


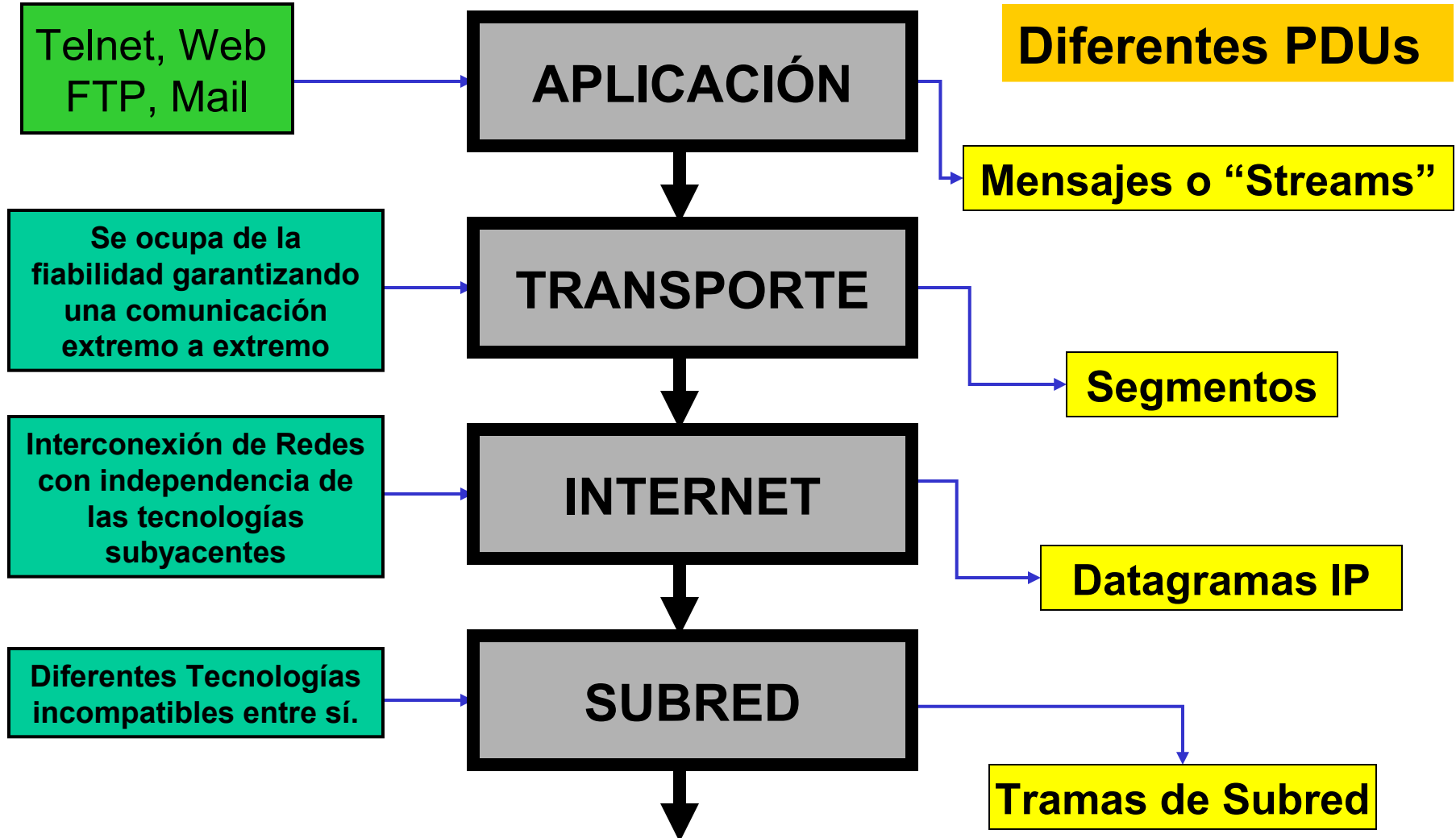
---

**IP**

- 
- 1 Generalidades**
  - 2 Protocolo IP**
  - 3 ICMP**
  - 4 Enrutamiento en Redes IP**
  - 5 Subnetting**

# Generalidades

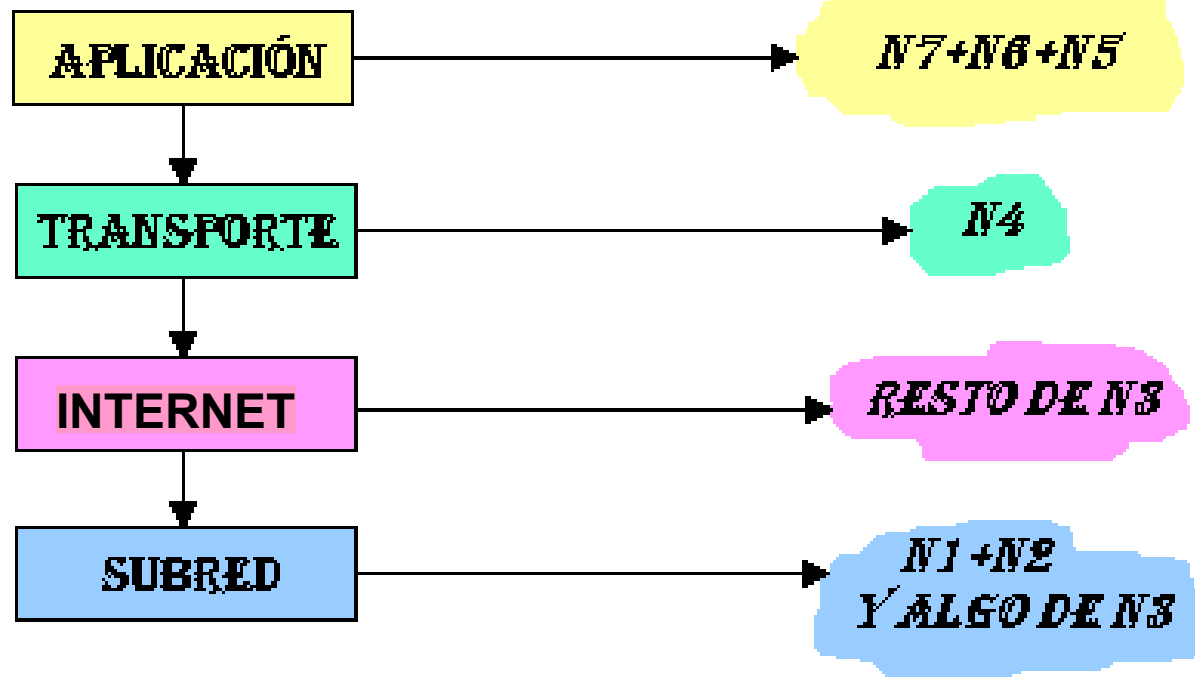
## Arquitectura TCP/IP (I)



## Arquitectura TCP/IP (II)

*ARQUITECTURA  
TCP/IP*

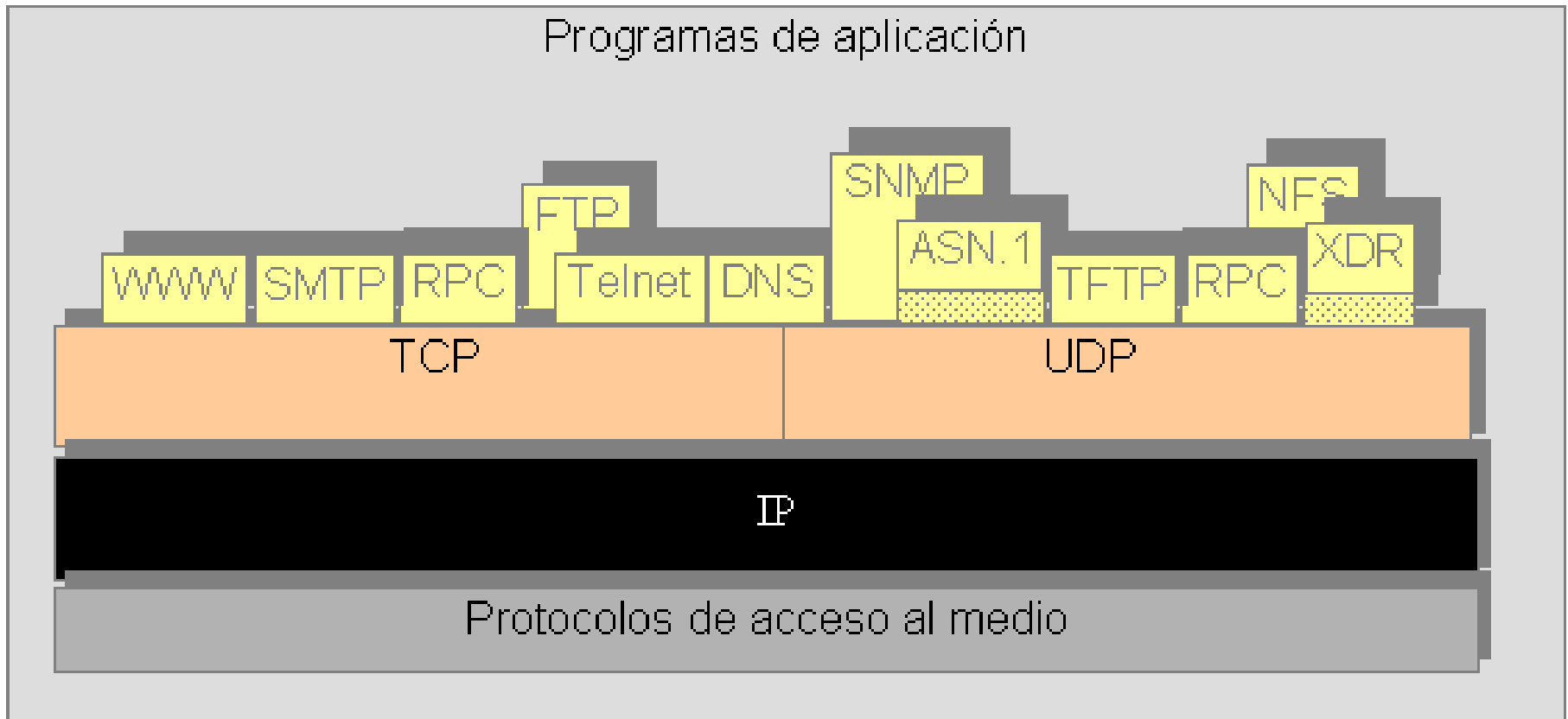
*EQUIVALENTE  
OSI*



Niveles TCP/IP frente a OSI

# Generalidades

## Mapa de Protocolos TCP/IP (I)



**1 Generalidades**

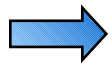


**2 Protocolo IP**

**3 ICMP**

**4 Enrutamiento en Redes IP**

**5 Subnetting**



**2.1 Funciones Básicas**

**2.2 Formato del DATAGRAMA IP**

**2.3 Segmentación**

**2.4 Direcciones IP**

✚ **Internet Protocol (IP)** es el protocolo **Internet** usado en la **Red Internet** (definido en **RFC 791**).

✚ Ofrece un servicio:

- ✚ Independiente de la Tecnología de la Subred

- ✚ No orientado a conexión

- ✚ No confirmado

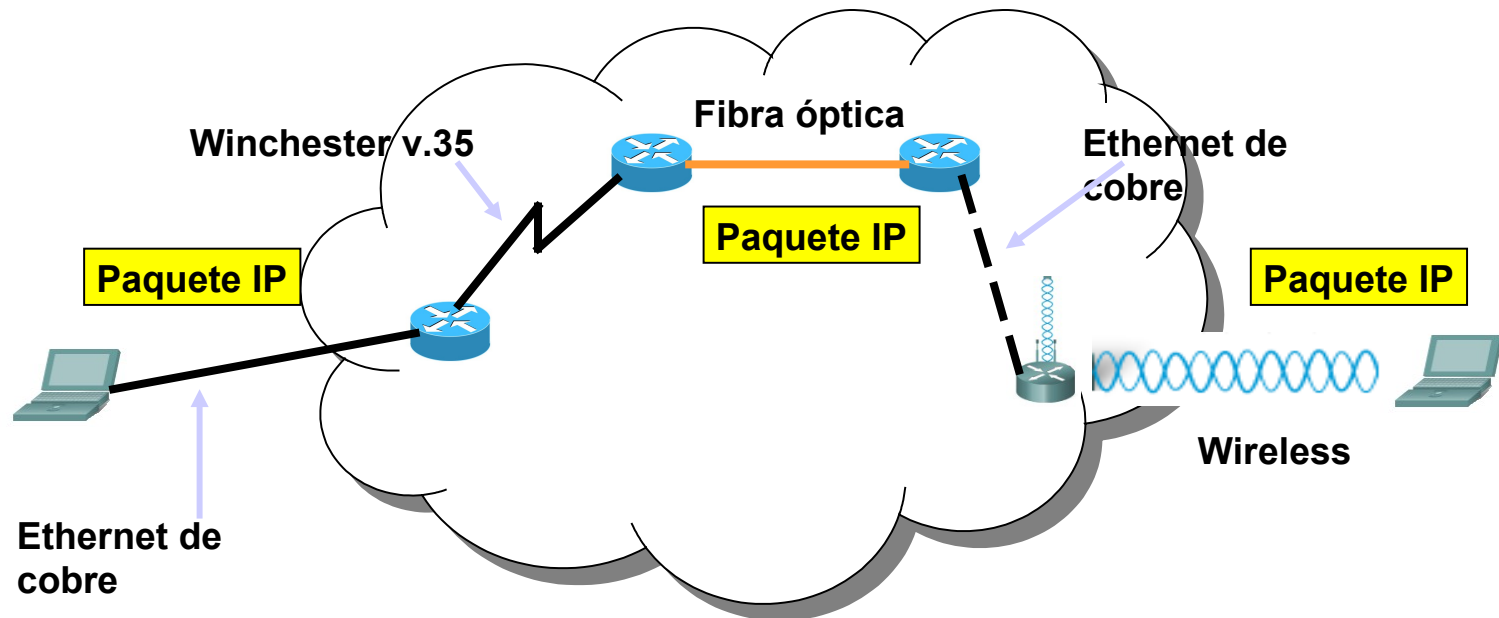
✚ La Internet “**hace lo que puede**” para entregar los datagramas al destino (**best-effort delivering**). Los datagramas pueden: perderse, duplicarse o desordenarse.



# Funciones Básicas

- **Independencia de los medios:**

El protocolo IP es independiente de la tecnología de los medios de transmisión. Esto significa que el IP puede transportarse sobre cualquier red de manera totalmente transparente. La red puede estar basada en pares de cobre, fibra óptica (monomodo o multimodo), o bien wireless. Existe un parámetro tecnológico denominado MTU (Unidad máxima de transmisión) que se negocia entre la capa de red y la capa de enlace (nivel 2). Por ejemplo la MTU de Ethernet es 1500 bytes, en caso que el datagrama IP supere este valor será necesario la fragmentación de dicho paquete.



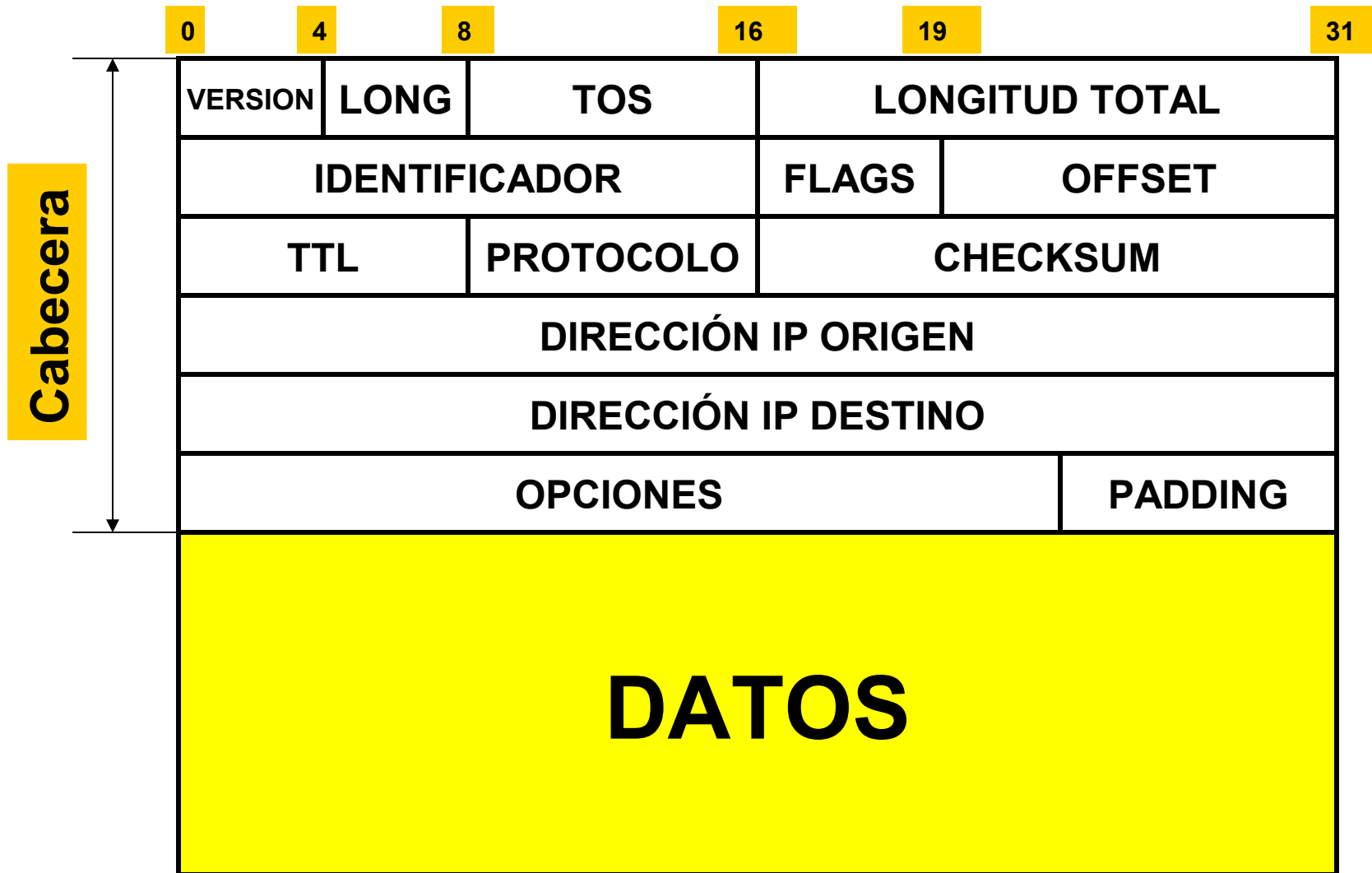
**2.1** Funciones Básicas

 **2.2** Formato del DATAGRAMA IP

**2.3** Segmentación

**2.4** Direcciones IP

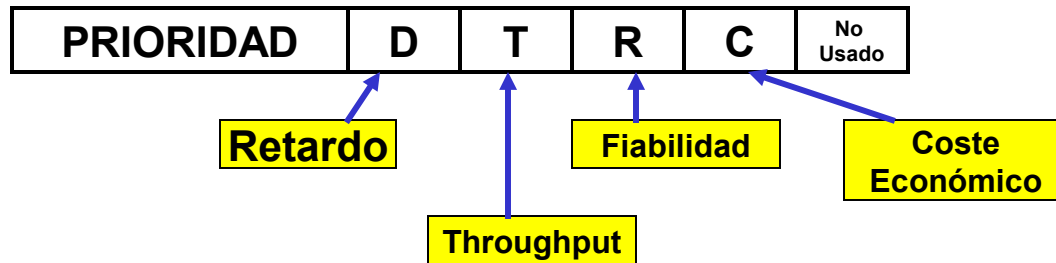
# Formato del Datagrama IP



# Formato del Datagrama IP

## Campos (I)

- + **VERS**: IP versión 4. Próximamente IP versión 6 o Internet 2 ?
- + **LONG**: longitud de la cabecera medida en unidades de 32 bits.
- + **TOS** (Type of service): tipo de servicio solicitado

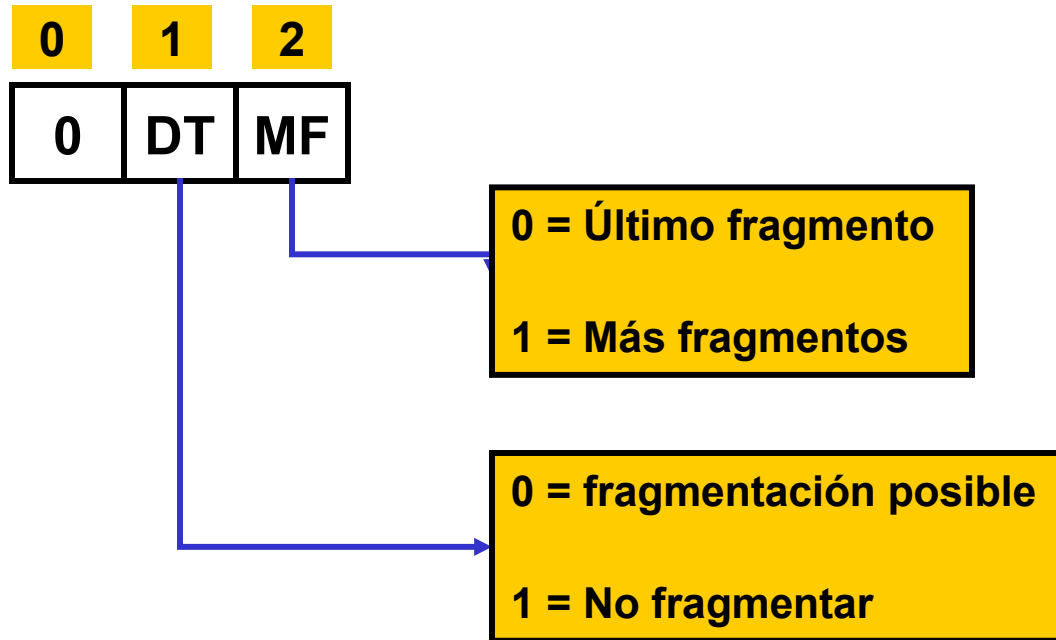


- + **LONGITUD TOTAL**: del datagrama completo (en bytes)
- + **IDENTIFICADOR**: valor asignado en origen al datagrama para ayudar al reensamblado de los paquetes.

# Formato del Datagrama IP

## Campos (II)

+ **FLAGS:**



+ **OFFSET:** posición del paquete dentro del datagrama original , (en unidades de 8 bytes, son 13 bits  $\therefore 2^{13} = 8192$  y  $8192 \cdot 8 = 64K$ , tamaño máximo del datagrama).

+ **TTL (Time to Live):** tiempo máximo que un datagrama puede permanecer en la red (expresado en número de saltos).

# Formato del Datagrama IP

---

## Campos (III)

- + **PROTOCOLO**: protocolo usuario de **IP** (Ej: **TCP**, **UDP**, etc.)
- + **CHECKSUM**: código de protección frente a errores. **Calculado sólo sobre la cabecera del datagrama IP.**
- + **IP origen, IP destino**: direcciones IP origen y destino
- + **PADDING**: relleno hasta que el header del datagrama sea múltiplo de **32** bits

## OPCIONES

- + **Campo de longitud variable**: facilidades para pruebas y depuración.
- + **Por ejemplo**:
  - + Registro de ruta
  - + Encaminamiento fijado en origen
  - + Marca de Tiempo

**2.1 Funciones Básicas**

**2.2 Formato del DATAGRAMA IP**

 **2.3 Segmentación**

**2.4 Direcciones IP**

# Segmentación

---

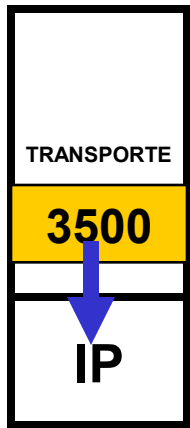
- + Consiste en dividir un datagrama IP en otros de menor tamaño, con el mismo formato, y de tal forma que a partir de ellos sea posible recuperar el **datagrama original**.
- + Necesaria cuando un datagrama ha de atravesar una subred con un tamaño máximo de paquete menor que el suyo (Concepto de **MTU**).
- + Una vez segmentado un datagrama, no se reensambla hasta llegar a su destino.
- + IP exige que las subredes por las cuales atraviesan los datagramas tengan una **MTU** mínima de 576 bytes.



# Segmentación

**LOS ROUTERS NO REENSAMBLAN!!!**

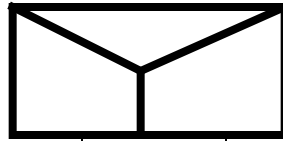
HOST 1



SUBRED 1

MTU  
1500

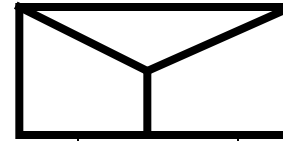
Router 1



SUBRED 2

MTU  
1000

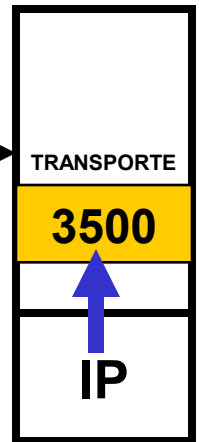
Router 2



SUBRED 3

MTU  
500

HOST 2



Nº	1	2	3
ID	A	A	A
OFFSET	0	1500	3000
MF	1	1	0
LONG.	1500	1500	500

Nº	1	2	3	4	5
ID	A	A	A	A	A
OFFSET	0	1000	1500	2500	3000
MF	1	1	1	1	0
LONG.	1000	500	1000	500	500

Nº	1	2	3	4	5	6	7
ID	A	A	A	A	A	A	A
OFFSET	0	500	1000	1500	2000	2500	3000
MF	1	1	1	1	1	1	0
LONG.	500	500	500	500	500	500	500

# Segmentación

---

- ✚ El bit **DT** (fragmentación posible) es interpretado por los routers como que si está a **1** no se puede **fragmentar**, en cuyo caso el router no tiene más remedio que **descartar** el datagrama.
- ✚ Los routers **no pueden reensamblar, sí segmentar**. Esto es así porque no se sabe el camino “**a priori**” que pueden adoptar los datagramas **IP** al atravesar las diferentes subredes.
- ✚ El encaminamiento puede ser **salto a salto**, o **fijado en origen**. En el primer caso lo único que hacen los routers es “*tirar el muerto*” (nadie en la red sabe el encaminamiento de origen a destino).
- ✚ El encaminamiento **fijado en origen** hace uso del **campo opciones** del datagrama **IP**. En este caso los routers **no consultan sus tablas** de encaminamiento, sino que hacen caso omiso a lo que dice el campo opciones para entregar el datagrama en destino.
- ✚ **Registro de ruta**: esto lo que hace es que cada router apunta sus direcciones en el campo de opciones y al final se sabe toda la ruta por la que el datagrama pasó.
- ✚ IP sólo resuelve el **transporte de datagramas**, **IP no es un protocolo de encaminamiento** (notar diferencia entre protocolos ruteables y ruteados)

**2.1 Funciones Básicas**

**2.2 Formato del DATAGRAMA IP**

**2.3 Segmentación**

 **2.4 Direcciones IP**

# Direcciones IP

- ✚ Plan de numeración independiente de las Redes físicas a las que estén conectados los sistemas.
- ✚ Cada **host** tiene asignado una dirección de 32 bits dividida en dos campos: **RED** y **HOST**.
- ✚ Clases de direcciones:



# Direcciones IP

---

✚ Las direcciones **IP** son direcciones **jerárquicas** como lo son los **números telefónicos** y los **códigos postales**. Brindan una mejor forma de organizar las direcciones de las computadoras que las direcciones **MAC**, que son **direcciones planas** como los números del **DNI** sin ningún tipo de relación entre sí. Las direcciones **IP** pueden configurarse por **software** y por lo tanto son de **carácter flexible**. Las direcciones **MAC** están dentro del hardware de la **NIC**. Ambos esquemas de direccionamiento son importantes para que las comunicaciones entre las computadoras sean eficientes.

✚ Las razones por las que los datos pueden encontrar su destino en la Internet son porque cada red conectada a la Internet tiene un **número de red único IP**. Para garantizar que cada número de red de la Internet seguirá siendo siempre único y diferente de cualquier otro número, existe una organización llamada Centro de Operaciones de la Red Internacional (**InterNIC – International Network Information Center-**). Es una organización que sirve a la comunidad de Internet brindando asistencia al usuario, documentación, capacitación, servicio de registro de nombres de dominio de Internet y otros servicios). **InterNIC** asigna a las empresas **bloques de direcciones IP** en base al tamaño de sus redes (en base al nº de hosts).

✚ Hay **tres clases de direcciones IP** que una empresa, escuela o Universidad puede recibir del **InterNIC**. **InterNIC** reserva las direcciones **IP** clase “**A**” para los gobiernos de todo el mundo o para grandes multinacionales norteamericanas (tal el caso de **IBM** y **AT&T**), las direcciones IP clase “**B**” para las empresas de mediano tamaño o alguna Universidad, y las direcciones IP clase “**C**” para el resto.

# Direcciones IP

## Rangos de direcciones IP

### + Las direcciones clase A incluyen:

- Rango de números de red: **1.0.0.0 a 126.0.0.0**
- La dirección **127.0.0.0** queda reservada para **Loopback (127.0.0.1-127.255.255.254)**
- Cantidad de direcciones de host:  $2^{24} = 16.777.216$  – **GRAN DERROCHE DE DIRECCIONES!!**
- Una forma relativamente fácil de reconocer si un dispositivo forma parte de una red **clase “A”** es mirar el primer byte de su dirección IP. Los números del primer byte de todas las redes **clase “A”** oscilan entre **1 y 126 (Regla del 1º octeto)**.

### + Ejemplo de direcciones Clase A:

- **IBM** tiene asignada la dirección **9.0.0.0** y **AT&T** tiene asignada la **12.0.0.0**

### + Las direcciones clase B incluyen:

- Rango de números de red: **128.0.0.0 a 191.255.0.0**
- Cantidad de direcciones de host:  $2^{16} = 65.536$
- Una forma relativamente fácil de reconocer si un dispositivo forma parte de una red **clase “B”** es mirar los **dos primeros bytes** de su dirección IP. Las direcciones IP **clase “B”** **siempre tienen valores entre 128 y 191** en su primer byte. En el segundo byte, siempre tienen un valor comprendido entre **0 y 255**.

# Direcciones IP

## + Las direcciones clase C incluyen:

- Rango de números de red: **192.0.0.0 a 223.255.255.0**
- Cantidad de direcciones de host:  **$2^8 = 256$**
- Una forma relativamente fácil de reconocer si un dispositivo forma parte de una red **clase “C”** es ver los **tres primeros bytes** de su dirección **IP**. Las direcciones IP clase “C” siempre tendrán los valores comprendidos entre **192 y 223 en el primer byte**. El valor del segundo y del tercer byte puede ser cualquier valor comprendido entre **0 y 255**.

### Reconocimiento de Clases en Direcciones IP en base al primer byte

Bits de mayor orden	Byte en decimal	Clase de dirección
0	1 - 126	A
10	128 - 191	B
110	192 - 223	C

+ El rango de direcciones **clase D** es: **224.0.0.0 hasta 239.255.255.255**, mientras que el rango de direcciones **clase E** va desde **240.0.0.0 hasta 247.255.255.255**

# Direcciones IP

## Valores especiales

El número de *identificador de red* de cada dirección IP *identifica a la red* a la cual está conectado un dispositivo. El *número de host* de cada dirección IP *identifica la conexión del dispositivo a dicha red*.

✚ **0** en el campo de **Host**: significa “esta Red”

✚ **0** en el campo de **RED** y de **HOST**: o sea **0.0.0.0** lo emplean los routers para encaminar datagramas que no pertenecen a ninguna de las subredes a las cuales el router está conectado, **es la salida para Internet (GATEWAY POR DEFECTO)**.

✚ **255**: **difusión o broadcast**, todos unos en el campo de **HOST**, implica que el mensaje llega a todas las máquinas de la red.

✚ **Ejemplos:**

Red clase A	10.0.0.0	Broadcast Clase B	138.4.255.255
Host Clase A	10.1.2.3	Red clase C	192.16.192.0
Broadcast Clase A	10.255.255.255	Host Clase C	192.16.192.9
Red Clase B	138.4.0.0	Broadcast Clase C	192.16.192.255
Host Clase B	138.4.4.20	Loopback	127.0.0.1 - 127.255.255.254

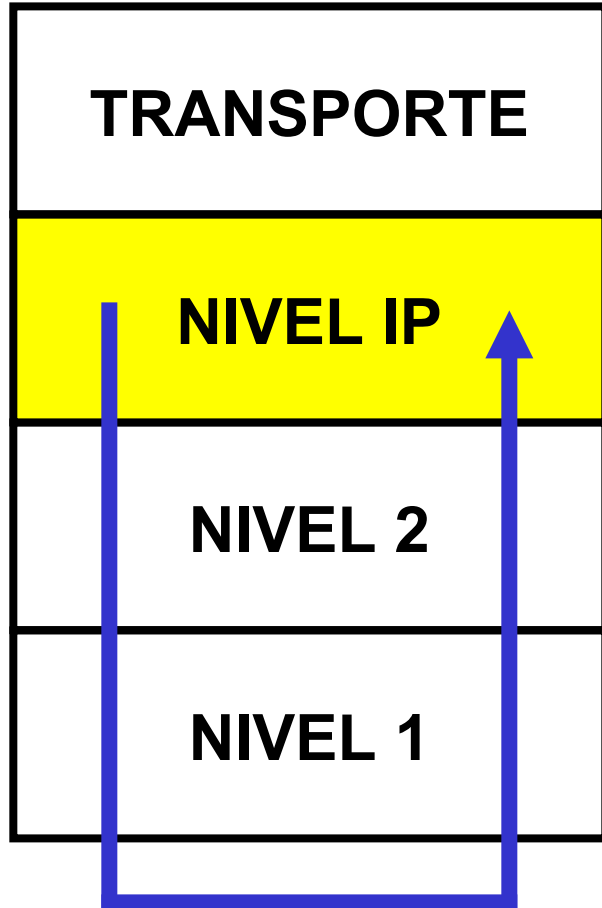


## Direcciones IP

**LOOPBACK**



**Permite probar la Arquitectura de Comunicaciones de un HOST!**



**127.0.0.1 – 127.255.255.254**

No todas las posibles direcciones se han asignado. Por ejemplo, la dirección **127.0.0.0**, valor del rango tipo clase **A**, se reserva para **loopback**, y está diseñada para utilizarse en las pruebas del TCP/IP y para la comunicación de los procesos internos en la máquina local. Cuando algún programa utiliza la dirección loopback como destino, el software de protocolo en una computadora regresa los datos sin generar tráfico a través de alguna red. Permite probar de esta manera la arquitectura de protocolos del propio HOST.

# Direcciones IP

## Resumen Direcciones IP

- ✚ Sólo tres de las clases de direcciones IP son utilizadas comercialmente, son las denominadas Clase **A**, **B** y **C** como vimos anteriormente.
- ✚ **InterNIC** reserva una serie de direcciones para **IP multicast** y para fines experimentales.
- ✚ **IP multicast** consiste en el envío de paquetes únicos copiados por la red y enviados a un **subconjunto específico de direcciones de red**. A tal efecto se han reservado en el primer byte los números entre **224 y 255**.
- ✚ Además de las direcciones IP reservadas, cualquier dirección IP que tenga todos los ceros en la parte correspondiente al host está reservada (**significa “esta red”**), al igual que toda dirección que tenga todos unos en la parte del campo de host (**significa Broadcast**).

## Ejercicios sobre direcciones IP

+ Indicar de qué tipo de dirección se trata, si es un **host**, si es de una **red**, si es **broadcast**, etc.

+ 124.95.44.15

+ 151.10.13.28

+ 201.110.231.28

+ 113.0.0.0

+ 176.10.0.0

+ 197.22.103.0

+ 256.241.13.103

+ Cuáles serían las direcciones de broadcast correspondientes a los ejemplos anteriores?

# Direcciones IP

## Ejemplo de Direcciones IP

Dirección	Clase	Red	Host
10.2.1.1	A	10.0.0.0	0.2.1.1
128.63.2.100	B	128.63.0.0	0.0.2.100
201.222.5.64	C	201.222.5. 0	0.0.0.64
192.6.141.2	C	192.6.141. 0	0.0.0.2
130.113.64.16	B	130.113.0. 0	0.0.64.16
256.241.201.1 0	No existe		

**1 Generalidades**

**2 Protocolo IP**

 **3 ICMP**

**4 Enrutamiento en Redes IP**

**5 Subnetting**

# ICMP

---

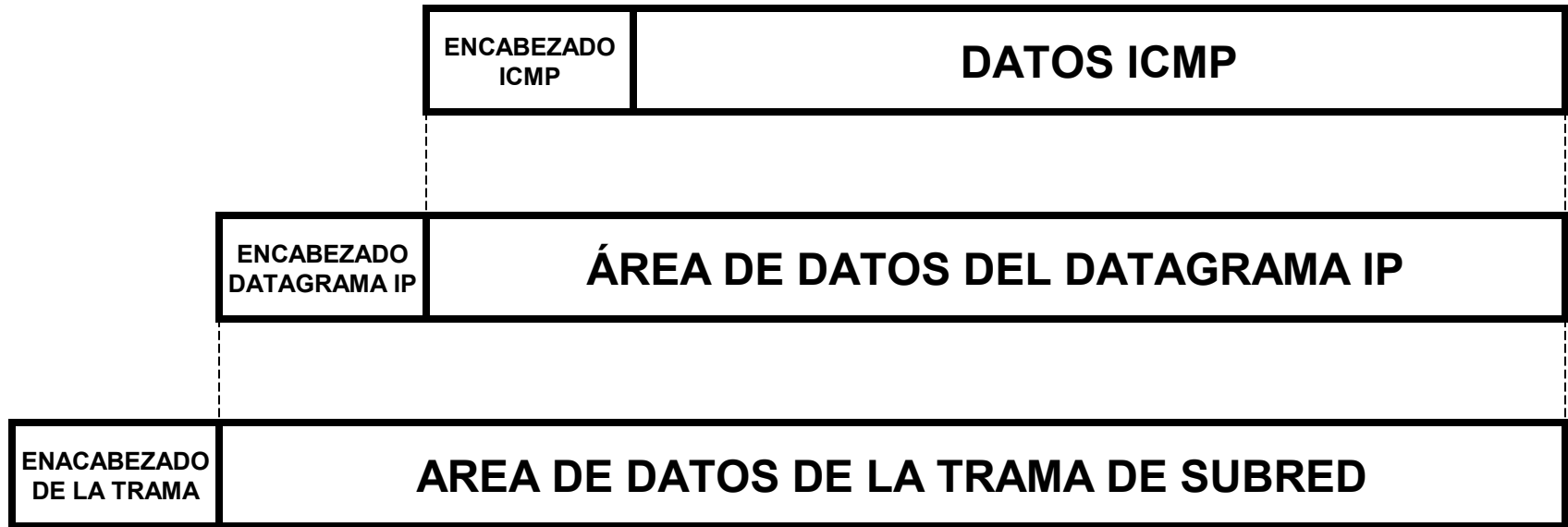
✚ Para permitir que los routers en Internet **reporten los errores** o proporcionen información sobre circunstancias inesperadas, los diseñadores agregaron a los **protocolos TCP/IP** un mecanismo de mensajes de propósito especial. El mecanismo, conocido como **Internet Control Message Protocol (ICMP)**, se considera como **parte obligatoria del IP** y se debe incluir en todas las implantaciones IP. **ICMP es parte integral del protocolo IP.**

✚ Los mensajes **ICMP** viajan **como datos** encapsulados en **datagramas IP**. Los errores producidos en la transmisión de datagramas con mensajes **ICMP NO generan** nuevos mensajes **ICMP**.

✚ **ICMP e IP se integran recién en IP versión 6.**

# ICMP

## FORMATO DEL MENSAJE ICMP (I)



Los mensajes **ICMP** requieren dos niveles de encapsulación. Cada mensaje **ICMP** viaja a través de la Internet en el área de **datos del datagrama IP**, el cual viaja a través de cada subred en el área de datos correspondiente de una trama. Los datagramas que llevan mensajes **ICMP** se **rutean** exactamente como los que llevan información de usuario; no existe ni una confiabilidad ni una prioridad adicionales. Por lo tanto los mensajes de error **se pueden perder o descartar**. Además en una red congestionada, los mensajes **ICMP** que reportan errores pueden causar **congestionamiento adicional**.

## FORMATO DEL MENSAJE ICMP (II)

✚ Aunque cada mensaje **ICMP** tiene su propio formato, todos comienzan con los mismos tres campos; un campo **TYPE** de mensaje , de **8 bits** y **números enteros** , que identifica el mensaje; un campo **CODE**, de 8 bits también que proporciona más información sobre el tipo de mensaje, y un campo **CHECKSUM**, de **16 bits**. Además, los mensajes **ICMP** que reportan errores siempre incluyen el encabezado y los primeros **64 bits** de datos del datagrama que causó el problema.

✚ Algunos ejemplos del campo **TYPE** son:

- 0** Respuesta de **eco** (comando **ping**)
- 3** Destino inaccesible
- 8** Solicitud de **eco** (hago un **ping**)
- 11** Tiempo excedido para un datagrama (**TTL =0**)

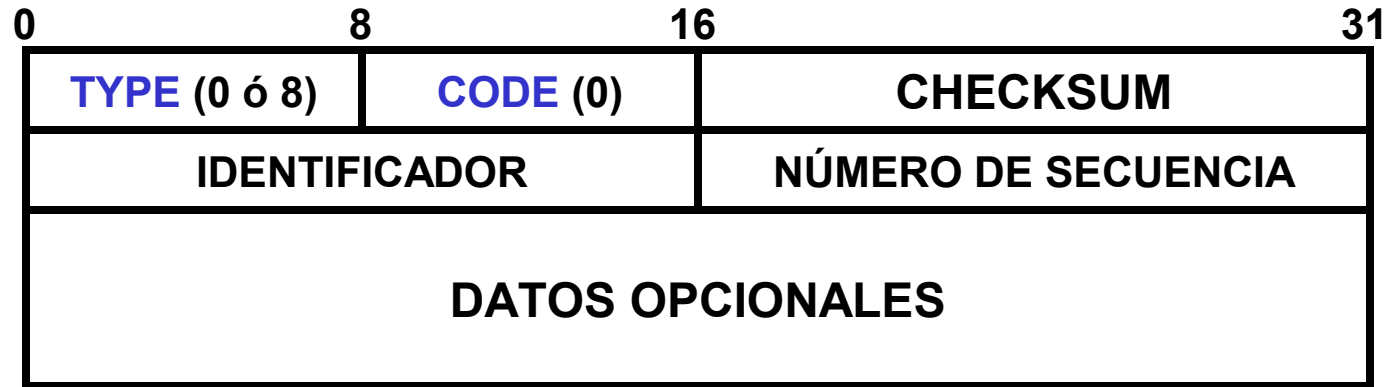
✚ Ejemplos del campo **CODE**:

- 0** Red inaccesible
- 1** Host inaccesible
- 2** Protocolo inaccesible
- 3** Puerto inaccesible
- 4** Se necesita fragmentar
- 5** Falla en la ruta de origen

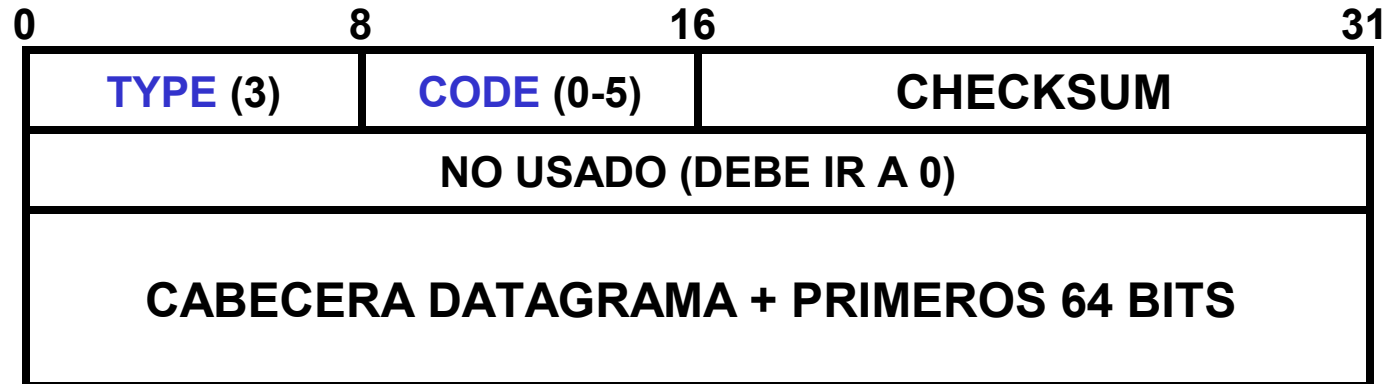


# ICMP

## Ejemplos de mensajes ICMP



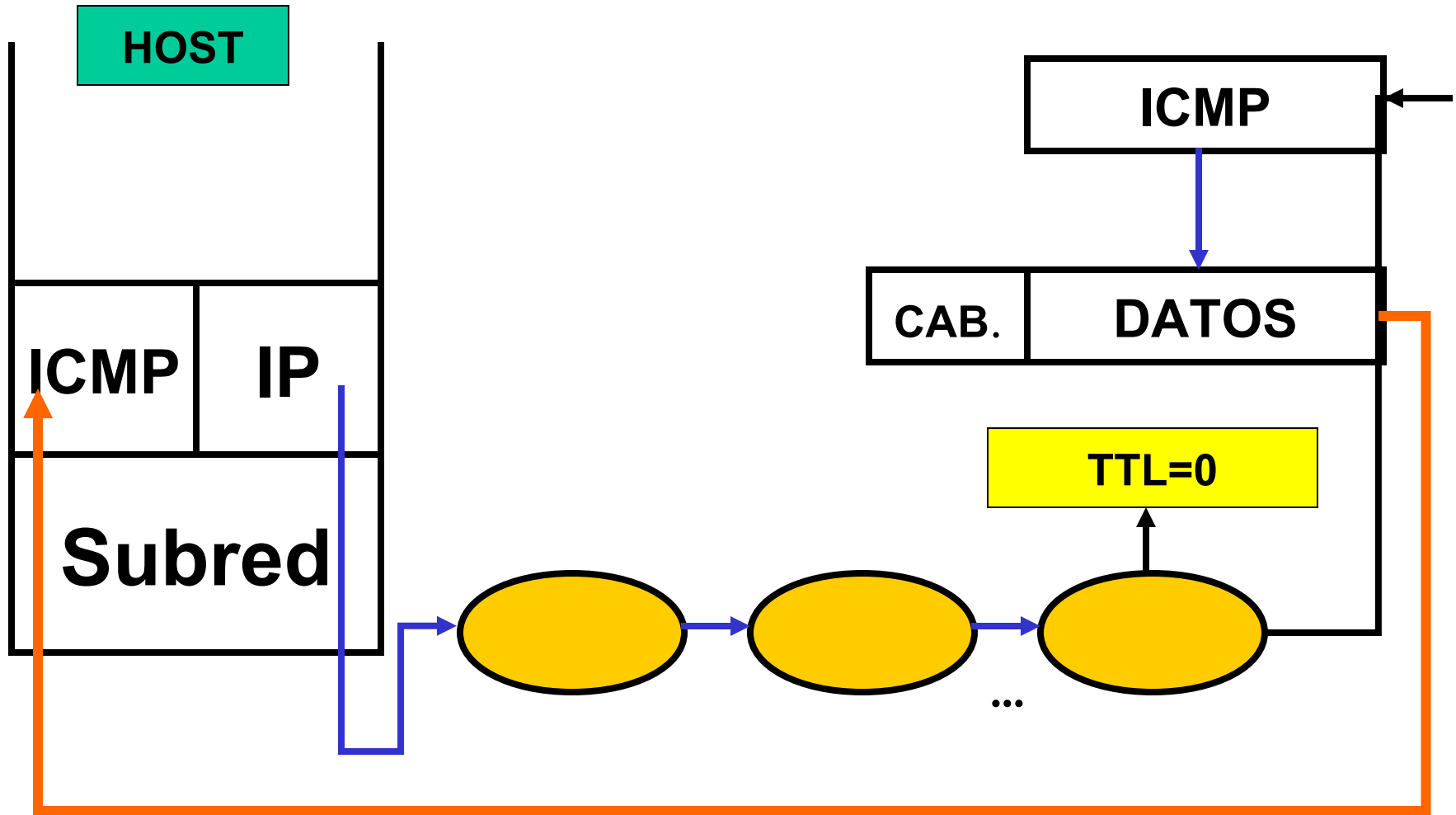
## Solicitud y Respuesta de Eco (comando **PING con red inaccesible**)



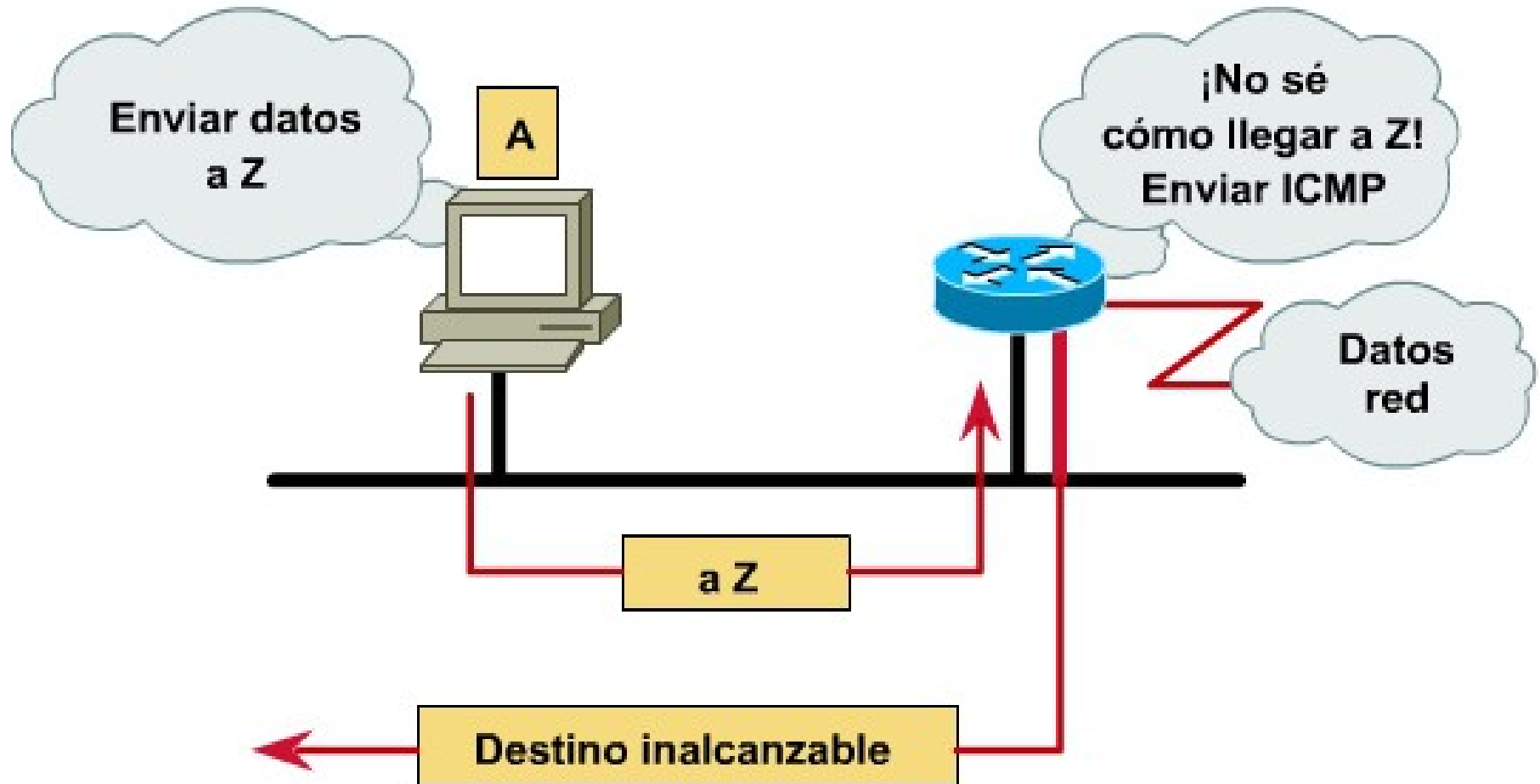
**Destino inaccesible**

# ICMP

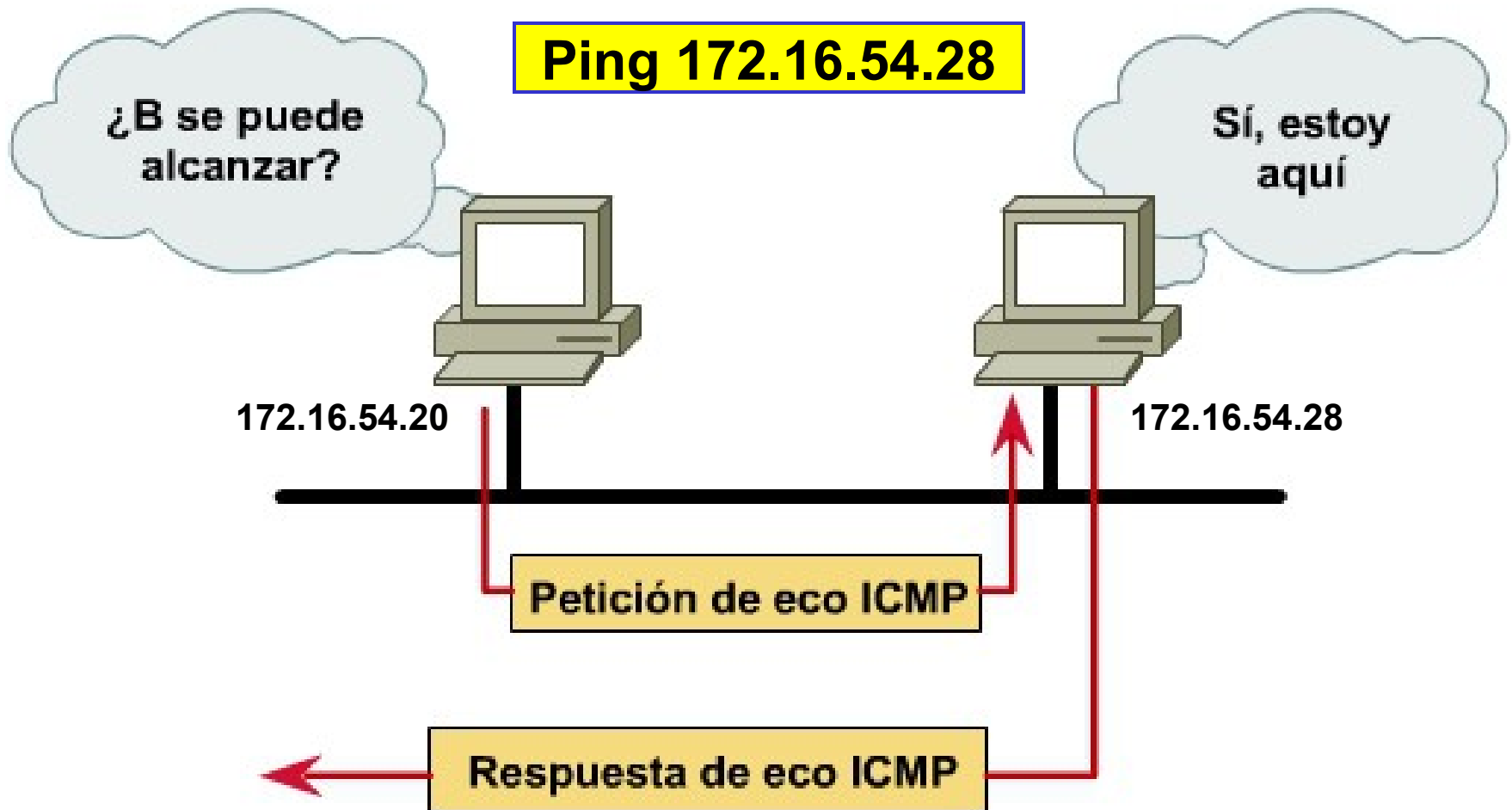
## Proceso de generación de un mensaje ICMP



## ICMP Testing



## Prueba de ICMP



## Ejemplos Prácticos (I)

+ **Ping** permite conocer si un sistema está **accesible o no**. Se basa en **ecos ICMP**.

+ **Traceroute** permite conocer la ruta seguida por un **datagrama IP**. Se basa en enviar **ecos ICMP** con tiempos de vida bajos para provocar **ex profeso** que los sistemas, por los cuales atraviesan los datagramas, generen **mensajes de error** (Tiempo de vida excedido, o sea **TTL=0**) y así conocer el camino seguido por dichos **datagramas IP**.

## Ejemplos Prácticos (II)

## TRACEROUTE

✚ El **HOST origen** hace **TTL++**, comenzando con **TTL = 1**. Por lo tanto contesta el primer router con un **eco ICMP**, enviando entre otras cosas su dirección **IP**. Ahora el **HOST origen** envía un nuevo datagrama pero con **TTL = 2**, por lo tanto contestará el segundo router con su dirección **IP**. Luego se genera un datagrama con **TTL = 3** y contestará el tercer router, y así sucesivamente hasta que un router **no conteste más** y por ende al no llegar el **eco ICMP** sabemos hasta **dónde llega la conexión** y dónde está entonces el problema.

✚ En resumen estos dos comandos, **ping** y **traceroute**, son obviamente muy útiles para los operadores de red para **detectar** si los sistemas están **activos** y si no están activos ver en dónde está el problema que no permite **establecer la comunicación**.

**1 Generalidades**

**2 Protocolo IP**

**3 ICMP**

 **4 Enrutamiento en Redes IP**

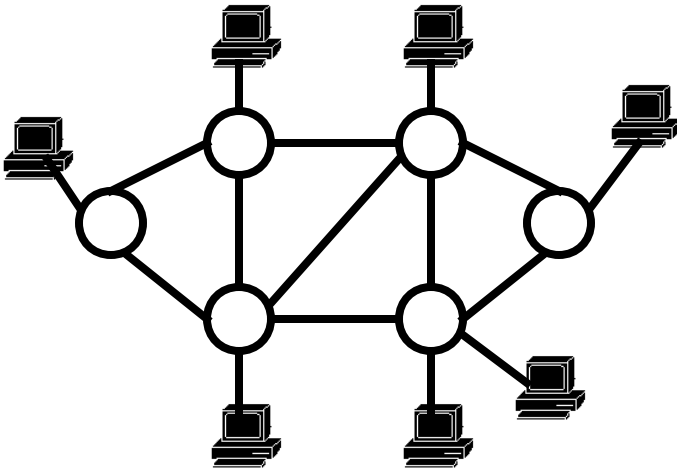
**5 Subnetting**

# Enrutamiento en Redes IP

## Definiciones (I)

### Objetivo:

Búsqueda de las rutas en una red, para todo origen y destino, que satisfagan una serie de condiciones. Por ejemplo, rutas de mínimo costo económico, de mínimo retardo, de máximo Throughput o que satisfagan algún criterio administrativo.



### Algoritmo de encaminamiento:

Método mediante el cual se calculan las rutas en una red.

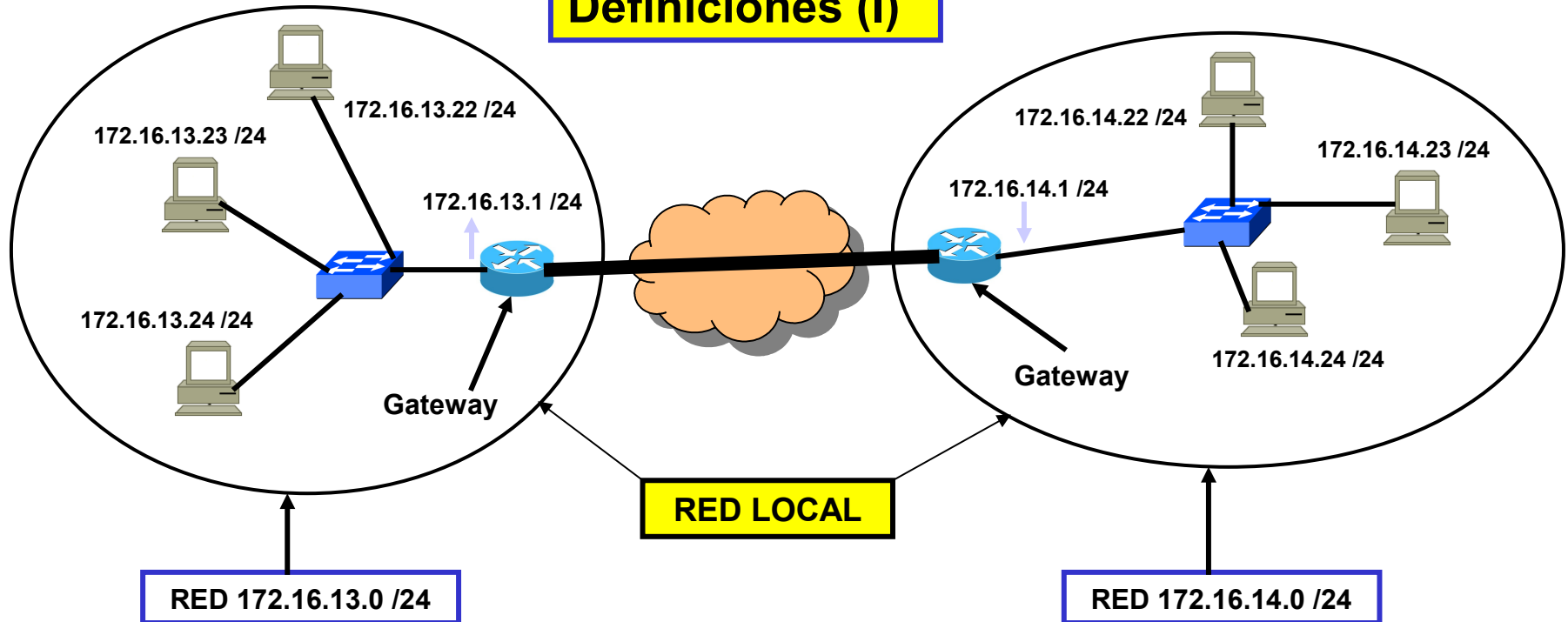
### Decisión de encaminamiento:

Si la red es **no orientada a conexión** la decisión debe tomarse para cada datagrama. Si es orientada a conexión, únicamente **durante el establecimiento del circuito virtual**.



# Enrutamiento en Redes IP

## Definiciones (I)

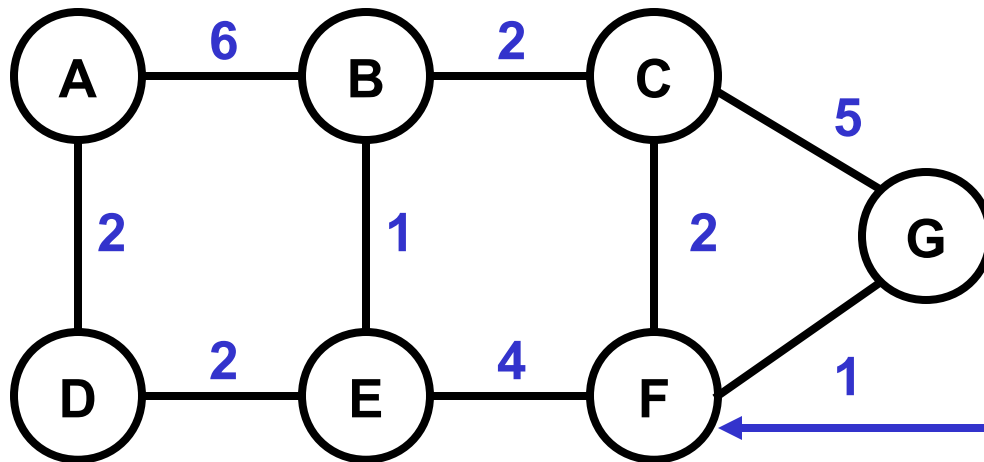


Resultaría imposible que cada host conozca las direcciones de todos los hosts que integran la Internet. En cada red local cada host sólo sabe llegar al resto de los hosts que están en su misma subred. Para que un host se comuniquen con otro host fuera de su RED LOCAL debe intervenir el Gateway. El Gateway es un router que sabe llegar al resto de las redes, ya que posee una tabla de enrutamiento. A su vez el Gateway sólo tiene conocimiento de direcciones de red, de esta manera se logra acotar las entradas de la tabla de ruteo.

# Enrutamiento en Redes IP

## Definiciones (II)

**Costo o Métrica:** puede ser dinámico  $C = f(t)$



**Métrica:** magnitud a optimizar (retardo, throughput, costo económico, etc.)

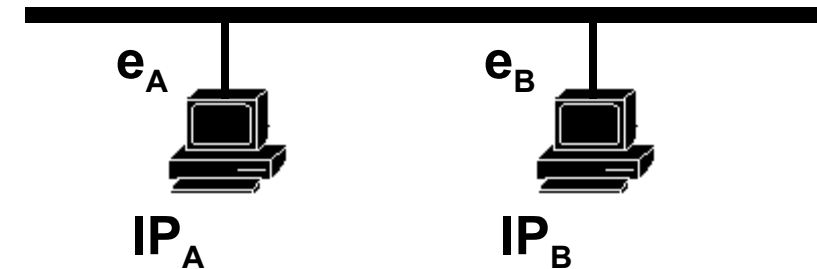
## Tabla de Encaminamiento

Nodo F		
Destino	Siguiente	Métrica
A	E	8
B	C	4
C	C	2
D	E	6
E	E	4
F	F	0
G	G	1

# Enrutamiento en Redes IP

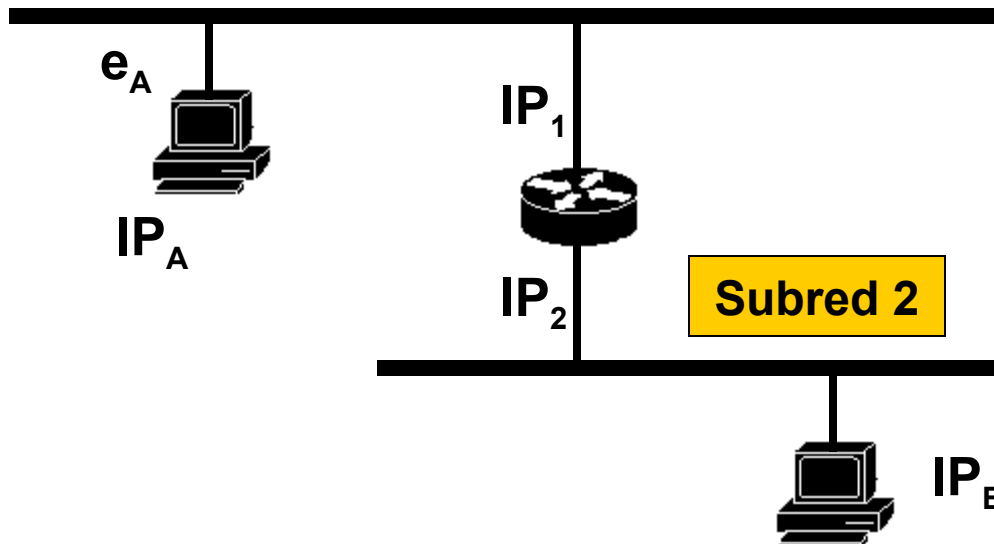
## Encaminamiento en IP

+ Dos situaciones básicas:



Transmisión directa entre hosts conectados a la misma subred.

Subred 1



Hosts en distintas subredes:  
Transmisión indirecta a través de un router

# Enrutamiento en Redes IP

---

## Funcionamiento Básico en IP

- ✚ La transmisión de **datagramas IP** entre máquinas conectadas a la misma subred se hace directamente:

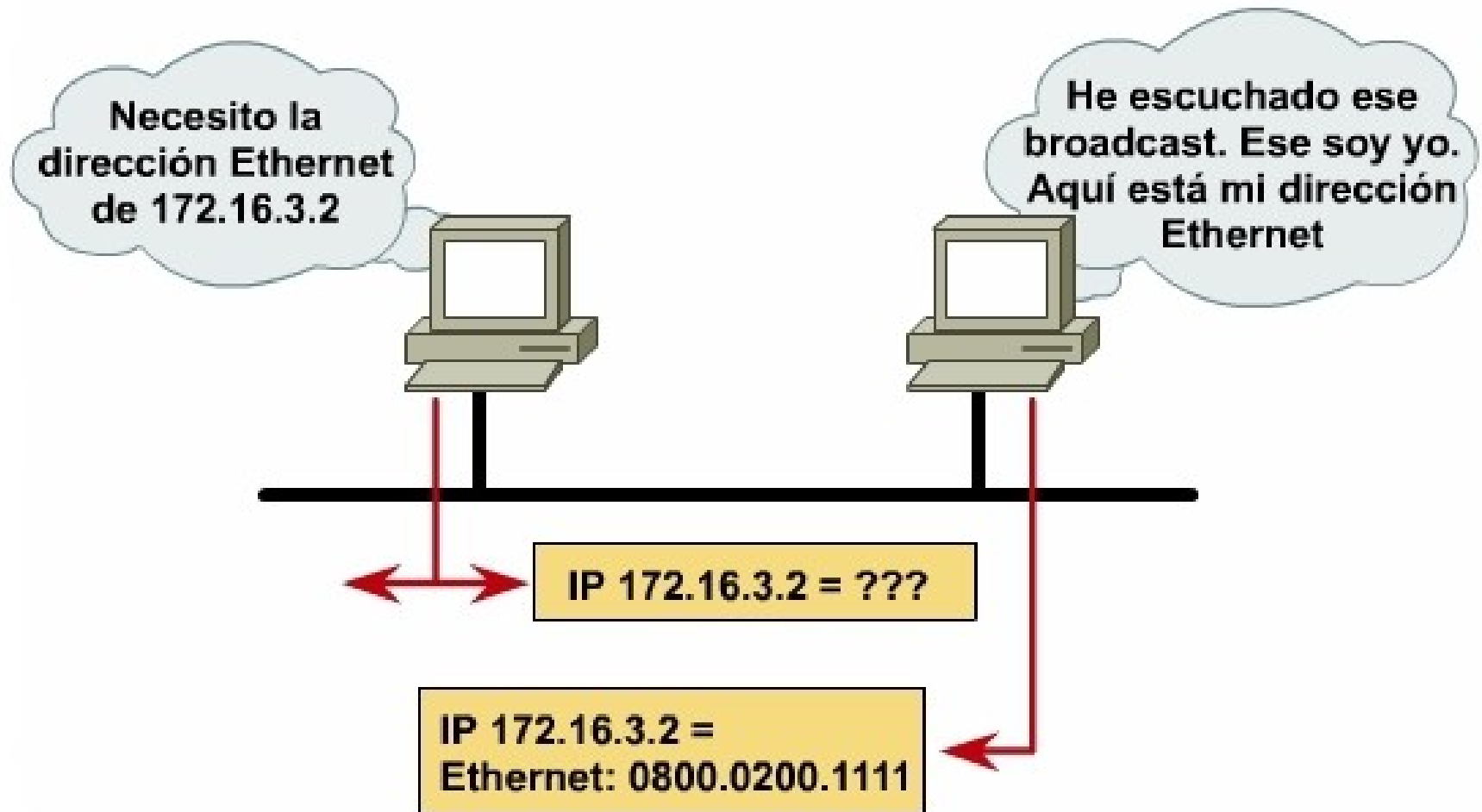
*Se encapsula el datagrama IP en una trama de subred (Ejemplo Ethernet o TR), se obtiene la dirección física del host destino y se envía (ARP).*

- ✚ Si la máquina destino **no está en la misma subred**, se envía el datagrama a un **router**, éste lo reenvía al siguiente, y así sucesivamente, hasta alcanzar un router conectado a la misma subred que la máquina destino. En este caso el **ARP previo** deberá obtener la **MAC del router**. De ahí el hecho que en cada host debe asignarse la **IP del default-gateway, es decir la del router**.

- ✚ **Resolución de direcciones**: se denomina así al proceso de obtención de una dirección de **subred** a partir de una dirección **IP (ARP)**.

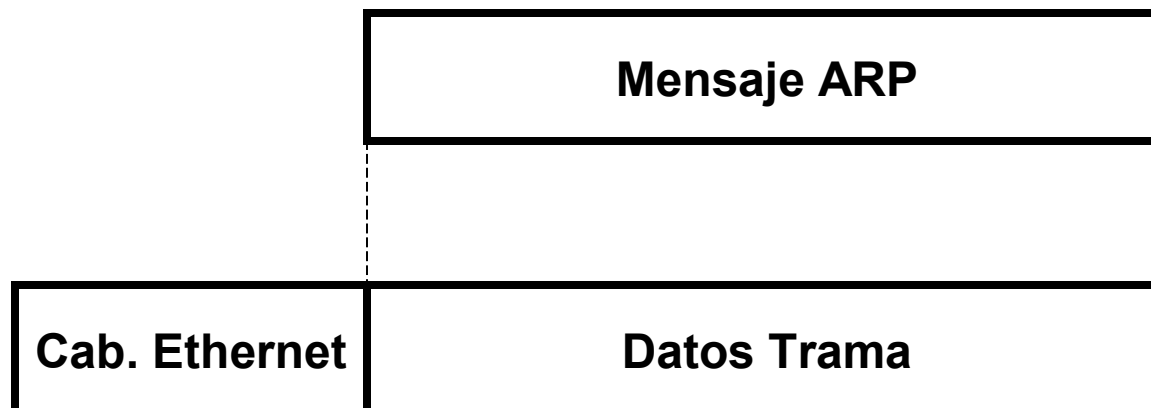
## Resolución de Direcciones: ARP

### Protocolo de resolución de direcciones



## Resolución de Direcciones: ARP

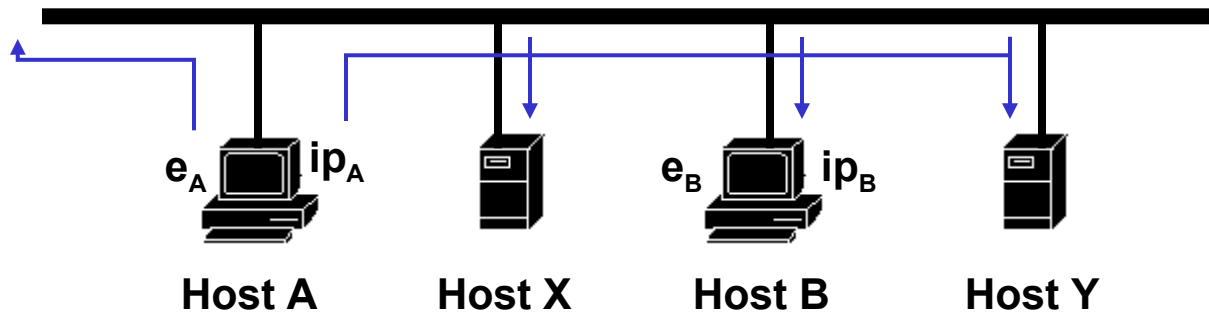
- + **Address Resolution Protocol.** Permite a un host conocer la dirección física de otro host en su misma subred a partir de su dirección **IP**.
- + Se utiliza en redes con mecanismo de **broadcast**. Ejemplo: Ethernet, Token Ring, FDDI, etc.
- + Los mensajes **ARP** se encapsulan en tramas de subred (Ethernet, TR, etc):



# Enrutamiento en Redes IP

## Funcionamiento ARP

**Pregunta:** ¿Cuál es la dirección física que corresponde a  $ip_B$ ?

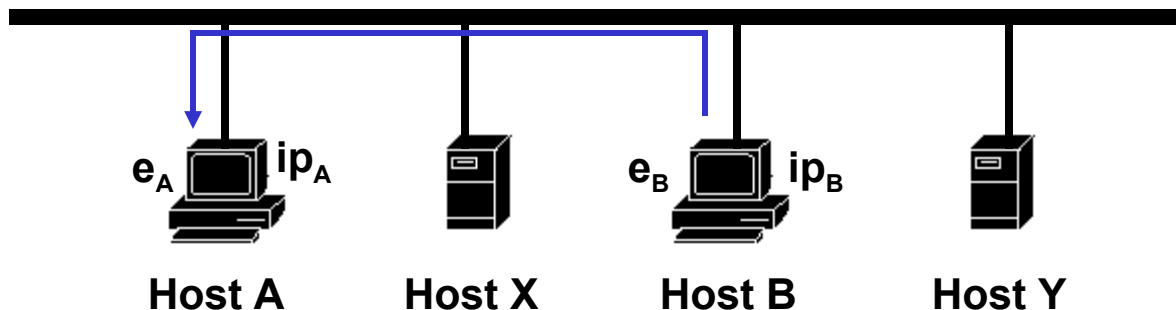


Paquetes ARP enviados

Sender	$ip_A$	$e_A$
Target	$ip_B$	??

**Respuesta:**

No se requiere ninguna configuración !!!



Sender	$ip_B$	$e_B$
Target	$ip_A$	$e_A$

# Enrutamiento en Redes IP

## Formato de mensajes ARP

0	8	16	32
Hardware Type		Protocol (N3)	
HLEN	IPLN	OPERATION	
Dir. MAC Sender (bytes 0-3)			
Dir. MAC Sender (bytes 4-5)		Dir. IP Sender (bytes 0-1)	
Dir. IP Sender (bytes 2-3)		Dir. MAC Target (bytes 0-1)	
Dir. MAC Target (bytes 2-5)			
Dir. IP Target (bytes 0-3)			



# Enrutamiento en Redes IP

**Hardware Type:** **Ethernet** es 1, **Protocol:** **0800** para **IP**, **HLEN** e **IPLen** son dos campos que especifican la **longitud de las direcciones MAC e IP**, permitiendo de esta manera el empleo de redes **totalmente arbitrarias**. El campo **OPERATION** especifica una **solicitud ARP (1)**, una **respuesta ARP(2)**, una **solicitud RARP (3)** o una **respuesta RARP (4)**.

## Resumen ARP

### + Ventajas:

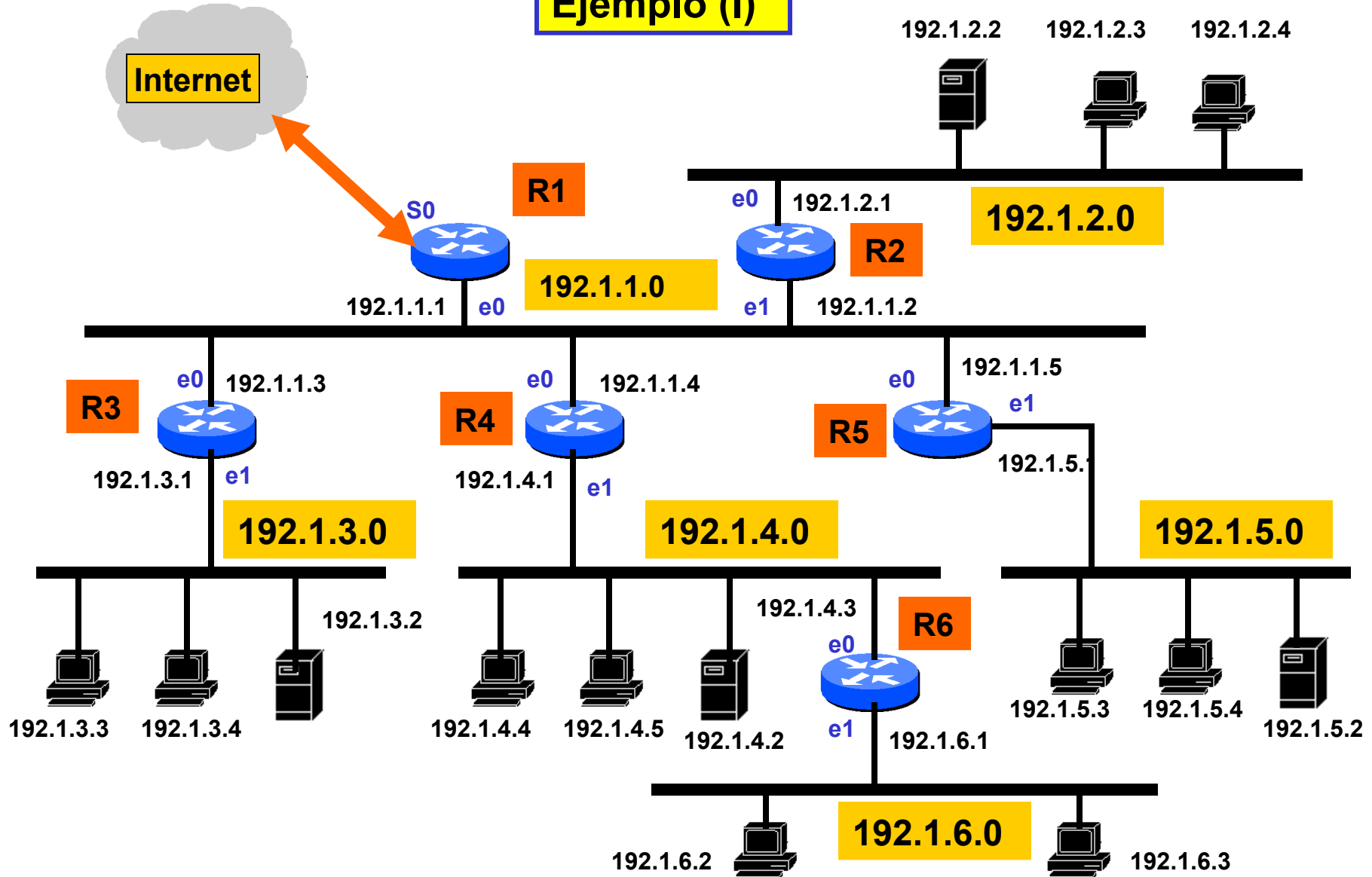
- + Muy simple
- + No requiere tablas estáticas
- + Permite añadir sistemas dinámicamente
- + **Independiza** las direcciones IP de las direcciones físicas

### + Desventajas:

- + Uso de **broadcast**
- + No detecta direcciones duplicadas

# Enrutamiento en Redes IP

## Ejemplo (I)



# Enrutamiento en Redes IP

## Ejemplo (II)

✚ Tablas de Encaminamiento de R3 y R4:

Tabla de R3	
Destino	Siguiente
192.1.1.0	Connected e0
192.1.2.0	vía 192.1.1.2
192.1.3.0	Connected e1
192.1.4.0	vía 192.1.1.4
192.1.5.0	vía 192.1.1.5
192.1.6.0	vía 192.1.1.4
0.0.0.0	vía 192.1.1.1

Tabla de R4	
Destino	Siguiente
192.1.1.0	Connected e0
192.1.2.0	vía 192.1.1.2
192.1.3.0	vía 192.1.1.3
192.1.4.0	Connected e1
192.1.5.0	vía 192.1.1.5
192.1.6.0	vía 192.1.4.3
0.0.0.0	vía 192.1.1.1

# Enrutamiento en Redes IP

## Ejercicio (I)

+ Completar las tablas de encaminamiento de R1 y R2:

Tabla de R1	
Destino	Siguiente
192.1.1.0	
192.1.20	
192.1.3.0	
192.1.4.0	
192.1.5.0	
192.1.6.0	
0.0.0.0	

Tabla de R2	
Destino	Siguiente
192.1.1.0	
192.1.20	
192.1.3.0	
192.1.4.0	
192.1.5.0	
192.1.6.0	
0.0.0.0	

# Enrutamiento en Redes IP

## Ejercicio (II)

+ Completar las tablas de encaminamiento de R5 y R6:

Tabla de R5	
Destino	Siguiente
192.1.1.0	
192.1.20	
192.1.3.0	
192.1.4.0	
192.1.5.0	
192.1.6.0	
0.0.0.0	

Tabla de R6	
Destino	Siguiente
192.1.1.0	
192.1.20	
192.1.3.0	
192.1.4.0	
192.1.5.0	
192.1.6.0	
0.0.0.0	

## Ejemplo de una tabla de ruteo real (CISCO)

1601# **show ip route**

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, \* - candidate default

U - per-user static route, o - ODR

Gateway of last resort is not set

S 10.0.0.0/8 [1/0] via 192.168.3.1

S 20.0.0.0/8 [1/0] via 192.168.3.1

S 30.0.0.0/8 [1/0] via 192.168.3.1

C 40.0.0.0/8 is directly connected, Ethernet0

S 192.168.1.0/24 [1/0] via 192.168.3.1

S 192.168.2.0/24 [1/0] via 192.168.3.1

C 192.168.3.0/24 is directly connected, Serial0

S 192.168.4.0/24 [1/0] via 192.168.3.1

# Enrutamiento en Redes IP

2501# show ip route

Codes: **C** - connected, S - static, **I** - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, \* - candidate default

U - per-user static route, o - ODR

Gateway of last resort is not set

C 20.0.0.0/8 is directly connected, Ethernet0

I 10.0.0.0/8 [100/8576] via 192.168.1.1, 00:00:03, Serial0  
[100/8576] via 192.168.2.1, 00:00:03, Serial1

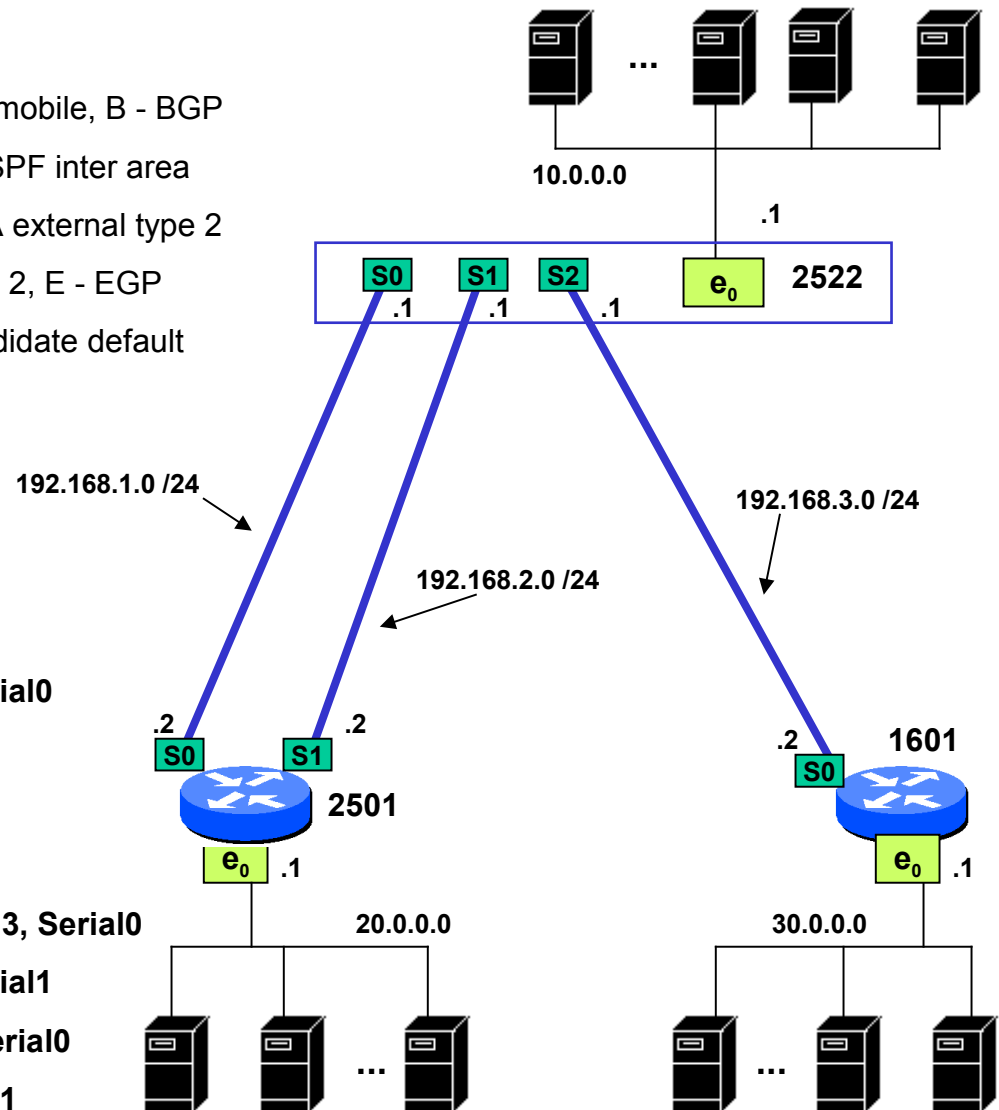
C 192.168.1.0/24 is directly connected, Serial0

C 192.168.2.0/24 is directly connected, Serial1

I 192.168.3.0/24 [100/90956] via 192.168.1.1, 00:00:03, Serial0  
[100/90956] via 192.168.2.1, 00:00:03, Serial1

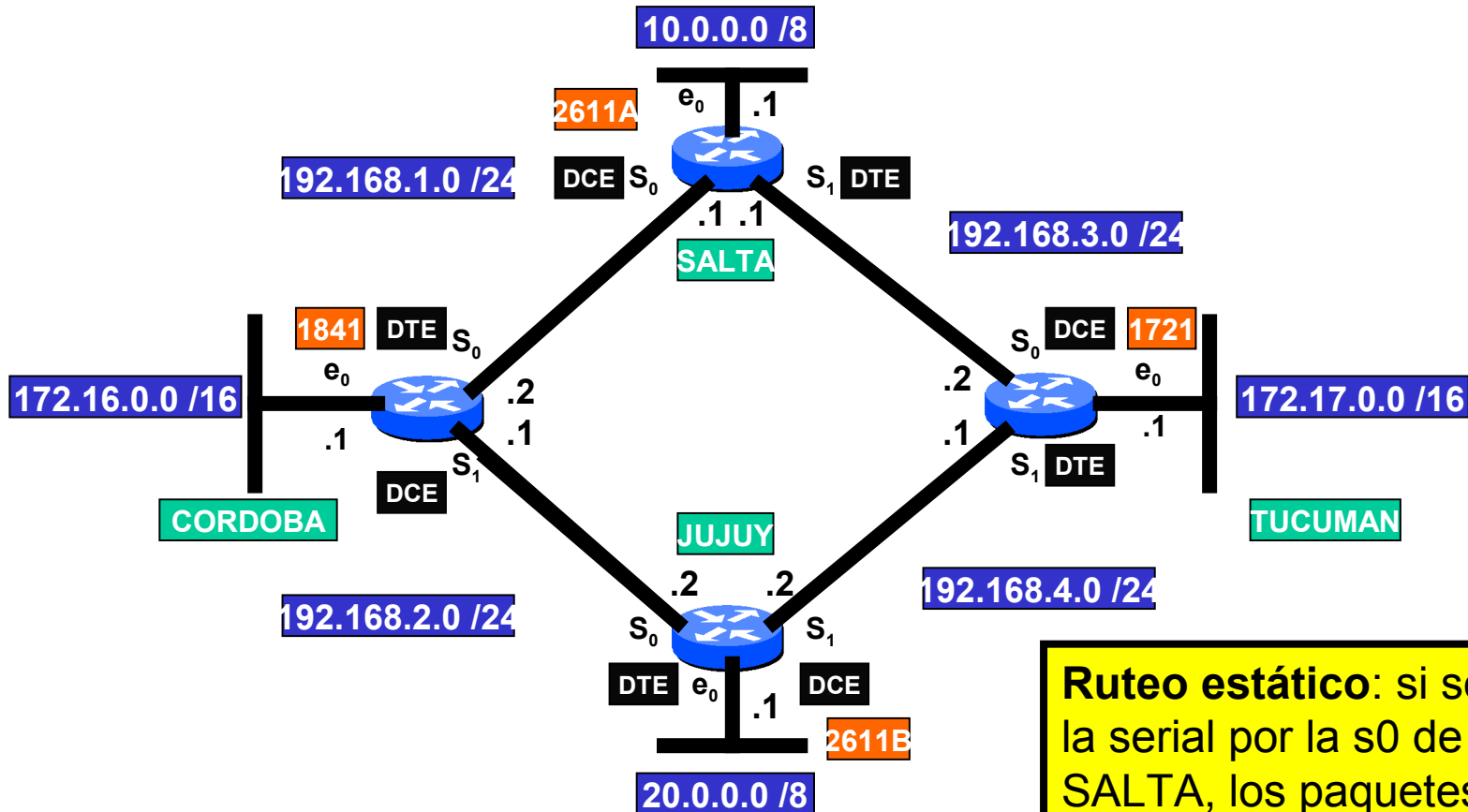
I 30.0.0.0/8 [100/91056] via 192.168.1.1, 00:00:03, Serial0  
[100/91056] via 192.168.2.1, 00:00:03, Serial1

2501#



# Enrutamiento en Redes IP

## Enrutamiento estático y dinámico



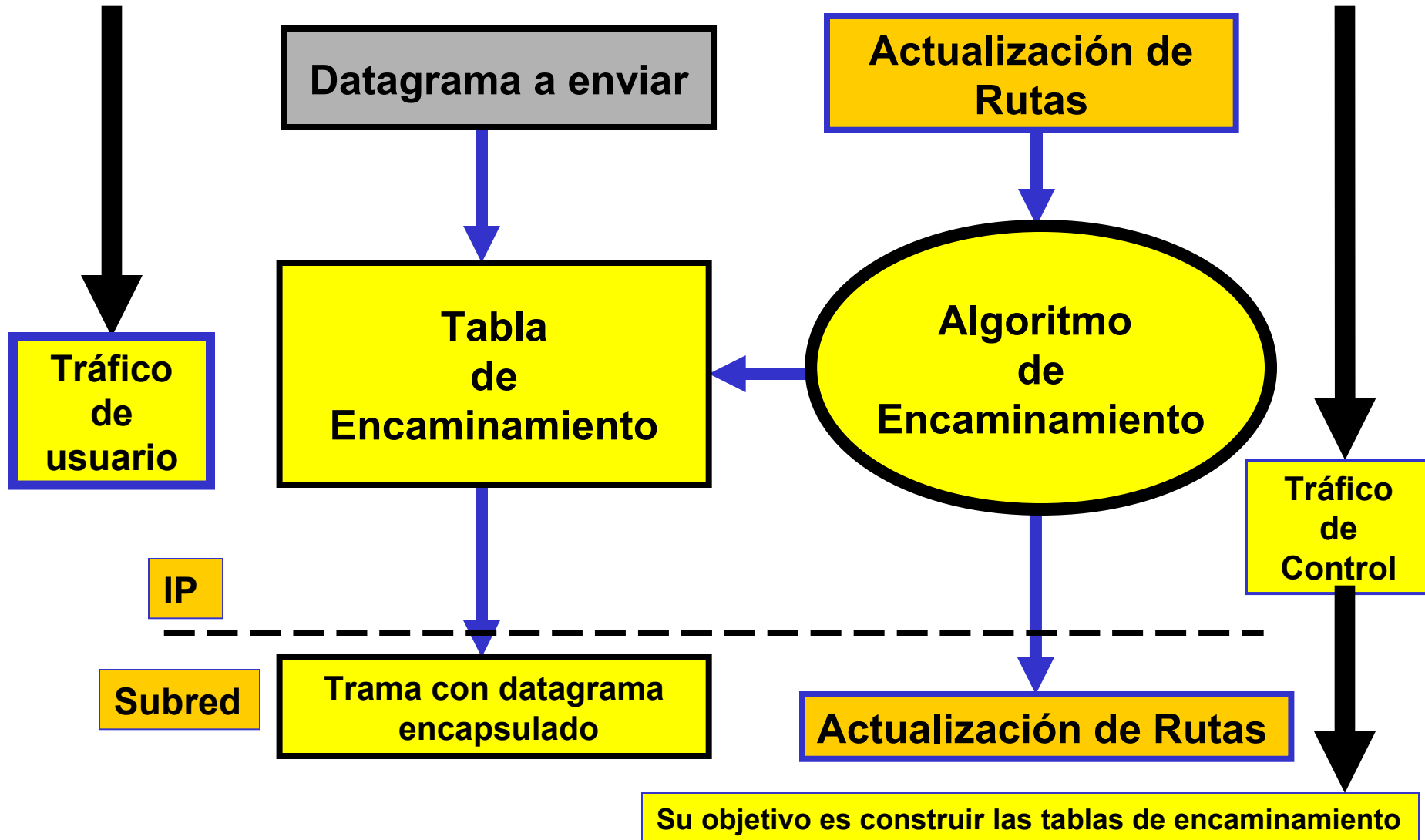
**Ruteo estático:** si se cae la serial por la s0 de SALTA, los paquetes se dropean, a pesar de existir una ruta alternativa por la s0 de JUJUY.

Ip route 172.17.0.0 192.168.1.1  
Ip route 20.0.0.0/8 192.168.2.2



# Enrutamiento en Redes IP

## Esquema Funcional de Actualización de Tablas de Encaminamiento



# Enrutamiento en Redes IP

## Pasos principales para llevar a cabo el Encaminamiento (I)

1. Identificar de la dirección **IP** del host de destino, la red de destino a la que va dirigido el datagrama.

**Ejemplo:** un datagrama enviado a **138.4.3.130** (máscara **255.255.0.0**)

$$I_r = 138.4.0.0 \text{ (red)}$$

2. Si  **$I_r$**  está directamente conectada a alguna de las interfaces del **router**, se envía el datagrama a esa interfaz - **envío directo** - (encapsular, resolver dirección física mediante **ARP** y mandar trama).
3. Si no, si existe una ruta específica para  **$I_r$** , mandar el datagrama al sitio especificado en dicha ruta (next hop).

## Pasos principales para llevar a cabo el Encaminamiento (II)

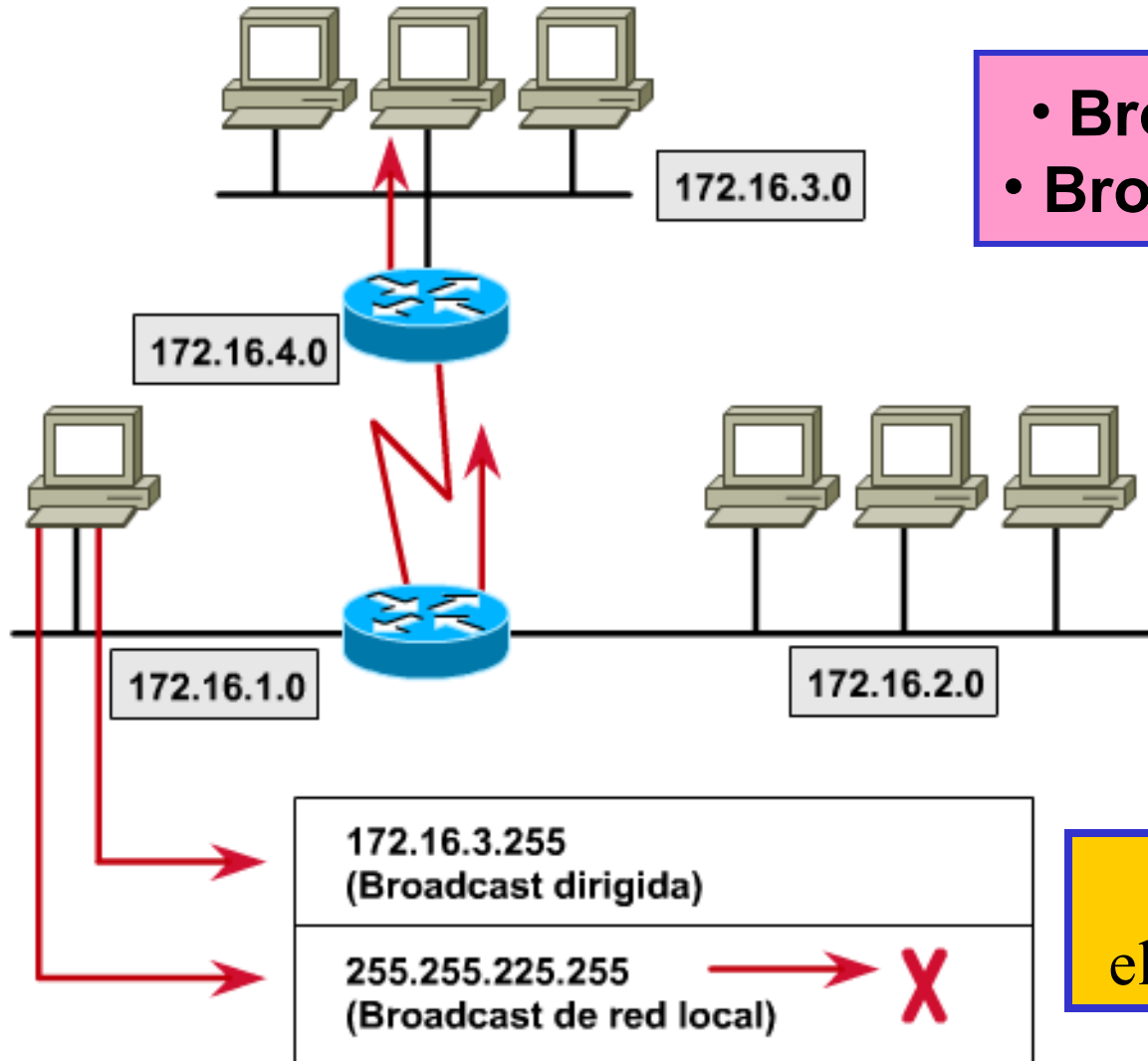
4. Si no existe una ruta específica en la tabla de encaminamiento, y si existe una ruta por defecto (**0.0.0.0**), mandar el datagrama a la interfaz especificada en **0.0.0.0**
5. Si no existe una ruta específica ni la ruta por defecto → **¡ Error, destino inalcanzable !** Se descarta el datagrama y se genera un mensaje **ICMP**.

## Resumen de Configuración de una NIC

- + Antes de transmitir o recibir un datagrama, un host debe conocer, al menos:**
  - + Su dirección IP**
  - + La dirección de un router en su subred (Default Gateway)**
  - + La máscara de subred**
  - + La dirección del servidor de nombres (DNS)**
  - + La dirección IP del Proxy y el puerto para el servicio web (se configura en el navegador).**

# Enrutamiento en Redes IP

## Direcciones de Broadcast



- Broadcast dirigido
- Broadcast inundado

Sólo se propaga  
el broadcast dirigido

**1 Generalidades**

**2 Protocolo IP**

**3 ICMP**

**4 Enrutamiento en Redes IP**

 **5 Subnetting**

# Subnetting

## Introducción (I)

- ✦ A la hora del encaminamiento entre los distintos routers que conforman la Internet, si el mismo se produjera a nivel de Host, las tablas de encaminamiento de los routers aumentarían su tamaño de una forma realmente explosiva.
- ✦ Por lo tanto lo lógico sería encaminar en función de una dirección **IP** (Clase **A**, **B** o **C**), asignada a cada red y no en función de una dirección **IP específica** de un **host**. **Esto reduce notablemente las entradas en las tablas de encaminamiento de los routers.**
- ✦ Pero para reducir aún más el número de direcciones de las tablas de encaminamiento, lo que se hace es compartir direcciones de red **entre varias subredes físicas diferentes**. A tal efecto se emplea la técnica denominada **Subnetting**.
- ✦ El Subnetting es **parte integral del direccionamiento IP** (todo sistema **IP** debe soportarlo).
- ✦ Consiste en subdividir el campo original de **HOST** de la dirección **IP** en:
  - ▶ Identificador de **Subred**
  - ▶ Identificador de **Host**

# Subnetting

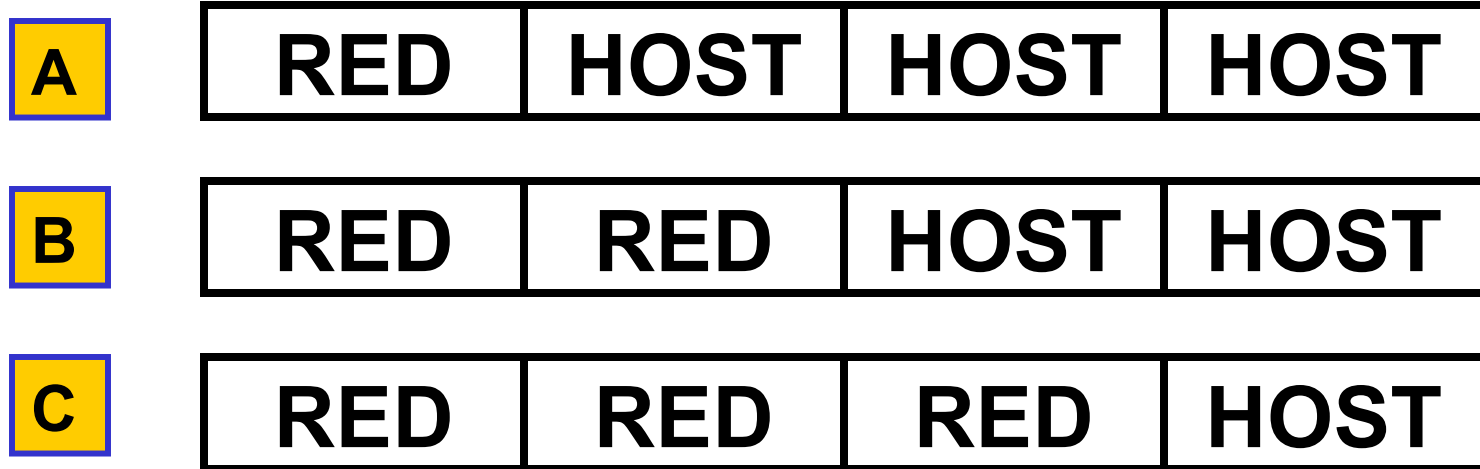
## Introducción (II)

- + Convendría además que el resto de Internet **viese mi red con el mismo prefijo** (pues podría asignar múltiples direcciones **C**, por ejemplo una por segmento, pero además de derrochar direcciones, desde fuera se vería nuestra red casi como una **telaraña**). La idea es que con esta técnica nuestra red **permanezca oculta hacia el exterior**.
- + Exigió modificaciones en los routers internos.
- + Se jerarquiza el encaminamiento
- + Se introduce el concepto de **máscara de Subred**, que permite realizar una separación entre identificadores de **subred** y de **Host**.
- + Todos los **routers deben conocer la máscara**
- + Todos los **hosts deben conocer la máscara**

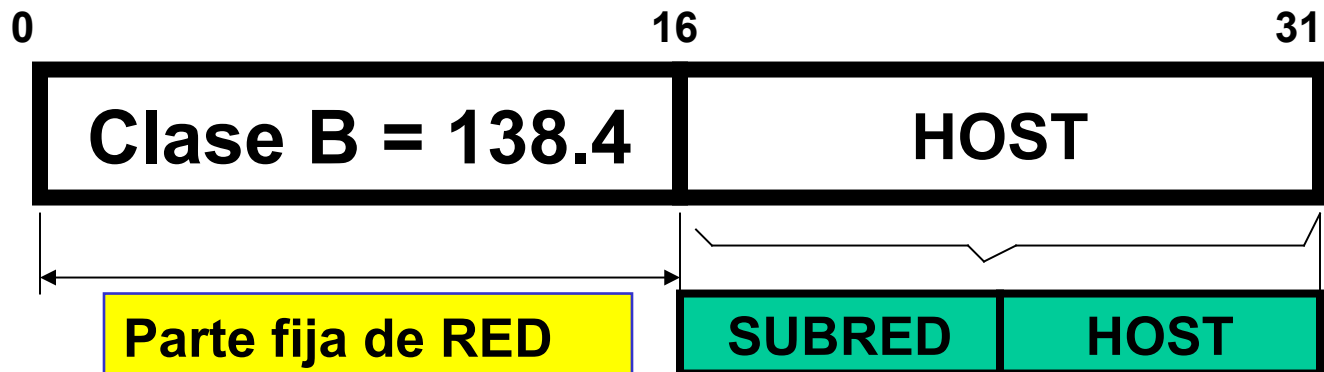


# Subnetting

**Antes**

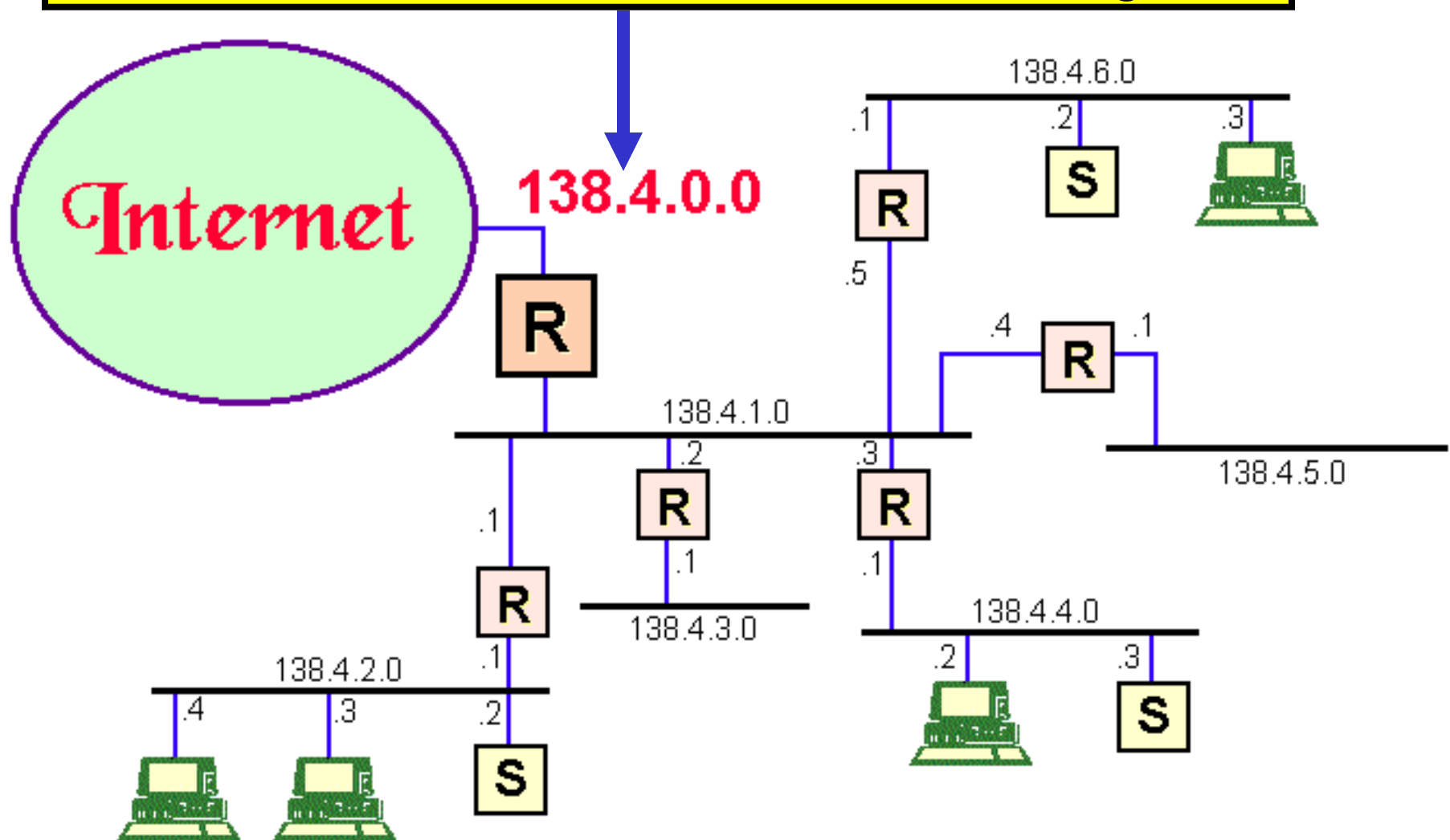


**Ahora por ejemplo**



# Subnetting

Toda la Internet me ve con una **única dirección IP**, se oculta el resto de la red hacia el exterior: finalidad del **Subnetting**.



# Subnetting

✚ De acuerdo al ejemplo anterior, tenemos **16 bits ya impuestos**, por ser una dirección tipo **Clase B**. Pero los otros **16 bits**, pertenecientes al campo de **Host**, los administramos nosotros de la manera más conveniente, volviendo a subdividir ese campo entre **subred y host**.

✚ Por ejemplo si el campo de host lo parto en dos, **dos de 8 bits**, entonces podría asignar **256 subredes** con **256 host** por cada subred. A esto en realidad habría que descontar por lo menos dos direcciones, las correspondientes a **todos ceros** en el campo de host (**que indica la red**) y la correspondiente a todos unos (**broadcast**), quedando en realidad **254 hosts**. Luego habría que descontar también el número de direcciones que se asignan a los dispositivos de encaminamiento (**routers**).

## Ejemplo de Tabla de encaminamiento

Dirección Destino	Máscara	Dirección IP del siguiente salto
138.4.2.0	255.255.255.0	138.4.1.1
138.4.3.0	255.255.255.0	138.4.1.2

## ✚ ¿Quién asigna las direcciones de Subred?

Al igual que la parte correspondiente al número del host de las direcciones clases **A**, **B** y **C**, las direcciones de subred se asignan localmente. En general lo hace el administrador de la red.

## ✚ ¿Qué incluye una dirección de Subred?

Las direcciones de subred incluyen un número de la red, un número de subred dentro de la red y un número del host dentro de la subred. Mediante este tercer nivel de direccionamiento, las subredes brindan mayor flexibilidad al administrador de la red.

## ✚ ¿Cómo se crean las direcciones de subred?

Para crear una dirección de subred, el administrador de la red “**toma prestados**” bits del campo de host y los designa como campo de subred. El resto de los bits libres determinarán el número de hosts dentro de la subred. Se pueden tomar prestados cualquier cantidad de bits (a partir de **2**) y siempre y cuando queden dos bits libres para el **HOST**.

# Subnetting

---

## ✚ ¿Cómo se ocultan las direcciones de subred de las redes externas?

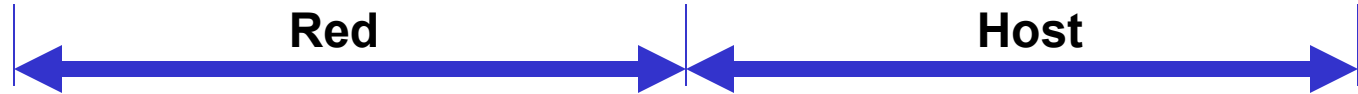
Las subredes se ocultan de las redes externas utilizando una máscara, denominada máscara de subred. La función de la máscara de subred es decirle a los dispositivos qué parte de una dirección es el número de la red, incluyendo la subred y qué parte es la correspondiente al host. **La máscara es un conjunto de 32 bits que se utiliza en el IP para indicar los bits de una dirección IP que se están utilizando para la dirección de subred.**

## ✚ ¿Qué formato utilizan las máscaras de Subred?

Las máscaras de subred utilizan el mismo formato que el direccionamiento **IP**. En otras palabras, tienen 32 bits de extensión y se dividen en cuatro bytes. Las máscaras de subred tienen **todos unos** en la parte correspondiente a la red (parte fija) y a la **subred**, y **todos ceros** en la parte correspondiente al **host**. Por defecto si no se toman prestados bits, la máscara de subred de una red clase **B** (clase pura o **classfull**), sería **255.255.0.0**, es la **máscara por defecto o máscara natural**. Sin embargo si se toman prestados **8 bits**, la máscara de subred de la misma red clase **B** sería pues **255.255.255.0**

# Subnetting

## Ejemplo de una máscara de Subred para una dirección Clase B



Dirección  
IP

165

12

0

0

Máscara de  
Subred por  
defecto

255

255

0

0

Máscara de  
Subred de 8  
bits

255

255

255

0

Todas las redes tienen máscara de subred por defecto. Para la red 200.39.200.0, la máscara de subred por defecto es 255.255.255.0



Los bits del host deben utilizarse comenzando en la posición del bit de mayor orden

# Subnetting

## Ejemplo de planeamiento de una Subred Clase B

✚ Dirección de Host IP: 172.16.2.120

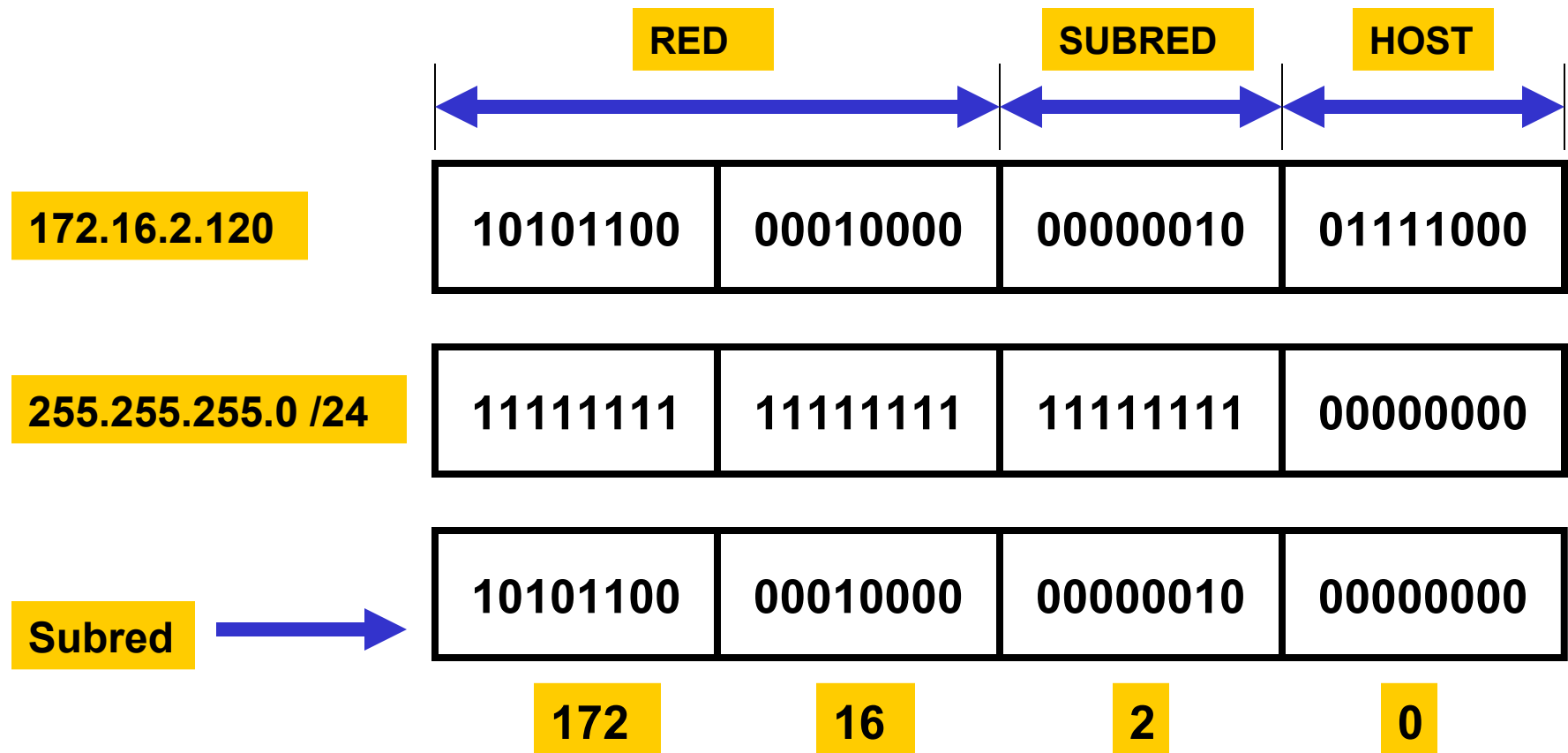
✚ Dirección de Host = 172.16.2.1 – 176.16.2.254 /24

✚ Máscara de Subred: 255.255.255.0 /24

✚ Dirección de Broadcast = 172.16.2.255

✚ Dirección de Subred: 172.16.2.0

✚ Ocho bits de Subred y ocho bits para HOSTs



# Subnetting

**Máscara resultante, N° de Subredes y N° de Hosts en función de la cantidad de bits que se toman prestados al campo de HOST de la dirección IP Clase B**

N° bits	Subnet Mask	N° Subnets	N° Hosts
2	255.255.192.0 /18	2	16382
3	255.255.224.0 /19	6	8190
4	255.255.240.0 /20	14	4094
5	255.255.248.0 /21	30	2046
6	255.255.252.0 /22	62	1022
7	255.255.254.0 /23	126	510
8	255.255.255.0 /24	254	254
9	255.255.255.128 /25	510	126
10	255.255.255.192 /26	1022	62
11	255.255.255.224 /27	2046	30
12	255.255.255.240 /28	4094	14
13	255.255.255.248 /29	8190	6
14	255.255.255.252 /30	16382	2



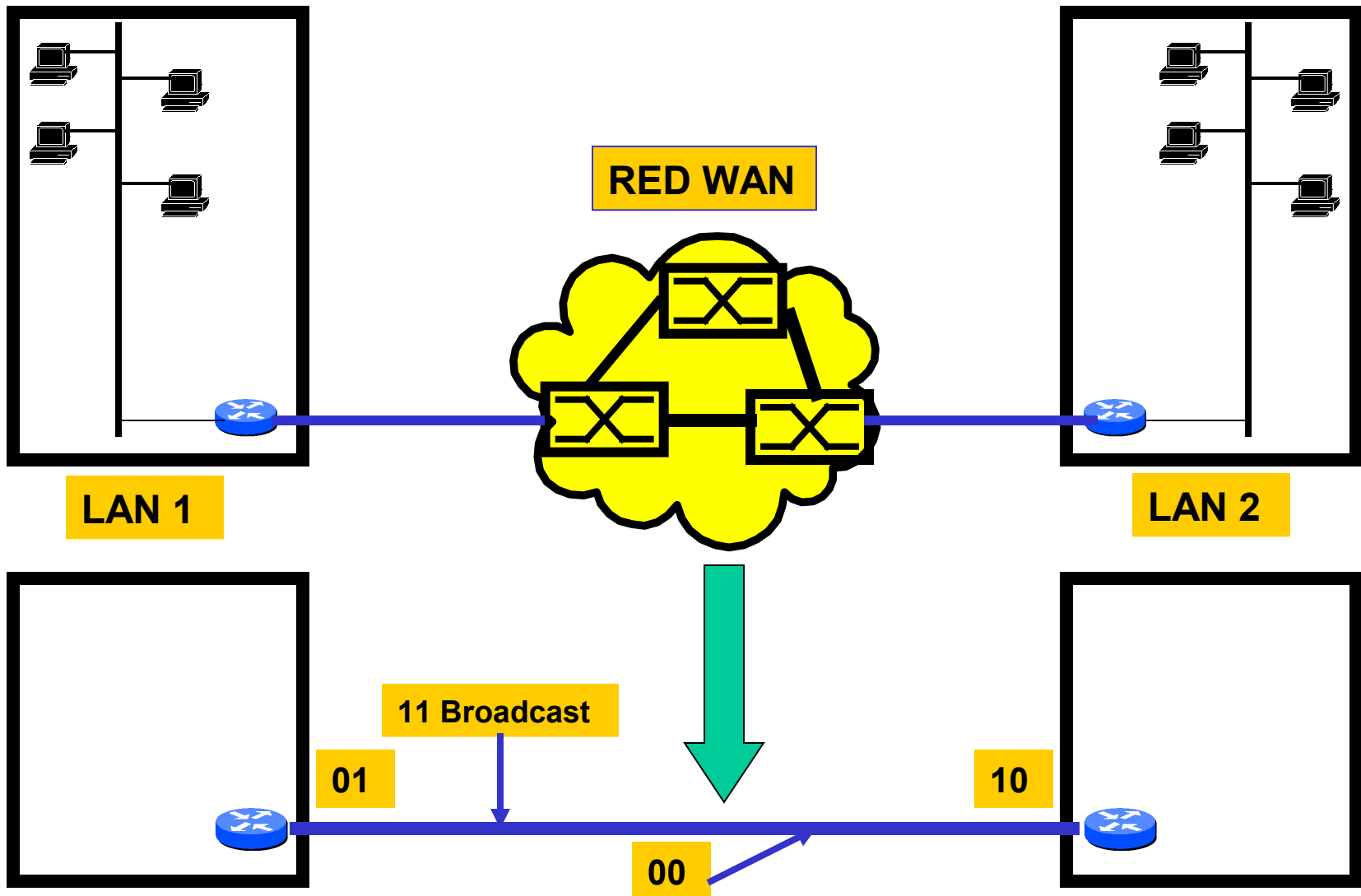
# Subnetting

**Máscara resultante, N° de Subredes y N° de Hosts en función de la cantidad de bits que se toman prestados al campo de HOST de la dirección IP Clase C**

N° bits	Subnet Mask	N° Subnets	N° Hosts
2	255.255.255.192 /26	2	62
3	255.255.255.224 /27	6	30
4	255.255.255.240 /28	14	14
5	255.255.255.248 /29	30	6
6	255.255.255.252 /30	62	2

# Subnetting

## Ejemplo de máscara /30



# Subnetting

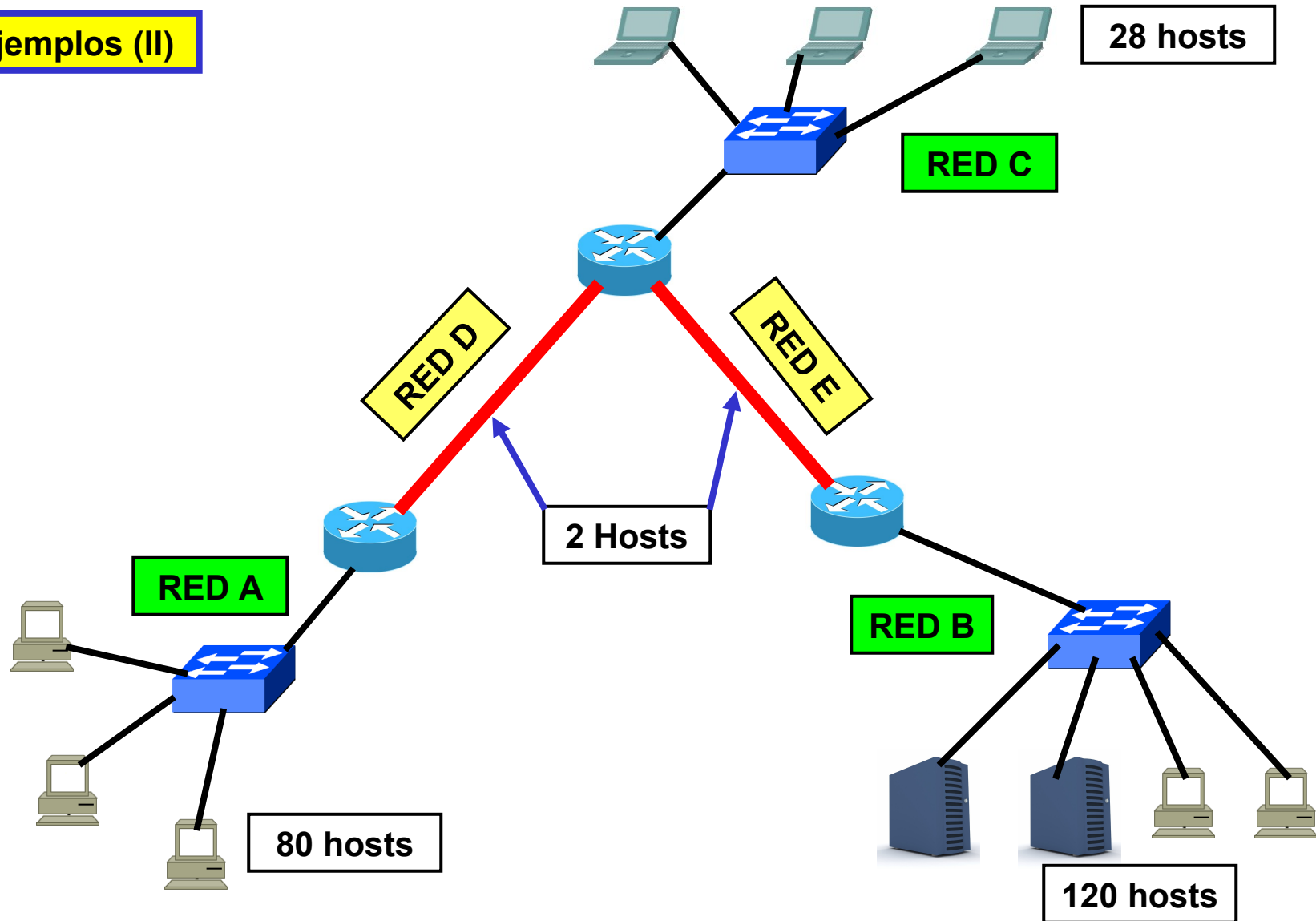
## Ejemplos (I)

Dirección de HOST	Máscara	Dirección de Subred	Dirección de Broadcast	Direcciones Disponibles
10.2.3.5 /24	255.255.255.0	10.2.3.0	10.2.3.255	10.2.3.1 A 10.2.3.254
175.10.5.2 /30	255.255.255.252	175.10.5.0	175.10.5.3	175.10.5.1 A 175.10.5.2
175.10.5.5 /30	255.255.255.252	175.10.5.4	175.10.5.7	175.10.5.5 A 175.10.5.6
10.36.45.10 /28	255.255.255.240	10.36.45.0	10.6.45.15	10.36.45.1 A 10.36.45.14
10.36.45.18 /28	255.255.255.240	10.36.45.16	10.36.45.31	10.36.45.17 A 10.36.45.30
200.56.0.66 /26	255.255.255.192	200.56.0.64	200.56.0.127	200.56.0.65 A 200.56.0.126

# Subnetting

## Direcccionamiento de una red mediante el empleo de subnetting

### Ejemplos (II)



## Ejemplos (III)

[illegible]

---

# ANEXO

# Cableado en redes LAN y WAN

Los tipos de medio pueden ser:

- UTP (categorías 5, 5e, 6 y 7)
- Fibra óptica multimodo o monomodo
- Wireless



UTP

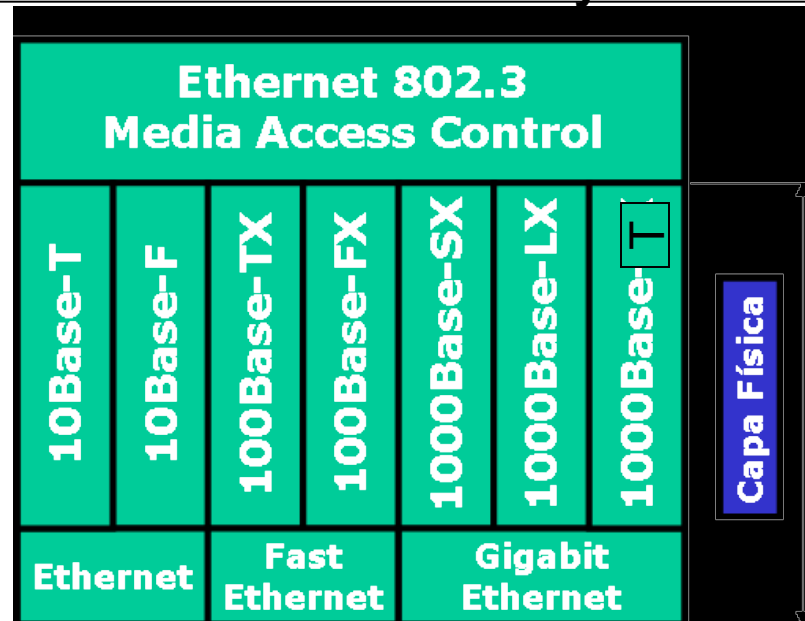


FIBRA



WIRELESS

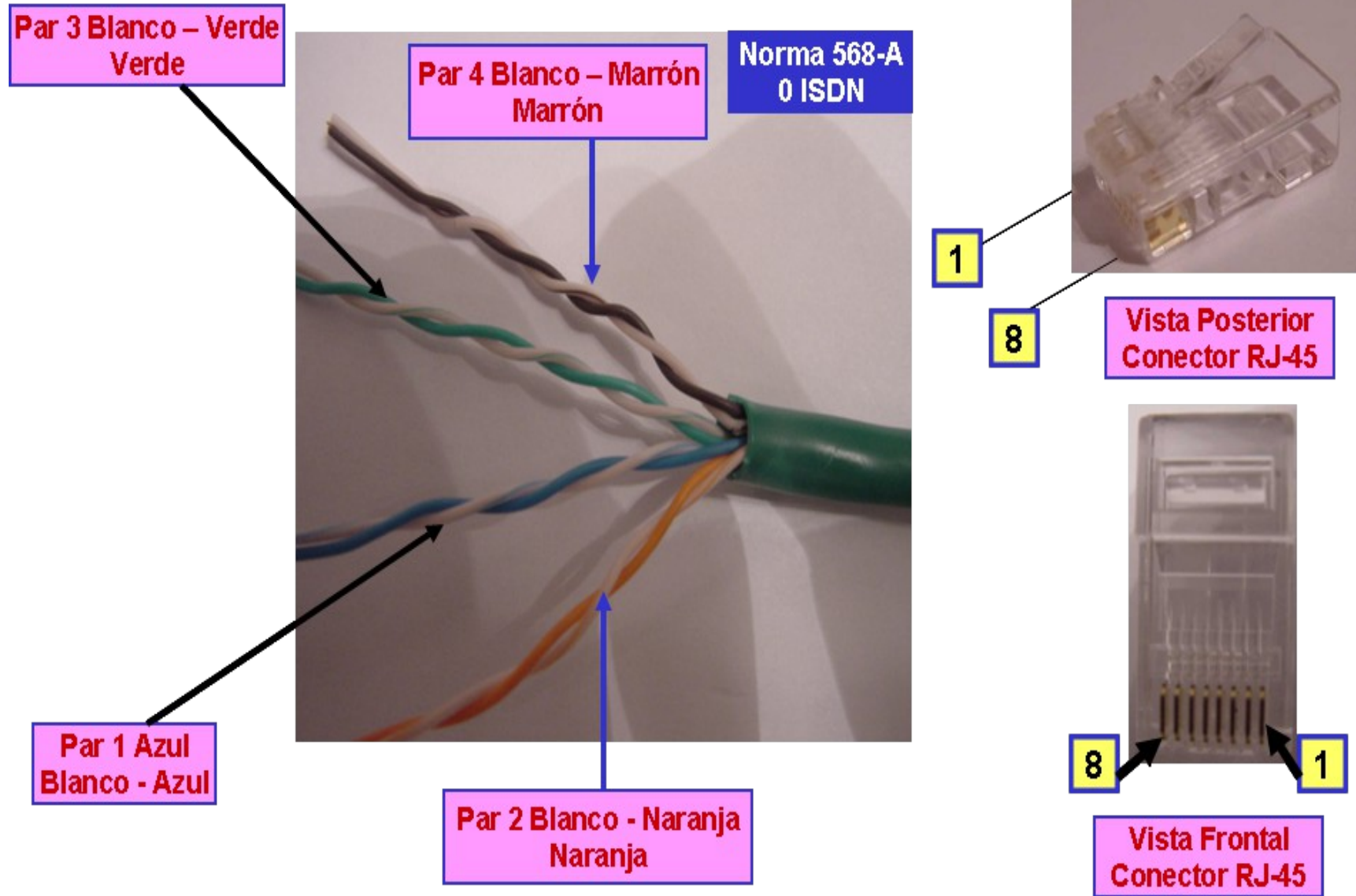
## Cableado en redes LAN y WAN



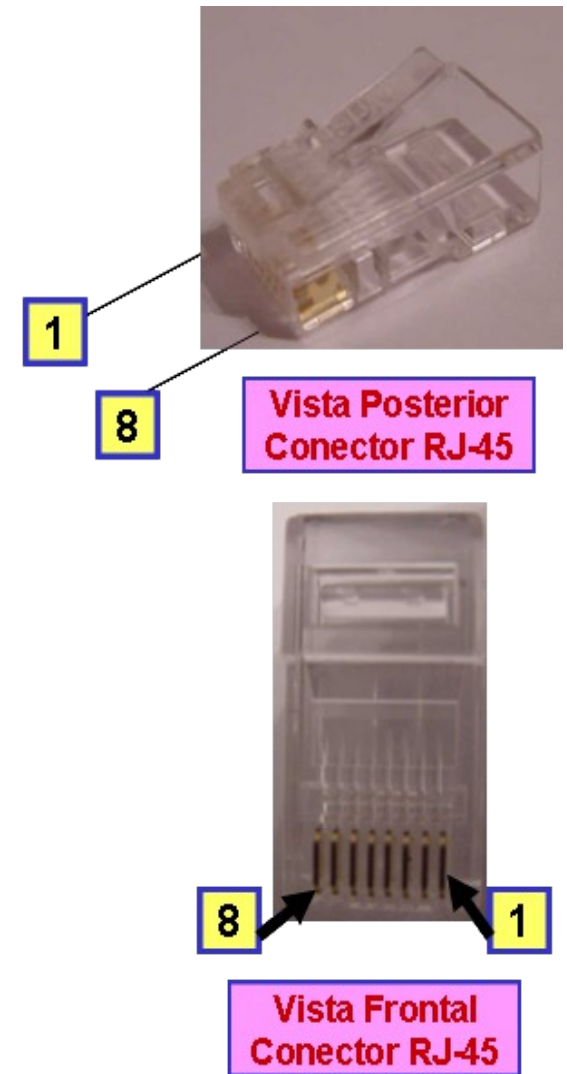
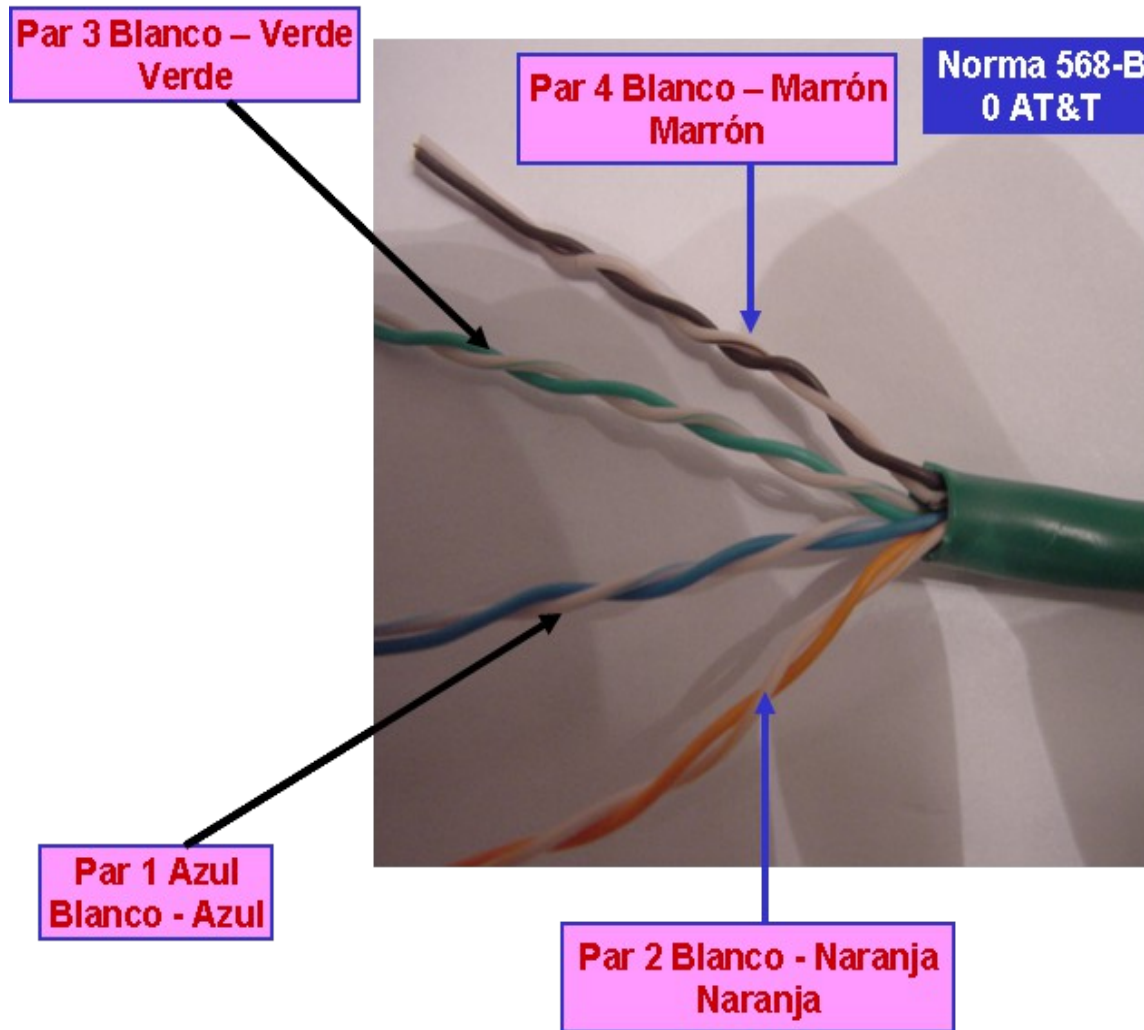
Interface	Medio	Velocidad	Distancia
10Base-T	UTP Categoría 5	10 Mbps	100 m
10Base-F	Fibra	10 Mbps	2 Km
100Base-TX	UTP Categoría 5	100 Mbps	100 m
100Base-FX	Fibra óptica Multimodo	100 Mbps	2 km
1000Base-T	UTP Categoría 5E	1000 Mbps	100 m
1000Base-SX	FO multimodo (62.5 μm)	1000 Mbps	220 m
1000Base-LX	FO monomodo (10 μm)	1000 Mbps	5 Km



## Cableado en redes LAN y WAN

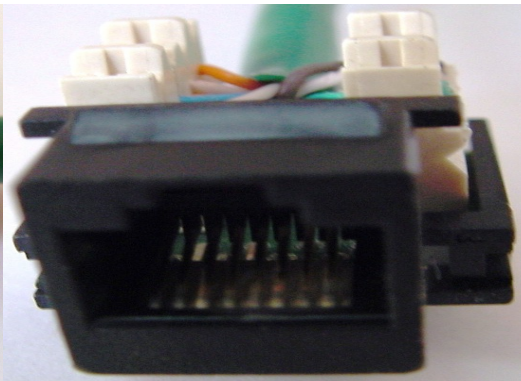
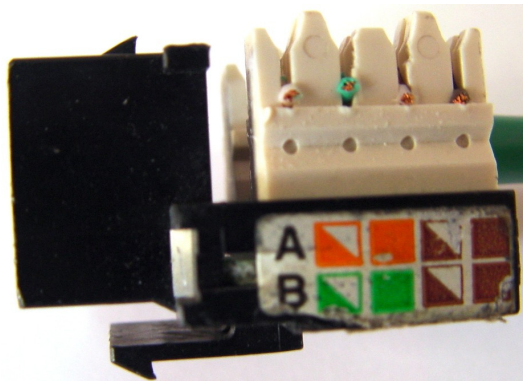


## Cableado en redes LAN y WAN



## Cableado en redes LAN y WAN

Diversas Herramientas empleadas en cableado de LAN



## Cableado en redes LAN y WAN

Norma 568-A 0 ISDN

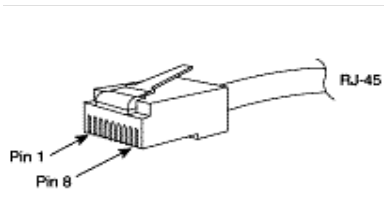
PIN	PAR	Función	COLOR	10/100 BaseT Ethernet	100 BaseT4 y 1000BT Ethernet
1	3	TX	Blanco Verde	SI	SI
2	3	RX	Verde	SI	SI
3	2	TX	Blanco Naranja	SI	SI
4	1	Telefonía	Azul	NO	SI
5	1	Telefonía	Blanco Azul	NO	SI
6	2	RX	Naranja	SI	SI
7	4	Respaldo	Blanco Marrón	NO	SI
8	4	Respaldo	Marrón	NO	SI

Norma 568-B 0 AT&T

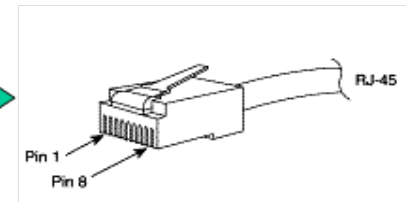
PIN	PAR	Función	COLOR	10/100 BaseT Ethernet	100 BaseT4 y 1000BT Ethernet
1	2	TX	Blanco Naranja	SI	SI
2	2	RX	Naranja	SI	SI
3	3	TX	Blanco Verde	SI	SI
4	1	Telefonía	Azul	NO	SI
5	1	Telefonía	Blanco Azul	NO	SI
6	3	RX	Verde	SI	SI
7	4	Respaldo	Blanco Marrón	NO	SI
8	4	Respaldo	Marrón	NO	SI

# Cableado en redes LAN y WAN

**Hub o Switch**



**PC o Router**

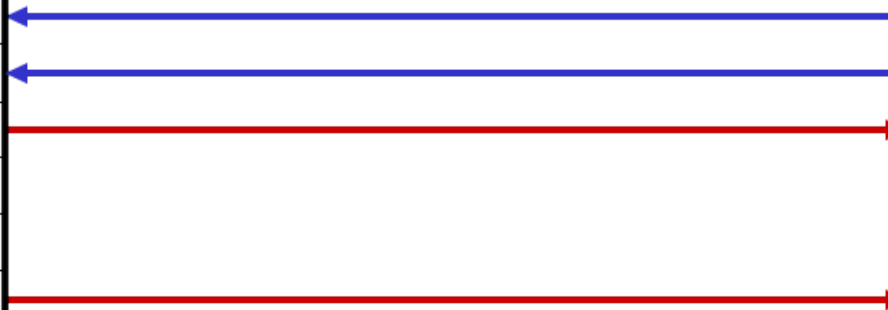


Pin	Señal
1	Rx +
2	Rx -
3	Tx +
4	nc
5	nc
6	Tx -
7	nc
8	nc

**nc: no conectado**

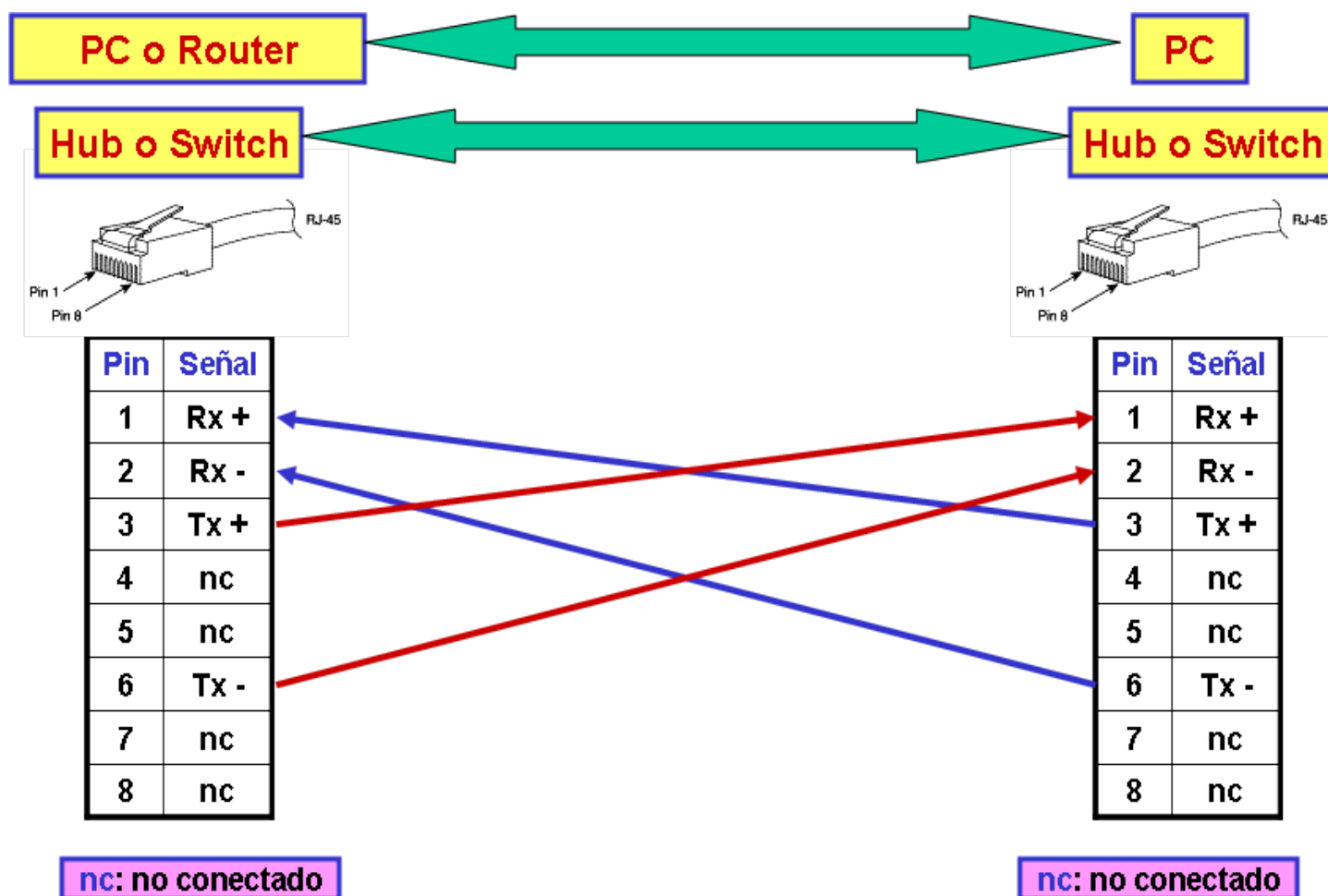
Pin	Señal
1	Tx +
2	Tx -
3	Rx +
4	nc
5	nc
6	Rx -
7	nc
8	nc

**nc: no conectado**



**CABLE DERECHO**

## Cableado en redes LAN y WAN



**CABLE CRUZADO O CROSSOVER**



### ✚ Cable derecho

#### ■ Para conectar entre

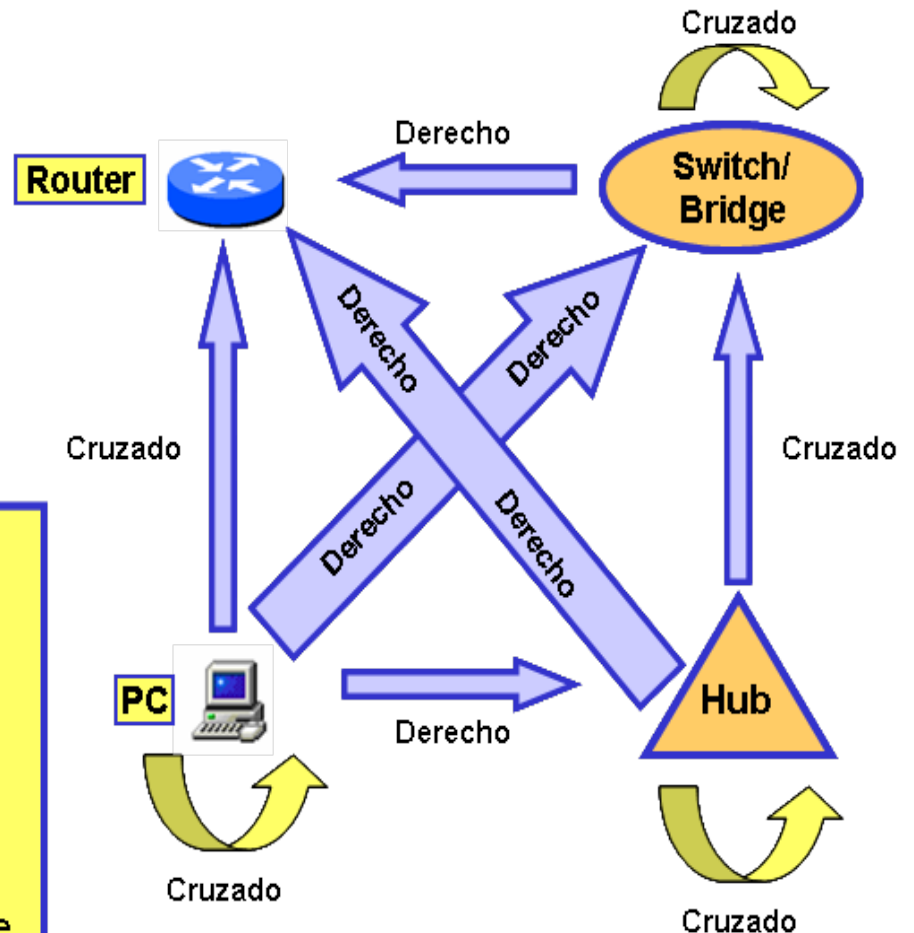
- ▶ PC y Hub
- ▶ PC y Switch / Bridge
- ▶ Hub y Router
- ▶ Switch /Bridge y Router

### ✚ Cable cruzado

#### ■ Para conectar entre

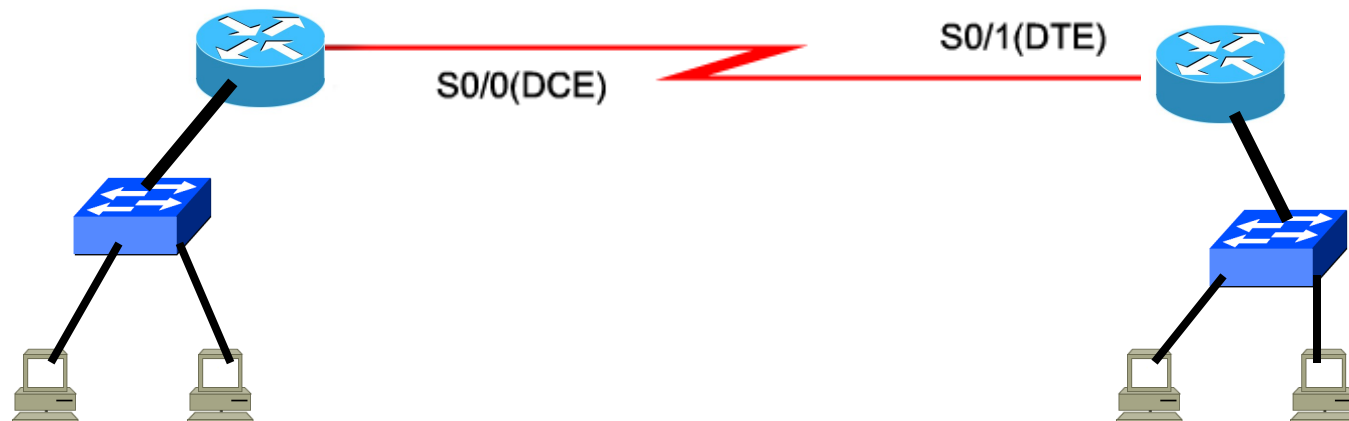
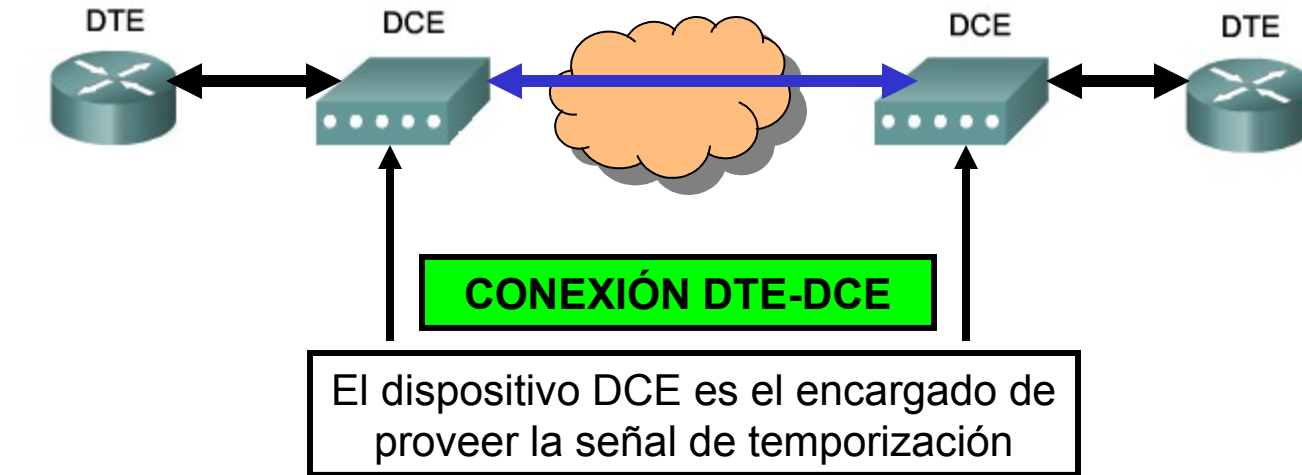
- ▶ PC a Router
- ▶ PC a PC
- ▶ Hub a Hub
- ▶ Switch /Bridge a Switch / Bridge
- ▶ Hub a Switch /Bridge

### RESUMEN CABLEADO LAN



# Cableado en redes LAN y WAN

## CABLEADO EN WAN



Conexión de laboratorio DTE-DCE Back to Back



# Cableado en redes LAN y WAN

## CABLEADO EN WAN



DTE SERIAL



DTE SMART SERIAL

## Conectores DB-60 a V.35



DCE SERIAL



DCE SMART SERIAL

## Cableado en redes LAN y WAN

