PAR02.- Integración de elementos en una red.

Caso práctico

Una vez que Tomás ha conseguido introducirse en la terminología informática, y que además tiene una noción de la organización y clasificación de las redes (conoce conceptos como protocolo IP, LAN, etc.), ha decidido meterse de lleno en el mundo de las redes para así conocer su funcionamiento interno.

El primer paso consistirá en conocer los conceptos relativos a los tipos de transmisión y los problemas que se dan en ella. Quiere saber cuál es la función del módem y por qué debe tener uno para conectarse a Internet. Para su sorpresa, ha descubierto que no es lo mismo un Router que un Módem.

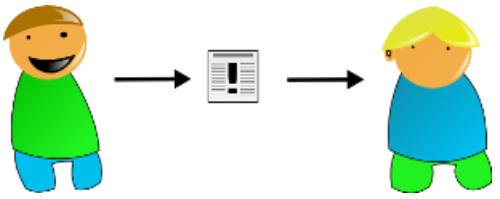
En esta unidad aprenderás cosas tan importantes como las direcciones IP, la creación de subredes, los dominios de colisión o las tecnologías usadas en las redes WLAN.

Al igual que Tomás, aprenderás que hay un montón de cosas a tener en cuenta para que los equipos de una red se puedan comunicar de forma eficiente y segura entre sí. No basta con saber conectar los equipos a través de simples cables, hay que saber realizar una instalación y una configuración adecuada de la red, que asegure que las necesidades de comunicación están plenamente cubiertas.

Y no hay que olvidarse de cosas tan importantes como la documentación y el mantenimiento de la red. No basta con realizar una instalación de una red que funcione, sino que además hay que documentarla para luego poder realizar un mantenimiento sencillo de la misma. La labor de mantenimiento de una red, y la capacidad para solucionar un problema existente, dependen directamente de la calidad de la documentación elaborada después de realizar una instalación o una modificación en la misma.

Transmisión de datos.

En un **diagrama básico de comunicaciones** existen los siguientes elementos:



- Emisor.
- Receptor.
- Canal de comunicaciones.
- Información.

El objetivo es que el emisor genere información que pueda ser recibida por el receptor gracias a la utilización del canal de comunicaciones. En este proceso intervienen todos los elementos que hacen que el emisor y el receptor manejen la información (DTE – Equipo Terminal de Datos), así como aquellos que acomodan la información generada por los DTE al canal de comunicaciones (DCE – Equipo Terminal del Circuito de Datos).

Ejemplos de DTE son los ordenadores y de DCE los módem. Los ordenadores personales y sus aplicaciones nos permiten manejar información en formato digital y los módem transforman esa información en datos que pueden viajar por el canal de comunicaciones (modulación y demodulación).

La transmisión de los datos se basa en las ondas electromagnéticas y por lo tanto, todos los factores que afecten a este tipo de ondas afectarán al proceso de comunicación.

Autoevaluación

El router ADSL que nos suministra nuestro ISP es un:

- Módem.
- Un DCE.
- Un DTE.
- Un concentrador.

Conceptos básicos.

Antes de nada, vamos a revisar algunos conceptos básicos relacionados con la transmisión. La transmisión es, en resumen, un proceso mediante el cual dos ordenadores pueden intercambiar información. En el proceso de intercambio de información, la comunicación entre ordenadores se puede producir de diferentes formas:

- **Simplex:** La comunicación se da en un solo sentido. Por ejemplo, una emisión de radio.
- **Dúplex:** La comunicación se puede dar en ambos sentidos de manera simultánea. Por ejemplo, una conversación telefónica.
- **Semidúplex:** La comunicación se puede dar en ambos sentidos pero no de manera simultánea. Por ejemplo, en una comunicación con un equipo de radio-aficionado, un interlocutor tiene que dejar de

Comunicación dúplex.

hablar para que pueda hablar el otro (“cambio y corto”).

Además, en todo proceso de comunicación intervienen como mínimo los siguientes elementos:

- **Emisor:** Persona que quiere transmitir una información. Es el encargado de buscar un código que permita que esa información sea comprensible para el medio. Utilizando ese código creará un mensaje.
- **Código:** Es el sistema de signos con el que se elabora el mensaje que se quiere transmitir.
- **Mensaje**: Es la información codificada que quiere transmitir el emisor.
- **Canal**: Es el medio utilizado por el mensaje para llegar hasta el receptor.
- **Receptor:** Persona que recibe el mensaje enviado por el emisor. Para poder interpretar el mensaje, deberá conocer el código con el que el emisor ha codificado la información.
- **Ruido:** Todo aquello que acompaña a la información y no forma parte de ella, llegando incluso a modificarla.
- **ETD:** Equipo Terminal de Datos. Medios físicos utilizados por el emisor y receptor para crear los mensajes (ordenador).
- **ECD:** Equipo Terminal de Circuito de Datos. Dispositivos que sirven para adaptar los mensajes al canal de comunicaciones (módem).

Autoevaluación

Una comunicación telefónica es una comunicación:

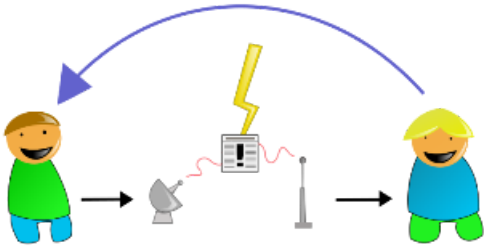
- Simplex.
- Dúplex.
- Semidúplex.
- Triplex.

Problemas en la transmisión.

En una transmisión de información puede haber problemas producidos por cualquiera de las partes que intervienen (emisor, receptor, canal, información).

Los problemas más fáciles de detectar son los causados por las personas (emisor o receptor). Por ejemplo, podemos quejarnos de que no nos ha llegado un mensaje a nuestro ordenador, y darnos cuenta de que no teníamos encendido nuestro router.

Los problemas más difíciles de solucionar son los relacionados con la naturaleza de la señal a transmitir y del medio empleado, generalmente problemas de tipo electromagnético. Los parámetros que se pueden alteran son la amplitud, la frecuencia y/o la fase de la señal.



Todas las señales sufren alteraciones en amplitud, frecuencia y/o fase porque no existen canales ideales de comunicación. Las alteraciones de la señal las denominaremos distorsiones.

Las distorsiones se producen principalmente por los siguientes factores:

- **Distancia entre emisor y receptor.** A mayor distancia, mayor probabilidad de problemas en la transmisión ya que la señal va perdiendo potencia. A la pérdida de potencia se le denomina**atenuación de la señal o distorsión por atenuación**.
- **Entorno en el que se da la transmisión.** Si el entorno está afectado por más emisiones electromagnéticas existen muchas posibilidades de que interactúen unas con otras. Cuando esto ocurre se dice que la señal sufre **interferencias** o **distorsión por interferencias.**
- **Elementos por los que tiene que pasar una señal.** A mayor número de componentes que se tengan que atravesar, más modificaciones sufrirá la señal.

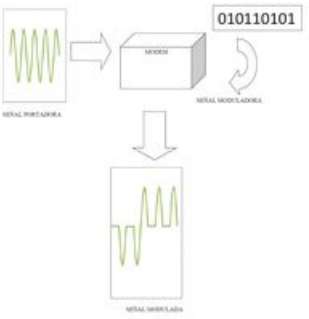
Autoevaluación

El eco de la voz es un ejemplo de:

- Distorsión por atenuación.
- Distorsión por interferencia.
- Distorsión por cambio de fase.
- Distorsión por eco.

Modulación.

La modulación es un proceso en el que se modifican las características de una señal (amplitud, frecuencia o fase) para poder transmitirla por el canal de comunicaciones. Todo proceso de modulación lleva aparejado un proceso de demodulación. El dispositivo que se encarga de este proceso recibe el nombre de módem (modular/demodular). Hoy en día, el módem se haya integrado con otros dispositivos y reciben nombres como router-módem, cable-módem y router-ADSL.



La señal que se modifica se denomina señal portadora, la señal que sirve para modificar la portadora se denomina señal moduladora y la señal resultante se denomina señal modulada. La señal que representa el mensaje que queremos transmitir es la señal moduladora.

Existen varios tipos de modulación y casi todas son combinaciones entre las modulaciones básicas:

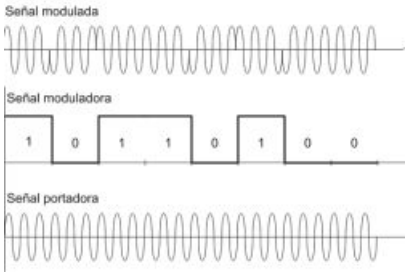
- Modulación en Amplitud.
- Modulación en Fase.
- Modulación en Frecuencia.

Según la naturaleza de las señales portadora y moduladora, podemos hacer una clasificación de los tipos de modulación como se muestra en la tabla siguiente:

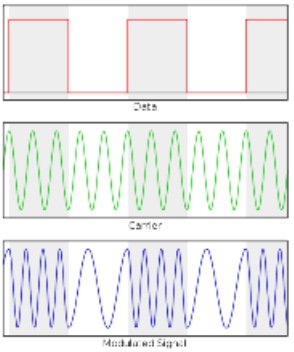
	Moduladora analógica	Moduladora digital.
Portadora analógica.	AM, FM, PM	ASK, FSK, PSK
Portadora digital	PAM, PDM, PCM, PPM	NRZ, RZ, Bifase, Bipolar

En la siguientes imagenes se pueden apreciar distintas señales moduladoras y moduladas. Vemos como la señal moduladora es digital (1 y 0) y la señal modulada es analógica (se deduce que la portadora es también analógica).

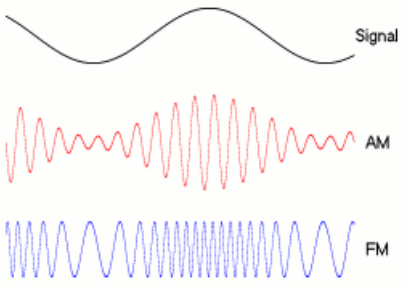
Modulación PSK



Modulación FSK



En esta otra imagen vemos un ejemplo de modulación AM y FM con señales analógicas.



Si tomamos como ejemplo la transmisión de radio, la onda portadora sería la onda que las instituciones han asignado a una determinada cadena de radio. Las ondas portadoras son las que pueden viajar porque son de alta frecuencia. La música y las palabras de los locutores son de baja frecuencia por lo tanto no pueden viajar a largas distancias (ondas moduladoras). Utilizando la modulación se puede conseguir una onda modulada (con ayuda de elementos que transformen la voz en radiación electromagnética, micrófonos, antenas, etc.) que pueda viajar a distancias lejanas.

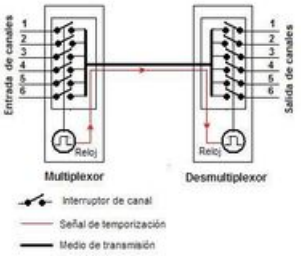
Multiplexación.

Es el proceso a partir del cual un número de señales independientes se combinan formando una señal única que se puede transmitir por un único canal. Consiste en la transmisión de información proveniente de diferentes fuentes utilizando un mismo canal físico.

Los tipos de multiplexación más comunes son:

- **FDM:** División de frecuencias. Asignación de sub-bandas de frecuencia (radio-difusión).
- **TDM:** División de tiempos. Asignaciones de time-slots (ranuras de tiempo).
- **SDM:** División de espacios. Asignaciones de direcciones espaciales (arreglo de antenas).
- **PDM:** División de polarización. Asignación de polarizaciones ortogonales para separar señales.
- **CDM:** División de código. Asignación de código digital para acceso al canal.

La imagen siguiente representa el funcionamiento de un multiplexor y un demultiplexor por tiempo.



El canal de comunicaciones transporta solamente una señal de las 6 entrantes, el reloj del sistema es el encargado de activar el sistema que gestiona los interruptores del canal. La activación de los interruptores de las señales entrantes suele ser secuencial, aunque también existen multiplexores capaces de escoger el interruptor a activar para la señal de entrada.

En una TDM lo lógico es que cada una de estas señales disponga de un espacio de tiempo para ocupar el canal y llegar hasta el multiplexor, donde se sufre el fenómeno inverso.

Autoevaluación

La multiplexación:

- Es lo mismo que la modulación.
- Es el proceso contrario a la modulación.
- Mezcla señales de diferentes frecuencias.
- Transmite la información de varios canales por un único canal.

Ancho de banda y tasa de transferencia.

Caso práctico

Hoy Tomás ha recogido la publicidad de su buzón y tiene varios folletos en los que dos compañías de telefonía ofrecen un "ancho de banda" a diferente precio para la conexión a Internet. Él ya sabía que hay varias modalidades para navegar en Internet a diferentes velocidades, pero pensaba que dependía del módem que tuviera instalado. Al llamar al teléfono de una de las compañías, le han dicho que para variar la velocidad es suficiente con los elementos que tiene instalados (router y cable-módem), lo único que le falta es pagar más cuota mensual. Le han ofrecido duplicar su ancho de banda actual, pero él se pregunta: ¿qué es el ancho de banda?.

Aunque son dos términos que a menudo se utilizan en los mismos contextos, la realidad es que son dos términos diferentes.

El ancho de banda es la capacidad máxima disponible para transmitir bits y la tasa de transferencia son los bits por segundo que se transmiten. El ancho de banda también se puede definir como la diferencia entre la frecuencia máxima y mínima de las señales que se pueden transportar en dicho canal sin atenuación.

La tasa de transferencia total o throughput son los bits de control y datos transferidos por segundo. La tasa de transferencia efectiva son los bits de datos transferidos por segundo (sin los bits de control).

Hay frases que dejan muy claro cuál es la diferencia entre los dos términos, por ejemplo, podemos decir que "Las limitaciones de ancho de banda provocan problemas en la tasa de transferencia de la red porque la red entera sólo puede funcionar tan rápido como su enlace más lento". También podemos decir que la tasa de transferencia es el ancho de banda real medido en un instante determinado de tiempo.

La tasa de transferencia nunca es mayor que el ancho de banda, esto se debe a las limitaciones impuestas por los medios de transmisión, medios de interconexión, topologías y todos los dispositivos y aplicaciones que operan en la red.

¿BAUDIO Y BIT?

Un baudio es el número de símbolos por segundo transmitidos en una red. Un bit es la representación mínima de la información. Así pues, un baudio es igual a un bit solamente cuando cada segundo se transmite un 1 bit.

La velocidad a la cual dos módems se comunican por lo general se mide en baudios, aunque técnicamente es más adecuado decir bits por segundo o bps. Un módem que se comunique a 1000 baudios, puede transmitir 2000 bps (bits por segundo) si cada símbolo lleva 2 bits.

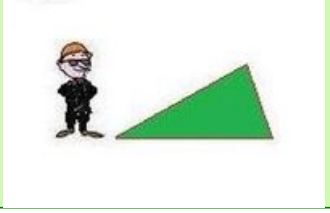
Autoevaluación

La información de un ISP dice “50 Megas reales por 30 euros al mes”, significa:

- Se transmite a una velocidad de 50 MHz.
- Se transmiten 5 millones de símbolos por segundo.
- El ancho de banda es 5000000 bits/seg.
- Se transmiten 52428800 bits/seg.

Factores físicos que afectan a la transmisión.

Caso práctico



Tomás lleva unos días con la nueva conexión a Internet y está bastante contento porque ha visto como las páginas web que visita aparecen en pantalla más rápido que antes. Navegando por Internet ha descubierto un sitio en el que se puede hacer un test de velocidad para saber cuál es la velocidad real de conexión, lo ha hecho y ha descubierto que el resultado no es el mismo que la velocidad que le habían prometido en la publicidad. Tomás se ha indignado mucho y ha llamado al teléfono de la compañía que le da servicio de acceso a Internet. La respuesta ha sido que la velocidad ofrecida es una velocidad en condiciones ideales, que la transmisión depende de varios factores. Además le han comentado algo de velocidad de subida y de bajada.

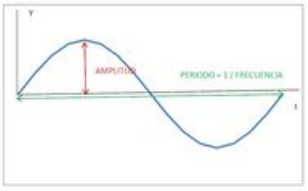
Para representar una señal electromagnética que se propaga, debemos recurrir a una función dependiente del tiempo. Después de varios experimentos y tomando como base los estudios matemáticos de **Fourier**, se dedujo que la función que mejor representaba a las ondas electromagnéticas era una función del tipo:

$$Y(t) = A\ sen(wt + \Phi)$$

Donde:

- *Y* representa a la posición de la perturbación en un instante de tiempo determinado.
- *A* es la amplitud máxima de la onda.
- *w* es un valor proporcional a la frecuencia ($w = 2\pi f$).
- Φ representa la fase.
- *t* representa el tiempo.

Amplitud, frecuencia y fase son los tres parámetros que se modifican o se pueden modificar en las ondas electromagnéticas. Por lo tanto, serán los parámetros sobre los que influirán todos los factores que afecten a estas ondas en la transmisión.



En la figura se representa lo que correspondería a una rotación angular entera (360º). Otra onda que estuviese en fase con esta, quedaría superpuesta. Si una segunda estuviera desfasada con esta, tendríamos que ver los grados de desfase, por ejemplo, si el desfase fuese de 180º, seguirían sentidos diferentes (si una sube la otra baja), el dibujo resultante de dos ondas desfasadas 180º sería algo parecido a:

La transmisión de estas señales supone el paso de ellas a través de medios físicos, y debido a los diferentes fenómenos físicos que pueden sufrir, la señal que llega al receptor difiere bastante de la señal emitida por el emisor.

Las perturbaciones más conocidas son:

- **Atenuación o distorsión de la amplitud. La intensidad, y por lo tanto la amplitud de una onda, disminuyen con la distancia al foco emisor. La atenuación también aumenta con la frecuencia.**

  Para corregir la atenuación se emplean amplificadores (amplitud) y ecualizadores (frecuencia).

- **Retardo o distorsión de la fase. Se suele producir solo en medios guiados. En estos medios la velocidad de propagación varía con la frecuencia. Los componentes de frecuencia de la señal llegan al receptor en distintos instantes de tiempo, originando desplazamientos de fase entre las distintas frecuencias.**
- **Ruido. Puede ser térmico (debido al movimiento de electrones), o por señales que se mezclan en el camino entre el emisor y el receptor (frecuencias parecidas).**

Otras perturbaciones son:

- **Diafonías o crosstalk. Señales de otros medios cercanos que interfieren debido a su proximidad. Se puede dar en cables de pares trenzados por ejemplo, para evitar este fenómeno hay que apantallar los cables o utilizar técnicas que generen pantallas (trenzado).**
- **Ecos.**

La transferencia de energía en un medio depende de ciertas propiedades electromagnéticas de éste, así como de propiedades similares del medio que le rodea.

La transmisión de las ondas electromagnéticas dependerá de las características físicas del medio donde se produce la transmisión.

Los medios utilizados para la transmisión se caracterizan entre otros por los siguientes parámetros:

- **Constante Dieléctrica (ε): Es la capacidad de un medio para almacenar energía electrostática. Un buen dieléctrico es un material no conductor, con constante dieléctrica alta. A la constante dieléctrica también se la denomina Permitividad.**
- **Permeabilidad (μ): Es la capacidad de un material para absorber radiaciones magnéticas.**
- **Conductividad (σ): Mide la capacidad de un medio para conducir la corriente eléctrica.**

Las tres magnitudes indican características electromagnéticas del medio, sabiendo cómo se comporta el medio, sabremos cómo influye en las ondas que lo atraviesan.

Autoevaluación

La técnica del trenzado de cables se utiliza para evitar:

- Qué el cable se rompa.
- El crosstalk.
- La atenuación.
- No se utiliza porque está en desuso.

La conexión inalámbrica.

Caso práctico

La compra de un ordenador portátil siempre ha sido una de las ilusiones de Tomás. Hoy ha estado investigando en Internet y ha descubierto que hay muchas ofertas asequibles. A él le preocupa cómo se conectará a Internet con la conexión de su casa y no sabe si tendrá que contratar una nueva línea. También ha oído que hay gente que se conecta en plena calle gracias a las redes inalámbricas. Cuando ha preguntado a algún amigo, todos parece que tienen dispositivos Wi-Fi y Bluetooth, incluso ha descubierto que el mando a distancia de la TV funciona con infrarrojos. Tomás ha decidido intentar comprender como funciona la conexión inalámbrica antes de comprarse un ordenador portátil.

Existen varios tipos de comunicación inalámbrica:

- **Ondas de radio**.
- **Microondas**.
- **Infrarrojos**.
- **Ondas de luz (láser)**.

Para transmitir a largas distancias hay que utilizar ondas direccionales, puesto que necesitamos enviarlas de un “repetidor” a otro estando estos muy alejados entre sí. Este es el caso de las microondas.

Cuando lo importante es emitir en un radio determinado, sin importar demasiado que el radio sea muy grande, utilizaremos ondas omnidireccionales (ondas de radio).

Entre los principales problemas que debe sortear una comunicación inalámbrica están:

- **La distancia entre emisor y receptor.**
- **Las condiciones climáticas.**
- **La seguridad de la transmisión.**

En la actualidad, las comunicaciones inalámbricas están tomando cada vez más relevancia. Aunque en un principio parecía que iban a sustituir a las comunicaciones por cable, sobre todo en las redes LAN, se están convirtiendo en un complemento perfecto. Son muchos los usuarios que mantienen sus equipos cableados a la red y los complementan con otros que utilizan la conexión inalámbrica, Wi-Fi en su mayoría.

Hoy en día, una persona puede conectarse a la red utilizando la tecnología inalámbrica prácticamente en cualquier lugar. En las ciudades utilizando las ondas de radio (Wi-Fi), y en núcleos que no estén tan poblados utilizando la tecnología de los teléfonos móviles.

Autoevaluación

Para transmisiones a largas distancias se utilizan:

- Ondas de radio porque son omnidireccionales.
- Infrarrojos porque pueden atravesar cualquier objeto.
- Microondas porque no hace falta dirigirlas.
- Microondas porque se pueden dirigir.

Estándares de transmisión inalámbrica.

Punto de acceso inalámbrico

La **norma IEEE 802.11** se estableció en junio de 1997 para definir las redes inalámbricas. Es similar al estandar 802.3 (Ethernet), con la diferencia de que se han tenido que adaptar todos sus métodos a un medio no guiado de transmisión.

Este estándar define las redes de área local inalámbricas (WLAN), que operan en el espectro de los 2,4 GHz. El estándar original especificaba la operación a 1 y 2 Mbps usando tres tecnologías diferentes:

- Frecuency Hopping Spread Spectrum (FHSS).
- Direct Secuence Spread Spectrum (DSSS).
- Infrarrojos (IR).

A partir del estándar 802.11 han surgido diferentes modificaciones que se reflejan en la siguiente tabla:

Nombre.	Descripción.
802.11a	Ancho de banda superior (el rendimiento total máximo es de 54 Mbps aunque en la práctica es de 30 Mpbs). Ocho canales de radio en la banda de frecuencia de 5 GHz.
802.11b	Rendimiento total máximo de 11 Mbps (6 Mbps en la práctica) y tiene un alcance de hasta 300 metros en un espacio abierto. Rango de frecuencia de 2,4 GHz con tres canales de radio disponibles.
802.11c	Es solamente una versión modificada del estándar 802.1d que permite combinar el 802.1d con dispositivos compatibles 802.11 (en el nivel de enlace de datos).
802.11d	El estándar 802.11d es un complemento del estándar 802.11 que está pensado para permitir el uso internacional de las redes 802.11 locales. Permite que distintos dispositivos intercambien información en rangos de frecuencia según lo que se permite en el país de origen del dispositivo.
802.11e	Destinado a mejorar la calidad del servicio en el nivel de la capa de enlace de datos. El objetivo del estándar es definir los requisitos de diferentes paquetes en cuanto al ancho de banda y al retardo de transmisión para permitir mejores transmisiones de audio y vídeo.
802.11f	Recomendación para proveedores de puntos de acceso que permite que los productos sean más compatibles. Utiliza el protocolo IAPP que le permite a un usuario itinerante cambiarse claramente de un punto de acceso a otro mientras está en movimiento sin importar qué marcas de puntos de acceso se usan en la infraestructura de la red.
802.11g	Ofrece un ancho de banda elevado (con un rendimiento total máximo de 54 Mbps pero de 30 Mpbs en la práctica) en el rango de frecuencia de 2,4 GHz. Es compatible con el estándar anterior, el 802.11b, lo que significa que los dispositivos que admiten el estándar 802.11g también pueden funcionar con el 802.11b.
802.11h	Tiene por objeto unir el estándar 802.11 con el estándar europeo (HiperLAN 2, de ahí la h de 802.11h) y cumplir con las regulaciones europeas relacionadas con el uso de las

	frecuencias y el rendimiento energético.
802.11i	Está destinado a mejorar la seguridad en la transferencia de datos (al administrar y distribuir claves, y al implementar el cifrado y la autenticación). Se basa en el AES (estándar de cifrado avanzado) y puede cifrar transmisiones que se ejecutan en las tecnologías 802.11a, 802.11b y 802.11g.
802.11Ir	Se elaboró para que pueda usar señales infrarrojas. Este estándar se ha vuelto tecnológicamente obsoleto.
802.11j	El estándar 802.11j es para la regulación japonesa lo que el 802.11h es para la regulación europea.
802.11n	Surge debido a la gran demanda de las WLAN (Wireless Local Area Network). La velocidad real de transmisión podría llegar a los 600 Mbps, llegando a ser hasta 10 veces más rápida que una red bajo los estándares 802.11a y 802.11g, y cerca de 40 veces más rápida que una red bajo el estándar 802.11b. El alcance de operación de las redes es incluso mayor con la incorporación de la tecnología MIMO (Multiple Input-Multiple Output), la cual permite la utilización de varios canales a la vez para enviar y recibir datos gracias a la incorporación de varias antenas.

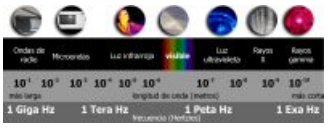
Debes conocer

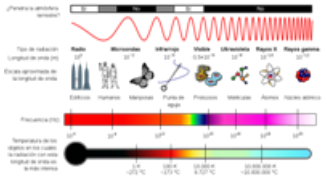
En los siguientes enlaces encontrarás más información sobre las diferentes tecnologías WiFi:

Introducción al estándar 802.11

Los espectros de onda de microndas y radio.

El **espectro electromagnético** es el mapa donde se representan los tipos de ondas electromagnéticas conocidas. Estas ondas se clasifican en función de su longitud de onda o de su frecuencia.





Analizando las dos figuras anteriores podemos extraer varias conclusiones:

- Los humanos solamente podemos ver un rango muy pequeño de longitudes de onda, el rango de la luz visible.
- Las ondas cuanto menor sea su longitud de onda, más direccionales son. Se puede dirigir un rayo X (radiografía) o un rayo Gamma (reacción nuclear) hacia un punto determinado mucho mejor que una emisión de radio.
- Las ondas que tienen longitudes de onda por debajo del espectro visible son más perjudiciales para el cuerpo humano.
- Las comunicaciones inalámbricas están basadas en Infrarrojos, Microondas y ondas de Radio.
- Para comunicaciones a grandes distancias se utilizan Microondas porque son más direccionales que las ondas de Radio.
- Para comunicaciones a muy pequeñas distancias se utilizan Infrarrojos (mandos de electrodomésticos) porque son direccionales y no tienen potencia suficiente para abarcar grandes distancias. Además, es más difícil que interfieran con otras señales como la señal de TV.
- Las ondas de Radio se utilizan en comunicaciones inalámbricas donde es más conveniente que una onda sea omnidireccional. La emisión de una antena de un punto de acceso debe cubrir un área dentro de la cual todo el mundo tenga cobertura.

Autoevaluación

¿Por qué Bluetooth y Wi-Fi pueden convivir sin interferencias si trabajan en las mismas frecuencias?

- ○ Si tienen interferencias.
- ○ Porque Wi-Fi está basada en la técnica de múltiples saltos de frecuencia.
- ○ Porque Bluetooth tiene un alcance de 10 metros aproximadamente.
- ○ Ninguna de las anteriores es correcta.

Topologías.

La topología es la disposición lógica o física de una red.

En redes inalámbricas hablaremos sobre todo de la topología lógica. Básicamente existen dos tipos:

- **Ad-hoc**. Enlaces punto a punto entre dispositivos que estén en el mismo rango.
- **Infraestructura**. Un dispositivo centraliza todas las comunicaciones (AP o punto de acceso). Todos los dispositivos que estén al alcance del AP, lo utilizan para poder comunicarse entre sí o para acceder a otra red a través de él.

Haciendo un símil con la comunicación por cable, el modo Ad-hoc sería equivalente a comunicar dos ordenadores entre sí mediante un cable y el modo Infraestructura equivaldría a comunicar los ordenadores utilizando un concentrador (hub).

Tanto si escogemos uno u otro tipo de conexión, debemos configurar nuestro adaptador inalámbrico (tarjeta) en uno u otro modo.

Si nos fijamos en la topología física, se puede decir que la topología en estrella es la estándar para redes inalámbricas.

En la figura anterior se observa una configuración típica de una red inalámbrica que usa un punto de acceso (AP) para poder conectar todos los equipos de la red local a Internet. Los clientes se conectan de manera inalámbrica al AP y este lo hace por cable a dispositivos que nos facilitan la conexión al exterior (enrutadores).

Los puntos de acceso junto con los enrutadores se pueden empaquetar en una misma “caja”, dando lugar a lo que conocemos como router inalámbrico.

Autoevaluación

Si quisiéramos utilizar un Punto de Acceso (AP) como si fuese un hub para unir varios ordenadores de manera inalámbrica:

- Configuraríamos la red en modo Infraestructura.
- Configuraríamos la red en modo Ad-hoc.
- Un AP nunca puede comportarse como un hub o concentrador.
- No podríamos hacerlo porque no tendríamos acceso a Internet.

Asociación y autenticación en la WLAN.

La autenticación de las WLAN se produce en la capa 2 del modelo OSI. Se autentica el dispositivo no al usuario.

El cliente envía una trama de petición de autenticación al punto de acceso (AP), esta trama se acepta o se rechaza por el AP. Si se acepta, se produce la asociación, en la que el cliente es autorizado a usar los servicios del AP para transferir datos.

Existen básicamente tres tipos de autenticación:

- **Abierto.**
- **WEP.**
- **WPA.**

WEP: Es un mecanismo simple de cifrado de datos. Utiliza el logaritmo RC4 para cifrar los datos y claves estáticas de 64, 128 e incluso 152 bits según el fabricante.

Se define una clave secreta que debe ser declarada a nivel de cada adaptador inalámbrico de la red así como en el punto de acceso. La clave se utiliza para generar un número aleatorio de longitud igual a la longitud de la trama. Cada elemento de la red que desee comunicarse con otro debe conocer la clave secreta que va a servir al cifrado WEP.

Una vez realizado, todos los datos transmitidos son obligatoriamente cifrados. De este modo WEP asegura el cifrado e integridad de los datos durante la transferencia.

WEP es bastante vulnerable. La clave de sesión compartida por todas las estaciones nunca cambia. Esto significa que para implementar un gran número de estaciones WiFi, es necesario configurarlas utilizando la misma clave de sesión. El conocimiento de la clave basta para descifrar la comunicación.

Además, 24 bits de la clave sirven únicamente para la inicialización, lo que significa que sólo 40 bits de la clave de 64 bits sirven realmente para cifrar (104 bits para el caso de las claves de 128 bits).

Existen muchos programas capaces de ejecutar ataques contra este tipo de encriptación y averiguar la clave correcta. Para que fuese más seguro, deberíamos cambiar la clave constantemente.

En cuanto a la integridad de los datos, el CRC32 permite la modificación de la cadena de verificación del paquete, la cual es comparada con otra generada a partir de los datos recibidos. Esto permite a un hacker hacer pasar sus informaciones como informaciones validas.

Aunque presenta demasiadas debilidades es uno de los mecanismos de seguridad que más se emplean. Mejora su seguridad si se utiliza el WEP de 128 bits.

WPA: Surge para subsanar todas las debilidades de WEP. La primera característica es que utiliza claves dinámicas.

WPA y WPA2 son protocolos diseñados para trabajar con y sin un servidor de manejo de llaves. Si no se usa un servidor de llaves, todas las

estaciones de la red usan una “llave previamente compartida” PSK (Pre Shared Key). El modo PSK se conoce como WPA o WPA2-Personal.

Cuando se emplea un servidor de llaves, al WPA2 se le conoce como WPA2-Corporativo (WPA2-Enterprise). En WPA-Corporativo, se usa un servidor IEEE 802.1X para distribuir las llaves.

Una mejora notable de WPA sobre WEP es la posibilidad de intercambiar llaves de manera dinámica mediante un protocolo de integridad temporal de llaves TKIP (Temporal Key Integrity Protocol). Este protocolo se encarga de cambiar la clave compartida entre punto de acceso y cliente cada cierto tiempo, para evitar ataques que permitan revelar la clave.

Autoevaluación

Si al configurar una red inalámbrica quiero establecer el máximo nivel de seguridad, ¿qué encriptación debo escoger?:

- WPA.
- WEP.
- SSID.
- Sistema OPEN o abierto.

Direccionamiento.

Caso práctico

Una vez que tiene el ordenador portátil, Tomás quiere configurarlo para la red que tiene montada en casa, sin llamar a ningún técnico para que le ayude. Para ello, ha pedido los apuntes a un sobrino que está estudiando el ciclo formativo de Administración de Sistemas Informáticos en Red. Su sobrino le ha prestado el capítulo de “Direccionamiento”, y como ya conoce el concepto de IP cree que puede intentarlo puesto que los apuntes parecen buenos.

Para poder identificar una máquina en Internet existe la dirección IP (Internet Protocol), la cual es asignada por InterNIC (Internet Network Information Center), ahora llamada ICANN (Internet Corporation for Assigned Names and Numbers).

El mecanismo que establece las normas que deben cumplir estas direcciones se denomina direccionamiento.

Hasta ahora, el método de direccionamiento más utilizado ha sido el direccionamiento IPv4, aunque cada vez está tomando más peso el IPv6.

A parte de los diferentes protocolos que se pueden utilizar, existen técnicas para poder aprovechar mejor estas direcciones (subredes, superredes, CIDR).

El direccionamiento se puede llevar a cabo también en el nivel 2 de la arquitectura de niveles OSI, con las direcciones MAC, pero tiene mucha más relevancia el direccionamiento de nivel 3 con las direcciones IP, ya que las direcciones MAC no pueden atravesar los enrutadores.

El direccionamiento en Internet es distinto del que podemos llevar a cabo en las redes LAN. En el espacio WAN las direcciones las gestiona InterNIC, mientras que en las LAN son gestionadas por el administrador de la red. Esto implica que en una LAN podemos escoger el número y el tipo de direcciones que queramos, pero no en Internet. Si queremos que una dirección sea válida para viajar en Internet tenemos que solicitarla y pagar por ella (esto es lo que nuestro ISP hace y nos lo repercute a nosotros).

El objetivo principal es el mismo, poder tener identificados todos los elementos de una red para poder establecer comunicaciones entre sí.

Reflexiona

Si hacemos un símil con la red telefónica, las direcciones IP equivaldrían a los números de teléfono. Si un usuario quiere establecer comunicación con otro, debe marcar un número en el terminal.

En las redes informáticas, si un PC quiere establecer comunicación con otro, debe disponer de una dirección (dirección IP). De hecho, cuando escribimos una dirección URL (http://www.urldeejemplo.com/camino/al/recurso) en nuestro navegador, estamos “marcando” realmente la dirección IP con la que queremos conectarnos. Esto es posible gracias al servicio DNS, con él podemos utilizar letras en lugar de números (son más fáciles de recordar).

Una vez que todos los equipos tienen asignada una dirección, se pueden emplear técnicas (subredes, superredes, CIDR) para que la gestión de estas direcciones agilice el funcionamiento de la red. En la red de teléfono se empleaban los prefijos (942 Cantabria, 985 Asturias, 91 Madrid, 93 Barcelona, etc.).

Autoevaluación

El direccionamiento consiste en:

- Asignar direcciones a los nodos de una red.
- Direccionar los paquetes que se envían a través de los routers.
- Convertir las direcciones IPv4 en IPv6.
- Ninguna de las anteriores.

IPv4.

Una dirección IPv4 consta de 32 bits, agrupados de 8 en 8 y representados en código decimal. Los valores de estos números decimales van entre 0 y 255.

Así por ejemplo, la dirección 192.168.1.1 se correspondería con el número binario `11000000.10101000.00000001.00000001`.

El direccionamiento IPv4 establece que de los 32 bits:

- Una parte de los bits determina el tipo de dirección.
- Otra parte de los bits determina el número de la red.
- Otra parte de los bits determinan el número de host.

Para poder identificar cuantos bits se utilizan para determinar los host y cuantos para las direcciones de red, se utiliza la **"máscara de red".** Cada dirección IP tiene asociada una máscara de red. La máscara de red está constituida por 32 bits, si un bit de la máscara vale 1 implica que ese bit en la dirección IP se dedica a las direcciones de red, si el bit vale 0 implica que ese bit en la IP se dedica a identificar host.

Por ejemplo, si una dirección IP tiene una máscara de red `11111111.00000000.00000000.00000000`, significa que mi dirección IP tiene los 8 primeros bits dedicados a especificar direcciones de red y los 24 restantes a especificar direcciones de equipo.

	Representación binaria.	Representación decimal.
Direccion IP.	`00000001.00000000.00000000.00000001`	1.0.0.1
Mascara de red.	`11111111.00000000.00000000.00000000`	255.0.0.0
Direccion de red.	`00000001.00000000.00000000.00000000`	1.0.0.0

La utilidad de las máscaras de red está en que nos sirven para saber cuál es la dirección de red asociada a una determinada dirección IP. Para poder hacer esto se realiza la operación AND entre la IP y la máscara de red, el resultado es la dirección de red. Esta operación es la que realizan los routers cuando les llega un paquete con una determinada IP y una máscara de red, con esto pueden saber cuál es la dirección de red destino de ese paquete y encaminarlo en sentido correcto.

Recordando la **operación AND binaria**:

Operación	Resultado
0 and 0	0
0 and 1	0
1 and 0	0
1 and 1	1

Si observamos la tabla anterior de direcciones se puede comprobar fácilmente como la operación AND entre la dirección IP (1.0.0.1) y la máscara (255.0.0.0) nos da como resultado la dirección de red (1.0.0.0).

Esto es muy importante porque hay que recordar que los routers trabajan con direcciones de red, aunque el paquete llegue con una dirección IP destino y origen, se necesita saber la dirección de red para poder encaminarlo correctamente.

Clases de direcciones.

Se dice que **existen las siguientes clases de direcciones**, dependiendo de cuales sean los dígitos por los que comienza dicha dirección:

Clase	Distribución de los bits entre número de red (r) y número de host (h).
Clase A	`0rrrrrrr.hhhhhhhh.hhhhhhhh.hhhhhhhh`
Clase B	`10rrrrrr.rrrrrrrr.hhhhhhhh.hhhhhhhh`
Clase C	`110rrrrr.rrrrrrrr.rrrrrrrr.hhhhhhhh`
Clase D	`1110xxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx`
Clase E	`1111xxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx`

Los tipos de direcciones utilizadas para identificar máquinas (host) son A, B y C. Reservando las direcciones D y E para multicasting y experimentos.

DIRECCIONES IP CLASE A:

En una dirección IP de clase A, el primer byte representa la red. El bit más importante (el primer bit a la izquierda) es siempre cero, lo que significa que hay 2^7 (de 00000000 a 01111111) posibilidades de red, lo que permite tener 128 redes diferentes. No obstante tienes que tener en cuenta que la red 0 (bits con valores 00000000) no existe, y que el número 127 está reservado para indicar su equipo.

Las redes disponibles de clase A son, por lo tanto, redes que van desde 1.0.0.0 a 126.0.0.0.

Los tres bytes restantes representan los equipos de la red. Por lo tanto, una red de clase A puede contener una cantidad de equipos igual a:

$$2^{24}\text{-}2 = 16.777.214 \text{ equipos.}$$

Se resta 2 porque ningún equipo puede tener una dirección de red asignada, y tampoco la dirección en la que la parte de los host esté a 1 porque se reserva para difusión.

La primera dirección IP posible de clase A es 1.0.0.1, donde la dirección de red es la 1.0.0.0. Para esta red la dirección de difusión sería 1.255.255.255.

DIRECCIONES IP DE CLASE B:

En este tipo de direcciones se utilizan los dos primeros bytes (empezando por la izquierda) para identificar a las redes. Todas las direcciones de este tipo comienzan por 10, por lo tanto tendremos 2^{14} redes (de `10000000.00000000.xxxxxxxx.xxxxxxxx` a `10111111.11111111.xxxxxxxx.xxxxxxxx`). La primera dirección de red sería la 128.0.0.0 y la última sería 191.255.0.0.

En este tipo de direcciones, por cada dirección de red podemos identificar a 2^{16}-2 equipos (se elimina la dirección de red y la dirección de difusión). Si tomamos como ejemplo la primera dirección de red 128.0.0.0, la primera dirección IP válida sería la 128.0.0.1 y la dirección de difusión de esta red sería la 128.0.255.255.

DIRECCIONES IP DE CLASE C:

Las direcciones IP de clase C comienzan todas por 110 y dedican 3 bytes para identificar a las direcciones de red, por lo tanto tendremos 2^{21} posibles direcciones de red (desde `11000000.00000000.00000000.xxxxxxxx` a la `11011111.11111111.11111111.xxxxxxxx`). La primera dirección de red sería la 192.0.0.0 y la última la 223.255.255.0.

Para cada dirección de red podemos identificar 2^8-2 equipos (se elimina la dirección de red y la dirección de difusión). Para la primera dirección de red (192.0.0.0) la primera dirección IP posible es 192.0.0.1 y la dirección de difusión la 192.0.0.255.

Si representamos en una tabla las redes posibles y las IP posibles por cada dirección de red, tendríamos que:

Clase.	Nº Redes.	Nº Equipos/Red.
A	2^7=128	2^{24}-2=16777214
B	2^{14}=16384	2^{16}-2=65534
C	2^{21}=2097152	2^8-2=254

A todas estas posibles direcciones **hay que restar direcciones reservadas que no es posible utilizar**:

- **127.0.0.1**: Se reserva para referirnos a direcciones de loopback, es decir para referirnos a nuestro propio equipo.
- **0.0.0.0**: Dirección que utilizan los equipos al arrancar.

También **existen un conjunto de direcciones que solamente son válidas en redes locales, que no sirven para identificar un host en Internet, son las direcciones privadas**.

Existen direcciones privadas para las tres clases de direcciones IP, como se puede ver en la siguiente tabla:

Clase.	Rango de IP.
A	10.0.0.1 a 10.255.255.254
B	172.16.0.1 a 172.31.255.254
C	192.168.0.1 a 192.168.0.254

NAT

La aparición de los enrutadores con la cualidad de NAT permitió que se pudieran utilizar varias direcciones privadas detrás del router consumiendo solamente 1 dirección pública de cara a Internet. Esta fue una de las primeras medidas adoptadas para intentar solucionar el problema de la escasez de IP.

Con este mecanismo se puede intercambiar información entre dos redes que a priori son incompatibles, por ejemplo, una red LAN y una WAN.

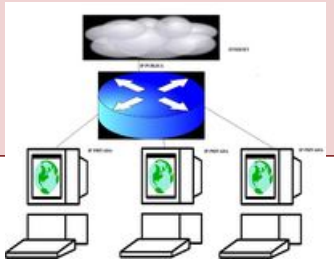
Esta propiedad, que ahora es vital, con la llegada de nuevos protocolos que impulsan las conexiones P2P como IPv6, irá perdiendo importancia.

Su funcionamiento se basa en el cambio de direcciones origen en cada paquete de salida y a veces del puerto. Todo esto se almacena en una tabla para que el dispositivo pueda recordar que cambios hizo y así devolver la información a quien la generó cuando haya una respuesta.

Reflexiona

Imaginemos que Internet (WAN) es un local donde hace falta tener un carnet especial para entrar (IP pública) y que la gente que quiere entrar al local y está esperando fuera forma la red LAN. Si alguien tiene 1 carnet y lo duplica podría hacer que entrasen todas las personas que

tuvieran el carnet “falsificado”. Al mismo tiempo, es necesario recordar a quien (IP privada) ha dado cada copia para que cuando salga a la calle se lo devuelva y se lo pueda prestar a otros, esa relación la lleva escrita en una hoja de papel que va actualizando constantemente con las entradas y salidas. La persona que copia los carnets, los presta y los recoge sería el dispositivo con propiedad NAT.



Autoevaluación

En una red LAN tenemos 257 ordenadores, no necesitamos conexión a Internet, disponemos de concentradores suficientes para conectar físicamente todos los equipos, tendremos que escoger para configurar los equipos las IP óptimas para no desaprovechar demasiadas direcciones de host:

- Dos direcciones IP de clase C privadas IPv4.
- Una dirección IP de clase A privada IPv4.
- Una dirección IP de clase B privada IPv4.
- Una dirección IP de clase A privada y una de clase C privada IPv4.

Subredes.

Como se ha visto en el punto anterior, uno de los mecanismos que se utilizaron para poder solucionar la escasez de IP fueron las direcciones privadas junto con NAT.

Las subredes son un método para poder crear varios dominios de difusión a partir de una dirección de red, esto nos ayudará a segmentar una red.

Por ejemplo:

Supongamos que hemos comprado una dirección de red y que necesitamos “aislar” varios equipos pero a la vez que se comuniquen entre sí (crear diferentes dominios de difusión), la solución estaría en crear subredes dentro de nuestra red, de tal manera que desde fuera solamente se viera una red pero internamente funcionara como un conjunto de pequeñas redes.

¿CÓMO?

Una dirección IP hemos visto que tiene bits dedicados a determinar las direcciones de red y bits dedicados a especificar el host. Las subredes se consiguen utilizando bits de host para aumentar los bits dedicados a determinar direcciones de red. En otras palabras, se “roban” bits a la parte de la IP que correspondiente a especificar direcciones de equipos. Con esto conseguimos tener varias direcciones de subred a partir de una dirección de red. Por el contrario se disminuye el número de equipos que puedo identificar.

Supongamos que tenemos la dirección de red 192.168.1.0 de clase C. Con esta dirección de red podríamos identificar a 254 equipos y tendríamos un dominio de difusión cuya dirección sería 192.168.1.255. La máscara de red que corresponde con esta IP sería 255.255.255.0.

Ahora se me ocurre “robar” 2 bits a la parte host para crear más dominios de difusión con lo cual la máscara de red quedaría como 255.255.255.192. En esta situación y poniendo la dirección de red original en binario tendríamos las siguientes direcciones de subred.

Dirección de subred	Dirección de subred	Máscara	IPs posibles por subred	Dirección difusión
11000000.10101000.00000001.00xxxxxx	192.168.1.0	255.255.255.192	2^6-2 = 62	192.168.1.63
11000000.10101000.00000001.01xxxxxx	192.168.1.64	255.255.255.192	2^6-2 = 62	192.168.1.127
11000000.10101000.00000001.10xxxxxx	192.168.1.128	255.255.255.192	2^6-2 = 62	192.168.1.191
11000000.10101000.00000001.11xxxxxx	192.168.1.192	255.255.255.192	2^6-2 = 62	192.168.1.255

Si analizamos la tabla se puede ver como hemos conseguido 4 dominios de difusión, pero también que hemos perdido algunas direcciones para poder definir direcciones de equipos (248 frente a 254).

CIDR y superredes.

El término CIDR se utiliza para referirse a “encaminamiento entre dominios sin clase”. Es una técnica que permite resumir un conjunto de direcciones IP contiguas de red de una clase en una misma dirección de red.

De esta manera se puede disponer de un espacio de direccionamiento superior sin necesidad de solicitar una dirección de rango superior.

Por ejemplo:

Podemos agrupar varias direcciones de tipo C en una de clase B, o varías de tipo B en una de tipo A. Con esto conseguimos que las tablas de encaminamiento de los routers no crezcan demasiado y se agilicen los mecanismos de control del encaminamiento.

Comparando esta técnica con las subredes, se puede decir que son inversas, con las subredes aumentamos los dominios de difusión (direcciones de red) y con las superredes disminuimos las direcciones de red.

En 1993 se eliminó la restricción del espacio de direcciones con clase, adoptándose un esquema o notación en el que se utiliza una longitud de prefijo común arbitraria para indicar la dirección común de red de un bloque de direcciones de red contiguas que se quieren resumir en una sola dirección de red. Este esquema o notación es lo que se conoce como formato CIDR o de superred y que representa una alternativa al direccionamiento IP con clase. Por consiguiente, el concepto de clases A, B y C desaparece al usar prefijos diferentes a los prefijos obligatorios de dichas clases.

¿CÓMO?

Como hemos visto anteriormente, una dirección IP tiene bits que definen características de red y bits que definen características de host. Si utilizamos la dirección 192.168.0.0, se podrían direccionar 254 hosts (2^8-2=254). Si los elementos que forman mi red soportan CIDR, se puede conseguir que esta dirección de red sea capaz de identificar más de 254 máquinas.

Con CIDR podemos utilizar bits del tercer octeto para generar más direcciones de host. Por ejemplo, si cogemos 2 bits del tercer octeto, podremos conseguir 2^{10} direcciones para equipos.

Para poder conseguir esto debemos especificar que la máscara de red utilizada es la 255.255.252.0 o utilizando otra notación 192.168.0.0/22.

Dirección de red.	Bits.	Máscara de red.
192.168.0.0	11000000.10101000.00000000.00000000	255.255.252.0

Por otra parte, con esta técnica, podemos agrupar direcciones de red en una sola. Supongamos que tenemos las siguientes direcciones de red:

Dirección de red.	Binario.	Máscara de red.
192.168.0.0	11000000.10101000.00000**00**.00000000	255.255.255.0
192.168.0.1	11000000.10101000.00000**01**.00000000	255.255.255.0
192.168.0.2	11000000.10101000.00000**10**.00000000	255.255.255.0
192.168.0.3	11000000.10101000.00000**11**.00000000	255.255.255.0

Si nos fijamos en las direcciones expresadas en modo binario se puede observar como las cuatro direcciones varían entre sí en los dos últimos dígitos del tercer octeto (resaltado en negrita). Si utilizamos CIDR, podemos aglutinar estas cuatro direcciones de red en una sola si utilizamos la máscara de red 255.255.252.0. La dirección de red que representaría a estas cuatro sería:

Dirección de red.	Binario.	Máscara de red.
192.168.0.0	11000000.10101000.00000000.00000000	255.255.252.0

Utilizando otra notación:

192.168.0.0/22

Como se puede ver, la clave de CIDR es utilizar una máscara según las nuestras necesidades, sin respetar el concepto de las máscaras asociadas a direcciones de tipo A, B o C. Para poder hacer esto, nuestros dispositivos de encaminamiento deben soportar CIDR.

IPv6.

IPv6 surge para poder solucionar todos los problemas que IPv4 no resuelve. El mayor de los problemas es la escasez de direcciones IP en Internet.

Mientras IPv4 tiene un espacio de direcciones de 2^{32} (4.294.967.296), IPv6 tiene 2^{128} (340.282.366.920.938.463.463.374.607.431.768.211.456).

En principio, con el protocolo IPv6 el problema de la escasez estaría solucionado, incluso podríamos dejar de utilizar NAT y poder establecer conexiones “punto a punto” entre todos los usuarios.

Aunque en informática no podemos aventurarnos a sentenciar nada, basta recordar la frase del presidente de IBM en 1943 en la que decía que “Pienso que el mercado de ordenadores en el mundo puede ser de 5 unidades” o la frase de Bill Gates en 1981 “640 Kbps deben ser suficientes para cualquier usuario”.

Una de las ventajas de de este protocolo es que puede convivir con IPv4 por lo que puede utilizar muchas de las infraestructuras ya creadas.

Las direcciones IPv6 identifican interfaces de red de manera individual o en grupo. A una misma interfaz se le pueden asignar múltiples direcciones.

Las direcciones se clasifican en tres tipos:

- **Unicast**: Identificador para una única interfaz (direcciones IPv4 actuales).
- **Anycast**: Identificador para un conjunto de interfaces. Un paquete enviado a una dirección de este tipo es entregado a cualquiera de las interfaces identificadas por esta dirección, llegará a la que esté más cerca.
- **Multicast**: Identificador para un conjunto de interfaces. El paquete enviado a una dirección de este tipo se entregará a todas las interfaces (parecido al broadcast de IPv4).

Las direcciones IPv6 se representan de la manera siguiente:

- **x:x:x:x:x:x:x:x**
  - Cada x es el valor hexadecimal de 16 bits.
  - 8 grupos (128/16 = 8).

- No es necesario escribir todos los ceros a la izquierda.
- Al menos debe existir un número en cada grupo.

Por ejemplo:

- `ABCD:BA98:7654:3210:FEDC:BA98:7654:3110`

- Se puede utilizar "**::**" para representar a las cadenas de ceros. Dicho símbolo podrá aparecer una sola vez en cada dirección. La dirección de loopback `0:0:0:0:0:0:0:1` se podrá representar como `::1`.
- **Cuando tengamos nodos IPv4 e IPv6 , podemos utilizar la notación `x:x:x:x:x:x:d.d.d.d`**, donde x representan valores hexadecimales de las seis partes más significativas (de 16 bits cada una) que componen la dirección y las d, son valores decimales de los 4 partes menos significativas (de 8 bits cada una), de la representación estándar del formato de direcciones IPv4.
  Ejemplos:
  - `0:0:0:0:0:0:13.1.68.3`
  - `0:0:0:0:0:FFFF:129.144.52.38`

  O de otra manera:
  - `::13.1.68.3`
  - `::FFFF:129.144.52.38`

Los prefijos de identificadores de subredes, routers y rangos de direcciones IPv6 son expresados de la misma forma que en la notación CIDR utilizada en IPv4.

Dominios de colisión y difusión.

Caso práctico

Tomás ha conseguido montar un red LAN en la que tiene dos ordenadores de sobremesa y un portátil conectados entre sí y con acceso a Internet gracias a un router. En esta situación se ha preguntado cómo es posible que los ordenadores se comuniquen entre sí y además puedan tener acceso a Internet al tiempo. Un amigo le ha comentado que eso se consigue gracias a que los routers crean diferentes dominios de colisión y difusión y de esa manera disminuyen el riesgo de colisiones en las comunicaciones.

Los **dominios de colisión** y de **broadcast** (difusión) son los espacios de la red donde la comunicación emitida por cada uno de los nodos puede interferir entre sí. Los dominios, tanto de colisión como de difusión van ligados a los dispositivos de interconexión más usuales que nos podemos encontrar (concentradores, conmutadores y enrutadores).

Una red LAN de tipo Ethernet (la más común) es un espacio con probabilidades altísimas de colisiones entre los paquetes de información que viajan. Los orígenes de estas redes están ligados a la tecnología de cable coaxial y no utilizaban dispositivos de interconexión para diferenciar dominios de colisión (hub), todos los equipos compartían el mismo medio (un único dominio de colisión).

La llegada de la tecnología de cable de par trenzado y los dispositivos de interconexión (switch y router) hizo posible que se redujera de manera considerable el riesgo de colisiones, debido a que los dispositivos eran capaces de dividir el dominio de colisión en dominios más pequeños y además podían comunicar redes con diferentes dominios de difusión (router).

Autoevaluación

El dominio de colisión es:

- ○ Sitio físico de la red donde todos los equipos tienen una IP del mismo tipo
- ○ El espacio de conexión de una red creado por un hub.
- ○ Es un dominio de difusión.
- ○ Una red de cable de par trenzado.

Dominio de colisión.

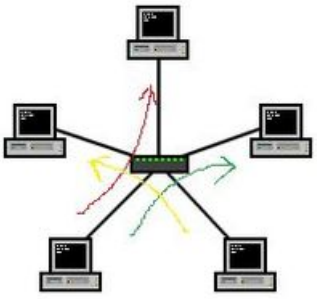
Un dominio de colisión es un sitio de nuestra red donde los paquetes enviados por cada uno de los nodos pueden "colisionar". El objetivo de una red es que funcione la intercomunicación entre cada uno de sus nodos con el mínimo número de problemas.

Parece obvio que cuanto mayor sea el espacio con probabilidades de choque más choques habrá. Para evitar los estas colisiones, una de las medidas empleadas es la separación de los espacios donde puede haber una colisión (es más fácil controlar varios espacios pequeños que un solo espacio grande). Si utilizamos una carretera como símil, una carretera en la que no estén delimitados los carriles tendrá más probabilidades de choques que otra en la que los carriles estén perfectamente separados. El concepto de carril para la carretera podría parecerse al concepto de dominio de colisión en la redes de ordenadores.

Si tenemos varios nodos conectados entre sí por un dispositivo incapaz de separar “carriles”, estamos hablando de un solo dominio de colisión. El dispositivo que se comporta de esta manera es el **hub o concentrador**.

Si por el contrario, utilizamos un **conmutador (switch) o un enrutador (router)**, podremos disfrutar de la separación de canales de comunicación, es decir de los “carriles”. En esta situación tendremos varios dominios de colisión, tantos como comunicaciones establecidas entre los diferentes nodos de la red. Cuantos más puertos tengan los dispositivos de interconexión, más capacidad para separar dominios de colisión.

La utilización de estos dispositivos, que son capaces de “gestionar” el tráfico, supone una ralentización de la comunicación pero disminuyen las probabilidades de colisión.



En la imagen se puede observar que los cinco equipos están conectados mediante un conmutador, este dispositivo es capaz de crear por ejemplo 3 dominios de colisión diferentes (rojo, amarillo y verde) de manera que las comunicaciones entre los distintos equipos no sufran colisiones en tiempo ni espacio.

Dominio de difusión.

Los dominios de difusión son los sitios de la red que se pueden separar de acuerdo a la dirección de red que los identifica. Los dispositivos capaces de crear dominios de difusión, o mejor dicho, de separar dominios de difusión, son los enrutadores (routers).

Es decir, una red local en la que hay varios concentradores y conmutadores, puede tener varios dominios de colisión separados pero un solo dominio de difusión.

Si en una red introduzco un enrutador, por lo menos tendré la capacidad de crear dos dominios de difusión diferentes, ya que un router como mínimo debe tener la capacidad de trabajar con dos direcciones de red diferentes.

El ejemplo más claro es un router con un puerto WAN y uno o varios puertos LAN (router común). Los equipos que “cuelguen” del puerto WAN pueden tener una dirección de red totalmente diferente a la dirección de red que tengan los equipos conectados a los puertos LAN y sin embargo que haya comunicación.

Si considerásemos el mar como un tipo de red y la tierra como otro tipo de red diferente y nos fijáramos en el transporte de mercancías en un puerto cualquiera, las grúas que cogen las mercancías de los barcos y las colocan en los camiones para su transporte por carretera estarían haciendo la función de un router.

Los barcos (al igual que los PC) se identifican con una numeración diferente a los camiones (matrículas) porque viajan por redes diferentes, tendrían direcciones IP diferentes, pero la grúa instalada en el puerto es capaz de coger la “información” de los barcos y colocarla en los camiones; Es el mismo proceso que un router hace con las redes LAN y WAN.

Un dominio de difusión sería el mar y otro dominio de difusión diferente sería el puerto en tierra firme.

Resolución de direcciones. ARP y RARP.

Caso práctico

Tomás ya tiene claro la razón de utilizar conmutadores o routers en una red para evitar colisiones, pero no se explica como un ordenador es capaz de encontrar el ordenador destino de su mensaje solamente utilizando la IP del destinatario.

¿Cómo encuentran el destinatario si solamente tenemos la dirección IP?

Las direcciones IP no son entendidas en los dos primeros niveles (físico, enlace), sin embargo las tarjetas de red sí que vienen identificadas con una dirección Ethernet que viene de fábrica (MAC) y que consta de 48 bits. Esta dirección tiene una parte que depende de cada fabricante, para asegurarnos de que no hay dos tarjetas con la misma dirección.

Las tarjetas envían y reciben tramas basadas en las direcciones MAC. Las direcciones Ethernet expresadas en hexadecimal tienen el siguiente aspecto:

```
90-4C-E5-9B-15-84
```

Los primeros 24 bits identifican al fabricante (`90-4C-E5`) y los 24 últimos cualquier otro dato como la serie del fabricante, de esta manera se asegura que cada tarjeta tiene una dirección diferente.

Realmente las tarjetas de red se comunican utilizando las direcciones MAC, pero es evidente que no se pueden utilizar las MAC para “atravesar” enrutadores y comunicarse en Internet.

Reflexiona

Ejemplo: Un host identificado como host.nombrededominio.com tiene la dirección IP 84.127.234.102 asociada, si quiero comunicarme con dicho host necesito:

- Traducir host.nombrededominio.com a la IP 84.127.234.102. (DNS)
- Encontrar la tarjeta Ethernet que está asociada a la dirección IP 84.127.234.102. (ARP)

Para poder encontrar la máquina se emite un paquete de difusión Ethernet para preguntar quién es la dirección IP 84.127.234.102, el host que tenga esa dirección responderá. Todo esto lo hace ARP.

ARP se podría sustituir por archivos de configuración en los que figurasen todas las IP asociadas a las direcciones MAC, cuando llegase un paquete con una determinada dirección destino IP, en este archivo encontraríamos la dirección MAC correspondiente a esa IP. Todo este proceso lo realiza el protocolo ARP, resuelve el problema de encontrar qué dirección Ethernet corresponde a una IP dada. Pero en ocasiones surge el problema contrario, dada una MAC ¿Cuál es la dirección IP?

En estas ocasiones se recurre al protocolo **RARP (Protocolo de Resolución de Direcciones de Retorno)**. RARP permite actuar a las estaciones como si lanzaran la pregunta “Mi dirección MAC es esta ¿alguien sabe mi IP?”. Para que RARP actúe se necesita un servidor RARP, para solucionar esto se diseñó el protocolo BOOTP. Este último tiene el inconveniente de que necesita configuración manual para relacionar IP con direcciones Ethernet.

Todos estos problemas los solucionó DHCP que surgió como resultado de la evolución del BOOTP.

Autoevaluación

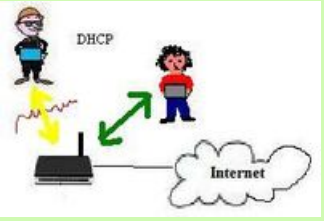
En una red de tipo Ethernet, sabiendo la dirección física del equipo, el protocolo que me permite saber la dirección IP es:

- ARP.
- RARP.
- MAC.
- IP.

Direccionamiento dinámico (DHCP).

Caso práctico

Hoy Tomás ha tenido que ir a casa de un amigo para ayudarle en un trabajo que estaba realizando. Todos los documentos que necesitaba, los tenía almacenados en el portátil por lo que decidió llevarse el ordenador a casa de su amigo. Cuando llegó a su casa, intentó conectarse a la red de su amigo pero no pudo, la señal era excelente y era capaz de ver la red pero fue imposible conectarse. Su amigo, no tiene ni idea de informática y tiene la red tal y como se la dejaron configurada los técnicos, puesto que lo intentaron varias veces sin éxito, decidieron llamar a la compañía telefónica. El técnico de la compañía, al otro lado del teléfono les preguntó varias cosas y todo parecía estar correctamente configurado hasta que les hizo una pregunta que les dejó paralizados “¿Tienen ustedes configurada la tarjeta de red en modo DHCP?”. La respuesta fue “No sabemos de que nos habla”, Tomás había sido capaz de configurar su red local con direcciones estáticas pero no con DHCP.



El direccionamiento dinámico es un mecanismo que nos proporciona una configuración de los parámetros de red de forma automática. La dirección proporcionada es la adecuada para que nuestro nodo funcione correctamente en la red, ya sea una LAN o una WAN. Este mecanismo recibe el nombre de servicio DHCP (Dinamic Host Configuration Protocol).

DHCP puede usarse cuando el número de direcciones IP es menor que el número de computadores y todos no están conectados a la vez, como en un proveedor de servicio de Internet (ISP), de esta manera se desaprovechan menos las direcciones.

Para que funcione este mecanismo deberá existir un servidor de direcciones DHCP en la red, encargado de asignar las direcciones a los host. Además, los host deberán configurar sus interfaces de red de manera que ejecuten el servicio DHCP, generalmente existe siempre una opción de configuración tal como “Obtener una dirección IP automáticamente”.

El protocolo DHCP se publicó en octubre de 1993, estando documentado actualmente en la RFC 2131. Para redes con IPv6 se ha creado DHCPv6 publicado como RFC 3315.

El protocolo DHCP incluye tres métodos de asignación de direcciones IP:

- Asignación manual o estática: Es capaz de asignar una dirección a una máquina determinada. Este tipo de asignación puede constituir una medida de seguridad porque se puede controlar en cada momento que máquina está conectada.
- Asignación automática: Asigna direcciones a los clientes de forma automática pero no las renueva hasta que el cliente quiere.

- Asignación dinámica: Asigna direcciones a los clientes de forma automática renovándolas cada cierto intervalo de tiempo. Es el administrador del servidor DHCP quien escoge el intervalo y la duración de cada dirección IP. Es muy útil cuando el número de host es grande.

Cuando el DHCP es incapaz de asignar una dirección IP, se utiliza un proceso llamado APIPA ("Automatic Private Internet Protocol Addressing").

Al no detectar la presencia de un servidor DHCP, el sistema por medio de APIPA se asigna una dirección IP privada, de clase B en el rango 169.254.0.1 a 169.254.255.254 con máscara 255.255.0.0.

Autoevaluación

DHCP asigna direcciones:

- ○ Públicas para poder conectarse a Internet.
- ○ De una duración limitada.
- ○ Utilizando el método APIPA.
- ○ Privadas porque solo funciona en redes LAN bajo servidores Windows.

Adaptadores de red.

Caso práctico

Tomás viaja constantemente con su ordenador portátil, incluso fines de semana porque ha descubierto que desde cualquier sitio puede conectarse a Internet o leer su correo electrónico. Ayer, regresando a casa se le cayó al suelo el maletín y desgraciadamente parece que ahora no puede conectarse a Internet. No sabe que pieza se ha roto pero está seguro de que ha sido a raíz del golpe. El técnico de la tienda donde se compró el portátil se lo confirma, se ha roto el adaptador de red inalámbrico PCMCIA. ¿Es grave? ¿Cuánto me va a costar? La respuesta le ha tranquilizado "No se preocupe, hay muchos tipos de adaptadores a precios muy asequibles, alrededor de 30 euros, le recomiendo un adaptador USB". Tomás se ha dirigido al stand de los adaptadores y se ha visto desbordado por la cantidad de ellos que hay. ¿Cuál será el adaptador ideal para mis necesidades?

Los adaptadores de red son dispositivos hardware que permiten que un equipo pueda conectarse a otro utilizando un cable o de manera inalámbrica.

Los adaptadores de red (tarjetas de red) convierten los datos en señales eléctricas que pueden transmitirse a través de un cable. Así mismo, convierten las señales eléctricas en paquetes de datos que el sistema operativo del equipo puede entender.

Existen distintos tipos de adaptadores de red que han evolucionado junto con los sistemas operativos y los medios de transmisión empleados.

En un principio, el medio de transmisión más empleado era el cable coaxial y los adaptadores de red eran tarjetas que incorporaban este tipo de conector. Si bien el cable coaxial sigue empleándose en la actualidad, es el cable de par trenzado el más utilizado, se le conoce de manera coloquial como "cable RJ45" aludiendo al tipo de conector empleado. También está creciendo el empleo de redes inalámbricas y con ellas los tipos de adaptadores para emplear esta tecnología.

Los adaptadores pueden estar incluidos en el hardware del equipo (internos) o externos con conexiones USB y PCMCIA. En la actualidad tienen mucho éxito los adaptadores USB para conexión 3G inalámbrica y también los adaptadores internos, sobre todo en portátiles.

Cada vez son más las ciudades e incluso pueblos que ponen a disposición del usuario el acceso libre a Internet y por ello los ordenadores portátiles con adaptadores inalámbricos están teniendo una gran acogida entre todos los usuarios. Es una imagen común, ver a personas sentadas en plazas y terrazas utilizando un portátil y disfrutando de Internet, algo impensable cuando se diseñó la primera red de ordenadores.

Los adaptadores se distinguen por el tipo de conexión a la placa base y por el tipo de conexión al medio de transmisión.

Las **conexiones a la placa base** más comunes son:

- **PCI.**
- **USB.**
- **PCMCIA.**

Las **conexiones al medio de transmisión** más empleadas son:

- **RJ45**.
- **Wi-Fi**.
- **Coaxial**.

Autoevaluación

Un ordenador portátil tiene:

- Tarjetas de red alámbricas únicamente.
- Tarjetas de red con conexión RJ45 y adaptadores PCMCIA entre otras.
- Tarjetas de red inalámbricas con conexión USB únicamente.
- Conexión inalámbrica únicamente.

Adaptadores de red cableada o alámbricos. Instalación y configuración.

Caso práctico

Aunque Tomás se decidió a comprar un adaptador de red inalámbrico con conexión USB, le ha entrado la curiosidad y ha decidido abrir el ordenador de sobremesa que tiene y extraer la tarjeta alámbrica. Ethernet que tiene instalada y volver a instalarla para practicar un posible futuro cambio y no tener que pedir ayuda a nadie. Para poder llevar a cabo esta labor ha conseguido a través de Internet un video explicativo de cómo hacerlo.

Cuando instalamos una tarjeta de red en un equipo, a parte de la instalación física tendremos que instalar el software correspondiente para que nuestro sistema reconozca al dispositivo (drivers).

Una vez instalado el adaptador tendremos que configurarle correctamente. Para ello introduciremos los valores adecuados para los siguientes parámetros:

- **Dirección IP del equipo.**
- **Máscara de red.**
- **Puerta de enlace.**
- **Servidor DNS.**

Si no conocemos estos valores tendremos que pedírselos a nuestro administrador de red (en redes LAN) o a nuestro ISP si lo que queremos es conectarnos a Internet.

Debes conocer

En los siguientes enlaces podrás ver videos explicativos de como instalar y configurar una tarjeta de red alámbrica.

Primer video sobre instalación de una tarjeta de red Ethernet

No se ha podido cargar el complemento.

Segundo video sobre instalación de una tarjeta de red Ethernet

Configurar una tarjeta de red en Molinux

No se ha podido cargar el complemento.

Configurar una tarjeta de red en Windows 7

No se ha podido cargar el complemento.

Autoevaluación

Un estudiante llega a su centro de estudios y le informan de que dispone de conexión a Internet cableada con DHCP habilitado, le indican la sala donde tiene acceso al router y le prestan un cable de red Ethernet para conectar su portátil, ¿qué necesita hacer para poder conectarse a la red?

- Configurar su tarjeta en modo "Obtener una dirección IP automáticamente".
- Dirección IP del equipo y la máscara de red.
- La clave de encriptación WEP.
- La puerta de enlace.

Adaptadores de red inalámbrica. Instalación y configuración.

Caso práctico

Tras la experiencia sufrida con el despiece del PC para encontrar la tarjeta de red alámbrica, Tomás ha decidido que la mejor opción es utilizar tarjetas con conexión USB. Parece mucho más sencillo la conexión y desconexión del adaptador USB que el adaptador PCI del PC de sobremesa. ¡Con muchos menos riesgos!

Cuando intentemos instalar una tarjeta inalámbrica, para su instalación física necesitaremos, igual que en el caso de las tarjetas alámbricas, los drivers. Una vez instalada, necesitamos los valores para los siguientes parámetros:

- Dirección IP del equipo.
- Máscara de red.
- Puerta de enlace.
- Servidor DNS.

Si no conocemos estos valores tendremos que pedírselos a nuestro administrador de red (en redes LAN) o a nuestro ISP si lo que queremos es conectarnos a Internet.

Además, para poder conectarnos a una red de manera inalámbrica necesitaremos el SSID de la red a la que queremos conectarnos y la contraseña de acceso en el caso de que dicha red utilice una seguridad WEP o WPA.

Debes conocer

En los siguientes enlaces podrás ver videos explicativos de como instalar y configurar una tarjeta de red inalámbrica.

Instalación y configuración de una tarjeta de red inalámbrica

No se ha podido cargar el complemento.

Instalación de una tarjeta de red inalámbrica PCI

No se ha podido cargar el complemento.

Configuración de una tarjeta de red inalámbrica

No se ha podido cargar el complemento.

Autoevaluación

Para instalar una tarjeta de red inalámbrica con conexión USB:

- Necesito un destornillador para desarmar la carcasa del equipo.
- Introduzco la tarjeta en uno de los puertos válidos para el dispositivo.
- Actualmente no se pueden instalar estos dispositivos porque llevan la tarjeta en el interior.
- Debo hacerlo en el interfaz PCMCIA y añadir los drivers.

La documentación de una instalación de red.

Caso práctico

Parece que la red de Tomás funciona de manera estable y que por el momento no va a agregar más equipos. Él es una persona bastante ordenada y ha decidido guardar en papel toda la información necesaria en la red para poder solucionar posibles problemas futuros, con sorpresa ha descubierto que no es el único que lo hace e indagando en Internet ha descubierto que hay un proceso, tan importante como los demás, que se da en todas las instalaciones; la documentación de la red.

Una de las partes más importantes y al tiempo más olvidada en el mundo informático es la documentación, ya sea en diseño de software como en diseño de hardware, topologías o configuraciones. La documentación supone un plus de calidad en cualquier trabajo realizado.

Es importante dejar bien documentada la instalación para recordar en un futuro el trabajo realizado. Esto va a facilitar las tareas de mantenimiento al administrador actual y a los futuros administradores que puedan sustituirnos.

Consiste fundamentalmente en la señalización de los componentes físicos y en la elaboración de unos documentos donde se recoja el trabajo realizado.

Una vez terminado el montaje de una red y si se ha hecho respetando las normas establecidas, el mantenimiento de un sistema de cableado es prácticamente nulo en condiciones normales. Es importante que el administrador de la red esté pendiente de las obras o reformas que se realicen en el edificio y que puedan afectar al correcto funcionamiento de la instalación.

Entre los puntos más importantes que debe incluir la documentación de un diseño de red están los siguientes:

- Diario de ingeniería.
- Topología física.
- Topología lógica.
- Conexiones.
- Tendidos de cable.
- Tomas y conexiones.
- Inventario de dispositivos.
- Relación de direcciones IP.
- Usuarios y contraseñas.

Realmente, si recordamos los conceptos relativos al “cableado estructurado”, la documentación de la instalación de la red sería una descripción detallada del cableado.

La documentación elaborada debe permitir que se conozca la topología física (como están instalados todos los elementos), la topología lógica y todo tipo de parámetros necesarios para que la red funcione correctamente (usuarios y contraseñas, direcciones IP, servidores, recursos compartidos de red).

Si el administrador de la red cambia, el nuevo administrador se hará preguntas como:

- ¿Cómo están conectados los equipos en este edificio?
- ¿Cómo están conectados los equipos de las distintas plantas?
- ¿Cuáles son las características de los equipos?
- ¿Qué tipo de cables se utilizan?
- ¿Existe red inalámbrica?
- ¿Dónde están los routers?
- ¿Dónde están el módem de acceso a Internet?
- ¿Dónde está el servidor?
- ¿Qué sistema operativo tienen instalados los equipos?
- ¿Cuáles son las contraseñas del usuario Administrador?
- ¿Qué personas tienen permisos para cambiar configuraciones de los equipos?

Todas estas preguntas y algunas más deberán resolverse con la documentación elaborada en la instalación de la red con planos, tablas y documentos. Todos ellos deben estar accesibles y deben ser de fácil comprensión.

Autoevaluación

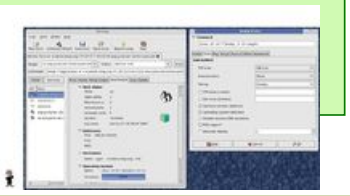
La documentación de una instalación de red:

- No es necesario hacerla.
- Señaliza componentes y documenta el trabajo realizado.
- Señaliza componentes y documenta el trabajo realizado, la realiza el programador.
- Siempre debe aparecer en papel y debe estar disponible para todo el mundo.

Motorización y resolución de incidencias en redes locales.

Caso práctico

Hoy un amigo le ha enseñado a Tomás una aplicación que se ha descargado de Internet que se llama nmap y que es capaz de ver puertos abiertos y aplicaciones que se están ejecutando en otros equipos de la red. Estas aplicaciones no están diseñadas para interferir en el funcionamiento de los demás equipos sino para observar y detectar posibles fallos. ¡Estamos monitorizando la red!



La monitorización de una red es el análisis del estado de los recursos. Para analizar los recursos de una red debemos estructurar nuestro estudio en partes diferenciadas.

- **Establecer que parámetros queremos monitorizar.**
- **Conocer los métodos para acceder a los parámetros monitorizados.**
- **Gestionar la información recopilada de los parámetros monitorizados.**

La monitorización puede ser parcial o total, continua u ocasional y se puede llevar a cabo de manera local o remota. Además, aunque puede ser diferida, la monitorización es conveniente que sea en tiempo real.

Existen múltiples herramientas para monitorizar una red.

Los sistemas operativos incorporan algunas sencillas, pero existen aplicaciones muy completas y gratuitas como:

- Monit (http://mmonit.com/monit/).
- Ganglia (http://ganglia.info/).
- Munin (http://munin-monitoring.org/).
- Cacti (http://www.cacti.net/).
- Nagios (http://www.nagios.org/).
- Zabbix (http://www.zabbix.com/).
- Nmap (http://nmap.org/).
- Zenoss (http://www.zenoss.com/product/network).
- Argus (http://argus.tcp4me.com/).

Autoevaluación

Si un administrador de red me dice “mira esto es una difusión MAC”:

- Esta monitorizando una dirección MAC.
- Esta monitorizando el sistema y puede ver protocolos ARP entre otros.
- Esta monitorizando el sistema y clonando una dirección física.
- Es imposible monitorizar un sistema y ver una difusión MAC.