conversa ahora con Samuel.

-"¿Tu crees, Samuel, ahora que está acabada la instalación, que podré trabajar de igual modo desde mi despacho con el ordenador de sobremesa, que con mi portátil? No estoy seguro de entender si el funcionamiento de un tipo de red, como la inalámbrica, es compatible con utilizar la red cableada.

-No te preocupes por eso Antonio. Las dos tecnologías que hemos instalado en la academia son totalmente compatibles entre sí. Ambos tipos de tecnologías forman parte de la misma red. Solo que como utilizan tecnologías diferentes, se dice que este tipo de redes son redes mixtas."

Una vez que ya conoces los dos tipos de redes de área local con los que se puede trabajar, vas a analizar en el siguiente apartado aquellas redes en las que la tecnología utilizada será a través de medios guiados y a través de medios no guiados. Este tipo de redes se las conoce como redes mixtas. Parte de la infraestructura y de los equipos será en un entorno cableado, aunque se cuenta con un router inalámbrico o puntos de acceso inalámbricos capaces de distribuir la señal a través de ondas para que cualquier dispositivo que sea capaz de recibir la señal y esté correctamente configurado pueda utilizar la red.

Utilización de redes mixtas.



Cuando vayas a decidir que tipo de instalación es mejor en un ámbito de trabajo plantéate lo siguiente: si la red que tienes que cablear está más o menos en horizontal y en un espacio reducido de metros, la solución más sencilla siempre será utilizar una red **cableada Ethernet**.

La mayor parte de los problemas sobrevienen cuando no existen conductos libres para el paso de los cables a través del edificio. Si además, el edificio o locales a cablear están en diferentes alturas, puede ser muy complicado pasar un cable entre un piso y otro. En este tipo de escenarios es mejor utilizar una **red inalámbrica**.

Este campo de trabajo que estamos planteando se trataría en el caso de que la academia de Antonio tuviera más de una altura o algún aula de difícil acceso. La solución propuesta sería utilizar un router WIFI. Dicho router, que será proporcionado por la operadora de ADSL, proporciona ya de por sí una conexión inalámbrica. Eso sí, que no se nos olvide que tenemos que protegernos para que la conexión inalámbrica no quede abierta.

Desde el router inalámbrico podremos sacar los cables que irían a cada una de las aulas y conectarlos con el switch correspondiente para poder dar servicio a todos los equipos de cada una de las aulas a través de un cableado tradicional.

Esta somera descripción de la red que vamos a instalar en la academia de Antonio se trata de una red mixta puesto que nos va a dar servicio a una serie de dispositivos en red utilizando distintas tecnologías, en este caso tecnología cableada Ethernet y tecnología inalámbrica WiFi.

Las **ventajas** que me ofrecen este tipo de redes:

- Proporciona a los ordenadores de las aulas una conexión rápida y segura a través de los cables.
- Posibilidad de aumentar el número de dispositivos sin necesidad de ampliar la infraestructura a través de la conexión inalámbrica.

Pero en este tipo de redes te encontrarás tres **inconvenientes** principalmente:

1. La red es más heterogénea, su mantenimiento es más complejo.
2. La dificultad de cablear las aulas sigue siendo la misma que si no utilizáramos una red mixta.
3. Hay que cuidar la seguridad en la red inalámbrica.

Autoevaluación

En una red mixta:

- Se llama así porque utiliza solamente tecnología cableada Ethernet.
- Se llama así porque utiliza solamente tecnología inalámbrica Wifi.
- No tiene ninguna ventaja respecto a las redes cableadas.
- Se denomina así a las redes que combinan distintas tecnologías para conectarse a la red.

No es del todo correcto.

No es del todo correcto.

Si tiene ventajas y muy importantes.

Correcto.

Solución

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

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:

Dominios de colisión y difusión.

https://www.youtube.com/embed/ie-InaCEGDQ

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

Video explicativo sobre Video explicativo sobre Video explicativo sobre

las redes WiFi. las redes Inalámbricas (parte 1). las redes Inalámbricas (parte 2).

http://www.youtube.com/embed/sQP2KvUImds

Artículo explicativo sobre las redes inalámbricas:

Artículo de las redes inalámbricas.

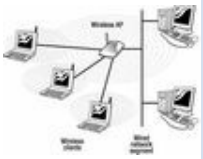
Artículo explicativo sobre WIFI:

Artículo de WIFI.

Anexo.- Licencias de recursos.

Licencias de recursos utilizados en la Unidad de Trabajo.

Recurso	Datos del recurso
	Autoría: Fernando. Licencia: C.C. 3.0. Procedencia: http://commons.wikimedia.org/wiki/File:EstacionBase-WLAN.JPG
	Autoría: Desconocido. Licencia: Dominio público. Procedencia: Montaje sobre http://es.wikipedia.org/wiki/Archivo:Tipus_xarxa.gif
	Autoría: WiFi Alliance. Licencia: Dominio público. Procedencia: http://commons.wikimedia.org/wiki/File:Wifi.png
	Autoría: Desconocido. Licencia: Dominio público. Procedencia: http://es.wikipedia.org/wiki/Archivo:Tipus_xarxa.gif
	Autoría: Appaloosa. Licencia: CC 2.0. Procedencia: http://commons.wikimedia.org /wiki/File:WLAN_PCI_Card.jpg
	Autoría: Francisco Vallejo. Licencia: Dominio Publico. Procedencia: http://es.wikipedia.org/wiki/Archivo:Lunausb.jpg
	Autoría: Edusand. Licencia: CC 2.0. Procedencia: http://es.wikipedia.org/wiki/Archivo:ModemWiFi.JPG

	Autoría: Lzur. Licencia: dominio público. Procedencia: http://es.wikipedia.org/wiki/Archivo:Planet_WAP-4000.JPG
	Autoría: RedEagle. Licencia: Dominio Publico. Procedencia: Montaje sobre http://commons.wikimedia.org/wiki/File:WirelessAP.JPG
	Autoría: E smith2000. Licencia: Dominio Público. Procedencia: http://commons.wikimedia.org/wiki/File:No_wireless_Internet_even_with_strong_signal.GIF
	Autoría: KyraVixen. Licencia: Dominio público. Procedencia: http://commons.wikimedia.org/wiki/File:Symbol_confirmed.svg?uselang=es

Condiciones y términos de uso de los materiales

Materiales desarrollados inicialmente por el Ministerio de Educación, Cultura y Deporte y actualizados por el profesorado de la Junta de Andalucía bajo licencia Creative Commons BY-NC-SA.

Antes de cualquier uso leer detenidamente el siguente Aviso legal

Historial de actualizaciones

Versión: 01.00.01	Fecha de actualización: 13/05/21
Actualización de materiales y correcciones menores.	
Versión: 01.00.00	**Fecha de actualización: 25/10/14**
Versión inicial de los materiales.	