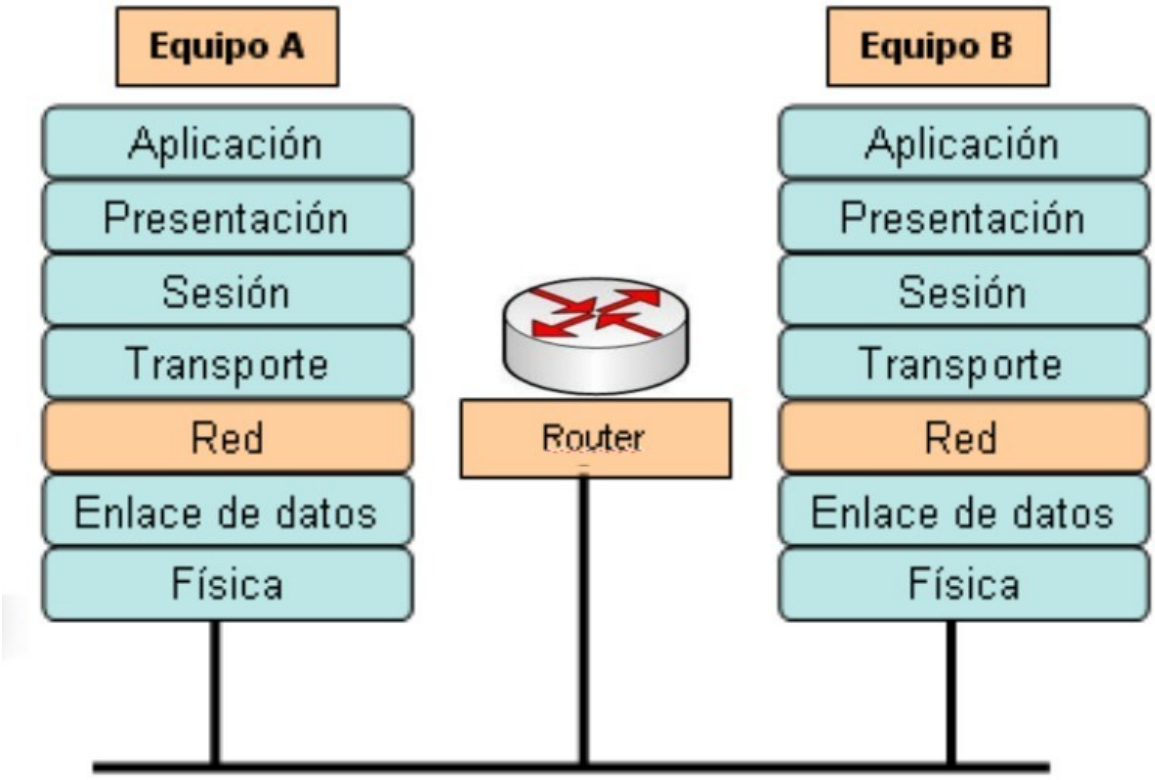
TEMA 1 : Nivel de Red I



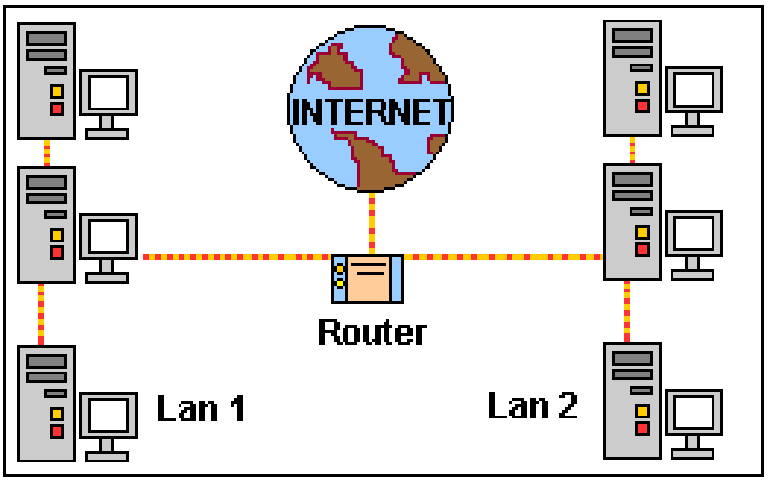
ÍNDICE

1. Introducción.

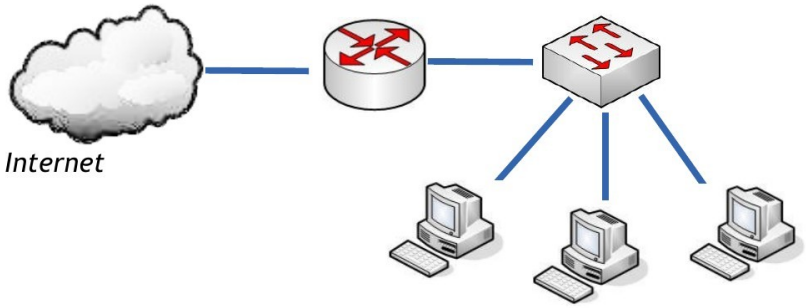
Al igual que pasaba con el nivel físico cuando empezamos a estudiar el nivel de enlace de datos, nos " despreocupamos " del nivel de enlace, en el sentido de que, a partir de ahora, vamos a trabajar con la comunicación entre dos ordenadores, y no nos importa si se hace con un medio o con otro, y si se hace bien o no… sabemos que cuando enviamos unos bits desde un ordenador a otro, van a llegar bien, ya que el nivel de enlace y el nivel físico se van a encargar de ello, y así nos podemos centrar en la transmisión tal cual.

Vamos a ver ahora cómo conseguir la comunicación entre dos equipos que están separados en diferentes redes: hasta ahora estábamos trabajando con redes pequeñas, en donde los switches almacenan las MAC de los equipos que tienen conectados y pueden redirigir las tramas hacia su destino. El problema se presenta cuando queremos conectar cientos, miles o millones de ordenadores que están en edificios, ciudades, países y/o continentes distintos. EL sistema de MAC deja de ser útil y hay que utilizar otro sistema distinto.

De esto se encarga el **nivel de red**: permite interconectar equipos que están en **redes distintas** utilizando para ello un mecanismo distinto al de las MAC, y además hacerlo de forma eficiente, pues debe encargarse de proporcionar por los diferentes nodos de la red o redes, a través del cual van a ir los datos, haciendo que la información llegue cuanto antes, pero evitando embotellamientos. También es misión del nivel de red el resolver todos los problemas que impidan que las redes sean heterogéneas y puedan ser interconectadas.



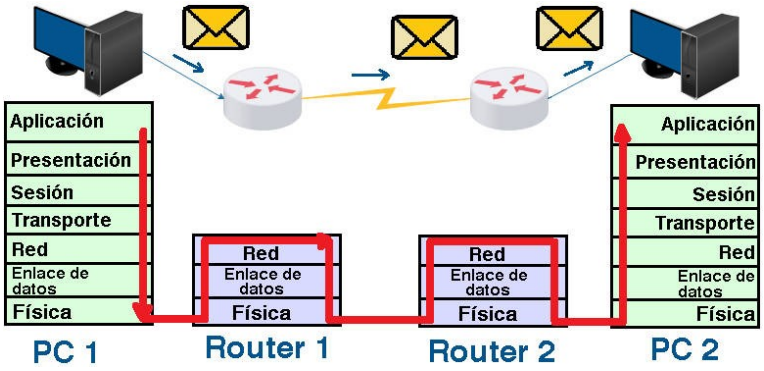
Hemos visto que para enviar tramas se debe conocer la MAC del destinatario. Cuando tenemos muchos equipos divididos en varias redes, es muy complicado saber en qué red está ese equipo conociendo solo su MAC. Por eso, se ideó un sistema de direccionamiento: la **dirección IP** (Internet Protocol)



2. La capa de red

La función principal de la capa de red es la de dirigir los paquetes de información desde la estación origen a la estación destino en redes que pueden estar geográficamente muy separadas. Es la responsable, por tanto, de encaminar todos los paquetes de datos a lo largo del trayecto, independientemente del número de de dispositivos que tengan que cruzar para completarlo.

Este movimiento de paquetes entre redes alejadas recibe el nombre de ***internetworking,*** ya que conecta redes de parámetros muy distintos.

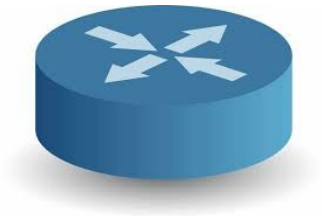


Para que la capa de red pueda proporcionar este servicio de una manera eficaz, debe conocer la topología de cada subred de comunicación y seleccionar la trayectoria más conveniente en cada caso. Uno de los grandes problemas de diseño de la capa de red será establecer las rutas que deben seguir los paquetes, para evitar sobrecargas en algunas líneas de comunicación mientras otras quedan desactivadas.

Para poder llevar a cabo esta tarea, en la capa de red aparece un dispositivo de vital importancia: **el router**.

El router es el encargado de:

- Delimitar cada una de las redes existentes
- Establecer cómo llegan los paquetes de una red a otra. Cada una de las redes delimitadas por el router recibe el nombre de subred.



2.1 Direccionamiento lógico.

En la capa de enlace de datos vimos que todas las tarjetas de red disponen de un direccionamiento físico para identificase, la dirección MAC.

Este tipo de direccionamiento posee, una gran limitación: debido a que es de naturaleza plana, sus números no proporcionan ninguna información acerca de dónde puede

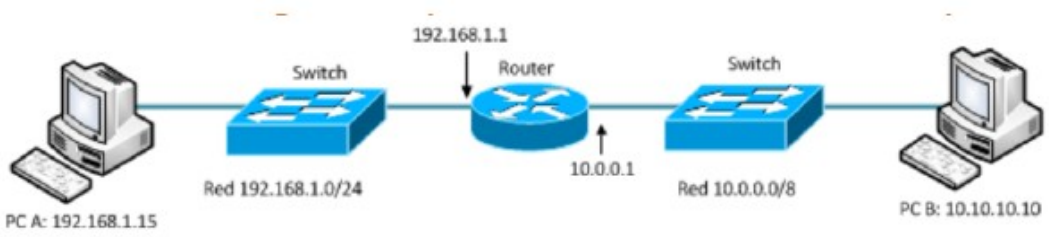
encontrarse el dispositivo que tiene tal dirección. Por ello, este direccionamiento solamente es válido para moverse por una única red.

Cuando queremos que nuestros paquetes circulen de una subred a otra, necesitamos un tipo de direccionamiento que nos dé cierta información acerca de dónde puede estar el dispositivo al que dirigida la información.

Por lo tanto las estaciones necesitan tener un número que les permita comunicarse entre subredes: **la dirección IP.**

> ***El número de dirección IP tiene una naturaleza lógica y jerárquica, gracias a la cual los routers son capaces de realizar rutas de encaminamientos para que los paquetes circulen de la subred origen a la subred destino***

Este número se llama dirección IP por ser el número usado por el protocolo IP (internet protocol).



2.2 Funciones de la capa de red.

La capa de red brinda servicios para permitir que los hosts puedan intercambiar datos en la red.

Para lograr el transporte completo, la capa de red utiliza cuatro procesos o funciones básicas:

a) Direccionamiento de terminales.

b) Encapsulamiento.

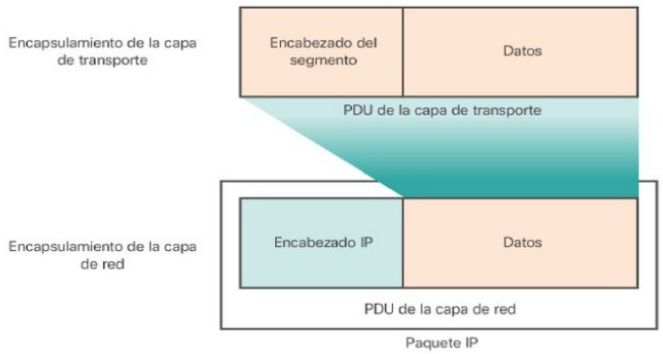
c) Routing (enrutamiento)

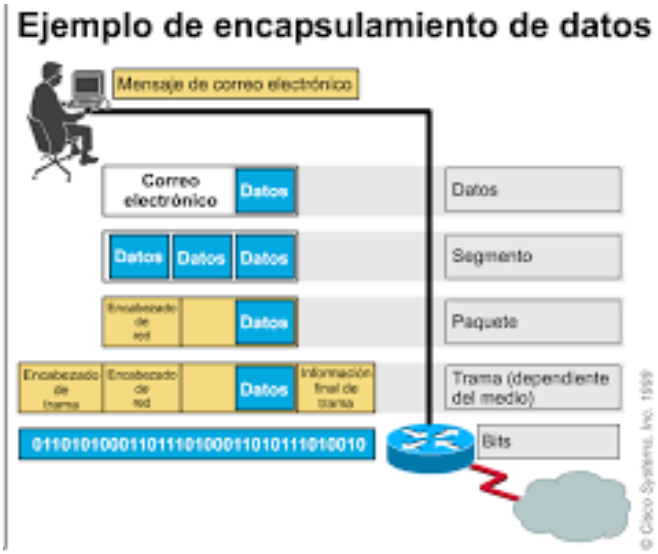
d) Desencapsulamiento

a) Direccionamiento de terminales.

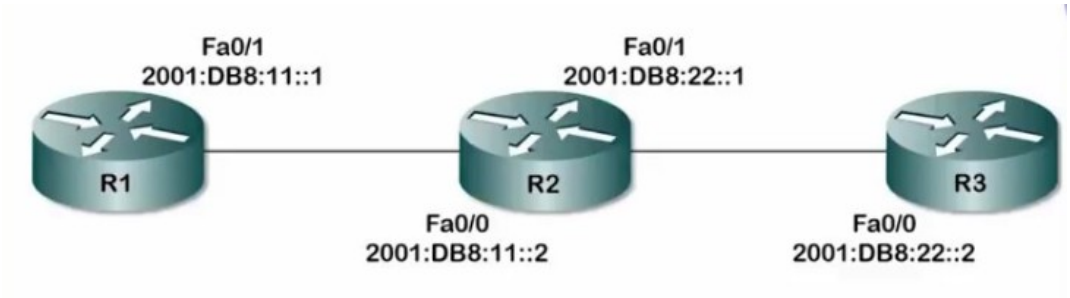
Los terminales se deben configurar con una dirección IP única para identificarlos en la red.

b) Encapsulamiento: La capa de red encapsula la unidad de datos del protocolo (PDU, que es la forma que adoptan los datos en cada capa) de la capa de transporte a un paquete. El proceso de encapsulación agrega información de encabezado IP, como la dirección IP de los hosts de origen (envío) y destino (recepción).

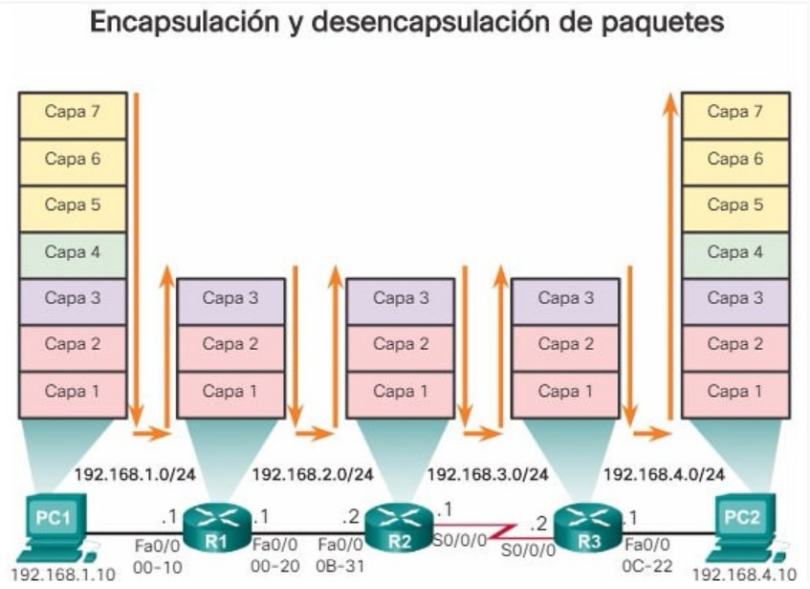




c) Enrutamiento o Routing: La capa de red proporciona servicios para dirigir los paquetes a un host de destino en otra red. Para viajar a otras redes, el paquete debe ser procesado por un Router. La función del Router es seleccionar la mejor ruta y los paquetes directos hacia el host de destino en un proceso conocido como enrutamiento. Un paquete puede cruzar muchos Routers antes de llegar al host de destino. Cada Router que un paquete cruza para llegar al host de destino se llama **salto**.



d) Desencapsulamiento: Cuando el paquete llega a la capa de red del host de destino, el host verifica el encabezado IP del paquete. Si la dirección IP de destino dentro del encabezado coincide con su propia dirección IP, el encabezado IP se elimina del paquete. Después de que el paquete es desencapsulado por la capa de red, la PDU de Capa 4 resultante se pasa al servicio apropiado en la capa de transporte. El proceso de desencapsulación lo realiza el host de destino del paquete IP.



Nota: Se denomina “salto” a cada router que cruza un paquete antes de alcanzar el host de destino.

2.3 Protocolos de la capa de red.

Dentro de la capa de red existen ciertos protocolos que, básicamente, definen como se dirige el tráfico por la red.

Hay varios protocolos enrutados, pero el más extendido y que nosotros estudiaremos es IP(Internet Protocol).

Existen dos versiones de IP:

- Protocolo de Internet versión 4 (IPv4).
- Protocolo de Internet versión 6 (IPv6).

Protocolo IP (internet protocol): Se trata de un protocolo orientado a datagrama, que tiene como objetivo principal ofrecer un mecanismo de direccionamiento de los dispositivos en una red de comunicación de paquetes.

Otros protocolos son:

- **Ipsec (internet protocol security):** son un conjunto de protocolos criptográficos que dotan de seguridad al protocolo IP proporcionando mecanismos de seguridad la protocolo IP proporcionando mecanismos de autentificación y cifrado de paquetes IP. Este tipo de protocolos se utilizan a menudo en las redes que requieren altos niveles de seguridad. En IPv6 el uso de Ipsec es obligatorio.
- IPX/SPX. En desuso
- NetBEUI. En desuso

2.3.1 Protocolo ARP

El protocolo ARP (Addres Resolution Protocol, protocolo de resolución de direcciones) es un protocolo de la capa de red que encuentra la dirección MAC de una determinada dirección IP.

Cuando dos equipos se comunican, en la capa de red tendrán que indicar las dirección de IP origen y destino. Una vez formado el paquete, se baja a la capa de enlace de datos, el cual será encapsulado en una trama. En dicha trama se añadirán las direcciones MAC origen y destino.

La dirección MAC origen la conoce el PC, pero la dirección MAC destino asociada a la IP destino (o puerta de enlace) no la conoce. Para descubrir dicha dirección MAC se utiliza el protocolo ARP.

El protocolo ARP envía una solicitud a toda la red, pidiendo la dirección MAC asociada a una determinada dirección IP. Todos los equipos de la red procesan dicha solicitud y comparan la dirección IP del paquete ARP con la suya, si alguno de ellos tiene esa dirección IP responderá al mensaje ARP con la dirección MAC. De esta forma, el host origen dispondrá de la MAC destino para completar la trama y poder enviarla.

Comando:

arp -a → Muestra la tabla ARP

```
C:\Users\Public>arp -a

Interfaz: 192.168.1.94 --- 0x14
  Dirección de Internet          Dirección física      Tipo
  192.168.1.1           78-29-ed-82-4d-38     dinámico
  192.168.1.25          60-a4-b7-22-e0-2b     dinámico
  192.168.1.49          44-00-49-e8-d2-b8     dinámico
  192.168.1.255         ff-ff-ff-ff-ff-ff     estático
```

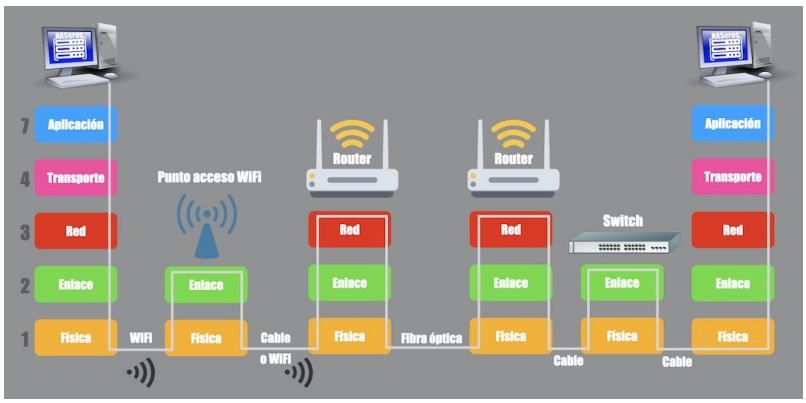
3. Dirección IP.

Dirección IP: Consiste en un número de 4 bytes que identifica de manera lógica y jerarquicamente a una máquina (habitualmente un ordenador) dentro de una red. Sería parecido a como funcionan los números de teléfono: el primer dígito indica si es fijo (9 o 8) o móvil (6 o 7), si es fijo, los tres primeros indican la provincia, los siguientes la localidad, la zona.. y los últimos el abonado. De esta forma, la llamada "va viajando" desde el remitente hasta el destinatario a través de las centralitas.

La idea es que los números de la dirección IP permitan encaminar el mensaje hacia su destino, sin necesidad de tener que almacenar todas las direcciones MAC de todos los equipos. Para ello, las tramas deben ampliarse con la información de la IP, convirtiéndose así en **paquetes** o **datagramas.**

Este es el objetivo de la nueva capa, la capa de RED: conseguir hacer que los datos lleguen desde el origen al destino, aún cuando ambos no estén conectados directamente (están conectados a través de otras redes).

Además de las Ips, se ideó un nuevo dispositivo: el ROUTER o enrutador. Mencionado anteriormente. Un router es como un switch inteligente que trabaja con IPs y que se encarga de comunicar una red con otra.



A continuación estudiaremos en profundidad el Protocolo de Internet versión 4 (IPv4).

El protocolo de Internet versión 6 (IPv6) lo veremos en lecciones posteriores.

3.1 IPv4

Es la cuarta versión del protocolo IP y la primera en ser utilizada a gran escala. A continuación veremos una amplia descripción de ella.

Formato de un paquete IPv4

Una dirección IP está formada por 32 números binarios agrupados en cuatro bytes. Para poder recordarlas más fácilmente, las direcciones IP se expresan en números decimales separados por puntos.

1 byte	1 byte	1 byte	1 byte
11000000	00000111	00100010	00001010
192	7	34	10

Se expresaría por tanto, así: 192.7.34.10

El valor máximo de cada uno de los bytes es 11111111, que da un valor decimal de 255. Por tanto, las direcciones que tienen un número mayor de 255 en alguno de sus octeto son consideradas **inválidas**

Una dirección IP **se puede representar:**

- En **decimal** (lo habitual), → desde 0.0.0.0 hasta 255.255.255.255

- En **hexadecimal**, → desde 00.00.00.00 hasta FF.FF.FF.FF
- En **binario,** → desde 00000000.00000000.00000000.00000000 hasta 11111111.11111111.11111111.11111111

Ejemplo:

- **decimal**: 128.10.2.30
- **hexadecimal:** 80.0A.02.1E
- **binario:** 10000000.00001010.00000010.00011110

Al llegar al router, los números IP se separan en dos partes:

- Una que identifica la red hacia la que va el paquetes.
- Otra que identifica el equipo destino.

Dependiendo del tipo de red, se escogen uno, dos o tres bytes para identificar el número de red y el resto de bytes de la dirección para identificar el host de destino.

Ejemplo de la división de la dirección IP

Red	Red	Host	Host
1 byte	1 byte	1 byte	1 byte
172	18	135	201

En este ejemplo, los dos primeros octetos del número de dirección IP pertenecería a la red de destino y los dos últimos al host al que va dirigido el paquete.

Esto es importante porque el número de bits que especifican para la parte que identifica el host determina el número máximo de equipos que podrán conectarse a esa red.

Ejemplo

Si reservamos **8 bits** para la parte de host podremos conectar a esa red un **máximo de 255** **2^8** equipos, (más adelante veremos que a esta cantidad habría que restar algún número)

De la misma forma, los bits reservados par la parte de red determinarán el número máximo de redes que pueden crearse. Este concepto está muy ligado a las clases de redes que veremos en la siguiente sección.

Las direcciones IP están formadas por una secuencia de 0's y 1's de 32 bits escritas en formato decimal y separadas por puntos. Cada dirección IPv4 está formada por cuatro octetos (grupo de 8 bits), donde cada byte almacena números entre 0 y 255.

Ejemplo: **164.12.123.65**

No obstante, una dirección IP se puede representar:

- **En decimal** (lo habitual), desde 0.0.0.0 hasta 255.255.255.255
- **En hexadecimal**, desde 00.00.00.00 hasta FF.FF.FF.FF
- **En binario,** desde 00000000.00000000.00000000.00000000 hasta 11111111.11111111.11111111.11111111

Ejemplo:

- **decimal:** 128.10.2.30
- **hexadecimal:** 80.0A.02.1E
- **binario:** 10000000.00001010.00000010.00011110

3.2 Redes con clase

Dependiendo del número de bits que se escoge para interpretar el número de red y de host, las direcciones IP se agrupan en clases.

Existen cinco tipos que reciben los nombres de clase A, B, C, D, E las dos últimas son de tipo experimental y no útiles en la práctica.

CLASE A

Las direcciones de clase A contienen 8 bits para direccionar la parte de red y 24 bits para direccionar la parte de host. Además el primer bit de la dirección de red siempre ha de valer 0.

N.º de bits →	1	7	24		
Clase A →	0	RED	Host	Host	Host

Del byte que se reserva para la parte de red, solo se utilizan 7 bits, ya que el primero vale 0; esto nos da un número de **2^7 = 128** redes potenciales de clase A.

De la misma manera, como se reservan **24 bits** para la parte de host, podremos conectar **2^{24} = 16777216** equipos a cada una de nuestras redes de clase A.

Este tipo de redes se utilizarán para redes muy grandes que tengan que dar cabida a muchos equipos conectados a la misma red.

Podremos saber si una dirección es de clase A fijándonos en el valor del primer octeto:

- **El rango de direcciones de clase A va desde 0 y 126** (el 127 no se incluye porque se ha reservado como dirección especial).

Ejemplo de dirección de clase A es 65.33.21.12

CLASE B

Las direcciones de clase B contienen 16 bits para direccionar la parte de red y 16 bits para direccionar la parte de host. Además los dos primeros bits de la dirección de red siempre ha de valer 10.

N.º de bits →	**2**	**14**		**16**	
Clase B →	**10**	**RED**	**RED**	**Host**	**Host**

Se reservan para redes 14 bits, **2^{14} = 16384** y para equipos por cada red **2^{16} = 65536**

Esta clase de redes se diseñó para redes de medio o gran tamaño.

- **El rango de direcciones de clase B va desde 128.0.0.0 hasta 191.255.0.0**

Un ejemplo de dirección IP de esta clase es 130.21.12.234

CLASE C

Las direcciones de clase C contienen 24 bits para direccionar la parte de red y 8 bits para direccionar la parte de host. Además los tres primeros bits de la dirección de red siempre ha de valer 110.

N.º de bits →	3	21			8
Clase C →	110	RED	RED	RED	Host

Se reservan para redes 21 bits, $2^{21} = 2097152$ y para equipos por cada red $2^{8} = 256$

Esta clase de redes se diseñó para redes pequeñas.

- **El rango de direcciones de clase C va desde 192.0.0.0 hasta 223.255.255.0**

Un ejemplo de dirección IP de esta clase es 195.233.24.250

Este tipo de redes son las que se utilizan con mayor frecuencia.

CLASE D

Las direcciones de clase D contienen 8 bits para direccionar la parte de red y 24 bits para direccionar la parte de host. Además los cuatro primeros bits de la dirección de red siempre ha de valer 1110.

N.º de bits →	4	4		24	
Clase D →	1110	RED	Host	Host	Host

- **Para que una IP sea de esta clase, su primer octeto debe estar comprendido entre el rango de 224 a 239.**

Este tipo de direcciones se utiliza únicamente para experimentación multicast, que es una dirección exclusiva que dirige los paquetes a grupos de equipos.

CLASE E

Las direcciones de clase E contienen 8 bits para direccionar la parte de red y 24 bits para direccionar la parte de host. Además los cuatro primeros bits de la dirección de red siempre ha de valer 1111.

N.º de bits →	4	4		24	
Clase E →	1111	RED	Host	Host	Host

En este tipo de direcciones solamente sería posible formar 16 tipos de redes, ya que $2^4 = 16$.

Para que una IP sea de esta clase, el valor de su primer byte debe estar comprendido entre 240 a 255.

Este tipo direcciones se reservan para que la IETF (i*nternet engineering task force)* realice investigaciones, por tanto no se emiten direcciones de clase E para ser utilizadas por Internet.

NOTA : Cómo saber el límite inferior y superior de una dirección IP

Para saber el límite inferior y superior que alcanza una clase de dirección IP, simplemente debemos rellenar los bit de la parte de red a 0 y 1 binarios respectivamente.

Por ejemplo

En las direcciones de clase B, como sabemos que comienzan por 10, si rellenamos a 0 el resto de bits aparece el límite inferior de la clase: 128.0 y si rellenamos a 1 el límite superior 191.255

Tabla resumen de clases de redes.

Clase	Formato(r=red, h=host)	Nº de redes	Nº de hosts por red	Rango de direcciones de redes
A	r.h.h.h	128	16.777.214	0.0.0.0 - 127.0.0.0
B	r.r.h.h	16.384	65.534	128.0.0.0 - 191.255.0.0
C	r.r.r.h	2.097.152	254	192.0.0.0 - 223.255.255.0
D	grupo			224.0.0.0 - 239.255.255.255
E	no válidas			240.0.0.0 - 255.255.255.255

3.3 Redes y direcciones IP especiales.

Independiente de la clase de dirección IP que posean las redes, todas tienen dos direcciones que no pueden colocarse a los dispositivos por estar destinadas a un uso más genérico:

- ✔ **La dirección de red** → Hace referencia a toda la red y define la red en la que se ubica un host.
- ✔ **La dirección Broadcast** → Representa la última dirección de una red.
- ✔ **La dirección Gateway** → Es la dirección por convenido que se le asigna al router de la red.

Para conocer la IP de estas dos direcciones anteriores haremos lo siguiente:

La dirección de red.

Colocaremos toda la parte de host de una dirección IP a cero

Ejemplo: Tenemos la siguiente IP → 115.10.15.25

Vemos que pertenece a la clase A, ponemos la parte del host a 0.

Sabemos que la clase A sigue el siguiente formato:

Clase A	rr	hh	hh	hh
En decimal	115	0	0	0
En binario	01110011	00000000	00000000	00000000

La dirección de red sería 115.0.0.0

La dirección de broadcast.

Colocamos toda la parte de host de una dirección IP a 1

Ejemplo: Tenemos la siguiente IP → 115.10.15.25

Vemos que pertenece a la clase A, ponemos la parte del host a 1.

Sabemos que la clase A sigue el siguiente formato:

Clase A	r	h	h	h
En decimal	115	255	255	255
En binario	01110011	11111111	11111111	11111111

La dirección de broadcast sería → 115.255.255.255

La dirección de Gateway o puerta de enlace.

Es la dirección por convenido que se le asigna al router de la red.

Puede ser cualquier dirección perteneciente a la red, pero se suele coger como dirección de Gateway la primer IP disponible.

Ejemplo: Tenemos la siguiente IP → 115.10.15.25

Una vez que conocemos la IP de la red 115.0.0.0, la primera IP disponible sería:

Clase A	r	h	h	h
En decimal	115	0	0	1
En binario	01110011	00000000	00000000	00000001

Direcciones IP especiales.

La dirección 127.0.0.0 se conoce como ***loopback address*** o simplemente ***loopback*** y define al dispositivo en el que uno se encuentra. Es decir, todos los dispositivos la usan para identificarse a sí mismos.

En principio solo se utiliza 127.0.0.0, pero todas las direcciones dentro del rango 127.x.x.x sirven para el mismo propósito.

Una IP dentro de ese rango no será una IP válida para un nodo de red.

4. Comandos

El comando ipconfig

Mostrará un listado con los datos de tu conexión de red.

Localiza en el listado la tarjeta de red que estás utilizando y fíjate en la entrada Dirección IPv4 que te indicará la IP asignada a ese equipo.

El comando ping

Funciones

Verificación de los protocolos TCP/IP

➔ La ejecución de **ping localhost (o ping 127.0.0.1)** permite verificar si el conjunto de protocolos TCP/IP está correctamente instalado y en funcionamiento. Es enviado y respondido internamente por el propio equipo.

➔ Verificación del adaptador de red

Si ejecutamos ping sobre la Ip de nuestro equipo, por ejemplo **ping 192.168.1.100 (IP del propio equipo)**, el comando es enviado a la red y recibido por el propio equipo, el cual envía la respuesta a la red y la recoge de ella. Esto permite verificar si la tarjeta de red está funcionando adecuadamente.

➔ Verificación de la red local.

Si ejecutamos ping 192.168.1.101 (**IP de un equipo próximo)** podremos verificar si el cableado del equipo hacia la red (o si el adaptador inalámbrico) funciona correctamente.

Si ejecutamos ping 192.168.1.1 (**IP de la puerta de enlace)** podremos verificar si el cableado general de la red funciona correctamente. las ip y puertas de enlace pueden variar en otras redes.

➔ Verificación de la conexión a Internet

Si ejecutamos ping 208.80.154.225 (IP de Wikipedia) podremos verificar si la conexión a Internet está funcionando.

➔ Verificación de lo servidores DNS

Si ejecutamos ping es.wikipedia.org (o cualquier otra URL conocida) podremos verificar si están correctamente configuradas las IP de los servidores DNS.

Estas sencillas acciones permiten la detección específica de errores en muy poco tiempo.