UD5. Capa de red

Módulo: Planificación y administración de redes

Unión Europea
Fondo Social Europeo
El FSE invierte en tu futuro

Germán Gascón Grau
g.gascongrau@edu.gva.es

Contenidos

- IPv4
  - Subnetting
  - CIDR
  - VLSM
  - Configuración de red
  - Protocolos de enrutamiento
- Otros protocolos de capa de red
- IPv6

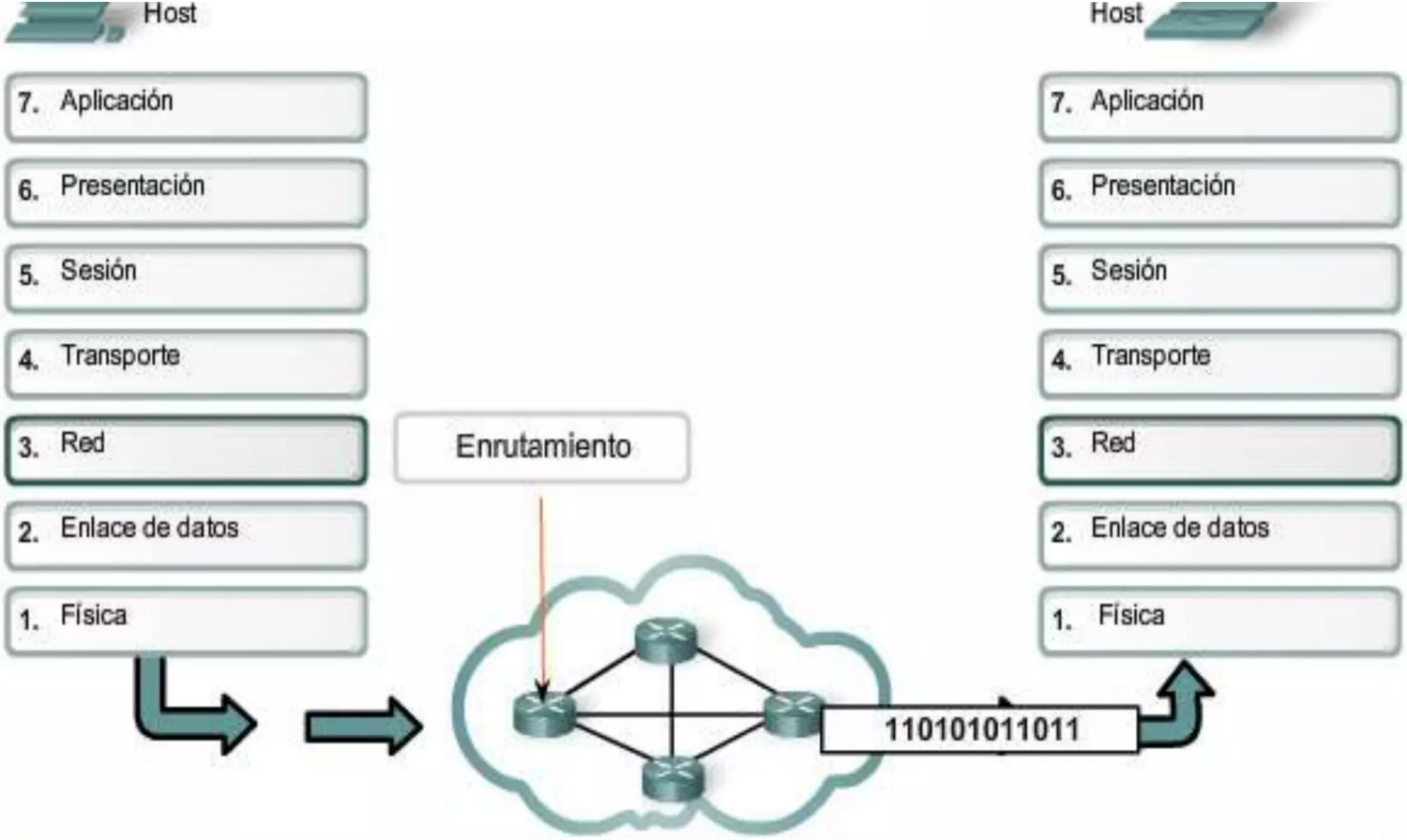
Introducción

En lo que va de curso hemos estudiado como se prepara la instalación de una red de área local, con todo el cableado y la instalación de todos los dispositivos físicos necesarios.

En esta unidad aprenderemos a configurar dichos dispositivos para que todo funcione correctamente. Para ello, tendremos que saber configurar una serie de parámetros en cada uno de los equipos que forman parte de la red. Dichos parámetros tendrán que seguir unas normas determinadas para que los equipos se reconozcan entre sí y puedan comunicarse.

Introducción

La **capa de red** es la tercera capa del modelo de referencia OSI.



Capa de red

La misión fundamental de la capa 3 es **conseguir que los datos lleguen desde el origen al destino** aunque estos se encuentren en redes diferentes y no tengan conexión directa. Dicho de otro modo, selecciona una ruta entre 2 equipos aunque se encuentren en redes geográficamente distintas.

La capa de red ofrece **servicios a la capa de nivel superior**, el nivel de transporte, y utiliza los servicios de la capa de nivel inferior, la capa de enlace de datos.

Procedimientos básicos de la capa de red

- **Direccionamiento**: la capa de red nos da un método para direccionar los distintos equipos, es decir, poder identificarlos de cierta manera con una dirección única.

- **Encapsulamiento**: Cuando se quiere enviar un mensaje a través de la red, el mensaje se genera en la capa de aplicación del host origen. Ese mensaje se va transformando a través de las distintas capas hacia abajo añadiéndole información en cada una de las capas. En concreto, en la capa tres se añaden, entre otras cosas: la dirección del host destino y la dirección del host origen. A este conjunto de información se denomina **paquete**.

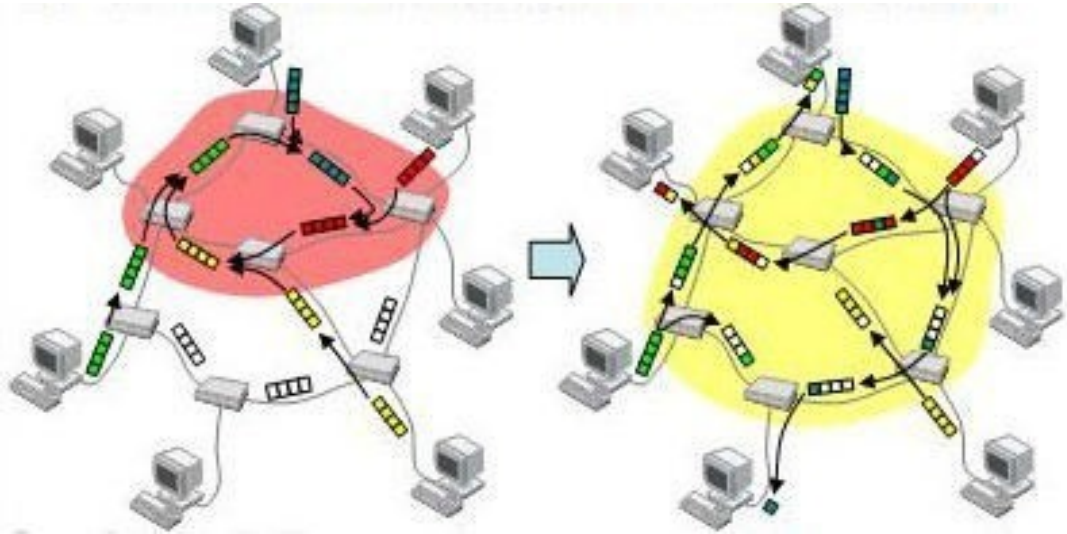
Procedimientos básicos de la capa de red

- **Desencapsulamiento**: Cuando el paquete llega al destino hay que procesarlo en la capa 3 del host destino. Se examina la dirección destino para verificar que el paquete fue direccionado a ese dispositivo. Si es correcto, el paquete se desencapsula por la capa de red, es decir, se retira la información añadida en la capa tres del host origen, y el resultado se envía a las capas superiores para que llegue al usuario.

- **Enrutamiento**: La capa de red provee los servicios para dirigir los paquetes a su host destino. Puede que el origen y el destino estén en redes diferentes y que el paquete pueda recorrer muchas redes diferentes. Los routers tienen la función de ir encaminando el paquete para que llegue al destino final.

Procedimientos básicos de la capa de red

- **Control de la congestión**: Cuando una red recibe más tráfico del que se puede procesar se puede producir una congestión. El problema de la congestión en un nodo es que tiende a extenderse por toda la red pudiendo llegar a bloquearla por completo. Existen técnicas de gestión y prevención de congestiones que se aplican en la capa 3.



Tipos de servicios ofrecidos por la capa de red

- Servicios **orientados a la conexión**: es aquel en el que primero se establece la conexión, luego se usa y finalmente se deshabilita (como por ejemplo el sistema telefónico). En estos servicios se mantiene el **orden de emisión**.

- Servicios **no orientados a la conexión**: Cada paquete debe llevar la dirección destino y cada uno de los nodos de la red decide el camino de cada paquete, pudiendo ser este camino diferente para dos paquetes de la misma comunicación. Los paquetes **pueden llegar al destino de forma desordenada**. Los dispositivos encargados de dar este servicio son los routers.

Protocolo IP

- **IP** (Internet Protocol). Es el protocolo de nivel de red más utilizado en el planeta.
- Protocolo **sin conexión** y **no fiable**.
- Ofrece servicio "**mejor ruta posible**" según la información que tenga cada router, pero **sin garantías**.
- Proporciona un **sistema de direcciones** para que cada nodo de la red quede indentificado por una **dirección IP**.
- El bloque de datos en este nivel se denomina **paquete** según OSI.
- Actualmente existen **2 versiones**:
  - IPv4
  - IPv6

Protocolo IPv4

La dirección IPv4 está formada por **32 bits**, divididos en 4 octetos (4*8 = 32).

Cada uno de esos octetos puede representar **256 combinaciones** posibles, y por tanto la dirección IP está formato por cuatro números enteros en el intervalo [**0 – 255**] separados por puntos.

Una dirección de IP fija podría tener el siguiente aspecto:

`11000101101010010101111001010010`

Dirección IP dividida en cuatro piezas de ocho bits (en bytes):

`11000101  10101001  01011110  01010010`

Cada byte lo representamos en decimal separado por puntos

`197.169.94.82`

Protocolo IPv4

- En un principio podríamos pensar que la cantidad de direcciones IP disponibles es de 2^{32} = 4 GB, pero como veremos en las siguientes diapositivas, no es así. No se pueden utilizar todas las direcciones disponibles hay algunas que están reservadas para el propio funcionamiento y organización del protocolo.

- No confundir la dirección IP, también conocida como dirección lógica, con la dirección MAC, conocida como dirección física.

Cabecera paquete IPv4

0-3	4-7	8-15	16-18	19-31
Versión	Tamaño Cabecera	Tipo de servicio	Longitud Total	
Identificador			Flags	Posición de fragmento
Time to Live		Protocolo	Suma de control de cabecera	
Dirección IP Origen				
Dirección IP Destino				
Opciones				Relleno

Cabecera paquete IPv4

- **Versión**: 4 bits. Siempre vale 0100
- **Tamaño cabecera**: 4 bits. Valor en palabras de 32 bits. Mínimo es 5 (5x32) y el máximo 15 (15x32).
- **Tipo de servicio**: 8 bits. Indica una serie de parámetros sobre la calidad de servicio deseada durante el tránsito por una red. No asegura el cumplimiento del tipo de servicio.
- **Longitud total**: 16 bits. Tamaño total en octetos del paquete (incluyendo cabecera y datos).
- **Identificador**: 16 bits. Identifica de forma única al paquete en caso que tenga que ser fragmentado.
- **Flags**: 3 bits. Se utiliza para la fragmentación de paquetes.
  - El bit 0 está reservado.
  - El bit 1. **DF** (Don’t Fragment). Si es 1 el paquete no puede fragmentarse.
  - El bit 2. **MF** (More Fragments). Si es 0 indica que es el último fragmento. Si es 1 indica que quedan más fragmentos.

Cabecera paquete IPv4

- **Posición de fragmento**: 13 bits. En paquetes fragmentados indica la posición, en unidades de 64 bits, que ocupa el paquete actual dentro del datagrama original. El primer paquete de una serie de fragmentos contendrá en este campo el valor 0.

- Tiempo de vida (**TTL**): 8 bits. Indica el máximo número de enrutadores que un paquete puede atravesar. En cada salto este valor es decrementado. Al llegar a 0 el paquete es destruido.

- **Protocolo**: 8 bits. Indica el protocolo de siguiente nivel utilizado en la parte de datos del datagrama. El valor más común es 0x06 que indica que utiliza TCP. Otros valores 0x01 ICMP, 0x17 UDP, etc.

- **Suma de control de cabecera**: 16 bits. Suma de Contol de cabecera. Se recalcula cada vez que algún nodo cambia alguno de sus campos (por ejemplo, el Tiempo de Vida).

- **Dirección IP origen**: 32 bits. La dirección IP del nodo que ha generado el datagrama.

- **Dirección IP destino**: 32 bits. La dirección IP del nodo al que van destinados los datos.

- **Opciones**: Nº bits variable. Es un campo opcional pero en caso de existir debe ser interpretado.

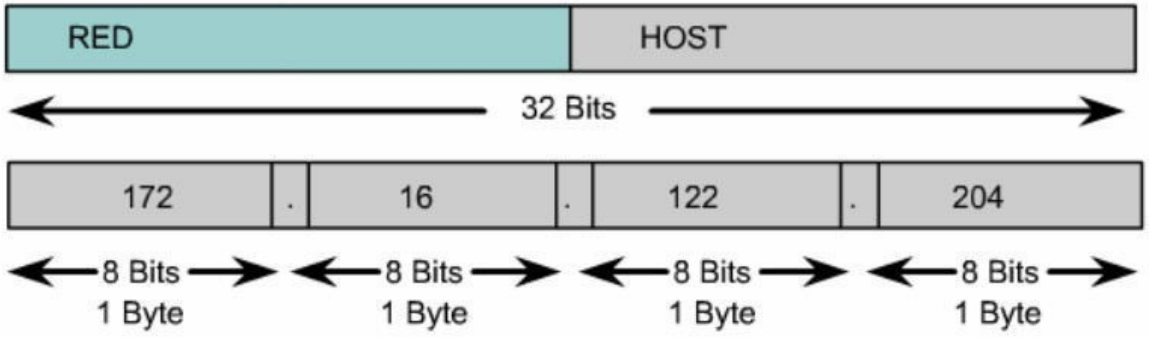
- **Relleno**: Nº bits variable. Es un campo opcional utilizado para asegurar que la cabecera es **múltiplo de 32**. Se rellena con ceros.

Parte de red y parte de equipo

Cuando un paquete llega a un router, este separa la dirección IP de destino en **dos partes** en las que se codifican elementos diferentes:

- Una parte identifica la red hacia la que va el paquete
- La otra, identifica el equipo (host).

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



Direcciones de red y de difusión

De todas las combinaciones de bits posibles que existen para la parte de la dirección IP de los equipos **dos** de ellas **están reservadas** y no las podemos utilizar para identificar equipos de la red.

- La primera de las direcciones reservadas es aquella que tiene todos los **bits a 0 para la parte que identifica los equipos**. Esta dirección se utiliza **para identificar la red**.
- La otra dirección reservada es es aquella que tiene todos los **bits a 1 para la parte que identifica los equipos**. Esta dirección se utiliza para identificar la dirección de **broadcast** de la red que se utiliza cuando queremos enviar un paquete a todos los equipos de la red.

Clases IPv4

- Las direcciones IP se dividen en 5 clases (A, B, C, D, E) pero sólo las 3 primeras pueden ser asignadas por la Internet Corporation for Assigned Names and Numbers (ICANN).
- Las direcciones IP de clase **D** se utilizan para **multidifusiones**.
- Las direcciones IP de clase **E** están **reservadas** y no se utilizan.

Clase A	Red	Host		
Octet	1	2	3	4

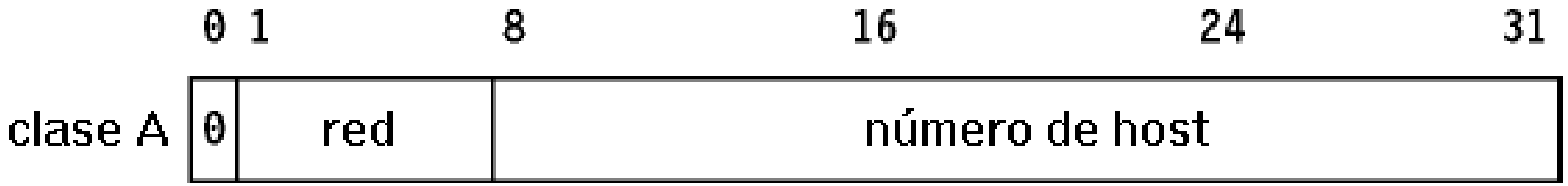
Clase B	Red		Host	
Octet	1	2	3	4

Clase C	Red			Host
Octet	1	2	3	4

Clase D	Host			
Octet	1	2	3	4

Direcciones IPv4 Clase A

Las direcciones de Clase A se diseñaron para admitir redes de tamaño extremadamente grande.



Rango [**1.0.0.0 – 126.255.255.255**]

Las direcciones **127.x.x.x** están **reservadas** para loopback.

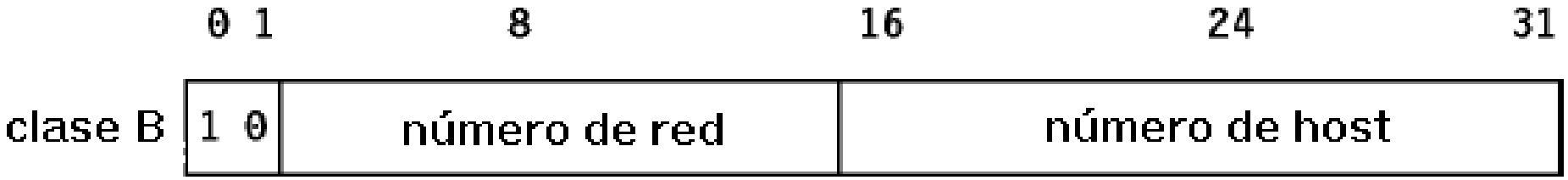
En una red de clase A, el primer bit de la dirección es 0.

Los **7 bits** siguientes **identifican la red**, de modo que la cantidad de subredes posibles es 27 - 2 (restamos 2 porque las direcciones todo a 0's y todo a 1's están reservadas), es decir tenemos 126 subredes posibles (de 1 a 126).

Los tres últimos octetos (24 bits) están reservados para que sean asignados a los hosts, de modo que la cantidad máxima de hosts es 2^{24} - 2 (las direcciones reservadas de broadcast [últimos octetos a 255] y de red [últimos octetos a 0]), es decir, **16.777.214 hosts**.

Direcciones IPv4 Clase B

Las direcciones de Clase B se diseñaron para admitir redes de tamaño moderado a grande.



Rango [**128.0.0.0 – 191.255.255.255**]

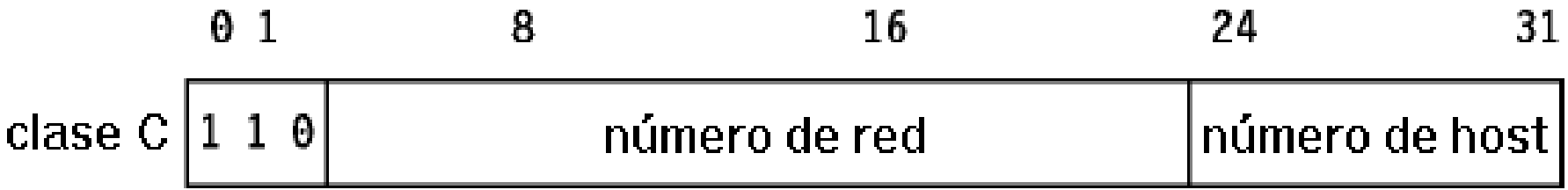
En una red de clase B, los primeros 2 bits de la dirección son 10.

Los **14 bits** siguientes identifican la red, de modo que la cantidad de subredes posibles es 2^{14} es decir, **16.384 subredes posibles**.

Los dos últimos octectos (16 bits) son destinados para hosts, de modo que la cantidad máxima de hosts posibles, por cada subred, es de 2^{16} - 2 (las direcciones reservadas de broadcast [últimos octetos a 255] y de red [últimos octetos a 0]) es decir, **65.534 hosts** distintos.

Direcciones IPv4 Clase C

Las direcciones de Clase C se diseñaron para admitir redes de tamaño pequeño.



Rango [**192.0.0.0 – 223.255.255.255**]

En una red de clase C, los **primeros 3 bits** de la dirección son **110**.

Los **21 bits siguientes identifican la red**, de modo que la cantidad de subredes posibles es 2^{21} es decir, 2.097.152 subredes posibles.

El último octecto (8 bits) es destinado para hosts, de modo que la cantidad máxima de hosts posibles, por cada subred, es de 2^8 - 2 (las direcciones reservadas de broadcast [últimos octetos a 255] y de red [últimos octetos a 0]) es decir, **254 hosts distintos**.

Direcciones IPv4 Clase D

La direcciones de Clase D se crearon para permitir multicast. Una dirección multicast es una dirección exclusiva de red que dirige los paquetes con esa dirección destino hacia grupos predefinidos de direcciones IP. Por lo tanto, una sola estación puede transmitir de forma simultánea una sola corriente de datos a múltiples receptores.

clase D	1 1 1 0	dirección multicast

Rango [**224.0.0.0 – 239.255.255.255**]

Los primeros cuatro bits de una dirección Clase D deben son **1110**.

Por lo tanto, el rango del primer octeto para las direcciones Clase D es de 11100000 a 11101111, o 224 a 239.

Direcciones IPv4 Clase E

El rango de direcciones de clase E está reservado por la IETF (Internet Engineering Task Force) para realizar investigaciones. Por lo tanto, no se han emitido direcciones Clase E para ser utilizadas en Internet.

clase E	1 1 1 1	reservado

Emplea 8 bits para la dirección de red y los 24 bits restantes para identificar a los equipos de la red.

Los primeros cuatro bits de una dirección Clase E siempre son 1s. Por lo tanto, el rango del primer octeto para las direcciones Clase E es 11110000 a 11111111, o 240 a 255.

Direcciones especiales

- Rango [**0.0.0.0** hasta **0.255.255.255**]

  Este rango de direcciones no puede asignarse como dirección IP a un equipo, ya que indica el estado de un host que está a la espera de que se le asigne una dirección IP válida.

- [**127.0.0.0** hasta **127.255.255.255**]

  Este rango de direcciones está reservado para **loopback** y define al propio equipo. En la práctica la dirección asignada a **localhost** es **127.0.0.1** que sirve para que un equipo se comunique consigo mismo a través de la pila de red, sin usar la red física.

- [**169.254.0.0** hasta **169.254.255.255**]

  Este rango de direcciones está reservado para IPv4 link-local (**APIPA**) que permite que un equipo se autoconfigure una IP automáticamente cuando no puede obtenerla por DHCP, permitiendo comunicación solo en el enlace local.

Reparto de direcciones IP públicas

Las direcciones IP públicas son concedidas por la **IANA** (Internet Assigned Numbers Authority) a través de los **cinco Registros Regionales de Internet** (RIR) existentes:

- **RIPE NCC** para Europa, Oriente Medio
- **ARIN** para Norteamérica
- **APNIC** para Asia–Pacífico
- **LACNIC** para Latinoamérica y Caribe
- **AFRINIC** para África

Direcciones IP privadas

Con el crecimiento de Internet, se vio pronto que no había suficientes direcciones públicas para todos los dispositivos.

Para mitigar el problema, se definieron rangos de direcciones reservadas para uso interno (privadas), que:

- No se enrutan en Internet
- Pueden reutilizarse en infinitas redes
- No necesitan ser únicas globalmente

Estas direcciones se combinaron con **NAT** (Network Address Translation), que permite que:

- Muchos dispositivos con IP privada
- Compartan una sola IP pública

Rango de direcciones IP privadas

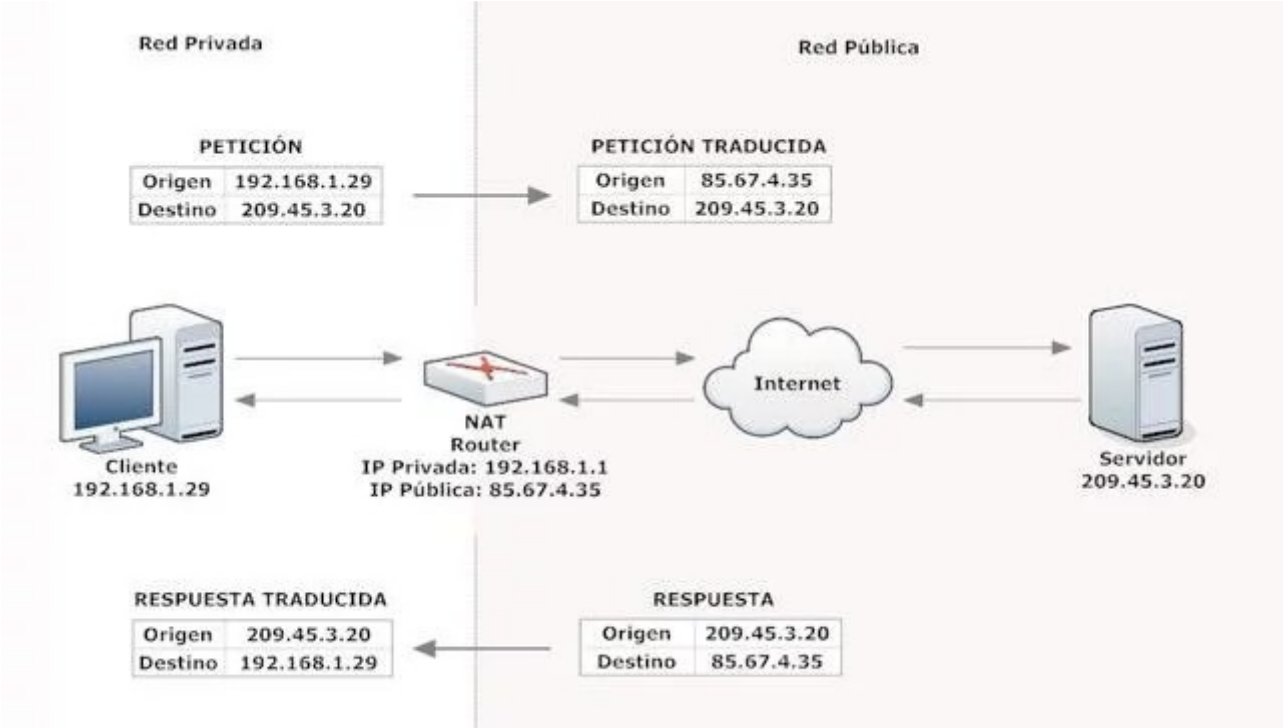
En el estándar IPv4 se reservaron tres bloques para uso privado, uno por cada clase:

- Clase A: **10.0.0.0** a **10.255.255.255** (8 bits red, 24 bits hosts)
- Clase B: **172.16.0.0** a **172.31.255.255** (12 bits red, 20 bits hosts)
- Clase C: **192.168.0.0** a **192.168.255.255** (24 bits red, 8 bits hosts)

Estos bloques están definidos en **RFC 1918**.

Funcionamiento de NAT

NAT reescribe las direcciones IP (y a menudo los puertos) de los paquetes para que una red privada pueda comunicarse con Internet usando IP públicas limitadas.



Funcionamiento de NAT

- Un host interno (ej: 192.168.1.29) envía un paquete a Internet.
- El router con NAT:
  - Cambia la IP origen privada por su IP pública (ej: 85.67.4.35)
  - Normalmente cambia el puerto origen (PAT).
- Guarda una entrada en su tabla NAT
  - mapeo IP:puerto interno , IP:puerto público
- Cuando llega la respuesta desde Internet:
  - Consulta la tabla.
  - Deshace la traducción y entrega el paquete al host correcto.

Tipos de NAT

- NAT **estático**
  - Mapeo 1:1 fijo entre IP privada y pública.
  - Útil para servidores internos accesibles desde fuera.
- NAT **dinámico**
  - Usa varias IP públicas y las asigna temporalmente (1:1) a equipos internos solo mientras dura la conexión.
  - Menos común hoy en día.
- **PAT** / NAT **Overload** (el más usado)
  - Muchos hosts internos salen con una sola IP pública.
  - Se distinguen por puertos TCP/UDP.
  - Es el NAT típico de casa.

Ventajas de las direcciones IP privadas

Además del ahorro de direcciones, las direcciones IP privadas aportaron:

- Aislamiento de redes internas
- Una capa extra de seguridad (no accesibles directamente)
- Mayor flexibilidad en el diseño de redes
- Simplificación del direccionamiento interno

Ejercicio

Dadas las siguientes direcciones IP, indica la clase a la que pertenecen y si son públicas o privadas:

- 21.33.54.21
- 10.21.22.23
- 128.8.4.1
- 192.168.0.1
- 225.22.1.2
- 223.21.11.1
- 172.30.221.1

Redes IP sin clase. La máscara de subred

Con el objetivo de frenar el agotamiento de Ipv4 y reducir el tamaño de las tablas de enrutamiento, en 1993 se creó **CIDR** (Classless Inter-Domain Routing), eliminando las rígidas clases A/B/C.

Con CIDR el tamaño de la red y el número de host, ya no viene predefinido por su clase, sino por la **máscara de subred** que consiste en un número de 32 bits con la **parte de red** colocada a **1** y la **parte de host** colocada a **0**.

Un ejemplo de máscara de subred sería:

`11111111 11111111 11111100 00000000`

En notación decimal punteada sería `255.255.252.0`

Notación CIDR

La notación **CIDR** escribe una red IP como dirección/prefijo, donde el prefijo indica **cuántos bits son de red** (están a 1 en la máscara de subred)

Ejemplo:

192.168.1.0/24

- 24 bits para red
- 8 bits restantes para host

La máscara de subred

Los dispositivos de red realizan una operación **AND** entre la **dirección IP** y la **máscara** para obtener la **dirección de red** a la que pertenece el host identificado por la dirección IP dada.

Dirección red = IP AND máscara

Los dispositivos de red realizan un **OR** entre la **dirección IP** y la **negación de la máscara** (NOT máscara) para obtener la **dirección de difusión** que le corresponde al host identificado por la dirección IP dada.

Dirección difusión = IP OR NOT máscara

Ejercicio

Obtener la dirección de red y de difusión de las siguientes direcciones:

- 192.168.10.5/24
- 10.0.0.2/8
- 130.34.121.112/16
- 140.23.43.1/17
- 190.34.121.3/25
- 172.16.0.3/18
- 10.0.0.5/10

Direcciones IPv4 asignables a hosts

A la hora de saber si una dirección de red es asignable a un equipo o host para configurarlo en una red hemos de tener en cuenta:

- Debe tener 32 bits
- No puede ser de red o de difusión
- No puede ser ninguna de las reservadas

Ejercicio

Indica el motivo por el que las siguientes direcciones IPv4 no pueden ser asignadas a un host:

- 123.257.23.33/16
- 224.35.22.11/24
- 195.233.43.0/24
- 0.0.0.1/8
- 175.23.255.255/16
- 127.0.1.1/8

Subredes y superredes

Una consecuencia de CIDR es que mediante la máscara de subred podemos modificar los bits destinados a la red y los destinados a los host.

El **subnetting** utiliza bits de la parte de host para asignárselos a la parte de red y así conseguir que los routers dentro de una misma organización puedan definir diferentes subredes en el conjunto de la red.

El **supernetting** utiliza bits de la parte de red para asignárselos a los hosts. Esta técnica no es muy utilizada.

Ejercicio

Imaginemos que en una red con dirección 199.134.3.0/24 queremos montar 5 subredes.

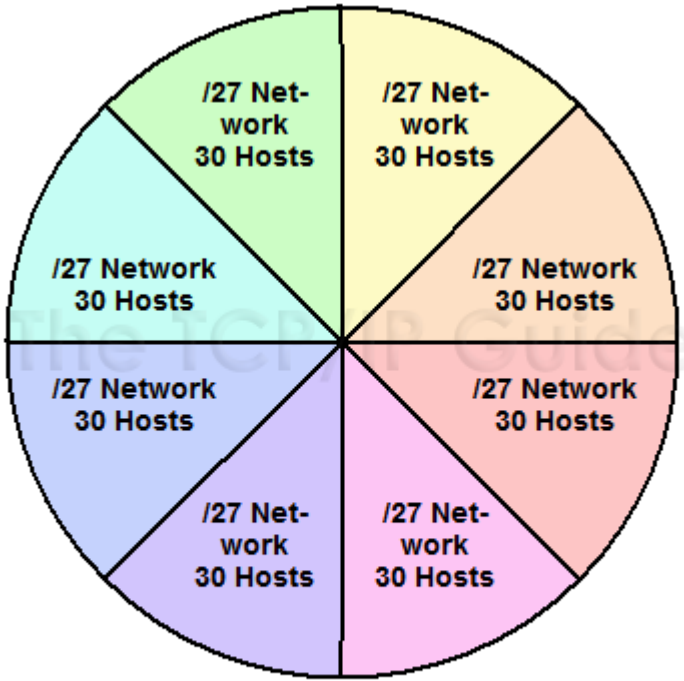
- ¿Cuantos bits le tenemos que quitar a la parte de host para crearlas?
- ¿De cuantos bits será nuestra máscara de red?
- ¿Cuál sería el valor de la máscara en formato decimal punteado y en notación CIDR?
- ¿Cuantos hosts como máximo podremos conectar a cada una de las subredes?
- ¿Cuáles serían las direcciones de red y de difusión de las 5 subredes?
- Si a un router de esta organización le llega la dirección IP 199.134.3.72 ¿a qué subred pertenece?

VLSM

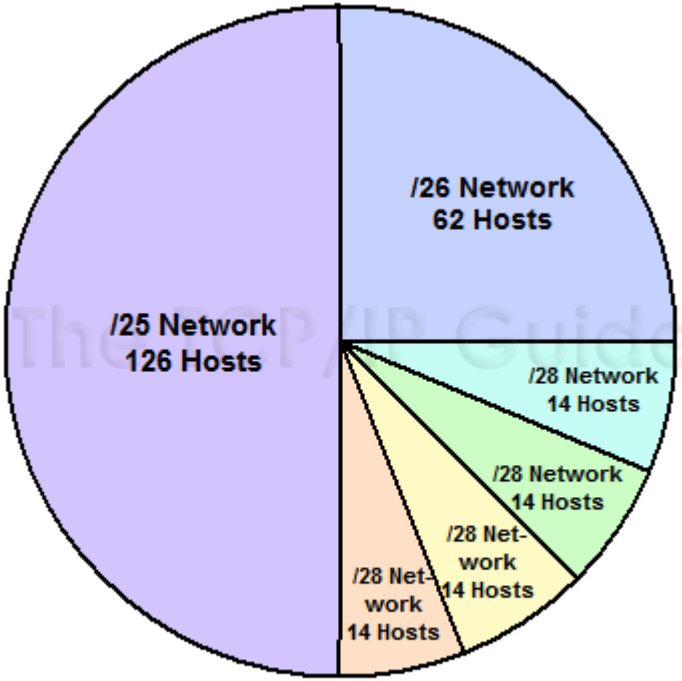
VLSM (Variable Length Subnet Mask) o Máscaras de Subred de Longitud Variable,es una solución de Subnetting (Dentro de la norma CIDR) que favorece el **aprovechamiento de direcciones ip** al máximo pues se utiliza cuando se desea dividir una red en **subredes de distintos tamaños**.

- Permite ajustar las subredes y su cantidad de hosts más eficientemente.
- Facilita el uso de redes contiguas.

Subnetting vs VLSM



Class C (/24) Network (254 Hosts)



Class C (/24) Network (254 Hosts)

Ejemplo de VLSM

Nos han dado la dirección **10.5.126.0/23** y deseamos crear las siguientes subredes:

- RED A : 130 equipos (+1 de red + 1 de broadcast)
- RED B: 70 equipos (+1 de red + 1 de broadcast)
- RED C: 40 equipos (+1 de red + 1 de broadcast)
- RED D: 10 equipos (+1 de red + 1 de broadcast)

Ejemplo de VLSM

Análisis Previo

Partimos de 10.5.126.0 /23 y descomponemos los 2 últimos octetos en binario :

```
Binario:    01111110.00000000 /23

Decimal:          126.0
```

El prefijo de red /23 significa que la red utiliza 23 bits, y por tanto, nos quedan (32 totales - 23 de la dirección de red) **9 bits para hosts**.

Hemos de **ordenar las redes de mayor a menor tamaño**. En nuestro caso ya está.

Ejemplo de VLSM

Desarrollo

RED A (132)

Primero debemos averiguar cuántos bits de host necesitamos para conseguir 132 hosts. Necesitamos **8 bits** (2^8 = 256), así que tendremos un prefijo /24.

Así que la parte de red le robará un bit a la parte de hosts actual, y por tanto vamos a utilizar 8 bits para los hosts

```
                    126.0
                01111110.00000000
Su broadcast será   01111110.11111111
```

La dirección de la Red A será la **10.5.126.0/24**

y su broadcast será la dirección **10.5.126.255/24**

Ejemplo de VLSM

Desarrollo

RED B (72)

Para esta red necesitaremos 72 hosts.

2^7 = 128 . Así que vamos a utilizar **7 bits para hosts**, lo que significa que el prefijo de esta red será **/25**

Partimos de la **última dirección de la red anterior** (sabemos que el broadcast de la red anterior es `10.5.126.255`) y obtendremos:

La dirección de la RED B será **10.5.127.0/25**

y su Broadcast será el **10.5.127.127/25**

Ejemplo de VLSM

Desarrollo

RED C (42)

La siguiente red será la `10.5.127.128`

Sabemos que necesitamos 42 host. Si 2^6=64, tendremos que utilizar **6**

bits. Prefijo **/26**

La dirección de la Red C será **10.5.127.128/26**

y su Broadcast será **10.5.127.191/26**

Ejemplo de VLSM

Desarrollo

RED D (12)

La última red necesitará 12 Hosts. Partimos de `10.5.127.192`

Veamos cuántos bits necesitamos: 2^**4** = 16

Así que sabemos que **necesitamos 4 bits**, y por tanto nuestro prefijo de red será **/28**

La red RED D será la **10.5.127.192/28**

con broadcast **10.5.127.207/28**

Protocolos de la capa de red

El principal protocolo de la capa de red es IP, pero también existen otros protocolos como:

- ARP
- RARP
- ICMP

Protocolo ARP

Estrictamente hablando, ARP es un protocolo de capa 2 que se situa entre la capa 2 y la capa 3 del modelo OSI.

Los switches y puentes trabajan con direcciones físicas (MAC) pero las aplicaciones emiten peticiones basadas en direcciones lógicas (direcciones IP) y por tanto se requiere de un mecanismo de traducción entre dirección IP y dirección MAC que precisamente es de lo que se encarga ARP.

Funcionamiento del protocolo ARP

Cuando un host quiere transmitir un paquete IP necesita averiguar la dirección MAC del host destinatario cuya dirección es la dirección de destino del campo “dirección IP destino” del paquete IP.

Para ello genera una **difusión** en toda la red preguntando **¿quién tiene la dirección IP x.x.x.x ?**

```
Ejemplo: who is 192.168.0.3?
```

Todos los nodos detectan esta trama de difusión pero sólo responderá el host que tiene dicha dirección IP indicando en la **respuesta su dirección MAC**.

```
Ejemplo: 192.168.0.3 is 52:54:00:ef:dc:63
```

El host emisor **guardará la relación IP → MAC** en memoria durante un corto intervalo de tiempo (variable en función del SO) ahorrarse tener que hacer de nuevo una difusión en futuras transmisiones hacia ese host.

Funcionamiento del protocolo ARP

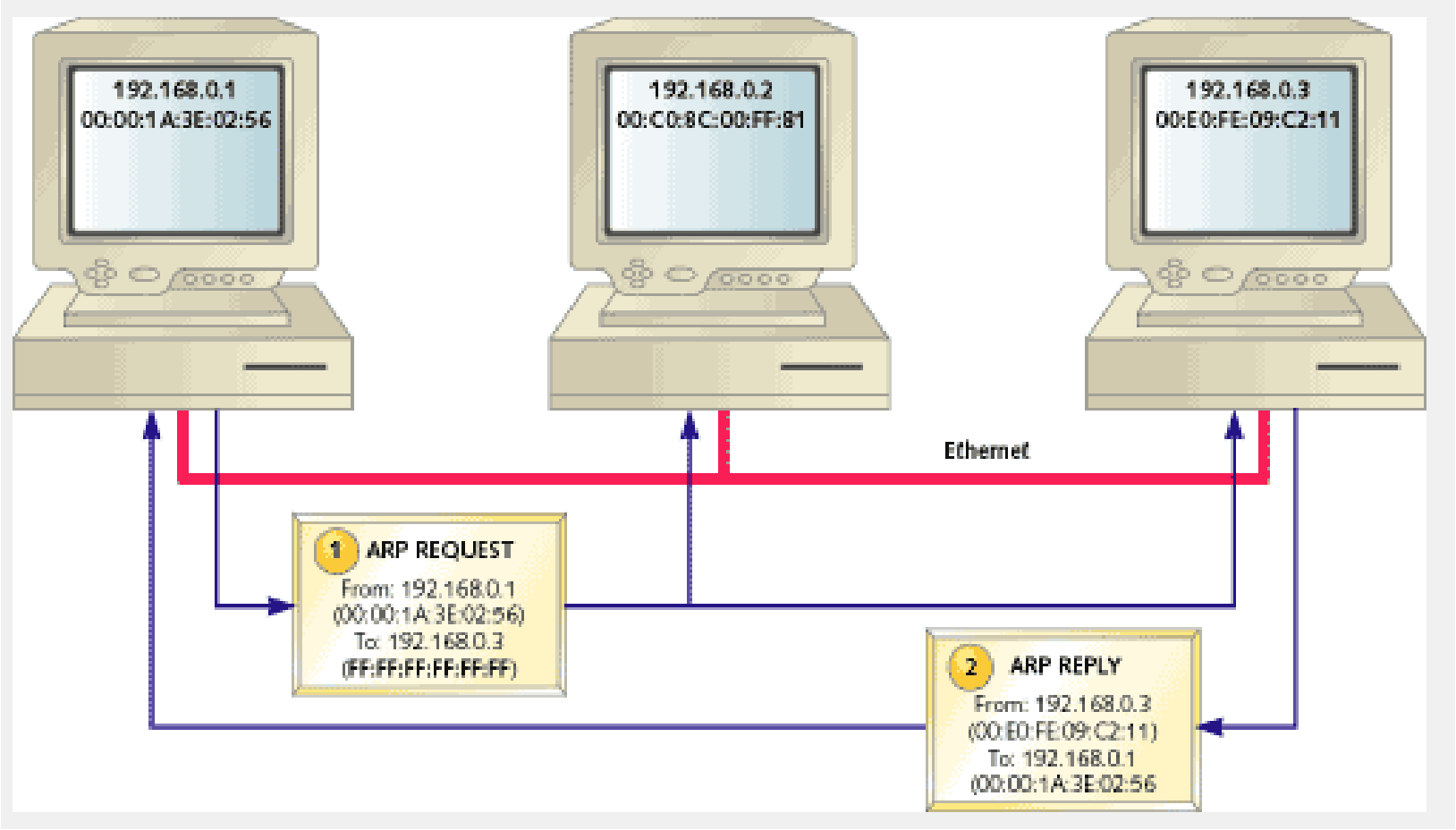


Tabla ARP

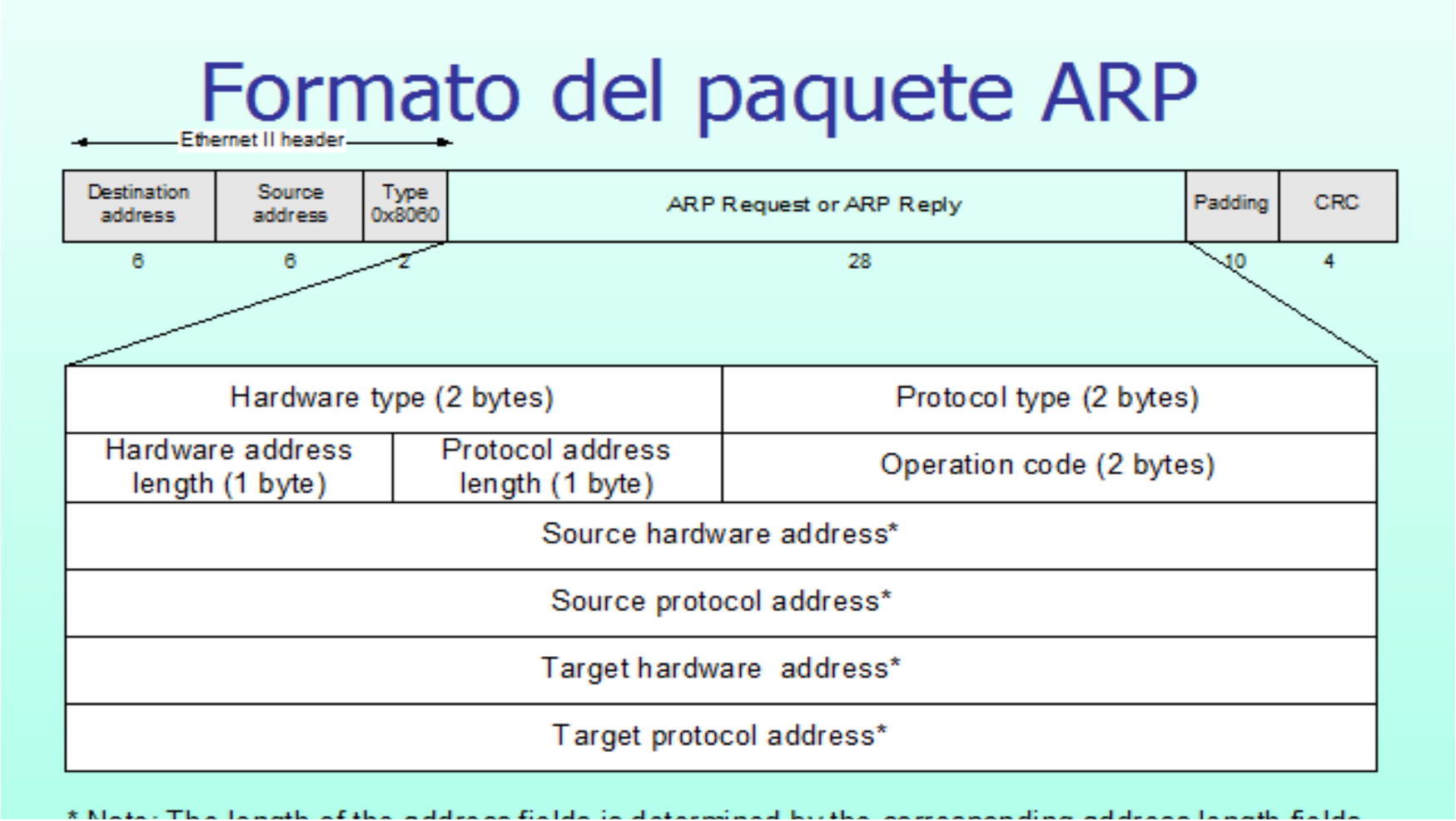
El sistema operativo de los equipos guarda en memoria cache un tabla llamada **tabla ARP** o tabla de búsqueda en la que en cada entrada hay correspondencias entre direcciones IP y direcciones MAC.

Cada una de estas entradas se guarda durante un periodo de tiempo corto ya que los equipos puede cambiar tanto sus direcciones IP como sus direcciones físicas (MAC).

```
C:\Documents and Settings\EPS>arp -a

Interfaz: 172.20.43.208 --- 0x2
  Dirección IP          Dirección física      Tipo
  172.20.43.206         00-0a-5e-76-8a-7e     dinámico
  172.20.43.207         00-0a-5e-76-ff-a6     dinámico
  172.20.43.211         00-0a-5e-76-ff-bc     dinámico
  172.20.43.219         00-0a-5e-76-ff-b8     dinámico
```

Formato trama ARP



Trama ARP

- **Tipo de hardware**: Especifica el tipo de hardware. Por ejemplo, Ethernet.
- **Tipo de protocolo**: Especifica el tipo de protocolo, de la misma manera que el campo Ethertype en la cabecera IEEE 802 (0x0800 para Ipv4; 0x0806 para ARP).
- **Longitud de la dirección hardware**. Especifica la longitud en bytes de la direcciones hardware incluidas en el datagrama. Para IEEE 802.3 es 6.
- **Longitud de la dirección de protocolo**. Especifica la longitud en bytes de la dirección de protocolo en el datagrama. Para IP es 4.
- **Código de operación**. Especifica si el datagrama es una solicitud ARP (1) o una respuesta ARP (2).
- **Dirección hardware del emisor/receptor**. Contiene la dirección hardware del dispositivo emisor/receptor. Para IEEE 802.3 son direcciones de 48 bit.
- **Dirección IP del emisor/receptor**. Contiene las direcciones IP del emisor/receptor. Son direcciones de 32 bit.

Protocolo RARP

RARP era el equivalente inverso a ARP, es decir, permitía obtener la dirección IP a partir de una dirección MAC.

Fue sustituido inicialmente por **BOOTP** y posteriormente por DHCP.

Protocolo ICMP

El Protocolo **ICMP** o Protocolo de Mensajes de Control de Internet (por sus siglas en inglés de Internet Control Message Protocol) es un protocolo de capa de red que permite **administrar información de control y notificación de errores** de los equipos de la red.

Se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado.

ICMP se encarga de manejar lo errores ocasionales que se pueden dar en IP.

Normalmente los paquetes ICMP son generados por los routers y el destinatario suele ser el usuario, por ejemplo, cuando intentas acceder a una IP que no existe, normalmente se te notificará por medio de un mensaje ICMP.

Protocolo ICMP

ICMP se puede utilizar también para **diagnosticar la conectividad**, en ese caso es el usuario el que genera los paquetes ICMP.

1. El usuario envía un mensaje llamado echo request (solicitud de eco) esperando recibir un mensaje echo reply (respuesta de eco)

2. Si no se recibe esta respuesta, se supone que no hay conexión a nivel de red entre los equipos

La herramienta PING

La ejecución del comando ping en Windows tiene el siguiente aspecto:

```
C:\>ping 127.16.1.2 ❶

Haciendo ping a 127.16.1.2 con 32 bytes de datos:

❷Respuesta desde 127.16.1.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 127.16.1.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 127.16.1.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 127.16.1.2: bytes=32 tiempo<1m TTL=128

❸Estadísticas de ping para 127.16.1.2 ❺
    Paquetes: enviados ❹ = 4, recibidos = 4, perdidos ❻ = 0
    (0% perdidos),
❼Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\>
```

La herramienta PING

El significado de cada uno de los elementos de la imagen es:

1) **Dirección de destino**, configurada en la dirección IP para la computadora local.

2) **Información de respuesta**:

- bytes: tamaño del paquete ICMP.
- tiempo: tiempo transcurrido entre la transmisión y la respuesta.
- TTL: valor TTL predeterminado del dispositivo DESTINATION, menos la cantidad de routers en la ruta. El valor TTL máximo es 255

3) **Resumen de información sobre las respuestas**

4) **Paquetes enviados**: cantidad de paquetes transmitidos.

5) **Paquetes recibidos**: cantidad de paquetes recibidos.

6) **Paquetes perdidos**: diferencia entre la cantidad de paquetes enviados y recibidos.

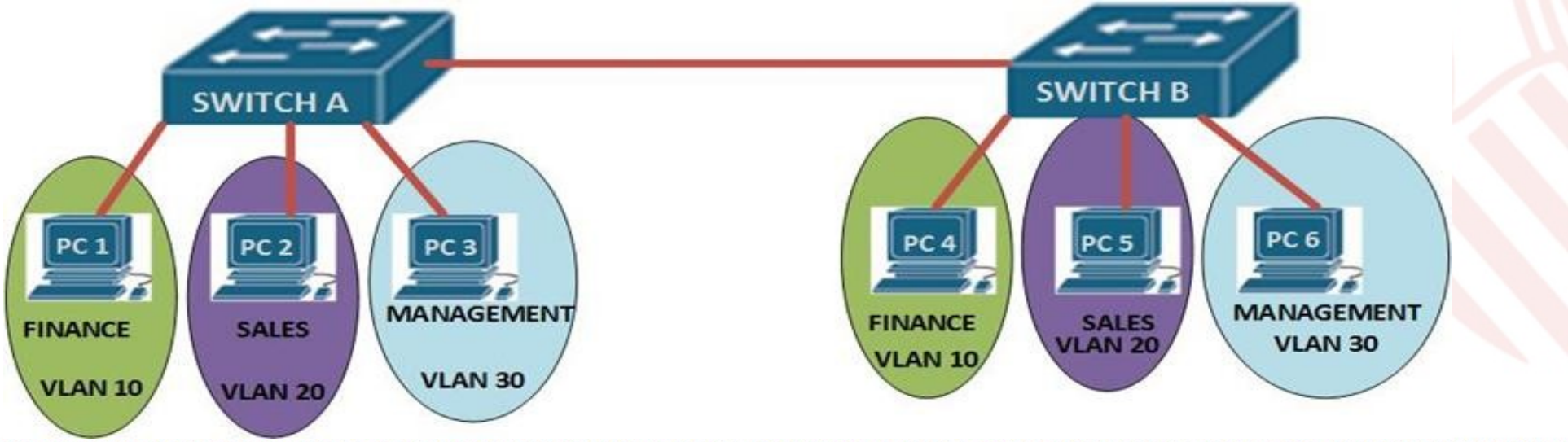
7) **Información sobre la demora de respuestas**, medida en milisegundos.

VLANs
Redes de Área Local Virtuales

¿Qué es una VLAN?

Una VLAN es una **red lógica** de capa 2 (OSI) dentro de una infraestructura de switching.

Cada VLAN suele equivaler a un **dominio de broadcast distinto**: los broadcasts de una VLAN no pasan a otra VLAN.



Ventajas de las VLANs

- **Segmentación**: separar grupos (Administración, Alumnos, Invitados, IoT…).
- **Seguridad**: limitar quién “ve” a quién por capa 2; reduces superficie de ataque y errores.
- **Orden y gestión**: el cableado puede ser el mismo, pero la red se organiza por VLANs.
- **Rendimiento**: menos broadcast “basura” por cada segmento.
- **Flexibilidad**: si un usuario cambia de sitio, puedes cambiar su puerto de VLAN sin rehacer cableado.

VLANs vs Redes físicas

Supongamos el siguiente escenario:

- Centro educativo con **3 subredes**: Administración, Alumnos y Profesores.
- 60 puestos distribuidos en varias aulas/despachos.
- Se necesita que no compartan la misma red y que haya control de acceso entre grupos.

VLANs vs Redes físicas

Dividir en **redes físicas** implica:

- Montar redes distintas físicamente: switches separados o infraestructura duplicada.
  - Más switches (uno por red o al menos por zona y red)
  - Más cableado (tiradas duplicadas o patching más complejo)
  - Más puertos uplink hacia router/firewall (o más routers)

VLANs vs Redes físicas

Dividir en **redes físicas** implica:

- Coste económico mayor
- Mayor coste de tiempo
- Dificulta el mantenimiento

Queremos el **diseño de red más simple** que cumpla con los objetivos marcados.

VLANs vs Redes físicas

Dividir en **redes lógicas** implica:

- Un mismo switch puede tener puertos en VLAN 10, 20, 30…
- Entre switches se usa un enlace troncal (trunk) **802.1Q**
- Para que VLANs se comuniquen: router-on-a-stick o switch capa 3.

Por tanto:

- Es mucho más económico
- Fácil de mantener y flexible a los cambios
- El tiempo se invierte principalmente en la configuración de red.

Conceptos clave de VLANs

VLAN ID

Número de la VLAN. Debido a que el campo ID de la VLAN en 802.1Q tiene **12 bits**, el rago posible es 2^{12}, es decir 4096. Aunque a nivel efectivo el rango es un valor entre **1 y 4094**

Tipos de puerto

En VLANs los Switches tienen 2 tipos de puertos

- **Puertos Access**: que son los puertos que conectan equipos finales (PCs, impresoras, Aps...).
- **Puertos Trunk** (802.1Q): son los enlaces troncales que transportan varias VLANs a la vez. Se usa entre switches o hacia el router (router-on-a-stick)

Etiquetado 802.1Q

En los enlaces troncales (puertos trunk), las tramas llevan una "**etiqueta**" con el VLAN ID.

Por defecto todos los puertos de un switch pertenecen a la **VLAN 1**. Esta VLAN llamada comunmente **VLAN nativa**, no va etiquetada al atravesar enlaces troncales.

Por tanto se recomienda **NO USAR la VLAN 1**.

Inter-VLAN Routing

El Inter-VLAN Routing es el proceso que permite que los dispositivos que se encuentran en diferentes VLANs se comuniquen entre sí.

Por diseño, cada VLAN es un dominio de difusión aislado. Para cruzar la frontera de la VLAN, necesitamos un dispositivo que trabaje en la Capa 3 (Red), como un router o un switch de capa 3.

Existen **3 métodos** para lograrlo:

- Router-on-a-Stick (el método clásico)
- Switch de Capa 3
- Enrutamiento Heredado (Legacy)

Router on a Stick

Utiliza **un único puerto físico en el router** para conectar con el switch.

¿Cómo funciona?

- El **enlace** entre el **switch** y el **router** se configura como un **Trunk** (troncal).
- En el router, el puerto físico **se divide lógicamente en subinterfaces** (por ejemplo, Gig0/0.10 para la VLAN 10)

Ventaja: Ahorra puertos físicos en el router.

Inconveniente: El puerto físico puede convertirse en un cuello de botella, ya que todo el tráfico inter-VLAN debe "subir y bajar" por el mismo cable.

Switch de Capa 3

Es el método más moderno y eficiente, utilizado en redes empresariales. Aquí no se necesita un router externo para el tráfico interno.

¿Cómo funciona?

El switch actúa como router. Se crea una **interfaz virtual para cada VLAN** (llamada SVI). Por ejemplo: interface Vlan 10 con una dirección IP que servirá como gateway para los hosts.

Ventaja: Es más rápido ya que el **enrutamiento** se hace **por hardware** (ASIC) y **no hay saturación en cables físicos** externos.

Inconveniente: El switch debe soportar funciones de Capa 3.

Enrutamiento heredado (Legacy)

Es el método antiguo y ya no se utiliza debido a su ineficiencia.

¿Cómo funciona?

Se conecta un **cable físico por cada VLAN** desde el switch hacia un puerto físico distinto en el router.

Inconvenientes

- Escala muy mal. Si tenemos 10 VLANs, necesitamos 10 puertos en el router y 10 en el switch solo para conectarlos entre sí.
- Requiere mayor cantidad de cables.

Ejemplo VLANs

Topología

- 1 Router: R1 (4331)
- 1 Switch: S1 (2960)
- 3 PCs: PC-A (Administración), PC-S (Alumnos), PC-P (Profesores)
- Cableado:
  - PC-A → S1 Fa0/2
  - PC-S → S1 Fa0/3
  - PC-P → S1 Fa0/4
  - S1 G0/1 → R1 G0/0

Ejemplo VLANs

Objetivo de red

- **VLAN 10** ADMINISTRACIÓN
  - Red: 192.168.10.0/24
  - Puerta de enlace: 192.168.10.1
- **VLAN 20** ALUMNOS
  - Red: 192.168.20.0/24
  - Puerta de enlace: 192.168.20.1
- **VLAN 30** PROFESORES
  - Red: 192.168.30.0/24
  - Puertas de enlace: 192.168.30.1

Ejemplo VLANs

Simulación en Packet Tracer

- Colocar
  - Un Router 4331
  - Un Switch 2960
  - 3 PCs
- Conectar con cable directo:
  - PC-A: S1 Fa0/2
  - PC-S: S1 Fa0/3
  - PC-P: S1 Fa0/4
  - S1 G0/1 con R1 G0/0/0

Ejemplo VLANs

Configuración del Switch

Crear las VLANs

```
enable
configure terminal
```

- Creamos la VLAN 10

```
vlan 10
name ADMINISTRACION
exit
```

- Creamos la VLAN 20

```
vlan 20
name ALUMNOS
exit
```

- Creamos la VLAN 30

```
vlan 30
name PROFESORES
exit
```

Ejemplo VLANs

Switch. Asignar puertos Access a cada VLAN

```
interface fa0/2
switchport mode access
switchport access vlan 10
exit

interface fa0/3
switchport mode access
switchport access vlan 20
exit

interface fa0/4
switchport mode access
switchport access vlan 30
exit
```

Ejemplo VLANs

Switch. Configurar el enlace al router como trunk

```
interface g0/1
switchport mode trunk
switchport trunk allowed vlan 10,20,30
exit

end
write memory
```

Verificamos

```
show vlan brief
```

Ejemplo VLANs

Configuración del Router

Habilitamos la interfaz

```
enable
configure terminal

interface g0/0/0
no shutdown
exit
```

Verificamos **en el Switch** que los enlaces troncales están activos y bien configurados.

```
show interfaces trunk
```

Ejemplo VLANs

Configuración del Router. Subinterfaces 802.1Q

```
        enable
        configure terminal
Subinterfaz ADMINISTRACION
        interface g0/0.10
        encapsulation dot1Q 10
        ip address 192.168.10.1 255.255.255.0
        exit
Subinterfaz ALUMNOS
        interface g0/0.20
        encapsulation dot1Q 20
        ip address 192.168.20.1 255.255.255.0
        exit
Subinterfaz PROFESORES
        interface g0/0.30
        encapsulation dot1Q 30
        ip address 192.168.30.1 255.255.255.0
        exit
Guardamos y verificamos
        end
        write memory
        show ip interface brief
```

Ejemplo VLANs

Configuración de los Pcs

En cada PC → Desktop → IP Configuration:

PC-A (ADMINISTRACION)

- IP: 192.168.10.10
- Mask: 255.255.255.0
- Gateway: 192.168.10.1

PC-S (ALUMNOS)

- IP: 192.168.20.10
- Mask: 255.255.255.0
- Gateway: 192.168.20.1

PC-P (PROFESORES)

- IP: 192.168.30.10
- Mask: 255.255.255.0
- Gateway: 192.168.30.1

Ejemplo VLANs

Pruebas

Desde PC-A:

- ping 192.168.10.1 (gateway)
- ping 192.168.20.10

  La primera vez probablemente fallará, porque antes de enviar el primer ping, los equipos necesitan averiguar la dirección MAC del destino (o del gateway) usando ARP. Ese proceso tarda un pequeño instante y hace que el primer ping se pierda, pero una vez aprendidas las MAC, los siguientes pings funcionan.

- ping 192.168.30.10

  Lo mismo, probablemente la primera vez fallará.

Ejemplo VLANs

Pruebas

Si algo falla, comprobar:

- ¿Trunk activo y permitiendo VLANs?
- ¿Subinterfaces bien etiquetadas (encapsulation dot1Q X)?
- ¿Gateways correctos en PCs?

Enrutamiento

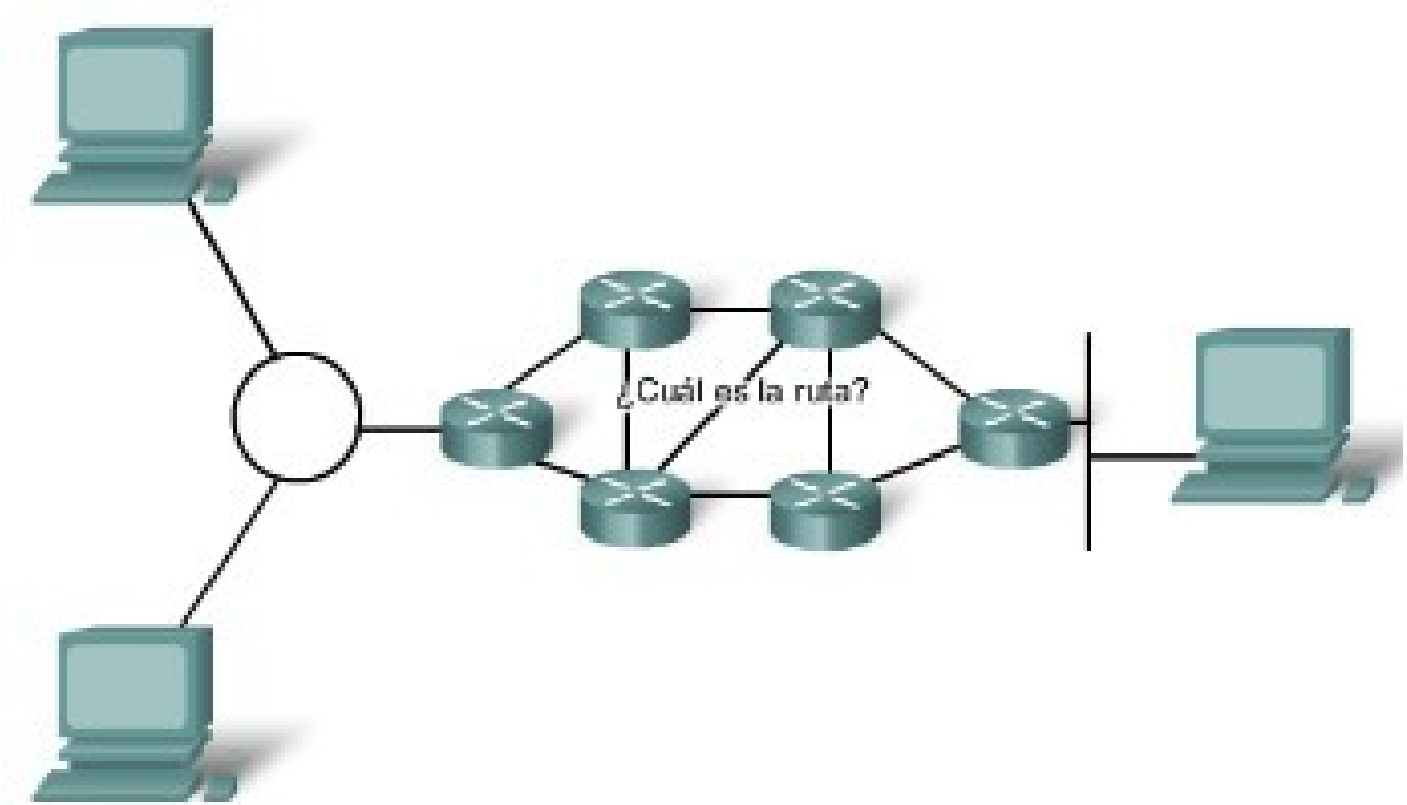
Enrutamiento

Un enrutador o **router** es un dispositivo de red cuya función principal es proporcionar conectividad entre redes ubicadas en lugares distintos.

Para ello el enrutador se encarga de dirigir el tráfico de paquetes, determinando la **ruta óptima** que deben seguir.

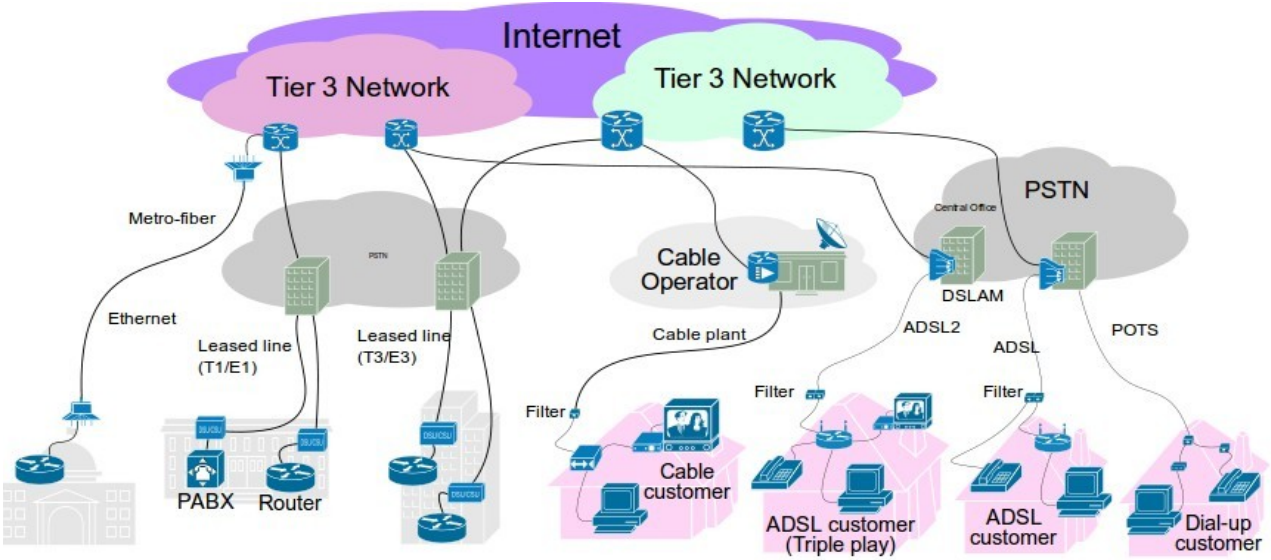
El router **actúa en la capa tres del modelo OSI** y, por tanto, extrae las direcciones IP que le llega en las tramas de la capa de enlace para hacer llegar los paquetes desde la red de origen a la red de destino.

Enrutamiento



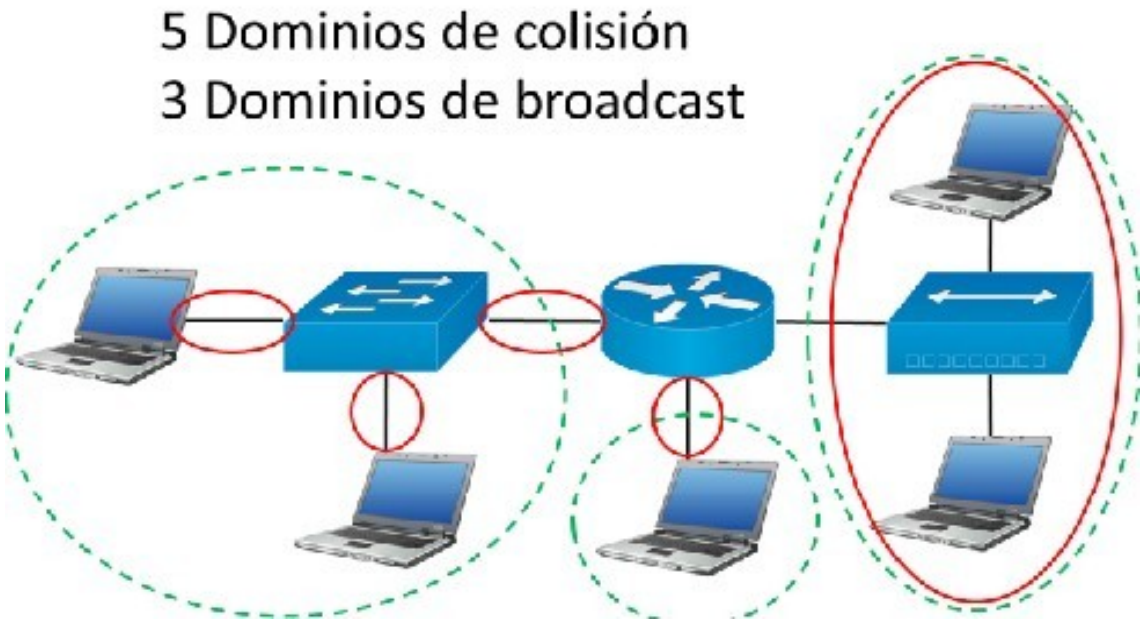
Enrutamiento

En organizaciones de gran tamaño que contienen varias redes locales, los routers permiten el intercambio de información entre ellas y se encargan también de conectar con el **ISP** (Internet Service Provider en español Proveedor de Servicios de Internet) que provee la conexión a Internet.



Enrutamiento

Los routers se encargan también de **definir el dominio Broadcast**. Con ello logra impedir que el tráfico de la capa dos no salgan de la red local con lo que consigue que las tramas de difusión no saturen la red global.



Tipos de enrutamiento

En general se habla de dos tipos de configuraciónes para redes remotas:

- El **enrutamiento estático** en el que la tabla de enrutamiento es creada por el administrador de la red.
- El **enrutamiento dinámico** en el que la tabla de enrutamiento es creada por el propio router. Pues está configurado para utilizar protocolos (RIP, IGRP, EIGRP, OSPF, IS-IS o BGP) que permiten descubrir redes vecinas y van recopilando información.

Enrutamiento estático vs dinámico

- El **enrutamiento dinámico** escala mucho mejor en redes más grandes, comparándolo con el enrutamiento estático, pero el costo es la utilización de más cantidad de recursos como RAM, ciclos del CPU (microprocesador del enrutador) y también más ancho de banda de la propia red.

- El **enrutamiento estático** permite un control total sobre la selección de la ruta, así como una total disponibilidad. Y es fácil de implementar en redes pequeñas. Aunque si por alguna razón la/s rutas estáticas fallan, el enrutador no calculará una ruta alternativa.

Tablas de enrutamiento

Para poder dirigir el tráfico de una red a otra, el router guarda información para determinar el **siguiente salto** de los paquetes que recibe en una tabla llamada **tabla de enrutamiento**.

Se trata de una base de datos con información sobre la ruta que deben seguir los paquetes que van de una red a otra.

Los routers en general no utilizan dispositivos de almacenamiento para guardar la tabla de enrutamiento, sino que lo hacen en su memoria RAM. Esto hace que cada vez que se reinicia el router se crea de nuevo la tabla de enrutamiento.

Sólo los routers de gama media y alta poseen una **NVRAM** que permite guardar la configuración del router incluida su tabla de enrutamiento.

Tablas de enrutamiento

No sólo los routers tienen tablas de enrutamiento, sino que en general cualquier dispositivo que ejecute TCP/IP como ordenadores y en general cualquier nodo de la red tiene tabla de enrutamiento.

Salida del comando: `route -n`

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         172.31.246.1    0.0.0.0         UG    0      0        0 eth0
0.0.0.0         172.31.246.1    0.0.0.0         UG    100    0        0 eth0
172.24.10.0     172.31.246.130  255.255.255.0   UG    0      0        0 br-ex
172.31.246.0    0.0.0.0         255.255.254.0   U     0      0        0 eth0
172.31.246.128  0.0.0.0         255.255.255.128 U     0      0        0 br-ex
192.168.122.0   0.0.0.0         255.255.255.0   U     0      0        0 virbr0
```

Campos de la tabla de enrutamiento

- **Red destino**: Es la dirección con la que se va a buscar que haya coincidencia con la dirección IP de destino. Con valores entre 0.0.0.0 (ruta por defecto) y 255.255.255.255 (multidifusion limitada).
- **Máscara de red**: establece los bits de la dirección IP de destino que deben coincidir. Una máscara 0.0.0.0 establece que nos es necesario que coincida ningún bit de la IP de destino, mientras que una máscara 255.255.255.255 precisa que todos los bits de la IP de destino coincidan, es decir, la IP de destino es única.
- **Puerta de enlace**: Es la dirección a la que se produce la redirección cuando se produce una coincidencia con esa entrada. Es como la puerta de enlace que utiliza el host para reenviar los paquetes a otras redes cuya ruta exacta desconoce, pero sabe que dicho equipo encontrará la ruta correcta.
- **Interfaz**: Es el adaptador de red por el que enviará el paquete. En Windows se muestra la dirección IP de dicho dispositivo mientras que en Linux se muestra el nombre del dispositivo físico (eth0, eth1, wlan0, ...)
- **Métrica**: Nos da información de las rutas disponibles y cual es la mejor. Indica el coste de la ruta que normalmente se determina por el número de saltos que realiza un paquete para llegar al destino, es decir, el número de routers que ha atravesado el datagrama hasta llegar. Si existen varias rutas que llevan al mismo destino con métricas distintas, se escoge la que tenga una métrica menor.

Proceso de encaminamiento

1. El router **recibe** un paquete por una de sus interfaces, lo desencapsula y **extrae su IP de destino**.

2. **Recorre la tabla de enrutamiento** aplicando la **máscara** de cada entrada a la dirección IP de destino del paquete:

- Si la dirección exacta o la obtenida al aplicar la máscara **coincide** con la dirección de alguna de las entradas de la tabla el paquete es enviado a la **puerta de enlace especificada** en dicha entrada.
- En caso de existir **dos o más** entradas en la tabla que se puedan aplicar, se utiliza aquella que tenga **métrica menor**.

3. Si la dirección de red obtenida **no coincide** con ninguna de las redes de la tabla, suele haber una entrada con máscara **0.0.0.0** que define la **ruta por defecto** de los paquetes.

4. Y si **no encuentra coincidencia** en la tabla el paquete es **descartado**.

Protocolos de enrutamiento

Un protocolo de enrutamiento, le indica al router como redirigir los paquetes. Es decir, un protocolo de enrutamiento se configura en un router para que él mismo aprenda las mejores rutas disponibles y luego "enrute" los paquetes a través de estas rutas, hasta su destino final.

Básicamente, establece las reglas sobre cómo un enrutador aprende redes remotas y luego anuncia estas redes a enrutadores vecinos dentro del mismo **sistema autónomo** (o AS en inglés).

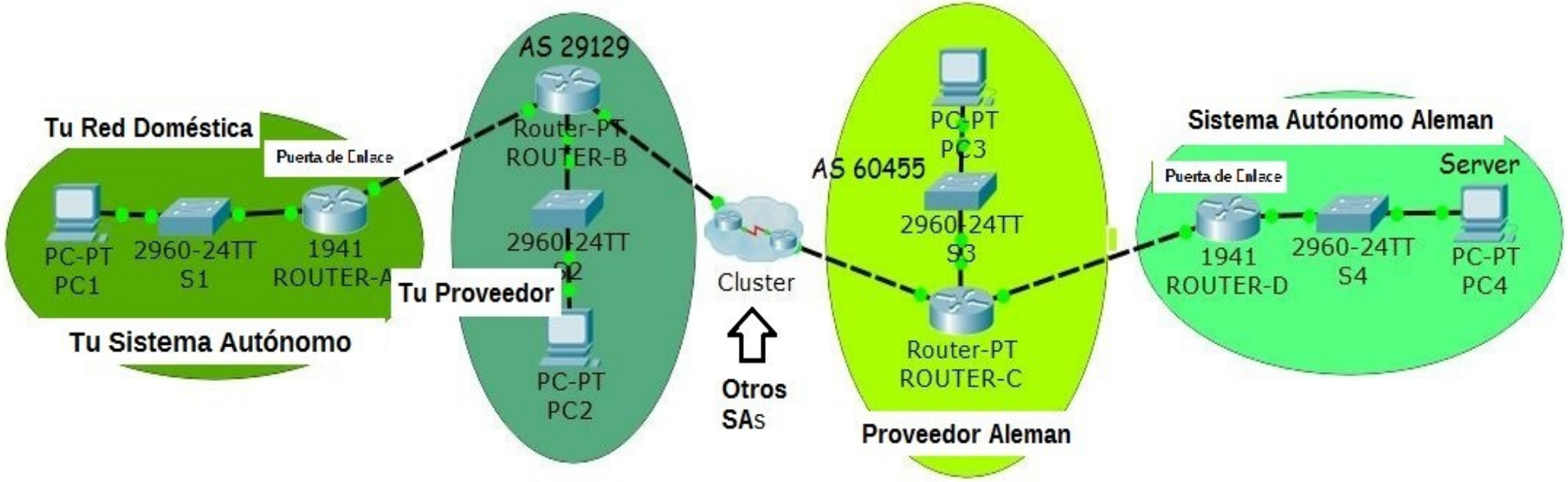
Sistema Autónomo

Un **Sistema Autónomo** (AS) se refiere a una red (o un grupo de redes) que está **bajo una sola administración**. Podría ser una empresa, un grupo de edificios pertenecientes a la misma empresa, tu propio proveedor de servicios de Internet, o incluso tu red doméstica. Internet está formada por AS conectados entre sí.

Los paquetes de datos son transmitidos, de un nodo a otro, dentro de un mismo AS hasta que necesiten llegar a otro nodo en un AS diferente.

Sistema Autónomo

Por ejemplo: Para ver una web en Alemania, los paquetes se transmiten desde tu AS (tu red) al AS de tu proveedor, luego a través de todos los AS intermedios hasta que llega al proveedor Alemán y luego al AS donde se encuentra el servidor web. Sin olvidar que las respuestas deben volver.



Númeración de Sistemas Autónomos

A cada AS se les asigna un número único (ASN) de 16 o 32 bits.

Estos números son administrados, al igual que las direcciones IP y hay números de AS privados y públicos.

- **AS privados**. No enrutables en Internet. Se usan dentro de redes privadas o laboratorios.
  - Los elige libremente el administrador de la red.
  - Rango reservado:
    - 64512 – 65534 (16 bits)
    - 4200000000 – 4294967294 (32 bits)
- **AS públicos**. Son únicos a nivel mundial. Se usan para enrutamiento real en Internet y se anuncian por BGP entre AS.
  - Asignados por la Internet Assigned Numbers Authority (IANA)
  - ¿Cuando es necesario un AS público?
    - Si te conectas a más de un ISP (multihoming).
    - Si anuncias tus propias rutas a Internet
    - Si quieres control total de políticas BGP.

Clasificación de protocolos de enrutamiento

Algunos protocolos de enrutamiento utilizan el concepto de AS en su lógica, es decir, entienden y reconocen los límites delineados por un sistema autónomo.

Ello especifica 2 grupos de protocolos en función de su ámbito o alcance:

- **Protocolos de Enrutamiento Interno**: éste es el tipo de protocolo de enrutamiento utilizado para enrutar paquetes dentro de un mismo sistema autónomo (RIP, EIGRP y OSPF).
- **Protocolos de Enrutamiento Externo**: el cual se utiliza para enrutar los paquetes entre sistemas autónomos, como ser protocolo llamado Border Gateway Protocolo (BGP).

Redes directamente conectadas vs redes remotas

Es importante recordar que:

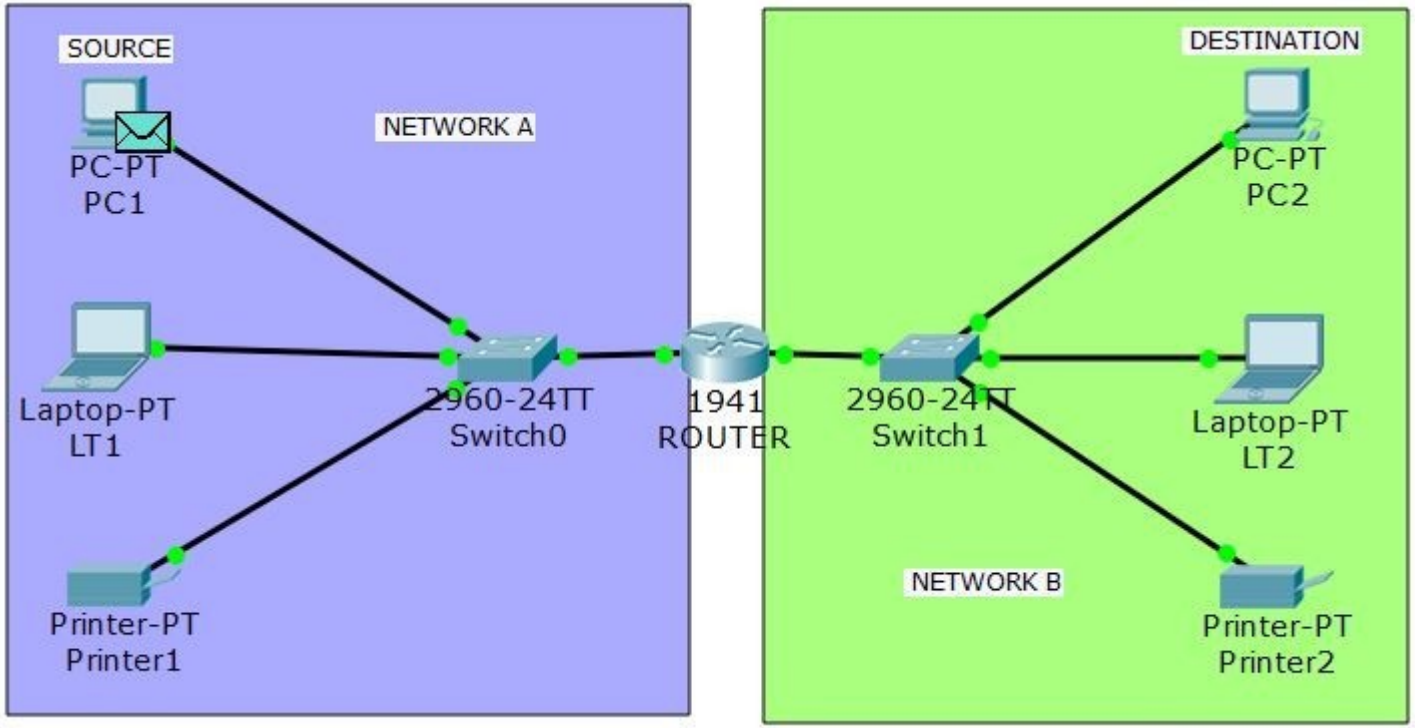
Cada una de las interfaces de un enrutador, pertenece a su propia red.

Por tanto podemos tener:

- **Redes Directamente Conectadas**: Son aquellas en las que el Router tiene una interfaz directamente conectadas (es decir, con una IP de esa subred).
- **Redes Remotas**: Son redes que están separadas por más de 1 enrutador.

Redes directamente conectadas vs redes remotas

Ejemplo: El PC1 en la red A está enviando datos a PC2 en la red B. Así, en este caso, el enrutador recibirá los paquetes enviados por PC1 desde la red A y lo enviará directamente a PC2 en la red B.



Concepto de salto

Es importante saber que después de que los paquetes salen de la interfaz de origen de un enrutador y cada vez que, a partir de entonces, los paquetes pasan a través de otro enrutador se denomina "salto" (Hop, en inglés), es decir, los paquetes entran en una interfaz y salen por otra interfaz del enrutador.

Por lo tanto, la información continuará "saltando" de enrutador en enrutador, hasta que llegue a su destino.

Algunos protocolos de enrutamiento utilizan un **conteo de saltos como métrica** para determinar las mejores rutas.

Protocolos de enrutamiento dinámico

RIP (Routing information Protocol)

Este protocolo de vector-distancia se implementa sobre UDP como protocolo de transporte. De este protocolo existen 2 versiones RIP v.1 y RIP v.2

La **métrica** que utiliza RIP es el **conteo de saltos**. Por defecto esta métrica se fija en 15. Esto quiere decir que si es necesario pasar por más de 15 routers para llegar al destino, la red se considera inalcanzable y se descarta el paquete. Esta situación hace que RIP no sea muy escalable.

El protocolo RIP, hace envíos de **actualizaciones** de las tablas de enrutamiento en broadcast, en intervalos de 30 segundos. También hace uso de la regla del horizonte divido, envenenamiento de rutas y temporizadores de espera.

El tiempo de expiración es de 180 segundos, lo cual hace que en ese lapso de tiempo se pase por alto cualquier información nueva acerca de una red si esa red tiene una métrica menos conveniente, y aunque esto es ventajoso, también tiene el inconveniente de que evita que se instale una ruta alternativa válida.

En la actualidad se considera **obsoleto**.

IGRP (Interior Gateway Routing Protocol)

IGRP es un protocolo de enrutamiento de **vector-distancia** desarrollado por Cisco.

IGRP envía **actualizaciones** de enrutamiento a intervalos de **90 segundos**, las cuales publican las redes de un sistema autónomo en particular.

Las métricas que utiliza IGRP son:

- **Ancho de banda**: el menor valor de ancho de banda en la ruta.
- **Retardo**: El retardo acumulado de la interfaz a lo largo de la ruta.
- **Confiabilidad**: La confiabilidad del enlace hacia el destino, según sea determinada por el intercambio de mensajes de actividad (keepalives).
- **Carga**: La carga sobre un enlace hacia el destino, medida en bits/s.

IGRP (Interior Gateway Routing Protocol)

IGRP utiliza una **métrica compuesta**. Esta métrica se calcula como función del ancho de banda, el retardo, la carga y la confiabilidad, pero por defecto, sólo se considera el ancho de banda y el retardo. Los parámetros restantes sólo se consideran si se habilitan a través de la configuración.

El retardo y el ancho de banda no son valores medidos, sino que se fijan a través de los comandos de interfaces relativos al ancho de banda y al retardo.

Al igual que RIP v.1, IGRP no soporta el manejo de **VLSM**.

Cisco luego desarrolló una versión mejorada de IGRP, denominada **EIGRP**.

EIGRP (Enhanced Interior Gateway Routing Protocol)

EIGRP es un protocolo de enrutamiento propietario de Cisco basado en IGRP que **admite CIDR y VLSM**, y ofrece tiempos de convergencia más rápidos, mejor escalabilidad y gestión superior de los bucles de enrutamiento. Además, funciona en las redes IPX y AppleTalk con potente eficiencia.

EIGRP es un protocolo de **enrutamiento avanzado** que se basa en las características normalmente asociadas con los protocolos del estado de enlace.

Es una opción ideal para las grandes redes **multiprotocolo** construidas principalmente con routers Cisco.

EIGRP (Enhanced Interior Gateway Routing Protocol)

Los routers **EIGRP** mantienen información de **ruta y topología** a disposición en la RAM, para que puedan reaccionar rápidamente ante los cambios.

Mantiene las siguientes tres tablas:

- **Tabla de vecinos**: Enumera a los routers adyacentes.
- **Tabla de topología**: todas las tablas de enrutamiento del AS.
- **Tabla de enrutamiento**: mantiene las rutas que se aprenden de forma dinámica.

OSPF (Open Shortest Path First)

OSPF es uno de los protocolos del estado-enlace más importantes. Es un protocolo estándar descrito en el RFC 2328 y la versión para IPv6 se publicó en el RFC 2740.

Características

- Usa el **algoritmo Dijkstra (SPF)** para calcular la metrica más baja hasta un destino. La métrica, denominada **costo**, se define como un valor arbitrario que puede variar según el fabricante o modelo de router. El IOS de Cisco utiliza los anchos de banda acumulados de las interfaces de salida desde el router hasta la red de destino para calcular el valor de la métrica.
- Las **actualizaciones** de enrutamiento producen tráfico cuando ocurren cambios en la topología de la red.
- Es un protocolo **classless** o sin clase. No realiza una sumarización automática de los bordes de la red principal.
- Cada router mantiene una **base de datos** que describe la **topología** exacta de la red. A partir de la cual se construye un árbol SPF, del que se extraen las rutas más cortas para incluirlas en la tabla de encaminamiento.
- Proporciona **balanceo** de carga entre rutas de igual peso. Si un administrador especifica múltiples rutas hacia un destino con el mismo coste, el protocolo OSPF distribuye el tráfico de la misma manera.
- **Recalcula** las rutas rápidamente cada vez que hay un cambio en la topología, intercambiando el mínimo tráfico de red para las notificaciones entre routers. No existen actualizaciones **periódicas**.

OSPF (Open Shortest Path First)

1) **Descubrimiento de vecinos** (Hello)

   Cada router envía mensajes Hello periódicos para detectar routers vecinos y comprobar parámetros (área, timers, autenticación). Si coinciden, pasan a ser vecinos OSPF.

2) **Elección de DR y BDR (en redes multiacceso)**

   Se elige un DR (Designated Router) y un BDR (Backup DR) con el objetivo de reducir el tráfico de control.

3) **Intercambio de información de estado de enlace (LSA)**

   Cada router anuncia: Sus interfaces, sus costes y sus vecinos

4) **Base de datos de estado de enlace (LSDB)**

   Con todas las LSAs, cada router construye la LSDB.

5) **Cálculo de rutas (SPF / Dijkstra)**

   Cada router ejecuta SPF para calcular el camino de menor coste hacia cada red.

6) **Instalación en la tabla de enrutamiento**

   Las mejores rutas se instalan en la tabla de routing

IPv6

IPv6

El 3 de febrero del 2011, la IANA entregó el último bloque de direcciones Ipv4 disponibles a la RIR APNIC.

A principios de los años 90 ya prevía que esto sucedería, y se empezó a trabajar con el protocolo **IPv6**. En 1994 se creó la especificación básica, y en 1998 se publica la especificación completa.

La principal novedad de esta nueva versión es la cantidad de direcciones que puede manejar. Con IPv6 las direcciones son de **128 bits**, por tanto podemos manejar 2^{128} (340 sextillones) de direcciones IP.

Para hacernos una idea de lo que significa esto, si el espacio de direccionamiento de IPv4 fuera el equivalente a un milímetro, IPv6 sería el equivalente a recorrer 240.000 veces la distancia de la tierra al sol.

Novedades IPv6

- **Simplificación del formato de cabecera**. Algunos campos de la cabecera se han suprimido o se han hecho opcionales con el objetivo de reducir el costo de procesamiento de los paquetes y ahorrar ancho de banda.
- **Soporte mejorado para las extensiones y opciones**. Los cambios en la manera en que se codifican las opciones de la cabecera IP permiten un reenvío más eficiente, límites menos rigurosos en la longitud de opciones, y mayor flexibilidad para introducir nuevas opciones en el futuro.
- **Capacidad de etiquetado de flujos**. Una nueva capacidad se agrega para permitir el etiquetado de paquetes que pertenecen a "flujos" de tráfico particulares para lo cuál el remitente solicita tratamiento especial, como la calidad de servicio no estándar o el servicio en "tiempo real".
- **Capacidades de Autenticación y Privacidad**. IPv6 incluye la especificación de extensiones que proveen autenticación, integridad, y (opcionalmente) confidencialidad de los datos.

Formato de las direcciones IPv6

Las direcciones IPv6 están formadas por 128 bits. Para facilitar su lectura se expresan en números hexadecimales agrupados de cuatro en cuatro y cada grupo está separado por dos puntos (:).

Se necesitan **32 dígitos hexadecimales** agrupados en 8 grupos de 4 dígitos para representar los 128 bits de las direcciones IPv6.

Un ejemplo de dirección IPv6 podría ser:

`FEDC:BA98:7654:3210:FEDC:BA98:7654:3210`

Notación IPv6

Para hacer más manejables las direcciones IPv6 si hay un grupo de ceros en una dirección podemos comprimir la dirección dejando sólo los dos puntos (:). Por ejemplo, la dirección:

```
2001:0DB8:0000:0000:0000:0000:1428:57ab
```

Es esquivalente a:

```
2001:0DB8:0000:0000:0000::1428:57ab

2001:0DB8:0:0:0:0:1428:57ab

2001:0DB8:0::0:1428:57ab

2001:0DB8::1428:57ab
```

Sólo se puede comprimir una parte de la dirección. Por ejemplo:

```
2001::25de::cade
```

No sería válida porque no queda claro cuántos grupos nulos hay en cada lado.

Diferencias IPv4 vs IPv6

Característica	IPv4	IPv6
Tamaño dirección	32 bits	128 bits
Notación	Decimal con puntos	Hexadecimal con :
Broadcast	Sí	No existe (sustituido por multicast)
Multicast	Opcional	Fundamental
NAT	Muy común	No necesario
Autoconfiguración	Limitada	Integrada
Seguridad	Opcional	Integrada en el diseño

Dirección de red y dirección de host

Las direcciones de red IPv6 también se separan en parte de red y parte de host y para especificarlo se utiliza la notación **CIDR**, es decir, después de la dirección IP y separados por una barra inclinada (/), se especifican los bits que pertenecen al prefijo de la red.

Este número recibe el nombre de **longitud del prefijo de subred**.

Por ejemplo, la dirección

`2001:db8:abcd:0012::/64`

Significa:

- 64 bits de red
- 64 bits de identificador de interfaz

Prefijo /64

- Es el tamaño estándar de red Ipv6.
- Permite:
  - Autoconfiguración SLAAC
  - Diseño uniforme de redes
  - Número de direcciones en un /64: 2^{64}

Longitudes de prefijos más comunes

Prefijo	Uso típico
/128	Dirección individual
/64	Red estándar (LAN)
/56	Hogares (ISP)
/48	Empresas
/32	ISP grandes

Tipos de direcciones IPv6

IPv6 define 3 tipos principales de direcciones:

- **Unicast**: Identificador para una **única interfaz**. Un paquete enviado a una dirección unicast es entregado solo a la interfaz identificada con dicha dirección.

- **Multicast**: Identifica un **grupo de interfaces**. Un paquete enviado a multicast lo reciben todos los miembros del grupo. Sustituyen al broadcast de Ipv4.

  Prefijo `ff00::/8`

  Muy usadas en: Autoconfiguración, Neighbor Discovery y Descubrimiento de routers

- **Anycast**: dirección que es **asignada a más de una interfaz** (que normalmente pertenecen a diferentes nodos), con la propiedad que un paquete enviado a una dirección anycast es enrutado a la interface más cercana que tenga dicha dirección.

  Uso típico: Servicios distribuidos y alta disponibilidad

Comparación tipos de direcciones IPv6

Tipo	Destino	¿Cuántos lo reciben?	Uso típico
Unicast	Uno	1	Comunicación normal
Multicast	Grupo	Varios	Descubrimiento
Anycast	El más cercano	1	Servicios distribuidos
Broadcast	❌	❌	No existe

Direcciones IPv6 reservadas y especiales

IPv6 define bloques de direcciones con funciones concretas, como comunicación local, direcciones privadas, direcciones públicas globales o multicast. Cada prefijo indica cómo y dónde puede usarse una dirección.

- Direcciones especiales
- Direcciones Link-local Unicast Adresses (LLA)
- Direcciones Global Unicast (GUA)
- Direcciones Unique Local Unicast Adressess (ULA)
- Direcciones Multicast

Direcciones IPv6 especiales

Dentro de las direcciones unicast existen algunas cuyo uso está reservado:

- La dirección de **loopback** `0:0:0:0:0:0:0:1`, que también puede expresarse como **`::1/128`**
- La dirección con todos sus bits a 0, que se expresa como **`::/128`** que recibe el nombre de dirección **indefinida**. Al igual que en IPv4, esta dirección se usa por las interfaces cuando a la interfaz no se le ha asignado ninguna dirección.

Direcciones Link-local Unicast Adresses (LLU)

Las direcciones de enlace local:

- Tienen el prefijo **`FE80::/10`**
  - Rango de direcciones; `FE80:: - FEBF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF`
- Tienen su alcance **limitado al enlace**
- No son enrutables
- Son generadas dinámicamente
- Son obligatorias en IPv6: toda interfaz IPv6 tiene al menos una

Su uso es similar a APIPA. El objetivo es tener una comunicación básica en la red local para:

- Neighbor Discovery
- Router Discovery
- Autoconfiguración

Direcciones Global Unicast (GUA)

Las direcciones Global Unicast:

- Son utilizadas para el tráfico global y, por supuesto, son ruteables en la Internet IPv6.
- Similares a las direcciones públicas de Ipv4.
- En la actualidad IANA y RIR están asignando para este tipo, direcciones del rango **`2000::/3`**
  - Rango: `2000:: - 3FFF::FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF`

Direcciones Unique Local Addresses (ULA)

Las direcciones Unique Local Addresses:

- Prefijo: **`FC00::/7`**
  - Rango: `FC00:: - FDFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF`
- Son de uso privado
- No son enrutables en Internet, pero si dentro de la organización. Por lo que su alcance está limitado al sitio local.
- Tienen uso similar al de las direcciones privadas IPv4.
- Ejemplo: **`FD12:3456:789A::1`**

Direcciones Multicast

Las direcciones Multicast

- Prefijo: **`FF00::/8`**
- Son direcciones para grupos
- El segundo byte indica el alcance:
  - ff02:: → enlace local
  - ff05:: → sitio (limitado a una red administrativa. Ej: empresa o campus).
  - ff0e:: → global
- Ejemplos importantes:
  - ff02::1 → todos los nodos del enlace local
  - ff02::2 → todos los routers del enlace local

Direcciones IPv4 embebidas en IPv6

Para facilitar la transición y mantener la compatibilidad, las direcciones IPv4 pueden ser embebidas dentro de direcciones IPv6.

Para ello se ha reservado un espacio para direcciones:

`::ffff:x`

Donde x es la dirección IPv4

Ejemplo:

`::ffff:192.168.1.1`

Resumen de tipos de direcciones

Prefijo	Tipo	Uso
`fe80::/10`	Link-local (LLA)	Enlace local
`2000::/3`	Global Unicast (GLA)	Internet
`fc00::/7`	Unique Local (ULA)	Red privada
`ff00::/8`	Multicast	Grupos
`::1`	Loopback	Host local
`::`	Indefinida	Inicialización

Autoconfiguración en IPv6

IPv6 permite que un equipo se configure automáticamente, sin necesidad obligatoria de DHCPv6, gracias a SLAAC (Stateless Address Autoconfiguration).

¿Cómo funciona SLAAC?

- El router anuncia
  - El prefijo de red
  - Información básica de la red
- El host:
  - Construye su propia dirección IPv6

Detalle del funcionamiento de SLAAC

1. El host se conecta a la red
2. Envía un Router Solicitation (RS)
3. El router responde con un Router Advertisement (RA)
4. El RA incluye:
   - Prefijo de red (normalmente /64)
   - Flags de configuración
5. El host genera su ID de interfaz lo añade al prefijo recibido
6. El host envía un DAD (Duplicate Address Detection) para averiguar si alguien más está usando esa dirección.
7. El host configura como Gateway el link-local del router.

Cabecera de IPv6

Bits	0-3	4-11	12-15	16-23	24-32
0	Versión	Clase de Tráfico	Etiqueta de flujo		
32	Longitud campo de datos			Cabecera siguiente	Límite de Saltos
64	Dirección IP Origen				
96					
128					
160					
192	Dirección IP Destino				
224					
256					
288					

Características de la cabecera IPv6

La cabecera es de tamaño fijo: 40 bytes (320 bits). Esto tiene la ventaja de que los routers pueden procesar los paquetes más rápidamente.

- **Versión**: 4 bits. Siempre vale 0110.
- **Clase de tráfico**: 8 bits. Para indicar la prioridad del paquete.
- **Etiqueta de flujo**: 20 bits. Para manejar la calidad del servicio.
- **Longitud del campo de datos**: 16 bits. Para indicar el tamaño de la parte de datos. Tamaño máximo 65.535 bytes pero se puede ampliar con Jumbogramas.
- **Cabecera siguiente**: 8 bits. Una de las grandes novedades de IPv6 es el uso de un formato flexible de cabecera que permite ir añadiendo funcionalidades de forma paulatina. Este diseño aporta gran eficacia y flexibilidad ya que se pueden definir en cualquier momento a medida que se vayan necesitando entre la cabecera fija y la carga útil.
- **Límite de saltos**: 8 bits. Para limitar el tiempo de vida de los paquetes. El equivalente a TTL.
- Dirección **IP origen**: 128 bits.
- Dirección **IP destino**: 128 bits.