

# Integración de elementos en una red.

## Caso práctico



[Alain Bachellier \(CC BY-NC-SA\)](#)

La instalación de la nueva sala de formación en **BK Sistemas Informáticos** está al completo, pero **Víndio** explica que ahora es necesario completar la documentación que él ha ido preparando durante todo el desarrollo, imprescindible para que cualquier técnico sea capaz de llevar a cabo un mantenimiento adecuado de la misma, así como implementar mejoras que puedan surgir más adelante, cuando sea necesario adaptarse a nuevas necesidades.

Es el momento de tener muy claros algunos conceptos básicos de la comunicación, porque eso va a condicionar y justificar la toma de decisiones, no solo para la red actual, también para las ampliaciones y cambios que, sin duda, se van a presentar en un periodo más o menos largo, dependiendo del uso que tenga la sala de formación.

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.

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.

No podemos olvidar cosas tan importantes como la documentación y el mantenimiento de la red. No es suficiente 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.



[Brenda algarin \(CC BY-SA\)](#)

# 1.- Transmisión de datos.

## Caso práctico

La sala de formación que acaban de montar está destinada a un uso exclusivamente de formación, en la que podrán asistir grupos de personas para clases presenciales y también para ser usada de forma individual por cualquier miembro de la empresa para realizar algún tipo de formación a través de Internet en momentos puntuales. En cualquier caso, será necesario el uso de una red de ordenadores, que permita la interconexión entre ellos y también la salida a Internet.

**Noiba** tiene muy claro que actualmente uno de los usos más extendidos y útiles de los dispositivos informáticos es la comunicación en todos los aspectos; entre personas, entre dispositivos y también personas con dispositivos. Todos estos tipos de comunicaciones se realizan de forma idéntica en lo que se refiere a la trasmisión de datos se refiere, ya que requiere el establecimiento de una comunicación siguiendo el esquema tradicional de que un emisor va a enviar un mensaje a un receptor a través de un canal que puede presentar obstáculos que deben ser conocidos.



Alain Bachellier (CC BY-NC-SA)

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

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



Einar Faanes (CC BY-SA)

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), y que permiten la conexión en red.

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.**

No es del todo correcto. Un router ADSL es un router más un módem.

¡¡Correcto!! Un router ADSL se considera un Equipo Terminal de Circuito de Datos.

Un router no es un Equipo Terminal de Datos, puesto que no es el destinatario final de los datos.

No es correcto. Un router es más complejo que un concentrador y además tiene funciones diferentes.

## Solución

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

## 1.1.- 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 hablar para que pueda hablar el otro ("cambio y corto").

Comunicación dúplex.



[Greggregreg](#) (Dominio público)

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.

No es correcto. Simplex implica que solamente podría hablar una persona, la otra solamente podría escuchar.

¡ Correcto ! Las dos personas que utilizan el teléfono pueden hablar al mismo tiempo.

No es correcto. Una persona hablaría y la otra escucharía, pero deberían esperar su turno, como los radioaficionados.

No es correcto. Este concepto no se asocia a las comunicaciones

## Solución

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

## 1.2.- Problemas en la transmisión.

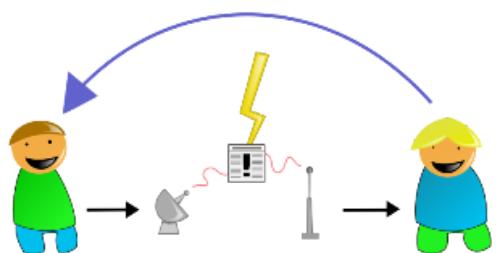
En una transmisión de información puede haber problemas producidos por cualquiera de las partes que intervienen (emisor, receptor, canal, información).

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 alterar 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.

No es correcto. La atenuación disminuye la intensidad de la señal pero no provoca eco.

No es del todo correcto. La distorsión por interferencia supone la mezcla con otras señales, pero no provoca el eco.

No es correcto. No es la fase lo que se altera cuando se produce el eco.

¡Correcto! Efectivamente la señal se distorsiona porque choca consigo misma por efecto de una reflexión.

### Solución

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

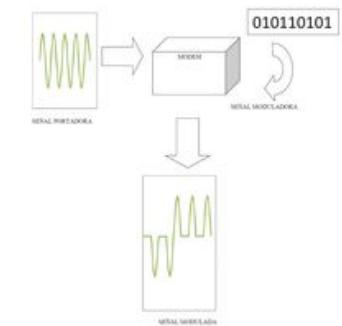
## 1.3.- Modulación.

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 (Phase).
- ✓ Modulación en Frecuencia.

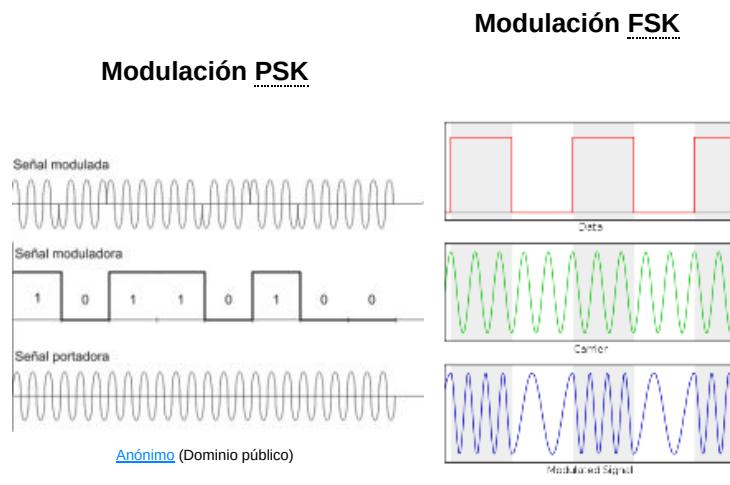


Tomás Fernández Escudero - Elab.Propia (Uso Educativo No comercial)

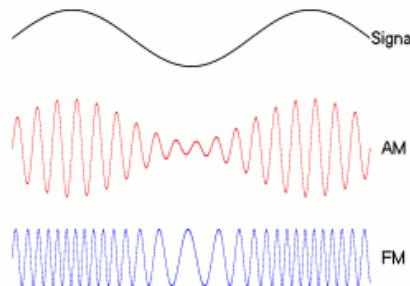
Según la naturaleza de las señales portadora y moduladora, podemos hacer una clasificación de los tipos de modulación como se muestra en la tabla siguiente:

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

En las siguientes imágenes 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).



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



[Berserkerus \(CC BY-SA\)](#)

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.

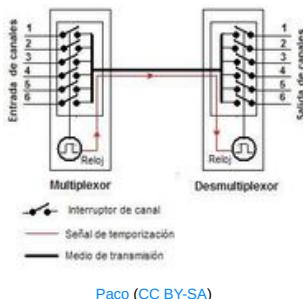
## 1.4.- Multiplexación.

La **Multiplexación** es el proceso a partir del cual un número de señales independientes se combinan formando una señal única que puede ser transmitida 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.

No es correcto. La modulación cambia parámetros como frecuencia, fase o amplitud en la señal.

No es correcto. No son contrarios, pero se complementan.

No es correcto. No mezcla señales, pero es capaz de hacer que un canal pueda transmitir varias señales.

¡Correcto! Enhorabuena, esta es la verdadera cualidad de la multiplexación.

# Solución

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

## 2.- Ancho de banda y tasa de transferencia.

### Caso práctico

Hoy **Laro** al salir de su casa se encuentra con un vecino que le quiere consultar algo, porque 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. El vecino dice que 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, y pregunta a **Laro** ¿qué es eso del ancho de banda que tanto se escucha actualmente?

**Laro** le explica que se escucha ahora por el tema de la publicidad de muchas compañías, pero es un concepto que se utiliza desde que aparecen las redes de comunicaciones y corresponde a la cantidad de datos que pueden ser transmitidos y recibidos, algo así como el diámetro de la sección de una manguera que permite enviar más o menos agua. Para simplificar le dice que va a depender del uso que quiera dar a su conexión, pero debe considerar que a mayor precio, tendrá mejores prestaciones que siempre pueden ser interesantes.



Alain Bachellier (CC BY-NC-SA)

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).

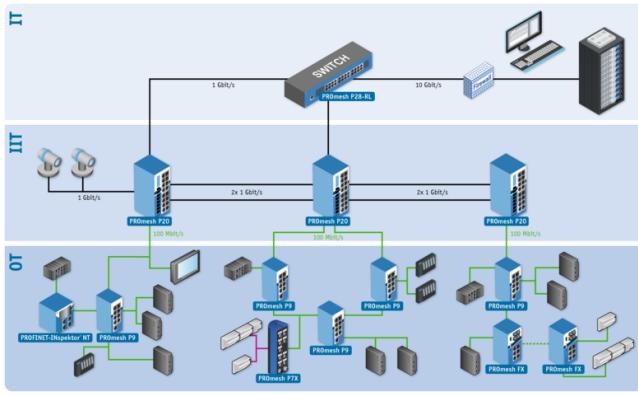
Hay frases que dejan muy claro cuál es la diferencia entre los dos términos, por ejemplo, podemos decir que "Las limitaciones de ancho de banda provocan problemas en la tasa de transferencia de la red porque la red entera sólo puede funcionar tan rápido como su enlace más lento". También podemos decir 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** si cada símbolo lleva 2 bits.



[Indu-Sol \(CC BY-SA-4.0\)](#)

## Debes conocer

Es importante saber y distinguir que la unidad por defecto en Informática para medir la cantidad de información es el **Byte (B)** (equivalente a 8 bits), pero en telemática/telecomunicaciones, para transmitir información y medir la velocidad por defecto se emplea el **bit/segundo o bps**. Fíjate bien que para Byte se usa una B mayúscula y para bit una b minúscula.

Al principio también habían diferencias en las **escalas (Kilo, Mega, Giga, Tera, Peta, etc.)**, puesto que originalmente en la informática se usaban las potencias de 2, mientras que en transmisión se usaban las potencias de 10. Sin embargo, con el tiempo esto llevó a confusión y se decidió **a partir de 1998** usar el estandard del Sistema Internacional (potencias de 10) para ambos ámbitos, y definir unas escalas específicas para las potencias de 2 llamadas Kibi, Mebi, Gibi, etc.

Más información en [Wikipedia](#).

## 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 50000000 bits/seg.
- Se transmiten 50000000 Bytes/seg.

No es correcto. Hz se asocia a velocidades de trabajo, frecuencia, por ejemplo en procesadores.

No es correcto. 5 millones serían casi 5 Megas y no sabemos si un símbolo equivale a 1 bit o más.

No es correcto. Esto serían 5 Megas.

¡Correcto! La velocidad de conexión a Internet nos la dan siempre en bits/seg y 1 Mega es  $1000 \times 1000$  bits ó  $10^6$  bits.

No es correcto porque por defecto las velocidades de transmisión se dan en bits/seg y no en Bytes/seg.

## Solución

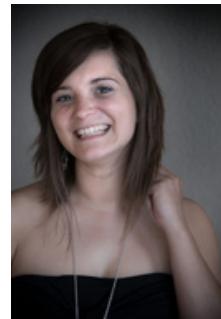
1. Incorrecto
2. Incorrecto
3. Incorrecto
4. Opción correcta
5. Incorrecto

### 3.- Factores físicos que afectan a la transmisión.

#### Caso práctico

En **BK Sistemas Informáticos** llevan unos días con la nueva conexión a Internet de fibra óptica y aprecian cierto aumento en la velocidad de navegación, que repercute en mejor respuesta de todas las aplicaciones web. **Jana** ha probado varios test de velocidad para saber cuál es la velocidad real de conexión y ha descubierto que el resultado no es el mismo que la velocidad que aparece en la publicidad. Se ha indignado mucho y se lo ha comentado a **Vindio** que le explica que la velocidad ofrecida por los diferentes proveedores de servicios siempre es una velocidad en condiciones ideales, sin tener en cuenta que la transmisión depende de varios factores.

Le explica que en una red pueden existir momentos de colapso y saturación de datos porque no todos los dispositivos trabajan a la misma velocidad, pero además hay momentos en los que se pueden producir algunas situaciones que dificulten la transmisión de datos, por ejemplo las condiciones de temperatura pueden afectar a las comunicaciones.



Alain Bachellier (CC BY-NC-SA)

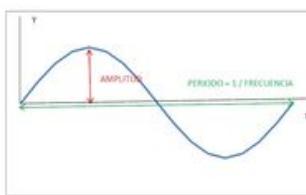
Para representar una señal electromagnética que se propaga, debemos recurrir a una función dependiente del tiempo. Después de varios experimentos y tomando como base los estudios matemáticos de **Fourier**, se dedujo que la función que mejor representaba a las ondas electromagnéticas era una función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

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

Donde:

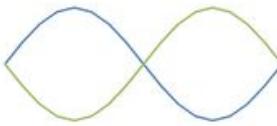
- ✓  $Y$  representa a la posición de la perturbación en un instante de tiempo determinado.
- ✓  $A$  es la amplitud máxima de la onda.
- ✓  $w$  es un valor proporcional a la frecuencia ( $w = 2\pi f$ ).
- ✓  $\phi$  representa la fase.
- ✓  $t$  representa el tiempo.

**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.



Tomás Fernández Escudero - Elab.Propia. (CC0)

En la figura se representa lo que correspondería a una rotación angular entera ( $360^\circ$ ). 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  $180^\circ$ , seguirían sentidos diferentes (si una sube la otra baja), el dibujo resultante de dos ondas desfasadas  $180^\circ$  sería algo parecido a:



Tomás Fernández Escudero. Elab.Propia.  
(Dominio público)

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 ( $\epsilon$ ):** 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 ( $\mu$ ):** Es la capacidad de un material para absorber radiaciones magnéticas.
- ✓ **Conductividad ( $\sigma$ ):** 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.

No, aunque la técnica favorece la resistencia.

¡Correcto! Con esta técnica unos hilos apantallan a otros.

No, con esta técnica no se evita la atenuación.

No, el cable de par trenzado en la actualidad es el más usado en las redes cableadas.

## Solución

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

## 4.- La conexión inalámbrica.

### Caso práctico

La compra de un ordenador portátil siempre ha sido una de las ilusiones de una de las amigas de **Naroba**, y ese es el principal motivo de que la haya llamado por teléfono el sábado antes de las 9:00 horas. Dice que lleva un buen rato investigando en Internet y ha descubierto que hay muchas ofertas asequibles, pero 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 leído que hay gente que se conecta en plena calle gracias a las redes inalámbricas. **Naroba** le explica casi sin despertar, que todas esas personas conectan mediante datos del móvil, dispositivos Wi-Fi y Bluetooth, algo así como el mando a distancia de la TV, que funciona con infrarrojos. **Naroba** le recomienda que debe comprender cómo funciona la conexión inalámbrica antes de comprarse un ordenador portátil, y que para eso es mejor que la invite a desayunar.



[Alain Bachellier \(CC BY-NC-SA\)](#)

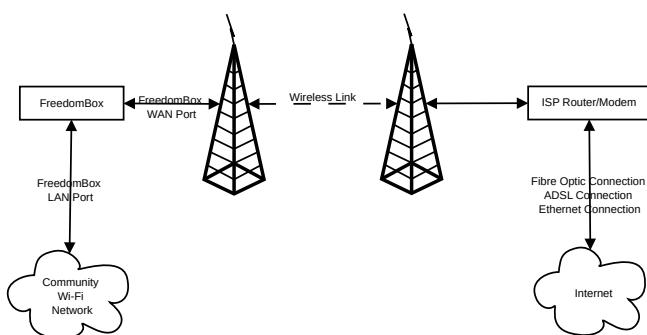
Existen varios tipos de comunicación inalámbrica:

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



[Anónimo \(CC0\)](#)

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.



[Sunil Mohan Adapa \(CC BY-SA-4.0\)](#)

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.



[Uhernandez \(CC BY-3.0\)](#)

## 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.

No es correcto. Para transmitir a largas distancias necesitamos dirigir las ondas a puntos concretos.

No es correcto. Uno de los inconvenientes de los infrarrojos es que no pueden atravesar muchos objetos.

No es correcto. Las microondas es necesarios dirigirlas porque son muy direccionales.

¡ Correcto ! Esta es una cualidad que nos permite conectar con puntos de comunicación muy lejanos.

## Solución

1. Incorrecto
2. Incorrecto

3. Incorrecto  
4. Opción correcta

## 4.1.- Estándares de transmisión inalámbrica.

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. **Punto de acceso inalámbrico**

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).



Xavi Gaya (GNU/GPL)

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 Mbps). 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 Mbps 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.

Nombre.	Descripción.
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 <u>AES</u> (estándar de cifrado avanzado) y puede cifrar transmisiones que se ejecutan en las tecnologías 802.11a, 802.11b y 802.11g.
802.11r	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 (Wi-Fi 4)	Surge debido a la gran demanda de las <u>WLAN</u> (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 <u>MIMO</u> (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.
802.11ac (Wi-Fi 5)	Estandarizada en dic 2013. Usa la banda de los 5GHz y canales de hasta 160MHz para llegar hasta los 3466.8 Mbit/s
802.11ax (Wi-Fi 6)	Desde sept 2019. Aprovecha en paralelo las frecuencias de 2.4, y 5 GHz para llegar hasta los 9608 Mbit/s. También conocido como <u>Wi-Fi 6</u> y <u>Wi-Fi 6E</u> ( <b>añade el uso del nuevo rango de 6GHz</b> ).

## Debes conocer

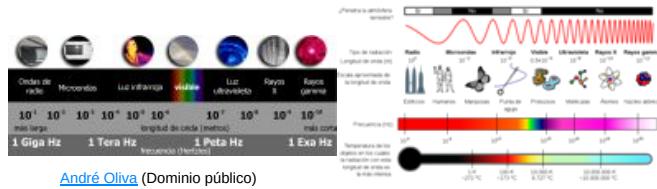
En los siguientes enlaces encontrarás más información sobre las diferentes tecnologías Wi-Fi:

[Introducción al estándar 802.11](#)

[Comparación de los estándares WiFi pasados y en desarrollo](#)

## 4.2.- 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.



[André Oliva](#) (Dominio público)

[Dora Oliveira](#) (Dominio público)

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 televisión.
- ✓ 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.

No es correcto. No interfieren entre sí, podemos tener una conexión Wi-Fi y un ratón Bluetooth conviviendo.

No es correcto. Wi-Fi se basa en las ondas de radio.

No es correcto. El alcance no influye en la interferencia con Wi-Fi.

¡Correcto! Bluetooth se basa en la técnica de múltiples saltos de frecuencia.

## Solución

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

## 4.3.- 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 (cerca en el espacio y usando una misma frecuencia del espectro electro-magnético).
- ✓ **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. El AP es el que **arbitra** quién puede transmitir en cada momento para **evitar colisiones** según el protocolo **CSMA/CA (Collision Avoidance)**.

Haciendo un símil con la comunicación por cable, el modo **Ad-hoc** sería equivalente a comunicar dos ordenadores entre sí mediante un **cable (punto a punto)** 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.



Tomás Fernández Escudero. Elab.Propia (Uso educativo no comercial.)

Si nos fijamos en la **topología lógica**, se puede decir que la topología en **estrella** es la estándar para redes inalámbricas con el AP en el centro gestionando el orden en el que cada una de las estaciones transmite en cada momento. Aunque a nivel físico sería más parecido a un bus por ser un medio compartido el campo electromagnético en determinada frecuencia.

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 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.

¡Correcto! Sí, porque necesitamos crear una red donde se conecten todos utilizando el AP como nexo.

No es correcto. Ad-hoc es un modo de configuración para unir ordenadores uno a uno.

No es correcto. Un AP se comporta como un hub inalámbrico.

No es correcto. No es necesario tener acceso a Internet si queremos unir los ordenadores utilizando un AP.

## Solución

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

## 4.4.- 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.**

[hatalar205](#) (Dominio público)

**WEP:** Es un mecanismo simple de cifrado de datos. Utiliza el algoritmo 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. 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. 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.

**WPA3** fue anunciado en enero de 2018, debido a una vulnerabilidad descubierta en WPA2.

El estándar WPA3 SAE reemplaza el intercambio de claves pre-compartidas (PSK) con la autenticación simultánea de iguales (SAE), lo que resulta en un intercambio inicial de claves más seguro en modo personal.

El nuevo estándar utiliza cifrado de **128 bits** en modo WPA3-Personal (192 bits en WPA3-Enterprise) y confidencialidad de reenvío.

También reducirá los problemas de seguridad que plantean las contraseñas débiles y simplificará el proceso de configuración de dispositivos sin interfaz de visualización.

## 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.**

¡ Correcto ! Si, se diseñó para mejorar las prestaciones de WEP.

No es correcto, aunque este fue uno de los primeros sistemas de encriptación para redes inalámbricas.

No es correcto. SSID es el nombre de la red. Hay una medida de seguridad, consistente en ocultar el SSID, pero no es una medida demasiado eficaz.

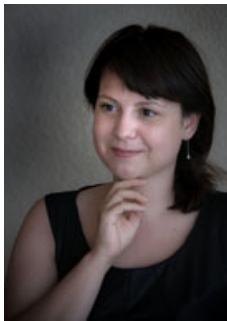
No es correcto. Si escogemos esta opción, todo el mundo podrá conectarse a nuestra red inalámbrica.

## Solución

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

## 5.- Direcccionamiento.

### Caso práctico



Alain Bachellier (CC BY-NC-SA)

Una vez comprado, **Naroba** tiene que configurar el ordenador portátil de su amiga para que conecte por con la red que tiene montada en casa, para que utilice el móvil como punto de acceso y también le explica cómo debe actuar para conectar a la red del colegio en el que trabaja de maestra, prestando especial atención a que el equipo esté protegido ante virus o ataques, y le hace prometer que bajo ningún concepto se conectará a una red desconocida.

**Naroba** configura el equipo correctamente para cualquier tipo de redes, sin dejar de responder pacientemente a todas las preguntas que hace su amiga por cualquier cambio en la configuración del sistema, a pesar de que sabe que no retendrá nada de lo que le explica, porque el único modo de entender y asimilar todos estos conceptos es practicando, algo que ellas ha estado haciendo últimamente con varios equipos durante la instalación de la sala de formación de la empresa en la que hace las prácticas.

Para poder **identificar** una máquina en Internet existe la dirección **IP**, y el mecanismo que establece las normas que deben cumplir estas direcciones se denomina **direcccionamiento**.

Las direcciones **IP públicas de Internet se asignan de forma única y centralizada, pero delegando por territorios.**

Históricamente se ha ido realizando de diversas formas y por distintos organismos, **InterNIC** (**Internet Network Information Center**) fue el principal organismo gubernamental de internet responsable de los **nombres de dominio** y las **Direcciones IP** hasta el 18 de septiembre de 1998, cuando este papel fue asumido por la **Internet Corporation for Assigned Names and Numbers** (ICANN).

A día de hoy, La Corporación de Internet para la Asignación de Nombres y Números (**ICANN**) delega los recursos de Internet a los Registros Regionales de Internet (**RIR**), y a su vez los RIR siguen sus políticas regionales para una posterior subdelegación de recursos a sus clientes, que incluyen proveedores de servicios de Internet (**ISP**) y organizaciones para uso propio.

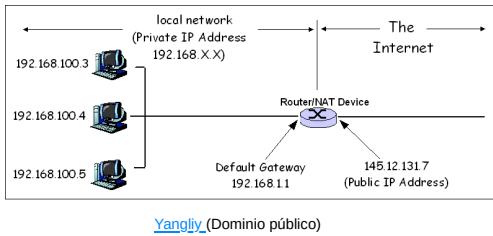
Hasta ahora, el método de direccionamiento más utilizado ha sido el direccionamiento **IPv4**, aunque cada vez está tomando más peso el **IPv6**.

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 enruteadores.

El direccionamiento en Internet es distinto del que podemos llevar a cabo en las redes **LAN**. En el espacio **WAN** las direcciones las gestionan organismo como la ICANN o los ISPs, 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 repercuten a nosotros).

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



[Yangliy](#) (Dominio público)

## 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 puesto (un ordenador) quiere establecer comunicación con otro, debe disponer de una dirección (dirección IP). De hecho, cuando escribimos una dirección URL (por ejemplo, algo similar a esto <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, 958 Almería, 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.

¡Correcto! Si, identifica los elementos que pueden soportar direcciones en una red.

No es correcto. Los paquetes los encaminan los dispositivos aprovechando las técnicas de direccionamiento.

No es correcto. Esta no es su labor.

No es correcto. Direccionamiento es asignar direcciones.

## Solución

1. Opción correcta
2. Incorrecto

3. Incorrecto  
4. Incorrecto
-

## 5.1.- IPv4.

Una dirección **IPv4** consta de **32 bits**, agrupados de 8 en 8 y representados en **4 números de código decimal**. Los valores de estos 4 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.
Dirección IP.	00000001.00000000.00000000.00000001	1.0.0.1
Máscara de red.	11111111.00000000.00000000.00000000	255.0.0.0
Dirección de red.	00000001.00000000.00000000.00000000	1.0.0.0

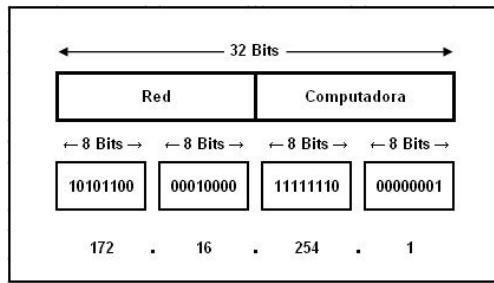
La utilidad de las máscaras de red está en que nos sirven para saber cuál es la dirección de red asociada a una determinada dirección IP. Para poder hacer esto se realiza la operación binaria AND entre la IP y la máscara de red, el resultado es la dirección de red. Esta operación es la que realizan los 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.



[IPv4 vs IPv6 \(CC BY-SA-3.0\)](#)

## Recomendación

Estos vídeos te pueden ayudar a comprender mejor estos conceptos tan importantes:

- 1.- [Direccionamiento IPv4 y Subredes](#)
- 2.- [Curso de Redes de AulaClic. 8.4 Direcciones IP y enrutamiento en un host.](#)
- 3.- [Cálculo: Nº hosts, dirección de red y broadcast, primera y última direcciones posibles](#)

## 5.2.- 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.aaaaaaaaaaaaaaaaaaaaaaaa
Clase B	10rrrrrr.rrrrrrrr.aaaaaaaaaaaaaaaa
Clase C	110rrrrr.rrrrrrrr.rrrrrrrr.aaaaaaaa
Clase D	1110xxxx.xxxxxxxxxx.xxxxxxxxxx.xxxxxxxxxx
Clase E	1111xxxx.xxxxxxxxxx.xxxxxxxxxx.xxxxxxxxxx

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

Una dirección IP consta de los siguientes campos y surge la siguiente clasificación:

**IDENTIFICADOR (TIPO) + NUMERO DE RED + NUMERO DE ESTACION**

Clase de IP	Bits iniciales en el primer octeto, Identificadores de la Clase	Número de bits que restan para identificar la parte de red	Número de bits para identificar la parte de estación
A	0	7 bits	24 bits
B	10	14 bits	16 bits
C	110	21 bits	8 bits
D	1110	28 bits	-
E	11110	27 bits	-

Y en resumen:

Clase	Rango de IPs	Número de redes posibles de esa clase	Número máximo de estaciones por cada red (restando 2 para la dirección de red y la de broadcast)
A	0.0.0.0 - 127.255.255.255	$2^7 = 128$	$2^{24} - 2 = 16777216$
B	128.0.0.0 - 191.255.255.255	$2^{14} = 16348$	$2^{16} - 2 = 65536$

C	192.0.0.0 - 223.255.255.255	$2^{21} = 2097152$	$2^8 - 2 = 256$
D	224.0.0.0 - 239.255.255.255	-	-
E	240.0.0.0 - 247.255.255.255	-	-

A continuación se detalla y explica cada clase:

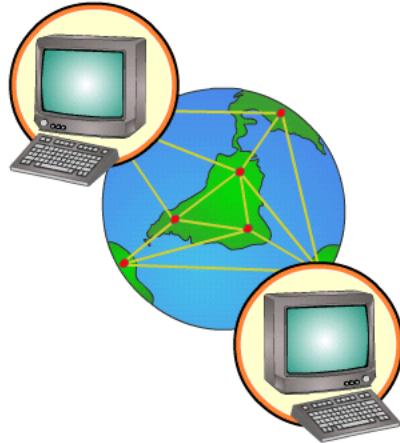
### DIRECCIONES IP CLASE A:

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 0000000 a 0111111) 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 local (localhost).

Las redes verdaderamente 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:

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



[turcon.blogia.com](http://turcon.blogia.com) (CC BY-SA-3.0)

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 (desde 10000000.00000000.xxxxxxx.xxxxxxx a 10111111.11111111.xxxxxxx.xxxxxxx). 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.xxxxxxx a la 11011111.11111111.11111111.xxxxxxx). 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.

### DIRECCIONES RESERVADAS y/o ESPECIALES:

De todas las direcciones IP, hay algunas que no se pueden utilizar porque están reservadas para el uso del protocolo IP y tienen una consideración "especial" como:

- ✓ 0.0.0.0: Tiene varios usos como se puede ver en [Wikipedia](#). Puede representar tanto "todas las IPs" como "ninguna" según el contexto. También se utilizaba cuando se están arrancando las estaciones, hasta la carga del sistema operativo, luego no se usa. Antiguamente se usaba también cuando no se obtenía una dirección mediante DHCP, pero ahora se usa [APIPA](#) en sistemas operativos Windows entre otros. **Todo el rango de IPs que comienza con el primer octeto a 0 está reservada.**
- ✓ 127.0.0.1: Para especificar la estación actual, cuando se desea especificar el ordenador local (**localhost**). Todo el rango de IPs que comienza en el primer octeto por 127 está reservada al mismo propósito, es decir

que en cualquier equipo que tenga su pila de protocolos TCP/IP instalada en el sistema operativo podrá hacer ping a la 127.0.0.1 o la 127.0.0.2 o la 127.22.22.22 y el ping debe responder positivamente.

- ✓ Dirección con **todos los bits a 0** en la parte de "host": Representa a la subred actual y no puede ser asignada por tanto a ningún equipo.
- ✓ Dirección con **todos los bits a 1** en la parte de "host": Difusión (broadcast) en su subred. Para enviar mensajes a todas las estaciones dentro de la misma subred (todas las estaciones con los mismos bits en la parte de red de su IP). Por lo tanto tampoco podrá ser asignada a ningún equipo de la subred.
  - ◆ No hay que confundir las direcciones de difusión (**broadcast**) de las subredes (para enviar mensajes a las estaciones de la misma subred) con las direcciones de la clase D, que más bien, se utilizan para agrupar estaciones en un mismo grupo/canal de multicast y enviarlas mensajes de multi-difusión o **multicast** (pueden pertenecer a redes o subredes distintas).

Además de las direcciones **reservadas** anteriores, se han establecido otros rangos de direcciones IP para ser asignados a redes locales **privadas**, que cuando se conectan a Internet a través de un proxy o mediante un router/encaminador que use un protocolo NAT serán convertidas a una (o varias) **IPs públicas**.

Clase	Rangos Reservados y Especiales
A	0.0.0.0 - 0.255.255.255 : reservado <b>10.0.0.0 - 10.255.255.255</b> : reservado para redes internas/privadas <b>127.0.0.0 - 127.255.255.255</b> – reservado para direcciones tipo loopback, solo a nivel interno del propio dispositivo
B	<b>169.254.0.0 – 169.254.255.255</b> : Direcciones usadas por <a href="#">APIPA</a> cuando falla el DHCP <b>172.16.0.0 - 172.31.255.255</b> : reservado para redes internas/privadas
C	192.168.0.0 - 192.168.255.255 : reservado para redes internas/privadas

## Recomendación

Vídeo: [Curso de Redes. 8.9 Direcciones especiales](#)

Se explica cuáles son las direcciones IP especiales, privadas y reservadas y para qué sirven.

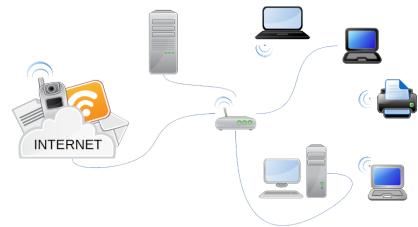
## 5.3.- NAT.

La aparición de los enruteadores con la cualidad de NAT permitió que se pudieran utilizar varias direcciones privadas detrás del router consumiendo solamente una 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. Aunque a día de hoy sigue usándose mucho y es uno de los conceptos más importantes a manejar como administrador de red.

**En la última unidad del curso se profundizará en NAT y se verán ejemplos de configuración, así como de apertura/redirección de puertos.**

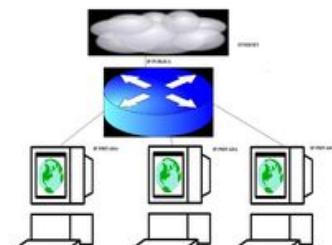


Alfonso Bonillo. Elab.Propia (Dominio público)

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 qué 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.



Tomás Fernández Escudero-Elab.Propia (Uso educativo no comercial.)

### 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 rangos de direcciones IP de clase C privadas IPv4.

- Un rango de direcciones IP de clase A privada IPv4.
- Un rango de direcciones IP de clase B privada IPv4.
- Un rango de direcciones IP de clase A privada y un rango de clase C privada IPv4.

¡ Correcto ! Si, con esta opción podríamos direccionar 508 equipos.

No es correcto. Con una dirección de clase A podemos direccionar  $2^{24}-2$  equipos.

No es correcto. Con una dirección de clase B podemos direccionar  $2^{16}-2$  equipos.

No es correcto. Con esta opción podemos direccionar  $(2^{24}-2) + 254$  equipos.

## Solución

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

## 5.4.- Subredes y máscaras de subred.

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.

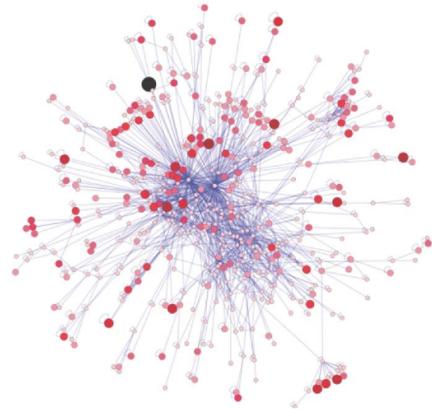
Las subredes son un método para poder crear varios dominios de difusión a partir de una dirección de red, esto nos ayudará a segmentar una red.

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 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.



[Eric Karsenti \(CC BY-SA-4.0\)](#)

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).

### Debes conocer

Para representar los bits a 1 de la máscara de subred es muy usual usar la Notación Diagonal o simplificada cómo puedes ver [aquí](#).

Por ejemplo, cuando queremos decir que un PC tiene configurada la dirección IP 192.168.0.213 y máscara 255.255.255.0, normalmente se dice que tiene la IP 192.168.0.213/**24**

## Para saber más

Esta calculadora de subredes online tiene mucha utilidad e información adicional. Cuando realices ejercicios de cálculo de subredes IP te puede servir para comprobar tus resultados:

<https://subnettingcalculator.com/>

Puedes practicar a resolver ejercicios de subredes forma manual y comprobar con la calculadora que están bien. Puedes practicar por ejemplo con esta [colección de ejercicios resueltos](#).

## Recomendación

Estos vídeos te pueden ayudar a comprender mejor estos conceptos tan importantes:

- 1.- [Direccionamiento IPv4 y Subredes](#)
- 2.- [Ejemplo de cálculo de Subredes](#)
- 3.- [Subneteo VLSM \(VLSM Subnetting\). Como crear subredes con el método de VLSM.](#)
- 4.- [VLSM \(Explicado en un ejemplo\)](#)

## 5.5.- CIDR y superredes. Sumarización de Redes.

El término **CIDR** se utiliza para referirse a “encaminamiento entre dominios de red sin clase”. Es una técnica que permite:

- 1.- **Subdividir** una red en varias subredes más pequeñas. Cómo vimos en el apartado anterior.
- 2.- **Resumir (o sumarizar o englobar)** un conjunto de direcciones IP **contiguas** de red de una clase en una misma dirección de red.

En el 2º caso 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 varias 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.

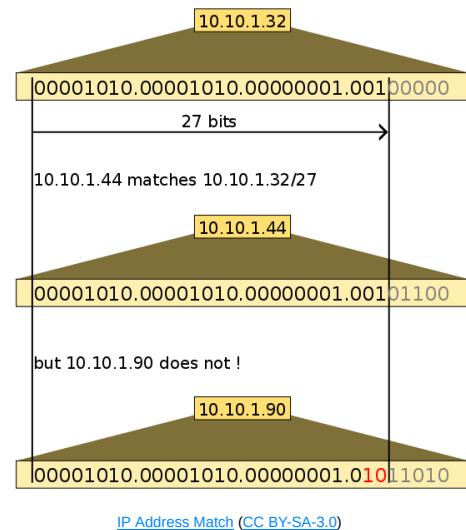
Con **CIDR** podemos utilizar bits del tercer octeto para generar más direcciones de host. Por ejemplo, si cogemos 2 bits del tercer octeto, podremos conseguir  $2^{10} = 1024$  direcciones para equipos.

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	11000000.10101000.00000000.<b>00</b>.00000000	255.255.255.0
192.168.1.0	11000000.10101000.00000000.<b>01</b>.00000000	255.255.255.0
192.168.2.0	11000000.10101000.00000000.<b>10</b>.00000000	255.255.255.0



Dirección de red.	Binario.	Máscara de red.
192.168.3.0	11000000.10101000.000000<b>11</b>.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 nuestras necesidades, sin respetar el concepto de las máscaras "clásicas por defecto" asociadas a direcciones de tipo A, B o C. Para poder hacer esto, nuestros dispositivos y protocolos de encaminamiento deben soportar CIDR.

## 5.6.- 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).

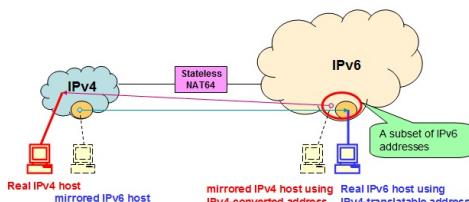
	Internet Protocol version 4 (IPv4)	Internet Protocol version 6 (IPv6)
Deployed	1981	1999
Address Size	32-bit number	128-bit number
Address Format	Dotted Decimal Notation: 192.149.252.76	Hexadecimal Notation: 3FFE:F200:0234:AB00: 0123:4567:8901:ABCD
Prefix Notation	192.149.0.0/24	3FFE:F200:0234::/48
Number of Addresses	$2^{32} = \sim 4,294,967,296$	$2^{128} = \sim 340,282,366,920,938,463,463,374,607,431,768,211,456$

[Tmthetom \(CC BY-SA-4.0\)](#)

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



[Xing333 \(CC BY-SA-3.0\)](#)

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

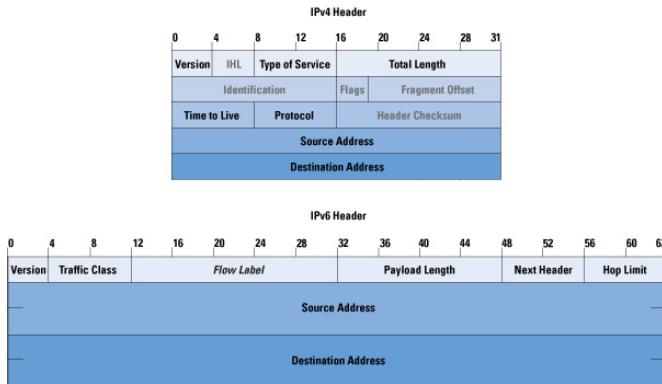
- ✓ Se puede utilizar ":" para representar a las cadenas de ceros. Dicho símbolo podrá aparecer una sola vez en cada dirección. La dirección de loopback 0:0:0:0:0:0:1 se podrá representar como ::1.
- ✓ **Cuando tengamos nodos IPv4 e IPv6, podemos utilizar la notación x:x:x:x:x:d.d.d.d, donde x representan 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:**

- ◆ 0:0:0:0:0:13.1.68.3
- ◆ 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.



[Cisco \(CC BY-SA-3.0\)](#)

## 6.- Dominios de colisión y difusión.

### Caso práctico

Comienza una nueva semana de prácticas para **Noiba**, **Naroba** y **Jana** en la empresa **BK Sistemas Informáticos** y llegan el lunes con ganas de seguir aprendiendo. **Jana** comenta que le gusta el trabajo y que en esta empresa estarían muy bien, añade que si al terminar las prácticas le ofrecen un contrato estaría encantada de aceptarlo, pero que le gustaría que esa oferta fuese para las tres. **Noiba** dice que eso es algo improbable, no hay ninguna empresa que ofrezca tres contratos y que deben intentar aprovechar este periodo para conocer el perfil profesional que mejore su formación y les permita optar a cualquier empresa del sector, que será similar a esta con compañeros igual de agradables.



Alain Bachellier ([CC BY-NC-SA](#))

**Naroba** interviene y les explica que todo es posible, quizás la empresa esté pensando en una expansión y precise personal preparado, así que deben aprovechar la oportunidad. Y añade que hoy van a hacer pruebas en la red local de la sala de formación sobre la comunicación entre equipos, con la impresora y el escáner y con el acceso a Internet, así que hay que comprobar la configuración de los routers para crear diferentes dominios de colisión y disminuir 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.

No es correcto. Puede haber una red en la que los equipos estén conectados a un switch o un router.

¡ Correcto ! Sí, porque un hub es como un cable, todos los equipos estarían en el mismo dominio de colisión.

No es correcto. En un dominio de difusión se pueden dar varios dominios de colisión.

No es correcto. La tecnología empleada en los cables no influye en la creación de los dominios de colisión.

## Solución

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

## 6.1.- 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.

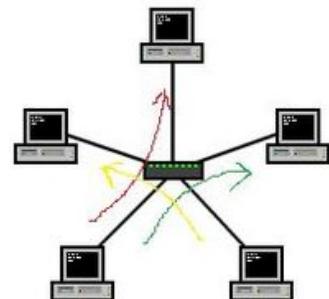
Parece obvio que cuanto mayor sea el espacio con probabilidades de choque más choques habrá. Para evitar los estas colisiones, una de las medidas empleadas es la separación de los espacios donde puede haber una colisión (es más fácil controlar varios espacios pequeños que un solo espacio grande). Si 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 **comutador (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 comutador, 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.



[Head \(CC BY-SA-3.0\)](#)

### Para saber más

- 1.- Una pequeña explicación extra sobre los dominios de colisión en [Wikipedia](#)
- 2.- Un [ejemplo sencillo en vídeo](#) sobre los dominios de colisión y de difusión en una red con hubs y en una red con switches

## 6.2.- 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 commutadores, 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 ordenadores) 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.



[Cesarious \(CC BY-SA\)](#)

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

## 7.- Resolución de direcciones. ARP y RARP.

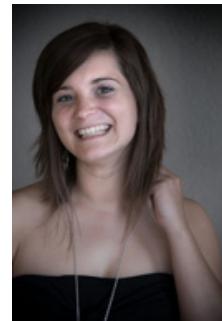
### Caso práctico

**Jana** lleva un rato con un equipo que ayer funcionaba perfectamente en red con salida a Internet sin problemas de comunicación con el resto de puestos, pero que hoy no consigue hacer nada con él por muchas vueltas que el está dando. No quiere preguntar a **Laro** para no parecer una tonta, pero es que no consigue avanzar y va a quedar aún peor, así que se decide a interrumpir a su compañero para salir del bloqueo en el que lleva casi una hora.



[Alain Bachellier \(CC BY-NC-SA\)](#)

**Laro** le explica que esta mañana, antes de que ellas llegasen a la empresa, **Juan** decidió cambiar la configuración del router para permitir el acceso por adaptadores de red y no por direcciones IP. Ante esa respuesta **Jana** se enfada un poco diciendo que lleva una hora perdida cambiando cosas en la configuración del equipo porque no ha sido informada de ese cambio. **Laro** con mucha paciencia la tranquiliza y dice que cada mañana al entrar en la empresa, lo primero que deben hacer es revisar el parte de trabajo diario en el que se recogen todos los cambios y las indicaciones a adoptar. **Jana** vuelve avergonzada a su puesto pensando que ha aprendido una buena lección, y no ha sido sobre redes.



[Alain Bachellier \(CC BY-NC-SA\)](#)

Las direcciones IP no son procesadas por los dos primeros niveles (físico y enlace), sin embargo las tarjetas de red sí que vienen identificadas con una dirección Ethernet que viene de fábrica (dirección 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

48 bits o 6 pares de números en hexadecimal. 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.

Las tarjetas de red de los equipos se comunican a nivel de enlace Ethernet utilizando sus respectivas direcciones MAC como origen y destino. Aunque a nivel de las capas superiores, y del usuario, el destino es definido por su dirección IP, así que el equipo de origen tendrá que lanzar una petición de difusión ARP para descubrir la dirección MAC del destino que corresponde a esa IP. A esa petición de difusión ARP solo responderá el equipo de destino que tenga esa IP.

Aunque... ¡jojo! esto es así solo dentro de su propio dominio de difusión, es decir, en su subred o segmento de red. Cuando hay que atravesar un router para llegar a otra subred de destino, entonces la MAC de destino siempre será la del interfaz del router que está en su subred, que le servirá de puerta de enlace predeterminada hacia otras subredes o dominios de difusión. Para conocer esa MAC del router, el equipo en origen por lo tanto tendrá que lanzar un ARP preguntando por la MAC correspondiente a la IP de su puerta de enlace predeterminada (o al siguiente salto a nivel de IP según su tabla de rutas), y el router al escucharlo le responderá con su MAC.



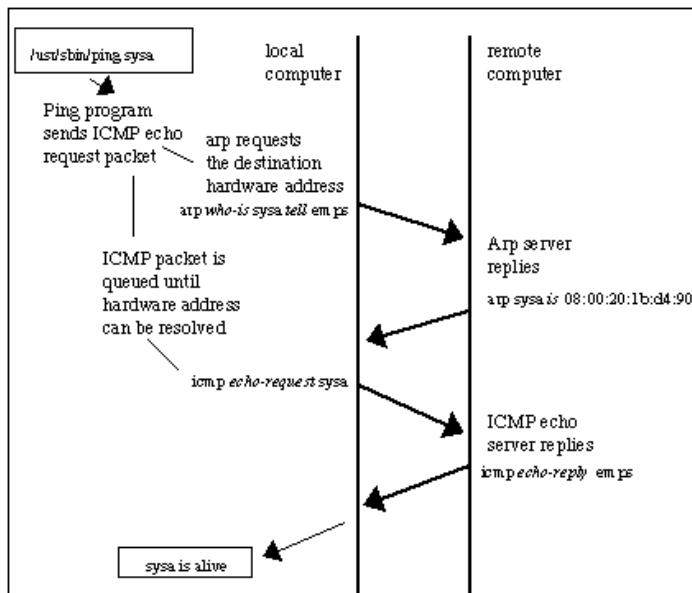
[Raimond Spekking \(CC BY-SA 4.0\)](#)

# Reflexiona

Ejemplo dentro de una misma subred: Un host identificado como "sysa" tiene la dirección IP **84.127.234.102** asociada, si quiero comunicarme desde un equipo en su misma subred con dicho host necesito:

- ✓ Traducir el nombre de host "sysa" a la IP **84.127.234.102**. (mediante una petición a un servidor de DNS)
- ✓ Encontrar la dirección MAC que está asociada a la dirección IP **84.127.234.102**. (mediante una petición de difusión ARP que llegará a toda la subred)

Para poder encontrar la máquina se emite un paquete de difusión (o broadcast) Ethernet (para preguntar quién es la dirección IP **84.127.234.102**, el host que tenga esa dirección responderá con su MAC. Y a partir de ahí se podrán comunicar porque ya conocen las direcciones de destino de capa 2 y capa 3.



[Badrah huder. Proceso de resolución ARP al lanzar un ping \(ICMP\) \(CC BY-SA\)](#)

ARP se podría sustituir por archivos de configuración en los que figurase 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. Es un protocolo muy usado y común porque normalmente se trabaja con direcciones IP (o nombres de equipos/dominios traducidos a direcciones IP), pero de primeras no sabemos las direcciones MAC de los destinos con los que nos queremos comunicar.

Pero en algunas 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

No es correcto. Descubre la dirección física sabiendo la IP.

¡Correcto! Si, devuelve la IP asociada a una dirección MAC, se complementa con ARP.

No es correcto. MAC no es un protocolo.

No es correcto. Este protocolo no entiende de direcciones físicas, aunque las puede transportar encapsuladas.

## Solución

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

## Recomendación

Debes conocer cómo funciona el protocolo ARP y sus cachés, para eso te recomiendo [esta página](#) qué explica qué es, cómo funciona y algunos comandos de configuración desde la terminal de un PC. También puedes profundizar en los comandos para [Windows](#) y para [Linux](#). También puedes consultar la [Wikipedia](#) que explica bien las tablas y las variantes.

Estos 2 videos muestran aspectos muy importantes del protocolo ARP que debes conocer puesto que serán la base para entender muchos otros conceptos posteriores:

1.- [Transferencia de datos en la red - MAC e IP \(Explicado\)](#) : Video explicativo sobre cómo la capa de red y la capa de enlace de datos son responsables de enviar los datos desde un dispositivo origen a un dispositivo destino, y de qué forma las direcciones trabajan conjunta y coordinadamente para la transferencia de datos.

2.- [Simulación Protocolo ARP con el programa Cisco Packet Tracer](#) : ARP significa Address Resolution Protocol o protocolo de resolución de direcciones. ARP se utiliza para supervisar y modificar la tabla de asignaciones de direcciones IP y direcciones MAC (Media Access Control). ARP utiliza un cache que consiste en una tabla que almacena las asignaciones entre nivel de enlace de datos y las direcciones IP del nivel de red. El nivel de enlace de datos se encarga de gestionar las direcciones MAC y el nivel de red de las direcciones IP. Sintetizando, ARP asocia direcciones IP a las direcciones MAC, justo a la inversa del protocolo RARP que asigna direcciones MAC a las direcciones IP. Para reducir el número de peticiones ARP, cada sistema operativo que implementa el protocolo ARP mantiene una cache en la memoria RAM de todas

las recientes asignaciones. No obstante el tiempo de duración predeterminado para el **cache** de la tabla de ARP es de **60 segundos**, con lo cual se irá renovando pasado este tiempo. Este vídeo es también muy recomendable porque te enseña a usar la **herramienta de inspección de paquetes** de Packet Tracer.

También es muy recomendable que te familiarices con la herramienta Wireshark para capturar y analizar paquetes desde tu PC. Puedes ver una [introducción a Wireshark y demo \(de un bucle infinito\) en Aulaclic](#), un [ejemplo de análisis de paquete](#) y otro [ejemplo de análisis del ARP](#).

## 8.- Direcccionamiento dinámico (DHCP).

### Caso práctico

**Laro** ha tenido que ir a casa de su vecino 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 del vecino. Intentó conectarse a la red que aparecía visible pero no fue posible a pesar de que la señal era excelente. Su vecino explica que tiene la red tal y como se la dejaron configurada los técnicos.

Después de llevar un rato sin entender cuál es el fallo por el que no puede realizar la conexión, decide llamar a **Vindio** que seguro que le ayudará.

Tras hacer varias pruebas según las indicaciones de **Vindio**, **Laro** descubre por si mismo el fallo al acceder a la configuración del router y comprobar que no asigna direcciones por DHCP, su vecino le dice que el técnico que hizo la instalación le explicó que iba a utilizar una configuración más segura, pero que no sabía a qué se refería.



Alain Bachellier (CC BY-NC-SA)

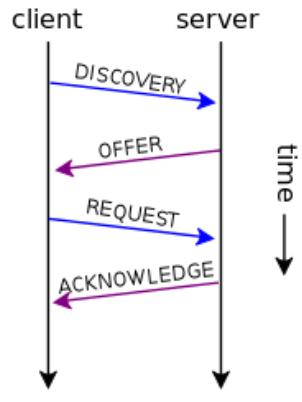
El **direcccionamiento dinámico** es un mecanismo que nos proporciona una configuración de los parámetros de red de forma automática. La dirección proporcionada es la adecuada para que nuestro nodo funcione correctamente en la red, ya sea una LAN o una WAN. Este mecanismo recibe el nombre de **servicio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



helix84 (Dominio público)

- ✓ 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.

No es correcto. Un servidor DHCP puede proporcionar direcciones públicas o privadas.

¡Correcto! Si, es una de sus cualidades, “prestar” direcciones durante un tiempo.

No es correcto. APIPA es otro mecanismo diferente de asignaciones de direcciones IP.

No es correcto. Puede proporcionar direcciones públicas también y con sistemas operativos como Linux.

## Solución

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

## 9.- Adaptadores de red.

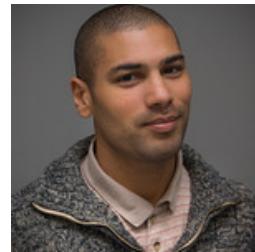
### Caso práctico

**Vindio** siempre lleva su ordenador portátil cuando está trabajando. Es un equipo que le facilitó la empresa como herramienta de trabajo y que él ha adaptado a sus necesidades. Tiene instalada la última distribución de un sistema Linux con diferentes máquinas virtuales de otros sistemas y también va instalando diferentes herramientas informáticas que va necesitando. Es un equipo que no utiliza para entretenimiento tal y como le pidió **Juan** cuando se lo entregó hace ya unos años, por lo que carece de adaptador de red inalámbrico y, llegado el momento tuvieron que adquirir uno USB que mantiene conectado permanentemente.

**Vindio** tiene especial cuidado con el portátil de la empresa, lo cuida y mantiene como si fuese suyo, mejor incluso, porque es su principal herramienta como técnico de sistemas.

De camino a la empresa de un cliente que ha planteado una incidencia, un coche le ha pasado tan cerca que le ha golpeado en la mano y en el maletín del portátil. No ha sido un fuerte golpe, y olvidando el dolor de la mano ha pensado de inmediato en el ordenador. Se detiene en un banco, lo abre para ver si ha sufrido daños y, aunque aparentemente todo está en orden, observa que el icono del adaptador de red no aparece y decide dirigirse a una tienda de informática cercana.

El técnico de la tienda lo confirma, se ha roto el adaptador de red inalámbrico. Pero lo tranquiliza diciendo que acaba de probar un nuevo adaptador de red que va mucho mejor, es más pequeño y más potente. Tras ver las características de varios modelos se decide por el que le ha recomendado y pide la factura porque espera que la empresa pueda hacerse cargo del gasto.



[Alain Bachelier \(CC BY-NC-SA\)](#)

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.



[Helix84 \(CC BY-SA-3.0\)](#)

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.
- ✓ WiFi.
- ✓ 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.

No es correcto. Puede tener más opciones.

¡Correcto! Si, hoy en día puede tener varias opciones de interfaces.

No es correcto. Puede tener además otras opciones como tarjeta de red cableada.

No es correcto. No es habitual pero puede que no tenga este tipo de conexión.

## Solución

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

## 9.1.- Adaptadores de red cableada o alámbricos. Instalación y configuración.

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 normalmente auto-configurará sus parámetros más importantes. Pero si no tuviéramos un **servidor de DHCP** (ver apartado 8) en la red, tendremos que configurarle manualmente los valores adecuados para los siguientes 4 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.



CEphoto, Uwe Aranas (CC BY-SA)

### Debes conocer

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

[Vídeo sobre instalación de una tarjeta de red Ethernet](#)

[Configurar una tarjeta de red en Linux](#)

[Configurar una tarjeta de red en Windows 10](#)

### 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.

¡Correcto! Si, el servidor DHCP de la red proporciona los parámetros para poder conectarse con éxito.

No es correcto. Con esto no es suficiente.

No es correcto. No se trata de una red inalámbrica.

No es correcto. No es necesario porque el servidor DHCP está habilitado y proporciona todo lo necesario.

## Solución

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

## 9.2.- Adaptadores de red inalámbrica. Instalación y configuración.

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, de nuevo si no tuviéramos un **servidor de DHCP** (ver apartado 8) en la red, tendremos que configurarle manualmente los valores adecuados para los siguientes 4 parámetros:

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



[Silverxxx \(CC BY-SA-3.0\)](#)

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 vídeos explicativos de como instalar y configurar una tarjeta de red inalámbrica.

[Instalación y configuración de una tarjeta de red inalámbrica PCI.](#)

[Instalación de un adaptador de red inalámbrica USB.](#)

### 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.

No es correcto. No es necesario desarmar nada.

¡Correcto! Si, se utiliza la tecnología P&P o PnP.

No es correcto. Los equipos pueden disponer de tarjeta interna pero si se pueden instalar en un puerto USB.

No es correcto. Son interfaces diferentes.

## Solución

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

## 9.3.- Comandos de redes para la consola de Windows

---

A lo largo de tu vida profesional te darás cuenta que es necesario conocer una serie de comandos de redes TCP/IP que te permitirán analizar e incluso configurar distintos aspectos de tu red en Windows. Todos los comandos que aprenderás en este apartado son para ejecutarlos en la ventana del símbolo del sistema, también llamada línea de comandos o consola, en cualquier sistema Windows.

Para abrir la ventana del sistema puedes hacerlo de **dos modos**:

- 1.- Inicio, todos los programas, accesorios, Símbolo del sistema.
- 2.- Inicio, Ejecutar, escribes el comando "**cmd**" y aceptar. También puedes usar el atajo de teclado "**Win+R**" para abrir el diálogo de ejecutar, y a continuación escribir "**cmd**".

Una vez en la ventana del sistema, existen una serie de comandos que te serán útiles cuando trabajes con redes desde Windows. En sistemas linux existen comandos similares y en ocasiones son incluso los mismos.

A continuación tienes un listado de **comandos** con sus opciones (escríbelos en minúsculas).

### Comandos de Información

- ✓ **Ping** [IP o host]: diagnostica la conexión entre la red y una dirección IP remota.
  - ↳ -t: permite hacer pings de manera continua, para detenerlo ctrl-c
  - ↳ -l: genera una carga de red, especificando el tamaño del paquete.
- ✓ **Tracert** [@IP o nombre del host]: muestra todas las direcciones IP intermedias por las que pasa un paquete entre el equipo local y la dirección IP especificada.
- ✓ **Ipconfig** /all [/release [tarjeta]] [/renew [tarjeta]] /flushdns /displaydns /registerdns [-a] [-a] [-a]: Sin opciones, este comando muestra la dirección IP activa, la máscara de red, así como, la puerta de enlace predeterminada al nivel de las interfaces de red conocidas en el equipo local.
  - ↳ **/all**: Muestra toda la configuración de la red, incluyendo los servidores DNS, WINS, DHCP, etc ...
  - ↳ **/renew [tarjeta]**: Renueva la configuración DHCP de todas las tarjetas (si ninguna tarjeta es especificada) o de una tarjeta específica si utiliza el parámetro tarjeta. El nombre de la tarjeta, es el que aparece con ipconfig sin parámetros.
  - ↳ **/release [tarjeta]**: Envía un mensaje DHCPRELEASE al servidor DHCP para liberar la configuración DHCP actual y anular la configuración IP de todas las tarjetas (si ninguna tarjeta es especificada), o de sólo una tarjeta específica si utiliza el parámetro tarjeta. Este parámetro desactiva el TCP/IP de las tarjetas configuradas a fin de obtener automáticamente una dirección IP.
  - ↳ **/flushdns**: Vacía y reinicializa el caché de resolución del cliente DNS. Esta opción es útil para excluir las entradas de caché negativas así como todas las otras entradas agregadas de manera dinámica.
  - ↳ **/displaydns**: Muestra el caché de resolución del cliente DNS, que incluye las entradas precargadas desde el archivo de host local así como todos los registros de recursos recientemente obtenidos por las peticiones de nombres resueltas por el ordenador. El servicio Cliente DNS utiliza esta información para resolver rápidamente los nombres frecuentemente solicitados, antes de interrogar a sus servidores DNS configurados.
  - ↳ **/registerdns**: Actualiza todas las concesiones DHCP y vuelve a registrar los nombres DNS.
- ✓ **Netstat** [-a] [-e] [-n] [-s] [-p proto] [-r] [intervalo]: Muestra el estado de la pila TCP/IP en el equipo local.
  - ↳ **-a** Muestra todas las conexiones y puertos de escucha. (Normalmente las conexiones del lado del servidor no se muestran).
  - ↳ **-e** Muestra estadísticas Ethernet. Se puede combinar con la opción **-s**.
  - ↳ **-n** Muestra direcciones y números de puerto en formato numérico.
  - ↳ **-p proto** Muestra las conexiones del protocolo especificado por proto; proto puede ser tcp o udp. Utilizada con la opción **-s** para mostrar estadísticas por protocolo, proto puede ser tcp, udp, o ip. **-r** Muestra el contenido de la tabla de rutas.
  - ↳ **-s** Muestra estadísticas por protocolo. Por defecto, se muestran las estadísticas para TCP, UDP e IP; la opción **-p** puede ser utilizada para especificar un subconjunto de los valores por defecto.
  - ↳ **intervalo** Vuelve a mostrar las estadísticas seleccionadas, con una pausa de "intervalo" segundos entre cada muestra. Con ctrl-c se detiene la presentación de las estadísticas.

### Comandos de enrutamiento

- ✓ **Route** [-f] [comando [destino] [MASK máscara de red] [puerto de enlace]]: Muestra o modifica la tabla de enrutamiento.
  - ⇒ -f Borra, de las tablas de enrutamiento, todas las entradas de las puertas de enlace. Utilizada conjuntamente con otro comando, las tablas son borradas antes de la ejecución del comando.
  - ⇒ -p Vuelve persistente la entrada en la tabla después de reiniciar el equipo.
  - ⇒ comando: Especifica uno de los cuatro comandos siguientes:
    - DELETE: borra una ruta.
    - PRINT: Muestra una ruta.
    - ADD: Agrega una ruta.
    - CHANGE: Modifica una ruta existente.
  - ⇒ destino: Especifica el host.
  - ⇒ MASK: Si la clave MASK está presente, el parámetro que sigue es interpretado como el parámetro de la máscara de red.
  - ⇒ máscara de red: Si se proporciona, especifica el valor de máscara de subred asociado con esta ruta. Si no es así, éste toma el valor por defecto de 255.255.255.255.
  - ⇒ puerta de enlace: Especifica la puerta de enlace.
  - ⇒ METRIC: Especifica el coste métrico para el destino.
- ✓ **ARP**: Resolución de direcciones IP en direcciones MAC. Muestra y modifica las tablas de traducción de direcciones IP a direcciones Físicas utilizadas por el protocolo de resolución de dirección (ARP).
  - ⇒ ARP -s adr\_inet adr\_eth [adr\_if]
  - ⇒ ARP -d adr\_inet [adr\_if]
  - ⇒ ARP -a [adr\_inet] [-N adr\_if]
  - ⇒ -a Muestra las entradas ARP activas interrogando al protocolo de datos activos. Si adr\_inet es precisado, únicamente las direcciones IP y Físicas del ordenador especificado son mostrados. Si más de una interfaz de red utiliza ARP, las entradas de cada tabla ARP son mostradas.
  - ⇒ -g Idéntico a -a.
  - ⇒ adr\_inet Especifica una dirección Internet.
  - ⇒ -N adr\_if Muestra las entradas ARP para la interfaz de red especificada por adr\_if.
  - ⇒ -d Borra al host especificado por adr\_inet.
  - ⇒ -s Agrega al host y relaciona la dirección Internet adr\_inet a la Física adr\_eth. La dirección física está dada bajo la forma de 6 bytes en hexadecimal separados por guiones. La entrada es permanente.
  - ⇒ adr\_eth Especifica una dirección física.
  - ⇒ adr\_if Precisado, especifica la dirección Internet de la interfaz cuya tabla de traducción de direcciones debería ser modificada. No precisada, la primera interfaz aplicable será utilizada.

- ✓ **Nbtstat**: Actualización del caché del archivo Lmhosts. Muestra estadísticas del protocolo y las conexiones TCP/IP actuales utilizando NBT (NetBIOS en TCP/IP).
  - ⇒ NBTSTAT [-a Nom Remoto] [-A dirección IP] [-c] [-n] [-r] [-R] [-s] [S] [intervalo]
  - ⇒ -a (estado de la tarjeta) Lista la tabla de nombres del equipo remoto (nombre conocido).
  - ⇒ -A (estado de la tarjeta) Lista la tabla de nombres del equipo remoto (dirección IP)
  - ⇒ -c (caché) Lista el caché de nombres remotos incluyendo las direcciones IP.
  - ⇒ -n (nombres) Lista los nombres NetBIOS locales.
  - ⇒ -r (resueltos) Lista de nombres resueltos por difusión y vía WINS.
  - ⇒ -R (recarga) Purga y recarga la tabla del caché de nombres remotos.
  - ⇒ -S (sesión) Lista la tabla de sesiones con las direcciones de destino IP.
  - ⇒ -s (sesión) Lista la tabla de sesiones establecidas convirtiendo las direcciones de destino IP en nombres de host a través del archivo host.

## Comandos de conexión

- ✓ **Telnet**: El comando telnet permite acceder en modo Terminal (Pantalla pasiva) a un host remoto. Este también permite ver si un cualquier servicio TCP funciona en un servidor remoto especificando después de la dirección IP el número de puerto TCP.
  - ⇒ telnet < IP o host >
  - ⇒ telnet < IP o host > < port TCP >

De este modo podemos verificar si el servicio SMTP, por ejemplo, funciona en un servidor Microsoft Exchange, utilizando la dirección IP del conector SMTP y luego 25 como número de puerto. Los puertos más comunes son:

- ✓ ftp (21),
- ✓ telnet (23),
- ✓ smtp (25),
- ✓ www (80),
- ✓ kerberos (88),
- ✓ pop3 (110),
- ✓ nntp (119),
- ✓ et nbt (137-139).

- ✓ **Hostname:** Muestra el nombre del equipo.
- ✓ **Ftp:** Cliente de descarga de archivos.
  - ↳ `ftp -s:<file>`
  - ↳ `-s:` esta opción permite ejecutar un FTP en modo batch: especifica un archivo textual conteniendo los comandos FTP.

## Autoevaluación

¿Qué comando se utiliza si quieres comprobar la conexión de tu equipo con una dirección remota?:

- Telnet.
- Arp.
- Ping.
- Tracerouting

Repasa el listado.

Vuelve a repasar.

Efectivamente es correcto.

No es correcta.

## Solución

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

# 10.- La documentación de una instalación de red.

## Caso práctico



Alain Bachellier (CC BY-NC-SA)

**Laro** es quien aparece como responsable de las comprobaciones de red en el parte de trabajo diario, que incluye poner a trabajar a las tres chicas para que lleven a cabo algunas de las comprobaciones y aprendan cómo deben realizar esa importante tarea antes de dar por concluida una instalación.

La lista de pruebas a realizar está clara y casi le supone más tiempo enseñar a **Noiba, Naroba y Jara** lo que deben hacer, que hacerlo por sí mismo. Pero pronto se da cuenta de que las chicas han aprendido a la primera y son capaces de chequear correctamente con las indicaciones que les ha dado, lo que influye positivamente en el tiempo dedicado a esta tarea.

Una vez que ha constatado que la red de la sala de formación se comporta del modo esperado ante las diferentes situaciones plantadas, se dedica a completar la documentación explicando pacientemente a sus compañeras cada uno de los documentos que va generando y que resumen todo el trabajo realizado con las configuraciones que previamente les había marcado **Juan**. Todo ello constituye 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.

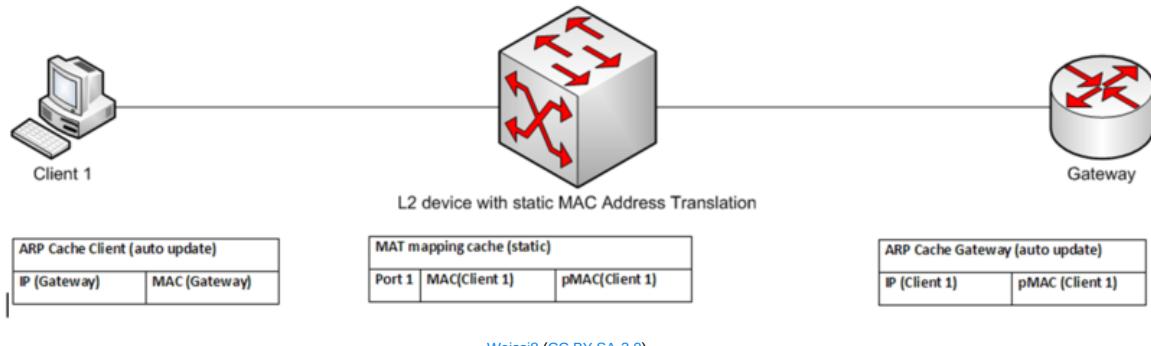
Una vez terminado el montaje de una red y si se ha hecho respetando las normas establecidas, el mantenimiento de un sistema de cableado es prácticamente nulo en condiciones normales. Es importante que el administrador de la red esté pendiente de las obras o reformas que se realicen en el edificio y que 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.
- Señala componentes y documenta el trabajo realizado.
- Señala componentes y documenta el trabajo realizado, la realiza el programador.
- Siempre debe aparecer en papel y debe estar disponible para todo el mundo.

No es correcto. El no tener una instalación documentada dificulta su administración.

¡Correcto! Si, estas son las dos funciones principales.

No es correcto. Esa no es la labor de un programador.

No es correcto. Puede estar en otros formatos y no es conveniente que sea accesible para todos.

## Solución

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

## Para saber más

- 1.- Tutorial donde se muestra como se puede [realizar un diseño lógico de una red utilizando el programa PacketTracer](#).
- 2.- Tutorial donde se muestra como se puede [realizar un diseño físico de la misma red utilizando el programa PacketTracer](#).

# 11.- Monitorización y resolución de incidencias en redes locales.

## Caso práctico

Ante su mesa de trabajo, **Juan** se dispone a monitorizar la red sobre la que, en la jornada anterior, **Laro** le hizo entrega de toda la documentación al dar por concluida la instalación y en la que se recogen todas las actuaciones llevadas a cabo, desde el montaje de los sistemas, dispositivos y elementos, hasta las diferentes configuraciones que él mismo había marcado al confiar el trabajo a **Laro**. Si todo es correcto, debe poder acceder a cada uno de los equipos de la red local, tomar el control del mismo y comprobar su funcionamiento en diferentes situaciones que tiene previamente diseñadas.

Para llevar a cabo esa monitorización de red, **Juan** dispone de una serie de herramientas estándares y otras que ha ido elaborando él mismo mediante script de comandos utilizando esas y otras herramientas, porque muchas de esas aplicaciones no están diseñadas para interferir en el funcionamiento de los demás equipos sino para observar y detectar posibles fallos, pero en su caso debe conocer la capacidad que tendrá la red para evitar problemas.



[Jonny Goldstein \(CC BY\)](#)

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.

El principal protocolo usado para la gestión y monitorización de redes es SNMP, del cual existen varias versiones.

Fue diseñado para ser flexible y extensible. Por eso no tiene un formato fijo. En su lugar, utiliza una estructura de árbol jerárquica denominada Base de información de administración (**MIB**).

Cada dispositivo en una red tiene un programa llamado **agente SNMP**, que recopila información sobre un dispositivo, lo organiza en entradas en un formato coherente y puede responder a las consultas de SNMP. Estos dispositivos pueden incluir teléfonos, impresoras, conmutadores y otro hardware, además de servidores y estaciones de trabajo. Estas consultas SNMP provendrán del **administrador SNMP**, que sondea, recopila y procesa información sobre todos los dispositivos habilitados para SNMP en la red.

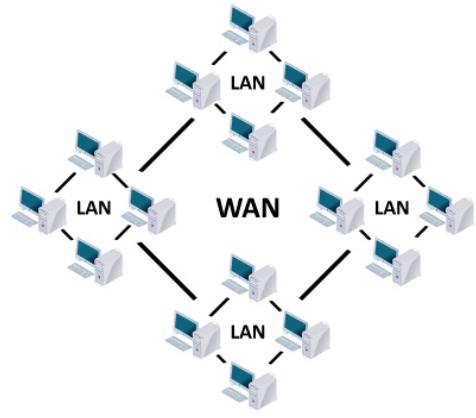
Existen múltiples herramientas para monitorizar una red.

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

- ✓ [Monit](http://mmonit.com/monit/) (<http://mmonit.com/monit/>).
- ✓ [Ganglia](http://ganglia.info/) (<http://ganglia.info/>).

- ✓ [Munin](http://munin-monitoring.org/) (<http://munin-monitoring.org/>).
- ✓ [Cacti](http://www.cacti.net/) (<http://www.cacti.net/>).
- ✓ [Nagios](http://www.nagios.org/) (<http://www.nagios.org/>).
- ✓ [Zabbix](http://www.zabbix.com/) (<http://www.zabbix.com/>).
- ✓ [Nmap](http://nmap.org/) (<http://nmap.org/>).
- ✓ [Zenoss](http://www.zenoss.com/product/network) (<http://www.zenoss.com/product/network>).
- ✓ [Argus](http://argus.tcp4me.com/) (<http://argus.tcp4me.com/>).

Muchas de estas herramientas usan SNMP para gestionar los dispositivos de red.



[Mdnz27 \(CC BY-SA-4.0\)](#)

## 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.

No es correcto. No utilizaría esa frase.

¡Correcto! Sí, hay aplicaciones de monitorización que ven como funcionan los protocolos ARP.

No es correcto, son acciones diferentes.

No es correcto. Si es posible ver como una difusión MAC busca una dirección física asociada a una IP.

## Solución

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

## Para saber más

- 1.- [Cómo usar SNMP para Monitorear Dispositivos de Red](#)
- 2.- [Zabbix - Monitoree un Switch a través de SNMP](#)
- 3.- [Cómo configurar SNMPv3 en Zabbix para monitorear el hardware de la red](#), cómo crear plantillas adecuadas en Zabbix y qué puede lograr organizando un sistema de alerta distribuido en una red grande.
- 4.- [Fragmentos de películas en los que aparecen "hackeando" con NMAP.](#)
- 5.- [Ánalysis de Tráfico de Red; Análisis de tráfico con Wireshark - Parte 1](#)

# 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 siguiente [Aviso legal](#)

## Historial de actualizaciones

Versión: 02.00.00

Fecha de actualización: 21/06/21

Autoría: Jesús Manuel Marín Navarro

**Ubicación:** Varios: Ver abajo

**Mejora (tipo 1):** Algunas sugerencias las había hecho el alumnado y no son del todo correctas. Copio aquí todo lo modificado y añadido además de lo anterior:

- Apartado 4. Actualizar todos los protocolos de WiFi y de telefonía . En la unidad 7 al final hay algo introductorio a WiMax y UMTS desactualizado
  - X 4.1 : enlace a Wi-Fi 6 y todos los protocolos Wi-Fi, y también marcados Wi-Fi 4 y Wi-Fi 5
  - X 4.3: Ad-hoc. Enlaces punto a punto entre dispositivos que estén en el mismo rango (cerca en el espacio y usando una misma frecuencia del espectro electro-magnético). 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. El AP es el que arbitra quién puede transmitir en cada momento para evitar colisiones según el protocolo CSMA/CA (Collision Avoidance). Haciendo un símil con la comunicación por cable, el modo Ad-hoc sería equivalente a comunicar dos ordenadores entre sí mediante un cable (punto a punto) y el modo Infraestructura equivaldría a comunicar los ordenadores utilizando un concentrador (hub).
  - X 4.3 (II) Si nos fijamos en la topología lógica, se puede decir que la topología en estrella es la estándar para redes inalámbricas con el AP en el centro gestionando el orden en el que cada una de las estaciones transmite en cada momento. Aunque a nivel físico sería más parecido a un bus por ser un medio compartido el campo electromagnético en determinada frecuencia.
  - X En el apartado 4.4: WP3 fue anunciado en enero de 2018, debido a una vulnerabilidad descubierta en WPA2. El estándar WPA3 SAE reemplaza el intercambio de claves pre-compartidas (PSK) con la autenticación simultánea de iguales (SAE), lo que resulta en un intercambio inicial de claves más seguro en modo personal. El nuevo estándar utiliza cifrado de 128 bits en modo WPA3-Personal (192 bits en WPA3-Enterprise)3 y confidencialidad de reenvío.
  - También reducirá los problemas de seguridad que plantean las contraseñas débiles y simplificará el proceso de configuración de dispositivos sin interfaz de visualización.
  - X Apartado 5. Direcciónamiento Avanzado - Ejercicio de Asignar direcciónamiento por subredes dado un rango y una topología de red. Segmentación.
  - X 5.3: Aunque a día de hoy sigue usándose mucho y es uno de los conceptos más importante a manejar como administrador de red. En la última unidad del curso se profundizará en NAT y se verán ejemplos de configuración, así como de apertura/redirección de puertos.
  - X 5.5: en la penúltima tabla del apartado 5.5 (CIDR y superredes). En concreto, en la primera columna, los dos últimos octetos están cambiados
    - apartado 5.1.- IPv4, habla sobre la operación AND binario en el siguiente párrafo.
    - “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 binaria AND entre la IP y la máscara de red, el resultado es la dirección de red.”
    - Desde mi punto de vista se queda corta, creo que sería bueno que se mostrara como se obtiene la dirección de red a partir de la máscara de red y de una dirección IP.
    - En el enlace se puede ver un video que contiene un ejemplo sobre como se obtiene la dirección de red en un router: <https://www.youtube.com/watch?v=aLoRDMZAHvc>
    - Asociar los distintos tipos de direcciónamiento en distintas capas. Vídeo [https://www.youtube.com/watch?v=h\\_PaKKw5riE](https://www.youtube.com/watch?v=h_PaKKw5riE)
    - Cálculo: Nº hosts, dirección de red y broadcast, primera y última direcciones posibles:

- <https://youtu.be/gAXS0x1kwWw>
- Sobre direccionamiento y subredes:
    - <https://www.youtube.com/watch?v=qEE0s9cnj34>
    - <https://www.youtube.com/watch?v=SHbBso63X38>
    -
  - Apartado 7. Explicar el ARP cuando hay que atravesar routers con un ejercicio práctico en Packet Tracer. Ver ejerc de Ángeles con tabla que muestra cómo van cambiando las direcciones de origen y destino a nivel 2 y 3 también. Explicar los comandos de red de Windows y Linux a nivel de arp y direccionamiento.
  - Inclusión de comandos básicos como arp -a o arp -d
  - Enlace Windows: <http://itroque.edu.mx/cisco/cisco1/course/module11/11.3.4.2/11.3.4.2.html>
  - Enlace Linux: <https://francisconi.org/linux/comandos/arp>
  - Explicación del funcionamiento del protocolo ARP y ARP caché (tiempo de duración de las tablas, información que contiene, etc.) Enlace: <https://www.ionos.es/digitalguide/servidores/know-how/arp-resolucion-de-direcciones-en-la-red/>
  - Añadidos 2 videos más recomendados
  - <https://commons.wikimedia.org/wiki/File:Arp-eg.gif>
  - Añadidas más explicaciones

Añadiría en el apartado 7 de la unidad información referente a como analizar

**Ubicación:** 7.- Resolución de direcciones. ARP y RARP.

**Mejora (tipo 1):** He adjuntado en el foro una imagen sobre el protocolo ARP a modo de esquema.

**Ubicación:** 10.- La documentación de una instalación de red.

**Mejora (tipo 2):** Sigo echando en falta hablar algo mas de seguridad. En este apartado, tratándose de la documentación, y citando textualmente La documentación supone un plus de calidad en cualquier trabajo realizado. Me sorprende que no se remita a ningún consejo de seguridad, pautas para una red o conexión segura, ya sea a nivel técnico, de configuración, o incluso de cara al usuario final al que se le configure la red.

**Ubicación:** 9.- Adaptadores de red.

**Mejora (tipo 2):** Estaría genial que se explicaran las limitaciones de cada puerto, así como su compatibilidad y la velocidad de carga/descarga de información. También como instalar los drivers de dichas conexiones.

**Ubicación:** Todo el tema

**Mejora (tipo 3):** Reordenar el tema para que quede clara la relación de este con el anterior tema y con los posteriores

Apartado 2 y 4.1: Actualizar las unidades de medida de la capacidad y transmisión de información. Actualizar los estándares WiFi

Apartado 4. Actualizar todos los protocolos de WiFi y de telefonía . En la unidad 7 al final hay algo introductorio a WiMax y UMTS desactualizado

En el apartado 4.4:

WP3 fue anunciado en enero de 2018, debido a una vulnerabilidad descubierta en WPA2. El estándar WPA3 SAE reemplaza el intercambio de claves pre-compartidas (PSK) con la autenticación simultánea de iguales (SAE), lo que resulta en un intercambio inicial de claves más seguro en modo personal. El nuevo estándar utiliza cifrado de 128 bits en modo WPA3-Personal (192 bits en WPA3-Enterprise)3 y confidencialidad de reenvío.

También reducirá los problemas de seguridad que plantean las contraseñas débiles y simplificará el proceso de configuración de dispositivos sin interfaz de visualización.

## Apartado 5. Direccionamiento Avanzado -

Revisar ejercicio del 5.5 que tiene errores en la penúltima tabla del apartado. En concreto, en la primera columna, de Dirección de red, los dos últimos octetos están intercambiados entre sí en las cuatro filas.

Hacer un nuevo Ejercicio de Asignar direccionamiento por subredes dado un rango y una topología de red.

Segmentación: Asociar claramente los dominios de difusión con los distintos segmentos de nivel 3 (subredes IP).

Asociar los distintos tipos de direccionamiento en distintas capas con ejemplo y Vídeo

[https://www.youtube.com/watch?v=h\\_PaKKw5riE](https://www.youtube.com/watch?v=h_PaKKw5riE)

Cálculo: Nº hosts, dirección de red y broadcast, primera y última direcciones posibles:

<https://youtu.be/gAXS0x1kwWw>

Sobre direccionamiento y subredes:

<https://www.youtube.com/watch?v=qEE0s9cnj34>

<https://www.youtube.com/watch?v=SHbBso63X38>

Apartado 7. Explicar el ARP cuando hay que atravesar routers con un ejercicio práctico en Packet Tracer. Ver ejerc de Ángeles con tabla que muestra cómo van cambiando las direcciones de origen y destino a nivel 2 y 3 también.

Explicar los comandos de red de Windows y Linux a nivel de arp , direccionamiento, rutas, puertos, etc. (En Materiales SMR está en varias unidades)

Inclusión de ejemplo con comandos básicos como arp -a o arp -d

Enlace Windows: <http://itroque.edu.mx/cisco/cisco1/course/module11/11.3.4.2/11.3.4.2.html>

Enlace Linux: <https://francisconi.org/linux/comandos/arp>

Explicación del funcionamiento del protocolo ARP y ARP caché (tiempo de duración de las tablas, información que contiene, etc.) Enlace: <https://www.ionos.es/digitalguide/servidores/know-how/arp-resolucion-de-direcciones-en-la-red/>

\*\* Añadir un apartado sobre mapas físicos y lógicos de la red. Como en SMR3-5.4

Introducción a Packet Tracer que se usará a partir de esta unidad en las tareas. Y se pueden probar todos los comandos de ejemplo también de los PCs y ver cómo funciona ARP básico, un ping y conexiones básicas de un PC con otro, con hub, switch, etc.

También habrá que tocar a las preguntas online, el mapa conceptual, las orientaciones para el alumnado, etc.

**Ubicación:** 5.5. CIDR y superredes

**Mejora (tipo 1):** Hay una errata en la penúltima tabla del apartado. En concreto, en la primera columna, de Dirección de red, los dos últimos octetos están intercambiados entre sí en las cuatro filas.

**Ubicación:** 7. Resolución de direcciones. ARP y RARP

**Mejora (tipo 2):** Habría que ampliar el apartado, incluyendo información práctica, con el uso de comandos básicos sobre ARP caché, como arp -a o arp-d, y y cómo funciona esa tabla (tiempo que dura, información que guarda, etc.). Aunque por lo que he visto parece que los comandos en Windows y Linux son similares, y como he dicho sea información muy básica, aquí dejo estos enlaces:

Para Windows: <http://itroque.edu.mx/cisco/cisco1/course/module11/11.3.4.2/11.3.4.2.html>

Para Linux: <https://francisconi.org/linux/comandos/arp>

Funcionamiento de ARP: <https://www.ionos.es/digitalguide/servidores/know-how/arp-resolucion-de-direcciones-en-la-red/>

**Ubicación:** 4.4 Asociación y autenticación en la WLAN

**Mejora (tipo 2):** Añadiría información sobre el nuevo protocolo WPA3, además de los WPA y WPA2 que aparecen.

WPA3 fue anunciado en enero de 2018, debido a una vulnerabilidad descubierta en WPA2. El estándar WPA3 SAE reemplaza el intercambio de claves pre-compartidas (PSK) con la autenticación simultánea de iguales (SAE), lo que resulta en un intercambio inicial de claves más seguro en modo personal. El nuevo estándar utiliza cifrado de 128 bits en modo WPA3-Personal (192 bits en WPA3-Enterprise) y confidencialidad de reenvío.

También reducirá los problemas de seguridad que plantean las contraseñas débiles y simplificará el proceso de configuración de dispositivos sin interfaz de visualización.

**Ubicación:** 5.4 Subredes y máscaras de subred.

**Mejora (tipo 2):** Encuentro necesario para el subnetting algún vídeo explicativo para realizar la práctica de crear subredes de las diferentes clases. Aporto un vídeo que a mi parecer es muy interesante:

[https://www.youtube.com/watch?v=KEYUQthSH\\_0&feature=emb\\_logo](https://www.youtube.com/watch?v=KEYUQthSH_0&feature=emb_logo)

**Ubicación:** Apartado 7

**Mejora (tipo 2):** En este apartado, para ampliación, he encontrado varias páginas que me han servido de bastante ayuda para complementar lo que ya viene en la unidad.

Amplía el apartado del protocolo ARP y el protocolo ICMP, que me parece bastante interesante.

<https://www.ionos.es/digitalguide/servidores/know-how/que-es-el-protocolo-icmp-y-como-funciona/>

<https://aprendederedes.com/redes/ip/arp-adress-resolution-protocol/>

**Ubicación:** 2 , 4.1

**Mejora (tipo 2):** Actualizar las unidades de medida de la capacidad y transmisión de información.

Actualizar los estándares WiFi

**Ubicación:** No han habido cambios

**Mejora (Mapa conceptual):** No han habido cambios

**Ubicación:** 9.3

**Mejora (Orientaciones del alumnado):** Añadido el 9.3

**Ubicación:** Sección 11

**Mejora (Orientaciones del alumnado):** Incluiría un video para tener un poco más claro el análisis del tráfico de red, tipo:

[https://www.youtube.com/watch?v=gF\\_8mjClj34&ab\\_channel=CiberseguridadParaTodos-DavidPereira](https://www.youtube.com/watch?v=gF_8mjClj34&ab_channel=CiberseguridadParaTodos-DavidPereira)

En general los videos son de mucha ayuda para aclarar ideas.

**Versión: 01.00.00**

**Fecha de actualización: 23/07/20**

Versión inicial de los materiales.

